VRIJE
UNIVERSITEIT
BRUSSEL

Thesis submitted in partial fulfillment of the requirements for the degree of Doctor of Sciences

SET-THEORETIC SOLUTIONS OF THE YANG-BAXTER EQUATION AND ASSOCIATED ALGEBRAIC STRUCTURES

Charlotte Verwimp

2021-2022

Supervisors: Prof. Dr. E. Jespers, Prof. Dr. L. Vendramin

Science and Bio-Engineering Sciences

Abstract

The Yang-Baxter equation is one of the essential equations in mathematical physics, initially appearing in both quantum and statistical mechanics. The problem of constructing and classifying its solutions has been fruitfully approached by Drinfeld who proposed the idea to focus on the subclass of set-theoretic solutions. So far, not all such solutions of the Yang-Baxter equation are known.

This PhD thesis is highly motivated by this open problem. An effective approach is to identify and study the underlying algebraic structures. More precisely, we focus on the (semi)group and ring theoretical aspects that occur, and study them for specific classes of set-theoretic solutions of the Yang-Baxter equation.

Initially, we deal with arbitrary set-theoretic solutions of the Yang-Baxter equation and discover connections, via 1-cocycles, between three (in general different) monoids associated to a set-theoretic solution, the structure monoid and the left and right derived structure monoids. In case the set-theoretic solution is left non-degenerate, the 1-cocycle between the structure monoid and the left derived structure monoid is bijective. This allows us to put two monoid structures on a same set, leading to the definition of a YB-semitruss. YB-semitrusses turn out to be the suitable associative algebraic structure to study left non-degenerate set-theoretic solutions of the Yang-Baxter equation. In particular, they can be used to prove that any such finite solution is right non-degenerate if and only if it is bijective, which is one of the main results in this thesis. If a solution is (left and right) non-degenerate and bijective, we determine when its structure monoid and derived structure monoids are Malcev nilpotent, and deal with multipermutation solutions.

Set-theoretic solutions that are not left nor right non-degenerate are explored to a much smaller extent. In the final part of this thesis, such solutions are generated using the theory of skew lattices. Moreover, the obtained set-theoretic solutions turn out to be idempotent or cubic.

Samenvatting

De Yang-Baxter vergelijking is een van de essentiële vergelijkingen uit wiskundige fysica en verscheen initieel in zowel kwantum als statistische mechanica. Het probleem om haar oplossingen te construeren en te classificeren werd, via Drinfelds idee, succesvol benaderd door te gaan focussen op de deelklasse van de verzamelingtheoretische oplossingen. Tot op heden zijn deze oplossingen van de Yang-Baxter vergelijking niet allemaal gekend.

Dit open probleem is de grootste drijfveer achter deze PhD thesis. Een doeltreffende manier om het probleem te benaderen, is om de onderliggende algebraïsche structuren te identificeren en te bestuderen. Meer gedetailleerd zullen we ons concentreren op de (semi)groep- en ringtheoretische aspecten die zich voordoen en bestuderen we deze voor specifieke klassen van verzamelingtheoretische oplossingen van de Yang-Baxter vergelijking.

Aanvankelijk onderzoeken we willekeurige verzamelingtheoretische oplossingen van de Yang-Baxter vergelijking en ontdekken we verbanden, via 1-cocycels, tussen drie (in het algemeen) verschillende monoïden die we associëren met een verzamelingtheoretische oplossing, de structuurmonoïde en de links en rechts afgeleide structuurmonoïden. Indien de verzamelingtheoretische oplossing links niet-gedegenereerd is, dan is de 1-cocycel tussen de structuurmonoïde en de links afgeleide structuurmonoïde bijectief. Dit laat toe om twee monoïde structuren te definiëren op eenzelfde verzameling, wat leidt tot de definitie van een YB-semitruss. YB-semitrussen blijken de geschikte associatieve algebraïsche structuur te zijn om links niet-gedegenereerde verzamelingtheoretische oplossingen van de Yang-Baxter vergelijking te bestuderen. In het bijzonder worden ze gebruikt om aan te tonen dat een eindige links niet-gedegenereerde verzamelingtheoretische oplossing rechts niet-gedegenereerd is enkel en alleen indien ze bijectief is. Dit is een belangrijk resultaat in deze thesis. Indien een oplossing (zowel links als rechts) niet-gedegenereerd en bijectief is, bepalen we bovendien wanneer de geassocieerde structuurmonoïde en afgeleide structuurmonoïden Malcev nilpotent zijn. We bestuderen daarenboven wat er gebeurt indien deze oplossingen multipermutatie oplossingen zijn.

Verzamelingtheoretische oplossingen van de Yang-Baxter vergelijking die niet links noch rechts niet-gedegenereerd zijn, zijn tot op heden vrijwel onontgonnen. In het laatste deel van deze thesis genereren we zo'n oplossingen gebruik makende van scheve tralies.

Bovendien blijken de bekomen verzamelingtheoretische oplossingen idempotent of kubiek te zijn.

Acknowledgements

While the goal of a PhD thesis is to present one's own achievements, the truth is that every thesis is much more a team effort. I want to sincerely thank everyone who has, each in their very own way, contributed to the existence of this thesis.

First and foremost, I would like to thank my supervisors, Eric Jespers and Leandro Vendramin, for their guidance and support during the past four years. Eric, thank you for the opportunity to explore the world as a mathematical researcher. It has been a fantastic experience where I got to meet so many interesting people, and discuss (not only) mathematics in wonderful places. Thank you for your quick responses to my emails during this final period, although you are actually on your well-deserved retirement. I hope I did not give you a heart attack with some of my questions. It has been an honor to be part of your ALGB group and to be your last PhD student. Leandro, I greatly appreciate you accepting me as your PhD student in times of need. Although we did not have much time to do research together, I know I could always reach you when I needed help.

To the members of the jury, thank you for being part of this final stage and the evaluation of this thesis, especially for the insightful comments and questions during the private defense.

To my close colleagues, Arne, Ilaria, and Łukasz, I will always cherish the time we spent not only doing research and discussing mathematics, but also sharing drinks, food, laughs, and even tears. It has been a pleasure to work along your side.

I would like to express my gratitude towards Karin Cvetko-Vah and Ferran Cedó. Karin, the world of skew lattices has been an utmost pleasure to discover thanks to you. Ferran, thank you for inviting me to Barcelona and taking me under your wing. Our collaborations have always been very enjoyable and fruitful, due to your admirable precise and quick computations and your patience. This and other research stays, conferences, meetings, etc. would not have been possible without the support of FWO.

Everyone I encountered at the VUB, especially from WIDS and the ALGB group, thank you for the numerous of interesting lunch and coffee (let's make that tea) breaks. It was a pleasure to be part of 6G and work among you. A special mention goes to Geoffrey, whose enthusiasm and support guided me to pursuing this PhD. I hope we will be able to collaborate one day soon. Timmy and Jonas, your insights in the first chapter of this thesis and help with LaTeX issues have been extremely valuable and highly appreciated.

Any attempt at anything can not be satisfactorily completed without the support of my family, friends, and basketball team. You reminded me that there is more in life than mathematics and writing a thesis. Your questions whether I had found the solution yet or if there would be a Parker equation soon always put a smile on my face.

To my parents, know that I could not have done this without you, and I am forever grateful to you. Your enthusiasm and attempts to read my papers or listen to my presentations are admirable.

Finally, to Pieter, words can not describe how much it means to me having you by my side throughout this journey. Thank you, for everything.

Bibliographical comments

The new results in this thesis are based on the following papers.

[47] F. Cedó, E. Jespers, Ł. Kubat, A. Van Antwerpen, and C. Verwimp. On various types of nilpotency of the structure monoid and group of a set-theoretic solution of the Yang-Baxter equation, 2020. arXiv:2011.01724

[52] F. Cedó, E. Jespers, and C. Verwimp. Structure monoids of set-theoretic solutions of the Yang-Baxter equation. *Publ. Mat.*, 65:499–528, 2021.

[53] F. Cedó, E. Jespers, and C. Verwimp. Corrigendum and Addendum to "Structure monoids of set-theoretic solutions of the Yang-Baxter equation", 2022. arXiv:2202.03174

[60] I. Colazzo, E. Jespers, A. Van Antwerpen, and C. Verwimp. Left non-degenerate set-theoretic solutions of the Yang-Baxter equation and semitrusses, 2021. arXiv:2109.04978

[69] K. Cvetko-Vah and C. Verwimp. Skew lattices and set-theoretic solutions of the Yang-Baxter equation. *J. Algebra*, 542:65–92, 2020.

Contents

Introduction

So it begins.

Lord of the Rings.

Solving equations is a tale as old as time and is part of our day to day life. While some equations are easy to solve, others are much more challenging or even unknown. This PhD thesis revolves around solving the Yang-Baxter equation. Given a vector space V, a linear map $R : V \otimes V \to V \otimes V$ is said to be a solution of the Yang-Baxter equation if in $\mathrm{End}(V \otimes V \otimes V)$,

$$R_{12}R_{23}R_{12} = R_{23}R_{12}R_{23},$$

where R_{ij} acts as R on the i-th and j-th component, and as the identity on the remaining component. The name of the equation is due to Yang and Baxter who initially discovered the equation in their works in quantum mechanics [184] and statistical mechanics [19] respectively. By now, the value of the Yang-Baxter equation can be seen in many different areas of mathematics and mathematical physics, for instance in knot theory, quantum computation, factorizable S-matrices, and quantum group theory.

Finding all solutions is presently beyond reach, so Drinfeld [72] thought it would be interesting to look at solutions where one replaces the linear map R by a map $r : X \times X \to X \times X$, where X is a non-empty set, and in $\mathrm{Map}(X^3, X^3)$,

$$r_{12}r_{23}r_{12} = r_{23}r_{12}r_{23},$$

where $r_{12} = r \times \mathrm{id}_X$ and $r_{23} = \mathrm{id}_X \times r$. Naturally, these solutions, called set-theoretic solutions of the Yang-Baxter equation, entail solutions on vector spaces by linearly extending them, considering X as the basis of the vector space. The goal of this thesis is to find and classify all set-theoretic solutions of the Yang-Baxter equation. We will often call them set-theoretic solutions or solutions instead of set-theoretic solutions of the Yang-Baxter equation.

A successful method to approach our goal is to study the underlying algebraic structures associated to the Yang-Baxter equation. Some of the algebraic structures were acknowledged prior to being connected to the Yang-Baxter equation, while others were introduced for this reason.

In the first chapter of this thesis, you can find a detailed background on the origin of Yang-Baxter equation, together with some applications. It also contains an introduction to set-theoretic solutions of the Yang-Baxter equation, including an overview on braces, cycle sets, and quandles, algebraic structures associated to such solutions. The first chapter contains no new results, but is primarily intended for motivation as to why one wants to find (set-theoretic) solutions of the Yang-Baxter equation.

After the first chapter, we solely focus on set-theoretic solutions of the Yang-Baxter equation. A set-theoretic solution (X,r), denoted by

$$r(x,y) = (\lambda_x(y), \rho_y(x)),$$

for all $x,y \in X$, is called left (resp. right) non-degenerate if each map λ_x (resp. ρ_y) is bijective. A left and right non-degenerate solution is simply called non-degenerate. A solution (X,r) is said to be involutive if $r^2 = \mathrm{id}_{X\times X}$, the identity map on $X \times X$, and in particular such a solution is bijective, meaning that r is a bijective map. Furthermore, (X,r) is called square-free if $r(x,x) = (x,x)$, for all $x \in X$. Finally, a solution (X,r) is called finite if the set X is finite.

To any set-theoretic solution of the Yang-Baxter equation (X,r), using the notation from above, one can associate a monoid,

$$M(X,r) = \langle X \mid x \circ y = \lambda_x(y) \circ \rho_y(x), \text{ for all } x,y \in X\rangle^1,$$

called the structure monoid associated to (X,r), and a semigroup (resp. group) $S(X,r)$ (resp. $G(X,r)$) with the same semigroup (resp. group) presentation, called the structure semigroup (resp. group) of (X,r). Both the structure monoid and structure group have been studied intensively for various types of solutions. For a finite non-degenerate involutive set-theoretic solution (X,r), it was shown by Etingof, Schedler, and Soloviev [75] that its structure group $G(X,r)$ is finitely generated, abelian-by-finite, and solvable. Furthermore, it is a Bieberbach group, i.e. a finitely generated abelian-by-finite, torsion-free group, by a result of Gateva-Ivanova and Van den Bergh [88]. For non-involutive, but still finite bijective non-degenerate solutions (X,r), Lu, Yan, and Zhu [135], and Soloviev [174] studied their structure groups and proved that they are still abelian-by-finite. The structure group of such solutions turns out to have a skew brace structure, in particular it is possible to define a solution on the set $G(X,r)$. However, in general, for any finite bijective non-degenerate set-theoretic solution, the natural map $\iota : X \to G(X,r)$ is not injective, resulting that we can not recover the original solution (X,r) from the solution defined on $G(X,r)$. This problem can be avoided by looking at the structure monoid instead of the structure group. It was shown by Gateva-Ivanova and Majid [86] that any set-theoretic solution of the Yang-Baxter equation (X,r) can be extended to a solution $(M(X,r), r_{M(X,r)})$ on its structure monoid $M(X,r)$ in such a way that the original solution (X,r) can be recovered from $(M(X,r), r_{M(X,r)})$. Also, the map $\iota : X \to M(X,r)$ is always injective. So no information of the original solution gets lost when studying the structure monoid. For finite bijective non-degenerate solutions

(X,r), it was realized by Jespers, Kubat, and Van Antwerpen [97, 98] that $M(X,r)$ is abelian-by-finite. Furthermore, the associated structure algebra $K[M(X,r)]$ (and also $K[G(X,r)]$), for any field K, was proven to be a Noetherian PI-algebra of finite Gelfand-Kirillov dimension. Moreover, many properties, such as being a domain or prime, of the algebra $K[M(X,r)]$ are equivalent with $M(X,r)$ being cancellative, or with the solution (X,r) being involutive.

Essential to prove the above results is the connection between the structure monoid and the left derived structure monoid, and between the structure group and the left derived structure group. Given an arbitrary set-theoretic solution of the Yang-Baxter equation (X,r), with the above notation, the left derived structure monoid is defined as

$$A(X,r) = \langle X \mid x + \lambda_x(y) = \lambda_x(y) + \lambda_{\lambda_x(y)}(\rho_y(x)), \text{ for all } x,y \in X\rangle^1.$$

Note that the relations are determined by the first components of r and r^2. By looking at the second components of these maps, one defines the right derived structure monoid as

$$A'(X,r) = \langle X \mid \rho_y(x) \oplus y = \rho_{\rho_y(x)}(\lambda_x(y)) \oplus \rho_y(x), \text{ for all } x,y \in X\rangle^1.$$

The left derived structure group is the group $A_{\text{gr}}(X,r)$ with the same (group) presentation as $A(X,r)$, while the right derived structure group is the group $A'_{\text{gr}}(X,r)$ with the same (group) presentation as $A'(X,r)$. For finite non-degenerate involutive set-theoretic solutions, the left and right derived structure monoid and group are free abelian, and it was shown by Etingof, Schedler, and Soloviev [75] that the structure group can be embedded as a regular subgroup into the semidirect product of the left derived structure group and $\operatorname{Sym}(X)$. A similar result was realized by Gateva-Ivanova and Van den Bergh [88] for the structure monoid. For finite bijective non-degenerate solutions and left non-degenerate solutions analogous results were obtained by Soloviev [174], Lu, Yan, and Zhu [135], and Jespers, Kubat, and Van Antwerpen [97].

In Chapter 2, the connection between $M(X,r)$, $A(X,r)$, and $A'(X,r)$ is studied for arbitrary set-theoretic solutions (X,r). The results of this chapter are stated in Sections 2 and 3 of [52]. We start by recalling a result of Gateva-Ivanova and Majid [86] on the extension of a solution (X,r) to a solution on its structure monoid $M(X,r)$. Originally, this result was given for bijective solutions, however the accurate observer sees that the latter is not used for this result. New developments appear in Section 2.2. A first new result, see Proposition 2.2.1, is that the λ-map and ρ-map of a solution (X,r) can be extended to endomorphisms of $A(X,r)$ and $A'(X,r)$ respectively.

Proposition (Proposition 3.1 in [52]). *Let (X,r) be a set-theoretic solution of the Yang-Baxter equation, where $r(x,y) = (\lambda_x(y),\rho_y(x))$, for all $x,y \in X$. Then, there exists a unique monoid homomorphism $\lambda' : M(X,r) \to \operatorname{End}(A(X,r),+)$ such that, $\lambda'(x)(y) = \lambda_x(y)$, for all $x,y \in X$, and there exists a unique monoid anti-homomorphism $\rho' : M(X,r) \to \operatorname{End}(A'(X,r),\oplus)$ such that, $\rho'(x)(y) = \rho_x(y)$, for all $x,y \in X$. Furthermore, if (X,r) is left (resp. right) non-degenerate, then $\operatorname{Im}(\lambda') \subseteq \operatorname{Aut}(A(X,r),+)$ (resp. $\operatorname{Im}(\rho') \subseteq \operatorname{Aut}(A'(X,r),\oplus)$).*

The previous result is then used in Theorem 2.2.2 to obtain unique 1-cocycles between the structure monoid and both derived structure monoids.

Theorem (Proposition 3.2 in [52]). *Let (X,r) be a set-theoretic solution of the Yang-Baxter equation. Then, there exists a unique 1-cocycle*

$$\pi : M(X,r) \to A(X,r), \quad \textit{(resp. } \pi' : M(X,r) \to A'(X,r)\textit{)},$$

with respect to the "left action" λ' (resp. "right action" ρ') such that $\pi(x) = x$ (resp. $\pi'(x) = x$), for all $x \in X$, and $\pi(a \circ b) = \pi(a) + \lambda'_a(\pi(b))$ (resp. $\pi'(a \circ b) = \rho'_b(\pi'(a)) \oplus \pi'(b)$), for all $a, b \in M(X,r)$. Furthermore, the mapping

$$f : M(X,r) \to A(X,r) \rtimes \operatorname{Im}(\lambda') : a \mapsto (\pi(a), \lambda'_a),$$

is a monoid homomorphism, and the mapping

$$f' : M(X,r) \to A'(X,r)^{op} \rtimes \operatorname{Im}(\rho') : a \mapsto (\pi'(a), \rho'_a),$$

is a monoid anti-homomorphism.

Afterwards, we study when exactly the 1-cocycles π and π' are bijective. We obtain that π (resp. π') is surjective if and only if all maps λ_x (resp. ρ_y) are surjective (Proposition 2.2.6), and π (resp. π') is injective if all maps λ_x (resp. ρ_y) are injective (Proposition 2.2.7). The converse of the latter is not true, which is shown by an example.

In Chapter 3, we focus on left non-degenerate set-theoretic solutions of the Yang-Baxter equation. To any left non-degenerate solution (X,r), one can associate its left derived solution (X,s), defined by

$$s(x,y) = (y, \lambda_y \rho_{\lambda_x^{-1}(y)}(x)) = (y, \sigma_y(x)),$$

for all $x, y \in X$. Following [60], we introduce a new algebraic object, called a YB-semitruss, and prove that YB-semitrusses provide left non-degenerate set-theoretic solutions of the Yang-Baxter equation (Proposition 3.1.3). Furthermore, structure monoids of left non-degenerate set-theoretic solutions of the Yang-Baxter equation are natural examples of YB-semitrusses (Theorem 3.1.13).

Theorem (Proposition 2.11 in [60]). *Let (X,r) be a left non-degenerate set-theoretic solution of the Yang-Baxter equation. The associated structure monoid $M = M(X,r)$ is a unital YB-semitruss and has the structure semigroup $S(X,r)$ as a sub-YB-semitruss (not unital). The associated solution (respectively left derived solution) of the unital YB-semitruss M, as defined in Proposition 3.1.3, is precisely the solution (M, r_M) (respectively the left derived solution (M, s_M) of (M, r_M)) from Theorem 2.1.1 i.e. the extension by Gateva-Ivanova and Majid [86]. Similar results hold for the YB-semitruss $S(X,r)$.*

The YB-semitruss $M(X,r)$ is called the unital structure YB-semitruss associated to the left non-degenerate solution (X,r), and $S(X,r)$ is called the structure YB-semitruss of (X,r). In addition, any YB-semitruss is an epimorphic image of a structure YB-semitruss or a unital structure YB-semitruss (Theorem 3.1.15).

Theorem (Corollary 2.14 in [60]). *Let $(A, +, \circ, \lambda, \sigma)$ be a YB-semitruss with associated solution (A, r_A). Then, the YB-semitruss A is an epimorphic image of the structure YB-semitruss $S(A, r_A)$. If A is a unital YB-semitruss, then A is an epimorphic image of the unital structure YB-semitruss $M(A, r_A)$.*

Hence, YB-semitrusses turn out to be the suitable associative algebraic structure to study left non-degenerate set-theoretic solutions of the Yang-Baxter equation. Next, in Subsection 3.1.2, we study YB-semitrusses $(A, +, \circ, \lambda, \sigma)$ with $(A, +)$ (and thus also $(A, \circ)$) left cancellative, called left cancellative YB-semitrusses. We show that it is possible to define a left cancellative congruence ν on $M(X, r)$ such that the left cancellative image $M(X, r)/\nu$ of $M(X, r)$ is a left cancellative YB-semitruss (Example 3.1.24). This result is stated and proven in [53]. Also, semi-braces and skew left braces are examples of left cancellative YB-semitrusses (Example 3.1.25 and Example 3.1.26). Afterwards, in Subsection 3.1.3 and Subsection 3.1.4, we study idempotents in YB-semitrusses and matched products of YB-semitrusses, and use the latter to construct new examples of YB-semitrusses. These new results are all contained in [60, Section 2]. In Section 3.2, we study non-degenerate YB-semitrusses $(A, +, \circ, \lambda, \sigma)$, i.e. YB-semitrusses with associated solution (A, r_A) non-degenerate, and show that in this case the diagonal map $\mathfrak{q} : A \to A : a \mapsto \lambda_a^{-1}(a)$ is always injective (Lemma 3.2.4). If the map $\mathfrak{q}$ is bijective (for example if A is finite), then the associated solution (A, r_A) is bijective (Lemma 3.2.5). Together with the results from Subsection 3.1.1, we obtain the following important theorem (Theorem 3.2.8).

Theorem (Theorem 3.1 in [60]). *Let (X, r) be a finite left non-degenerate set-theoretic solution of the Yang-Baxter equation. Then, r is bijective if and only if (X, r) is right non-degenerate.*

In Section 3.3, following [60, Section 3], it is proven that, for any non-degenerate YB-semitruss $(A, +, \circ, \lambda, \sigma)$, the set $\mathcal{G}(A) = \{f(a) = (\sigma_a, \lambda_a, \rho_a) \mid a \in A\}$ has a YB-semitruss structure (Theorem 3.3.5), which allows us to define the retract relation for non-degenerate set-theoretic solutions of the Yang-Baxter equation. Finally, following [60, Section 4], in Section 3.4, we study the algebraic structure of YB-semitrusses. More precisely, for finite left non-degenerate solutions, we prove that $K[A(X, r)]$ is left Noetherian, satisfies a polynomial identity, and is of finite Gelfand-Kirillov dimension (Theorem 3.4.3). If, moreover, the diagonal map $\mathfrak{q}$ is bijective, then also $K[M(X, r)]$ is left Noetherian satisfying a polynomial identity. Hence, so is $K[(A, \circ)]$ for any unital strongly $\mathbb{N}$-graded YB-semitruss $(A, +, \circ, \lambda, \sigma)$, with A_1 finite, $A_0 = \{1\}$, and diagonal map $\mathfrak{q} : A \to A$ bijective (Corollary 3.4.4). In the specific case when, for a YB-semitruss $(A, +, \circ, \lambda, \sigma)$, the semigroup $\mathcal{C}(A) = \{\sigma_a \mid a \in A\}$ is finite and left simple, then the left derived solution (A, s_A), with $s_A(a, b) = (b, \sigma_b(a))$, for all $a, b \in A$, is determined by bijective non-degenerate solutions and the idempotents of $\mathcal{C}(A)$ (Theorem 3.4.5).

In Chapter 4, following [47], we focus on bijective non-degenerate set-theoretic solutions of the Yang-Baxter equation, a subclass of all set-theoretic solutions containing the left non-degenerate ones. In the first part of Section 4.1, we study left cancellative congruences on $M(X, r)$, where (X, r) is a bijective non-degenerate solution, presenting results from both [52] and [53]. In particular, we prove that the least left cancellative congruence on $(M(X,r),\circ)$ is equal to the least left cancellative congruence on $(M(X,r),+)$ (Proposition 4.1.3). In the second part of Section 4.1, we discuss several types of permutation groups associated to a bijective non-degenerate set-theoretic solution.

Continuing the investigations of Lebed and Mortier [122] on finite quandles with abelian structure group, we study Malcev nilpotency of the structure monoid $M(X,r)$ of a finite bijective non-degenerate solution (X,r). In Section 4.2, we investigate the case where $M(X,r) = A'(X,r)$, i.e. $(X,r) = (X,s')$ is a rack solution, with, for any $x,y \in X$,

$$s'(x,y) = (\rho_x \lambda_{\rho_y^{-1}(x)}(y), x) = (\tau_x(y), x),$$

the right derived solution associated to (X,r), and obtain the following result (Proposition 4.2.1).

Proposition (Proposition 2.2 in [47])**.** *Let $(X,r) = (X,s')$ be a rack solution. If the permutation group $\mathcal{G}_\tau(X,r) = \mathrm{gr}(\tau_x \mid x \in X)$ is nilpotent of class n, then the structure monoid $M(X,r) = A'(X,r)$ of (X,r) is Malcev nilpotent of class not exceeding $n+2$. Similarly, the structure group $G(X,r) = A'_{\mathrm{gr}}(X,r)$ is nilpotent of class not exceeding $n+2$.*

For the structure group of a rack solution, the upper bound of the nilpotency class can be strengthened. Furthermore, we can say something about its solvability (Corollary 4.2.2).

Corollary (Corollary 2.4 in [47])**.** *Let $(X,r) = (X,s')$ be a rack solution with structure group $G = G(X,r)$. Then, the group $G/Z(G)$ is a homomorphic image of the permutation group $\mathcal{G}_\tau = \mathcal{G}_\tau(X,r) = \mathrm{gr}(\tau_x \mid x \in X)$. In particular, G is nilpotent if and only if $\mathcal{G}_\tau$ is nilpotent, and the nilpotency class of G is equal to or exceeds by one the nilpotency class of $\mathcal{G}_\tau$. Furthermore, G is solvable if and only if $\mathcal{G}_\tau$ is solvable, and the derived length of G is equal to or exceeds by one the derived length of $\mathcal{G}_\tau$.*

Next, we recall that, for any finite bijective non-degenerate set-theoretic solution of the Yang-Baxter equation, if its structure group $G(X,r)$ is nilpotent, then $G(X,r)$ is finite-by-(free abelian) and it has a finite commutator subgroup (Lemma 4.2.3). If $G(X,r)$ is torsion-free, then nilpotency and abelianess of $G(X,r)$ are equivalent (Lemma 4.2.3). This is used to prove that if $A_{\mathrm{gr}}(X,r)$ (resp. $A'_{\mathrm{gr}}(X,r)$) is nilpotent, then its torsion subgroup is equal to its commutator subgroup (Proposition 4.2.4). Section 4.2 ends with a description of finite abelian racks. Together with a result of Lebed and Mortier [122, Theorem 2.3], we obtain a full combinatorial description of all finite abelian racks. In Section 4.3, we deal with arbitrary finite bijective non-degenerate solutions and investigate when $M(X,r)$ is Malcev nilpotent, by giving a very concrete description of an ideal chain of $M(X,r)$. More precisely, we look at left divisibility of elements in $M(X,r)$ and create an ideal chain with Rees factors either power nilpotent semigroups or uniform subsemigroups of a completely (θ)-simple inverse semigroup with maximal subgroups isomorphic to the group of fractions of cancellative subsemigroups of $M(X,r)$ (Proposition 4.3.6). From this, using a result of Jespers and Riley [104, Theorem 11], we can characterize exactly when $M(X,r)$ is Malcev nilpotent (Theorem 4.3.7).

Theorem (Theorem 3.7 in [47])**.** *Let (X,r) be a finite bijective non-degenerate set-theoretic solution of the Yang-Baxter equation, and put $n = |X|$. Then, the structure monoid $M(X,r)$ is Malcev nilpotent if and only if all cancellative subsemigroups of $M(X,r)$ (actually it is sufficient that all cancellative components $m_Y M_{YY}$ with $m_Y \notin M_{|Y|+1}$) are Malcev nilpotent and the following condition, called the nilpotency condition, is not satisfied:*

$$\text{there exist subsets } Y \neq Z \text{ of } \{a_1,\dots,a_n\}, \text{ the generators of } A(X,r), \text{ with}$$
$$a_Y \text{ and } a_Z \text{ only divisible by elements of } Y, \text{ respectively } Z, \text{ and } a,b \in \langle Y \cap Z\rangle$$
$$\text{such that } \lambda'_{\pi^{-1}(b)}((\lambda'_{\pi^{-1}(a)})^{-1}(Y)) = Z \text{ and } \lambda'_{\pi^{-1}(b)}((\lambda'_{\pi^{-1}(a)})^{-1}(Z)) = Y.$$

The nilpotency condition is redundant in some specific cases (Corollary 4.3.8).

Corollary (Corollary 3.8 in [47])**.** *Let (X,r) be a finite bijective non-degenerate set-theoretic solution of the Yang-Baxter equation. If the group $\mathcal{G}_\lambda(X,r) = \mathrm{gr}(\lambda_x \mid x \in X)$ is of odd order or if the uniform components of $M(X,r)$ have degree one, then the structure monoid $M(X,r)$ is Malcev nilpotent if and only if all cancellative subsemigroups of $M(X,r)$ (actually it is sufficient that all cancellative components $m_Y M_{YY}$ with $m_Y \notin M_{|Y|+1}$) are Malcev nilpotent.*

Afterwards, finite bijective non-degenerate solutions of Lyubashenko type are studied in more details (Proposition 4.3.11).

Proposition (Proposition 3.10 in [47])**.** *Let (X,r) be a finite bijective non-degenerate Lyubashenko solution, defined by $r(x,y) = (f(y), g(x))$, for all $x,y \in X$, and some commuting permutations f and g on X. Then, the structure monoid $M(X,r)$ is Malcev nilpotent if and only if $f = c_1^{k_1}\cdots c_t^{k_t}$ and $g = c_1^{1-k_1}\cdots c_t^{1-k_t}$, where $c_1,\dots,c_t$ are disjoint cycles. In this case, all cancellative components are abelian and their group of fractions is of rank $1 \leq j \leq t$, and all such numbers j can be reached. Furthermore, all uniform components have degree one.*

Section 4.3 ends with some examples. In Section 4.4, we define the retract relation for bijective non-degenerate solutions that are not necessarily finite, and study bijective non-degenerate multipermutation solutions. We show that if (X,r) is a bijective non-degenerate multipermutation solution, with $|X| > 1$ and r of finite order, then the order of r must be even (Proposition 4.4.6). Furthermore, epimorphic images and subsolutions of bijective non-degenerate multipermutation solutions of finite level m are also multipermutation solutions of finite level bounded by m (Proposition 4.4.8 and Lemma 4.4.9). Afterwards, we work towards the following important result (Theorem 4.4.13).

Theorem (Theorem 4.13 in [47])**.** *Let (X,r) be a bijective non-degenerate set-theoretic solution of the Yang-Baxter equation. The following properties are equivalent.*

(1) The solution (X, r) is of finite multipermutation level.

(2) The associated solution on $M(X, r)$ is of finite multipermutation level.

(3) The associated solution on $G(X, r)$ is of finite multipermutation level.

Furthermore, we study the solvability of the structure group and the (Malcev) nilpotency of the left derived structure group and monoid of bijective non-degenerate multipermutation solutions (Theorem 4.4.15).

Theorem (Theorem 4.15 in [47])**.** *Let (X, r) be a bijective non-degenerate multipermutation solution of level m. Then, the group $G(X, r)$ is solvable of derived length bounded by $m + 1$. Moreover, the monoid $A(X, r)$ is Malcev nilpotent of class at most $m + 3$, and the group $A_{\mathrm{gr}}(X, r)$ is nilpotent of class at most $m + 1$.*

The upper bound for solvability and nilpotency is more accurate if the solution is square-free (Corollary 4.4.16).

Corollary (Corollary 4.16 in [47])**.** *Let (X, r) be a square-free bijective non-degenerate set-theoretic solution of the Yang-Baxter equation. If (X, r) is a multipermutation solution of level m, then the associated solution (G, r_G) on $G = G(X, r)$ satisfies $m - 1 \leq \mathrm{mpl}(G, r_G) \leq m$. If, furthermore, (X, r) is an injective solution, then $\mathrm{mpl}(G, r_G) = m$.*

Moreover, the additive group of the skew left brace G is nilpotent of class bounded by m, and the structure group G is solvable of derived length bounded by m.

The result that the torsion subgroup of the left (resp. right) derived structure monoid is equal to the commutator subgroup, for a finite bijective non-degenerate solution with left (resp. right) derived structure monoid being nilpotent, can be generalized in case the solution is also a multipermutation solution (Proposition 4.4.17).

Proposition (Proposition 4.17 in [47])**.** *Let (X, r) be a finite bijective non-degenerate multipermutation solution of the Yang-Baxter equation. If the structure group $G = G(X, r)$ is nilpotent, then the torsion subgroup $T = T(G)$ of $(G, \circ)$ is finite. Furthermore, the additive commutator subgroup $[G, G]_+$ of the additive group $(G, +) = A_{\mathrm{gr}}(X, r)$ of the skew left brace $(G, +, \circ)$ is a subgroup of $(G, \circ)$, and equal to T.*

The solutions that are studied in Chapter 3 and Chapter 4 are at least left (or similarly right) non-degenerate. This provides a certain amount of knowledge and playability on the structure monoid and derived structure monoids. Solutions that are not left nor right non-degenerate, i.e. degenerate solutions, are much less explored. In the final chapter, Chapter 5, following [69], we study skew lattices and show that they provide set-theoretic solutions of the Yang-Baxter equation that are either idempotent, i.e. $r^2 = r$, or cubic, i.e. $r^3 = r$, and that are degenerate in most cases. We start with some preliminaries on skew lattices for those who are unfamiliar with the subject. Hence, Section 5.1 contains no new results. Since skew lattices generate solutions of the Yang-Baxter equation, it is worth studying constructions of skew lattices. In Section 5.2, several constructions of skew lattices are presented, either starting with a family of pairwise disjoint sets or a family of pairwise disjoint skew lattices. In Section 5.3, we define idempotent set-theoretic solutions of the Yang-Baxter equation using arbitrary skew lattices (Theorem 5.3.4). The following result is the main theorem of Chapter 5.

Theorem (Theorem 3.3 in [69]). *Let $(S, \wedge, \vee)$ be a skew lattice. Then, (S, r) with*

$$r : S \times S \to S \times S : (x, y) \mapsto ((x \wedge y) \vee x, y),$$

is an idempotent set-theoretic solution of the Yang-Baxter equation.

In Section 5.4 and Section 5.5, we define other solutions using skew lattices with some more structure. Getting inspiration from the solution (L, r), with $r(x, y) = (x \wedge y, x \vee y)$, for all $x, y \in L$, and $(L, \wedge, \vee)$ a distributive lattice, we study skew lattices $(S, \wedge, \vee)$ for which (S, r), with $r(x, y) = (x \wedge y, x \vee y)$, for all $x, y \in S$, is a set-theoretic solution of the Yang-Baxter equation (Theorem 5.4.3).

Theorem (Theorem 4.3 in [69]). *Let $(S, \wedge, \vee)$ be a skew lattice which is both strongly and co-strongly distributive. Then, (S, r) with $r : S \times S \to S \times S : (x, y) \mapsto (x \wedge y, x \vee y)$, is a cubic set-theoretic solution of the Yang-Baxter equation.*

The converse, however, is not true, which is provided by an example (Example 5.4.7). Next, we study the map $r_L(x, y) = (x \wedge y, y \vee x)$, for all $x, y \in S$, and obtain the following result (Theorem 5.5.7).

Theorem (Theorem 5.7 in [69]). *Let $(S, \wedge, \vee)$ be a distributive and left cancellative skew lattice. Then, (S, r_L) with $r_L : S \times S \to S \times S : (x, y) \mapsto (x \wedge y, y \vee x)$, is an idempotent set-theoretic solution of the Yang-Baxter equation.*

Similarly, we study the map $r_R(x, y) = (y \wedge x, x \vee y)$, for all $x, y \in S$, and obtain the following conclusion (Theorem 5.5.8).

Theorem (Theorem 5.8 in [69]). *Let $(S, \wedge, \vee)$ be a distributive and right cancellative skew lattice. Then, (S, r_R) with $r_R : S \times S \to S \times S : (x, y) \mapsto (y \wedge x, x \vee y)$, is an idempotent set-theoretic solution of the Yang-Baxter equation.*

Finally, we study the map $r_W(x, y) = (x \wedge y \wedge x, x \vee y \vee x)$, for all $x, y \in S$, and obtain the following result (Theorem 5.5.11).

Theorem (Theorem 5.11 in [69]). *Let $(S, \wedge, \vee)$ be a distributive, simply cancellative and lower symmetric skew lattice. Then, (S, r_W) with $r_W : S \times S \to S \times S : (x, y) \mapsto (x \wedge y \wedge x, x \vee y \vee x)$, is an idempotent set-theoretic solution of the Yang-Baxter equation.*

The converses of Theorem 5.5.7, Theorem 5.5.8, and Theorem 5.5.11 were proven by the Automated Theorem Prover *Prover9* [139]. We include the input and output codes in the appendix.

Unless mentioned otherwise, all results in Chapters 2 to 5 are personal results, published in [47, 52, 53, 60, 69].

Chapter 1

Foreword on the Yang-Baxter equation

> Don't let anyone rob you of your imagination, your creativity, or your curiosity. It's your place in the world; it's your life. Go on and do all you can with it, and make it the life you want to live.
>
> Mae Jemison

The origin of the Yang-Baxter equation can be found in theoretical physics, more specific in the field of quantum mechanics and statistical mechanics. Although the equation itself clearly appeared in the works of Yang [184, 185] and Baxter [19], it was also hidden in several other papers, see for example [21, 22, 25, 140, 149, 188, 187, 119], as the star-triangle relation, the triangle equation or the factorization equation.

For a vector space V, we say that $R \in \operatorname{End}(V \otimes V)$ is a *solution of the Yang-Baxter equation* if it satisfies

$$R_{12}R_{23}R_{12} = R_{23}R_{12}R_{23}, \tag{1.1}$$

where $R_{ij} \in \operatorname{End}(V^{\otimes 3})$ acts as R on the i-th and j-th component, and as the identity on the remaining component. One can graphically interpret this equation as in Fig. 1.1.

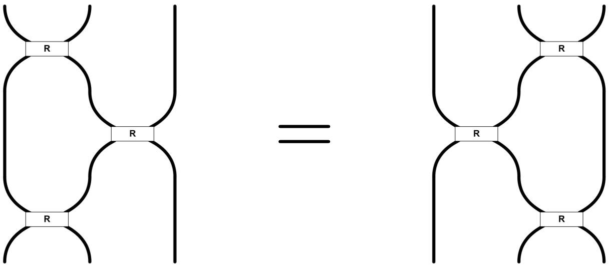


Figure 1.1: An illustration of the Yang-Baxter equation.

A map $R \in \operatorname{End}(V \otimes V)$ is a solution of the Yang-Baxter equation if and only if τR, where $\tau \in \operatorname{End}(V \otimes V)$ maps $x \otimes y$ to $y \otimes x$, is a *solution of the quantum Yang-Baxter equation*

$$R_{12}R_{13}R_{23} = R_{23}R_{13}R_{12}. \tag{1.2}$$

In this chapter, we dive a little bit deeper into both papers of Yang and Baxter, as well as some applications or connections with other fields. The first part concerns Yang's contribution to certain one-dimensional many-body problems in quantum mechanics. In order to find the exact wave function of the model, he uses the Bethe ansatz where the Yang-Baxter equation appears as some condition that has to be satisfied. The Yang-Baxter equation also appeared in an independent paper of Baxter in the field of statistical mechanics. Inspired by the results of the Bethe ansatz, Baxter found a new method, the commuting transfer matrices method, to find the eigenvectors of the transfer matrix that defines the partition function of the eight vertex model.

The second part discusses the influence of the Yang-Baxter equation in knot theory, quantum computation, factorizable S-matrices, and quantum group theory.

The third and final part deals with a specific class of solutions, namely the set-theoretic ones. In [72], Drinfeld posed the idea of looking at set-theoretic solutions of the Yang-Baxter equation. By linearly extending these (using the set as the basis of a vector space), one obtains solutions on vector spaces. We recall some classes of set-theoretic solutions and give a short overview of some known solutions or algebraic structures used to classify these solutions.

The aim of this chapter is to give the reader a broad idea of the motivation behind this thesis, an attempt to answer the question "Why do we want to find solutions of the Yang-Baxter equation?". This chapter is rather informative, and contains no new results. The reader should be aware that the author is not an expert in the field of theoretical physics, quantum or statistical mechanics, knot theory, quantum computation, factorizable S-matrices, or quantum group theory. In the upcoming chapters, it will be clear that the author focuses on the (semi)group theory and ring theory that is involved around set-theoretic solutions of the Yang-Baxter equation.

1.1 The origin of the Yang-Baxter equation

1.1.1 Quantum mechanics

For many years, scientists have been trying to describe the universe. As far as classical mechanics goes, everyone has an intuitive idea of how objects move in space. Beyond classical mechanics, quantum mechanics focuses on describing microscopic particles, their movement and their interactions. This, however, is much more complicated as there is an unavoidable and inherent element of uncertainty in quantum mechanics. To deal with this uncertainty, physicists try to find the wave function which describes the probability of a quantum system being in a given state.

Describing and predicting the behavior of many interacting microscopic particles, by discovering and understanding the wave function of such a system, is known as the many-body problem. The wave function of a quantum system holds a large amount of information on the system and helps to describe it as accurately as possible. Unfortunately, finding the exact wave functions of many-body quantum systems is difficult. However, the Bethe ansatz method can be used to find the exact wave functions for a numerous amount of one-dimensional many-body quantum models. This is where the Yang-Baxter equation first appeared. It is an equation that has to be satisfied in order to use the Bethe ansatz to describe the wave function. Before going deeper into the appearance of the Yang-Baxter equation, we first look into the famous Bethe ansatz.

Bethe ansatz

In classical mechanics, the Hamiltonian H denotes the total amount of energy of the system and is equal to the sum of the kinetic energy T and the potential energy V. The kinetic energy can also be expressed by the momentum p and mass m, i.e. $T = \frac{p^2}{2m}$. In quantum mechanics, however, things get more complicated. By the inescapable, yet fundamental, property of Heisenberg's uncertainty principle, the more precise the momentum of a particle is known the more uncertain its position is and vice versa. So it is impossible to know the momentum and position of a particle simultaneously. The Hamiltonian operator is defined as $\hat{H} = -\frac{\hbar^2}{2m}\frac{\partial^2}{\partial x^2} + V(x)$, with $\hbar$ the reduced Planck constant. For more information on the topic, see for example [91]. The one-dimensional N-body quantum system with repulsive δ-function interaction, the model that is studied by Yang in [184], has as Hamiltonian

$$H = -\sum_{i=1}^{N} \frac{\partial^2}{\partial x_i^2} + 2c \sum_{1\le i<j\le N} \delta(x_i - x_j), \qquad c > 0.$$

To gain insight into the particles of the quantum system, we need to determine the wave function $\Psi = \psi(x)e^{iEt/\hbar}$ by solving the Schrödinger equation $i\hbar\frac{\partial}{\partial t}\Psi = \hat{H}\Psi$ or the simpler time-independent Schrödinger equation $\hat{H}\psi = E\psi$, where E denotes the energy of the system. The eigenvalues of the Hamiltonian operator are also called the eigenstates and denoted by

$$|\psi\rangle = \sum_{1\le x_1\le\cdots\le x_n\le N} a(x_1,\ldots,x_n)\,|x_1,\ldots,x_n\rangle\,,$$

for n overturned spins. Another method, which can be used for a certain amount of one-dimensional many-body quantum models, is to use the Bethe ansatz to predict the form of the wave function, or rather to predict the form of $a(x_1,\ldots,x_n)$.

The English translation for the German word "ansatz" is attempt or approach. More precisely, in mathematics and physics an ansatz is some sort of educated guess of the solution, which is then later verified to indeed be (a part of) the solution. Take, for example, second order linear differential equations where, in some cases, one can guess the form of the solution. The Bethe ansatz is named after Bethe, who found an ansatz for the wave function of the one-dimensional antiferromagnetic Heisenberg model Hamiltonian [23]. The paper [23] presents an ansatz or hypothesis for the coefficients of the eigenfunction or wave function of this specific model.

The one-dimensional N-body problem with repulsive δ-function interaction

In [184], Yang considers the one-dimensional N-body problem,

$$H = -\sum_{i=1}^{N} \frac{\partial^2}{\partial x_i^2} + 2c \sum_{1\le i<j\le N} \delta(x_i - x_j), \quad c > 0,$$

with repulsive δ-function interaction, where $2c$ is the amplitude of the δ-function [134]. So the setting is a quantum system with N particles, where the particles repel each other according to the given δ-function. The δ-function, which is rather a measure or distribution than a function, can be seen as

$$\delta(x_i - x_j) = \begin{cases} \infty, & x_i = x_j \\ 0, & x_i \neq x_j \end{cases},$$

and has to satisfy $\int_{-\infty}^{+\infty} \delta(x)dx = 1$. So two particles only repel when they are at the same position, i.e. when they collide.

To determine the wave function of this model, Yang assumes Bethe's hypothesis to be valid [184]. Let Sym_N denote the symmetric group on N elements, $p_1, \dots, p_N$ are unequal numbers called the wavenumbers, $Q = [Q_1, \dots, Q_N] \in \mathrm{Sym}_N$, and $0 < x_{Q_1} < \dots < x_{Q_N} < L$ for some real number L, the wave function equals

$$\psi = \sum_{P \in \mathrm{Sym}_N} [Q, P] e^{i(p_{P_1} x_{Q_1} + \dots + p_{P_N} x_{Q_N})},$$

where $P = [P_1, \dots, P_N] \in \mathrm{Sym}_N$. We can see the coefficients $[Q, P]$ as the components of an $N! \times N!$ matrix, with columns denoted by ε_P. Sometimes $[Q, P]$ is also denoted as $A_Q(P) = A_{\sigma_{Q_1} \dots \sigma_{Q_N}}(p_{P_1}, \dots, p_{P_N})$, called the amplitude of the wave function (see for example [170, Chapter 5]). As the wave function needs to satisfy certain conditions, Yang deduces a condition for the columns ε_P. Namely, for any two consecutive numbers $a, b \in \{1, \dots, N\}$,

$$\varepsilon_P = Y_{kj}^{ab} \varepsilon_{P'},$$

where $P = [P_1, \dots, P_N], P' = [P'_1, \dots, P'_N] \in \mathrm{Sym}_N$, with $P_1 = P'_1, \dots, P_{a-1} = P'_{a-1}, P_a = j = P'_b, P_b = k = P'_a, P_{b+1} = P'_{b+1}, \dots, P_N = P'_N$. Putting $x_{jk} = ic(p_j - p_k)^{-1} = -x_{kj}$ and $y_{jk} = 1 + x_{jk}$, the operator Y is defined by

$$Y_{jk}^{ab} = (y_{jk}^{-1} - 1) + y_{jk}^{-1} P_{ab} = Y_{jk}^{ba},$$

with P_{ab} permuting Q_a and Q_b. Using that P_{ab}^2 is the identity, easy computations show that $Y_{ij}^{ab} Y_{ji}^{ab} = 1$. Furthermore, for any consecutive numbers $a, b, c \in \{1, \dots, N\}$, one can prove that

$$Y_{jk}^{ab} Y_{ik}^{bc} Y_{ij}^{ab} = Y_{ij}^{bc} Y_{ik}^{ab} Y_{jk}^{bc}. \tag{1.3}$$

So equation (1.3) appears in [184] as an identity that needs to be satisfied to use the Bethe ansatz to get the wave function for the quantum system. Looking at the consecutive numbers $a, b, c \in \{1, \dots, N\}$, equation (1.3) has a strong affinity to the formulation (1.1) of the Yang-Baxter equation that is known today.

Similar computations can be done using $A_Q(P) = A_{\sigma_{Q_1} \dots \sigma_{Q_N}}(p_{P_1}, \dots, p_{P_N})$ instead of $[Q, P]$. In [170], the S-matrix is defined satisfying

$$A_{\dots \sigma_j \sigma_i \dots}(\dots, p_v, p_u, \dots) = \sum_{\sigma_i' \sigma_j'} S^{\sigma_i \sigma_j}_{\sigma_i' \sigma_j'}(p_u, p_v) A_{\dots \sigma_i' \sigma_j' \dots}(\dots, p_u, p_v, \dots).$$

On $N = 3$ particles, it is then shown (see [170, Section 5.2]) that

$$\begin{aligned} &\sum_{\sigma_1' \sigma_2' \sigma_3'} S^{\sigma_1 \sigma_2}_{\sigma_1' \sigma_2'}(p_1, p_2) S^{\sigma_1' \sigma_3}_{\sigma_1'' \sigma_3'}(p_1, p_3) S^{\sigma_2' \sigma_3'}_{\sigma_2'' \sigma_3''}(p_2, p_3) \\ &\qquad = \sum_{\sigma_1' \sigma_2' \sigma_3'} S^{\sigma_2 \sigma_3}_{\sigma_2' \sigma_3'}(p_2, p_3) S^{\sigma_1 \sigma_3'}_{\sigma_1' \sigma_3''}(p_1, p_3) S^{\sigma_1' \sigma_2'}_{\sigma_1'' \sigma_2''}(p_1, p_2), \end{aligned} \tag{1.4}$$

which can graphically be represented as in Fig. 1.2.

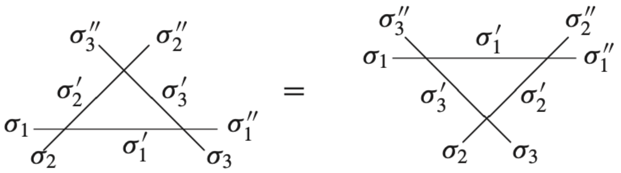


Figure 1.2: A constraint among the elements of the S-matrix [170, (5.17)].

Looking at the indices of the σ-maps of each S-matrix component, the quantum Yang-Baxter equation (1.2) naturally appears.

1.1.2 Statistical mechanics

Another part of physics, called statistical mechanics, focuses on describing the statistical behavior of a system based on weakly known initial conditions. The need for statistical methods comes from the lack of information on the quantum system. The initial conditions are mostly macroscopic variables, called macrostates, such as the volume, total energy, or temperature. Next to macroscopic variables, there are also microscopic variables, called microstates. Examples are given by the position and momentum of a particle in classical mechanics, and the exact value of the wave function of a particle in a quantum system. Given the knowledge of the microstates of a system, can we predict the relations between the observable macrostates?

Partition function

A fundamental key to describe the macrostates of the system is the partition function, denoted by Z, and defined by

$$Z = \sum_{\text{states}} e^{-E(\text{state})/kT},$$

where k is the Boltzmann constant and T is the temperature. For more details, see [20, 28]. The probability that the system is in a certain state is given by

$$P(\text{state}) = \frac{1}{Z} e^{-E(\text{state})/kT},$$

where the sum of the probabilities over all states should equal 1. The conserved energy of the total system, denoted by U, can be expressed by the partition function, namely

$$U = kT^2 \frac{\partial}{\partial T} \ln Z.$$

For more details, see for example [20, Section 1.4].

The goal is to find the partition function for specific models, because partition functions contain all information of the system. Once the exact partition function is found, the model is said to be solved. In [18, 19], Baxter solves the zero-field eight-vertex model, a generalization of the six-vertex or ice-type models which were solved in [131, 132, 133]. In the upcoming part, we see how Baxter solves this model. It is mostly based on Baxter's book [20].

The partition function of the eight-vertex model

In [19], Baxter exactly calculates the partition function of the zero-field eight-vertex model on a square $M \times N$ lattice, where a lattice is called a square lattice if the distance between two consecutive points in the same line or column are all equal. Zero-field means that there is no external electric field, so reversing all arrows does not change the model. In [131, 132, 133], the six-vertex models were solved. An example of such a model is a two-dimensional sample of ice (for this reason, the models are also called ice-type). Each oxygen atom is surrounded by four hydrogen atoms, two close by and two a bit further, to bond with other oxygen atoms. This can be illustrated by six different arrow configurations at a single vertex, see Figure 1.3.

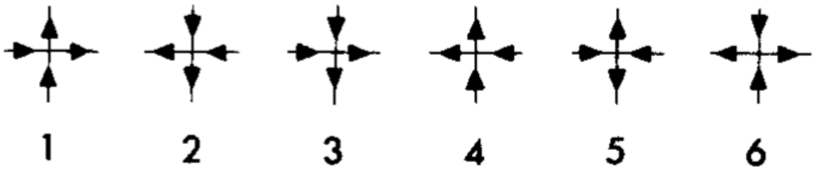


Figure 1.3: The six arrow configurations allowed at a vertex of an ice-type model [20, Fig. 8.2].

The problem of coloring the faces of a square lattice with three colors such that no two adjacent surfaces have the same color is equivalent to the ice-type model [133]. In [16], Baxter solves the three-coloring problem of the hexagonal lattice, i.e. counting the number of ways the edges of a hexagonal lattice can be colored such that no two adjacent edges have the same color. In [17] (see also [20, Section 8.13]), Baxter solves the three-coloring problem of a square lattice in case the colors have an associated activity, using the Bethe ansatz. A special case of this problem is reminiscent of the hard-square lattice gas [17].

Sutherland [177], and Fan and Wu [76], generalized the six-vertex model by adding two configurations, with the rule that an even amount of arrows should point to (or away from) each vertex, see Figure 1.4.

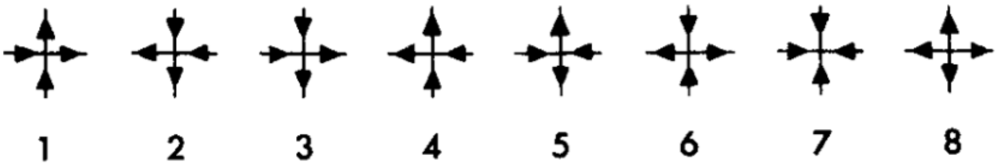


Figure 1.4: The eight arrow configurations of the eight-vertex model [20, Fig. 10.1].

Each vertex configuration is assigned with an energy ε_i and appears n_i times in the $M \times N$ lattice, for $i \in \{1, \dots, 8\}$. To solve the model, Baxter determines the associated partition function

$$Z = \sum_{\text{states}} e^{-\varepsilon/kT}, \tag{1.5}$$

with $\varepsilon = \sum_{i=1}^{8} n_i \varepsilon_i$, T the temperature and k the Boltzmann constant. We delve deeper into Baxter's calculations, following [19, 20], and see where the Yang-Baxter equation appears.

Assuming toroidal boundary conditions on the model, we get $n_7 = n_8$. By reversing all vertical arrows, vertex 5 and 6 become vertex 7 and 8 respectively, so also $n_5 = n_6$. Without loss of generality, one can choose $\varepsilon_5 = \varepsilon_6$ and $\varepsilon_7 = \varepsilon_8$. Baxter further assumes that $\varepsilon_1 = \varepsilon_2$ and $\varepsilon_3 = \varepsilon_4$. This is called the zero-field eight-vertex model, i.e. reversing the arrows does not change the model.

The Boltzmann weights or vertex weights are given by

$$\omega_i = e^{-\varepsilon_i/kT},$$

for $i \in \{1, \dots, 8\}$. In the zero-field eight-vertex model, set

$$\begin{aligned} \omega_1 &= \omega_2 = a, \\ \omega_3 &= \omega_4 = b, \\ \omega_5 &= \omega_6 = c, \\ \omega_7 &= \omega_8 = d. \end{aligned}$$

Then, the partition function becomes $Z = \sum_{\text{states}} a^{n_1+n_2} b^{n_3+n_4} c^{n_5+n_6} d^{n_7+n_8}$. Another way to denote the Boltzmann weight of the vertex is by using the notation $w(\mu, \alpha|\beta, \nu)$, where α, β, μ, and ν are the arrow-spins with values ±1 (or simply denoted ±) of the four edges of a vertex. See Figure 1.5.

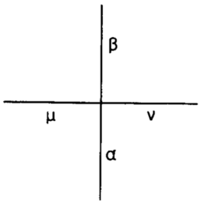


Figure 1.5: The arrow-spins α, β, μ and ν on the edges of a vertex [20, Fig. 10.2].

An arrow-spin has value +1 (resp. −1) if the corresponding arrow points right or up (resp. left or down). We obtain the Boltzmann weights

$$\begin{aligned} w(+,+|+,+) &= w(-,-|-,-) = a, \\ w(+,-|-,+) &= w(-,+|+,-) = b, \\ w(+,-|+,-) &= w(-,+|-,+) = c, \\ w(+,+|-,-) &= w(-,-|+,+) = d, \end{aligned} \tag{1.6}$$

and $w(\mu, \alpha|\beta, \nu)$ equals zero for all other values of α, β, μ and ν.

Another way to express the partition function is by using the transfer matrix V. If our lattice model has M rows and N columns, we obtain M rows of N vertical edges. A vertical edge has a thick line if its arrow points down, while a horizontal edge has a thick line if its arrow points left. This is illustrated in Figure 1.6 for the first six arrow configurations of the eight-vertex model.

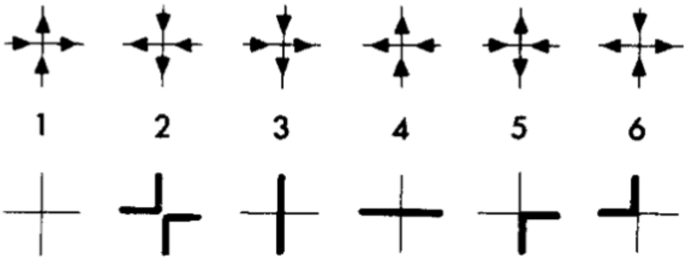


Figure 1.6: The six arrow configurations of the six-vertex model and the corresponding line configurations [20, Fig. 8.2].

By φ_r we denote the state of such a row, $r \in \{1, \dots, M\}$, and the labeling goes bottom to top, i.e. φ_i is the state of the row below the row with state φ_{i+1}. As there are N vertical edges in each row, φ_r can take 2^N possible values. The transfer matrix of this model is an $2^N \times 2^N$ matrix with elements

$$V(\varphi, \varphi') = \sum e^{-(\sum_{i=1}^{8} n_i \varepsilon_i)/kT}, \tag{1.7}$$

for two consecutive rows with state φ and φ' (with φ below φ'), or if φ is the state of the bottom row and φ' the state of the top row. Otherwise, $V(\varphi, \varphi') = 0$. The sum is taken over all possible states of thick horizontal lines between these two rows. An example of two different possibilities of thick horizontal lines is given in Figure 1.7.

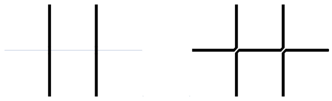


Figure 1.7: Two possible horizontal thick lines for given vertical thick lines.

The partition function of the zero-field eight-vertex model can be expressed by the transfer matrix, as

$$Z = \sum_{\varphi_1} \cdots \sum_{\varphi_M} V(\varphi_1, \varphi_2) \dots V(\varphi_{M-1}, \varphi_M) V(\varphi_M, \varphi_1) = \mathrm{Trace}(V^M).$$

For an eigenvalue λ of V and a corresponding eigenvector $\vec{x}$, we get $\lambda\vec{x} = V\vec{x}$. For M large, we obtain $Z \sim \lambda_{\max}^M$, where $\lambda_{\max}$ is the maximal eigenvalue of V. So, to find the partition function and to solve the model, we need to determine the eigenvalues of the transfer matrix V. For the six-vertex model, these eigenvalues are found using $\lambda\vec{x} = V\vec{x}$ and using the Bethe ansatz to find the form of the eigenvectors. This method builds upon the fact that, in a six-vertex model, each row has the same number of thick lines, i.e. the same amount of vertical arrows pointed down. This, however, is no longer the case for the eight-vertex model. In [19], Baxter uses a new method, called the "commuting transfer matrices" method, inspired by the results of the Bethe ansatz, to solve the eight-vertex model.

Commuting transfer matrices

The Bethe ansatz, which is used in the six-vertex model to find the eigenvectors and eigenvalues of the transfer matrix, can no longer be used in an eight-vertex model. Therefore, Baxter found another method, the "commuting transfer matrices" method, to solve the eight-vertex model. He shows that his method is derived from the Bethe ansatz and sufficient to determine the eigenvalues. He also notices that his alternative method can be established without using the Bethe ansatz. For the interested reader, we recommend [20, Section 9]. In what follows, we only focus on the appearance of the Yang-Baxter equation.

Following the notation of [20, Section 9.6], denote $\alpha = \{\alpha_1, \dots, \alpha_N\}$, $\beta = \{\beta_1, \dots, \beta_N\}$, $\mu = \{\mu_1, \dots, \mu_N\}$ and put $\mu_{N+1} = \mu_1$ (boundary condition).

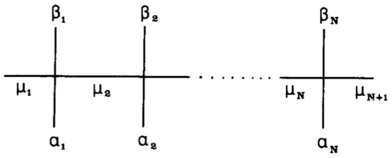


Figure 1.8: A row in the eight vertex model, where $\mu_{N+1} = \mu_1$ [20, Figure 9.1].

We can write the elements of the transfer matrix V in terms of α, β and μ instead of the notation used in (1.7), which used φ and φ' to denote the rows,

$$V_{\alpha\beta} = \sum_{\mu} w(\mu_1, \alpha_1|\beta_1, \mu_2) w(\mu_2, \alpha_2|\beta_2, \mu_3) \dots w(\mu_N, \alpha_N|\beta_N, \mu_1), \tag{1.8}$$

using the Boltzmann weights as defined in (1.6).

Let V' be another transfer matrix, i.e. the transfer matrix of another zero-field eight-vertex model, defined by

$$V'_{\alpha\beta} = \sum_{\mu} w'(\mu_1, \alpha_1|\beta_1, \mu_2) w'(\mu_2, \alpha_2|\beta_2, \mu_3) \dots w'(\mu_N, \alpha_N|\beta_N, \mu_1), \tag{1.9}$$

and

$$\begin{aligned}
w'(+,+|+,+) = w'(-,-|-,-) = a',\\
w'(+,-|-,+) = w'(-,+|+,-) = b',\\
w'(+,-|+,-) = w'(-,+|-,+) = c',\\
w'(+,+|-,-) = w'(-,-|+,+) = d'.
\end{aligned}$$

Denote $\gamma = \{\gamma_1, \dots, \gamma_N\}$ and $\mu' = \{\mu'_1, \dots, \mu'_N\}$ and put $\mu'_{N+1} = \mu'_1$. Since all elements $a, b, c, d, a', b', c', d'$ commute, then from (1.8) and (1.9),

$$\begin{aligned}
(VV')_{\alpha\beta} &= \sum_{\gamma} V_{\alpha\gamma} V'_{\gamma\beta}\\
&= \sum_{\gamma} \left(\sum_{\mu} w(\mu_1, \alpha_1|\gamma_1, \mu_2) \dots w(\mu_N, \alpha_N|\gamma_N, \mu_1) \right)\\
&\qquad \left(\sum_{\mu'} w'(\mu'_1, \gamma_1|\beta_1, \mu'_2) \dots w'(\mu'_N, \gamma_N|\beta_N, \mu'_1) \right)\\
&= \sum_{\mu} \sum_{\mu'} \prod_{i=1}^{N} \sum_{\gamma_i} w(\mu_i, \alpha_i|\gamma_i, \mu_{i+1}) w'(\mu'_i, \gamma_i|\beta_i, \mu'_{i+1}).
\end{aligned} \tag{1.10}$$

Define for each $i \in \{1, \dots, N\}$, a 4×4 matrix $S(\alpha_i, \beta_i)$ where the rows are labeled by (μ_i, μ'_i), the columns labeled by (μ_{i+1}, μ'_{i+1}), and with elements

$$S(\alpha_i, \beta_i)_{((\mu_{i+1}, \mu'_{i+1}), (\mu_i, \mu'_i))} = \sum_{\gamma_i} w(\mu_i, \alpha_i|\gamma_i, \mu_{i+1}) w'(\mu'_i, \gamma_i|\beta_i, \mu'_{i+1}).$$

Then, (1.10) can be rewritten as

$$(VV')_{\alpha\beta} = \mathrm{Trace}(S(\alpha_1, \beta_1) \dots S(\alpha_N, \beta_N)). \tag{1.11}$$

Similarly,

$$(V'V)_{\alpha\beta} = \mathrm{Trace}(S'(\alpha_1, \beta_1) \dots S'(\alpha_N, \beta_N)), \tag{1.12}$$

where S' is defined the same way as S, and

$$S'(\alpha_i,\beta_i)_{((\mu_{i+1},\mu'_{i+1}),(\mu_i,\mu'_i))} = \sum_{\gamma_i} w'(\mu_i,\alpha_i|\gamma_i,\mu_{i+1})w(\mu'_i,\gamma_i|\beta_i,\mu'_{i+1}).$$

It is clear by the right hand sides of (1.11) and (1.12) that the transfer matrices V and V' commute if there exists a 4×4 invertible matrix A for which

$$S(\alpha_i,\beta_i) = AS'(\alpha_i,\beta_i)A^{-1}, \tag{1.13}$$

for all $i \in \{1,\dots,N\}$. Denote the element in row (μ_i,μ'_i) and column (ν_i,ν'_i) of the matrix A by $w''(\mu'_i,\mu_i|\nu'_i,\nu_i)$. Then, (1.13) is equivalent to, for every row (μ_i,μ'_i) and column (μ_{i+1},μ'_{i+1}),

$$\begin{aligned}&\sum_{\gamma_i}\sum_{\nu_i,\nu'_i} w(\mu_i,\alpha_i|\gamma_i,\nu_i)w'(\mu'_i,\gamma_i|\beta_i,\nu'_i)w''(\nu'_i,\nu_i|\mu'_{i+1},\mu_{i+1})\\ &= \sum_{\gamma_i}\sum_{\nu_i,\nu'_i} w''(\mu'_i,\mu_i|\nu'_i,\nu_i)w'(\nu_i,\alpha_i|\gamma_i,\mu_{i+1})w(\nu'_i,\gamma_i|\beta_i,\mu'_{i+1}).\end{aligned} \tag{1.14}$$

This relation has a graphical interpretation as in Figure 1.9, which is accordingly called the star-triangle relation [149]. So the sum over the possible spins γ_i,ν_i,ν'_i of the weights of the left hand trilateral are equal to that of the right hand trilateral. Note the similarities with (1.4) and Fig. 1.2.

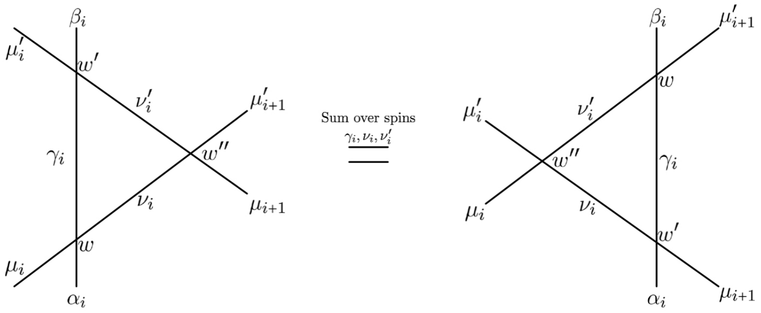


Figure 1.9: A graphical interpretation of equation 1.14.

If we define S_i as the matrix with elements

$$(S_i)_{\alpha\beta} = S(\alpha_1,\beta_1)\dots S(\alpha_{i-1},\beta_{i-1})w(\alpha_i,\alpha_{i+1}|\beta_i,\beta_{i+1})S(\alpha_{i+1},\beta_{i+1})\dots S(\alpha_N,\beta_N),$$

and similarly, define S'_i and S''_i by replacing w by w' and w'' respectively, then according to [20, Section 9.6], equation (1.14) implies $S_{i+1}S'_iS''_{i+1} = S''_iS'_{i+1}S_i$, and $S_iS'_j = S'_jS_i$ if $|i-j|\geq 2$. It is said that the operators S_i satisfy the star-triangle property. One can see a hint of the Yang-Baxter equation in the star-triangle property by looking at the indices of the operators. Therefore, in literature, the Yang-Baxter equation is also sometimes called the star-triangle relation. So, in this way, the Yang-Baxter equation plays a role in Baxter's method to solve the eight-vertex model.

Star-triangle relation

The star-triangle relation became famous after the discovery that it relates the Ising model on a triangular lattice with the same model on a honeycomb lattice [149]. In this context, $W_{ab}(p,q)$ and $\bar{W}_{ab}(p,q)$ denote the Boltzmann weights associated to the vertices shown in Figure 1.10.

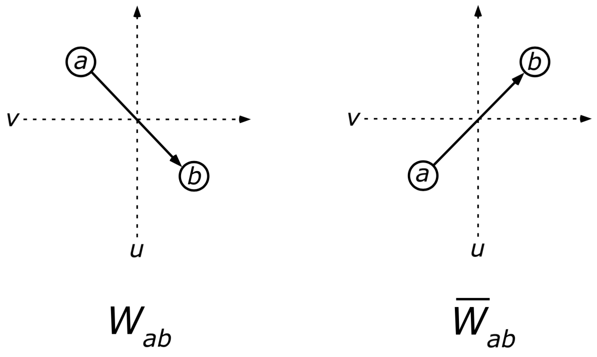


Figure 1.10: The Boltzmann weights of the spin model [150].

With this notation, the star-triangle relation states

$$\sum_d \bar{W}_{cd}(p,q)\bar{W}_{db}(q,r)W_{da}(p,r) = R(p,q,r)W_{ba}(p,q)W_{ca}(q,r)\bar{W}_{cb}(p,r),$$

where the sum is taken over all spins d and $R(p,q,r)$ is a scalar factor depending on the variables p,q,r called rapidities [150]. This relation is illustrated in Figure 1.11, which explains its name-giving. More detailed information can be found in, for example, [20, Sections 6.3 and 6.4].

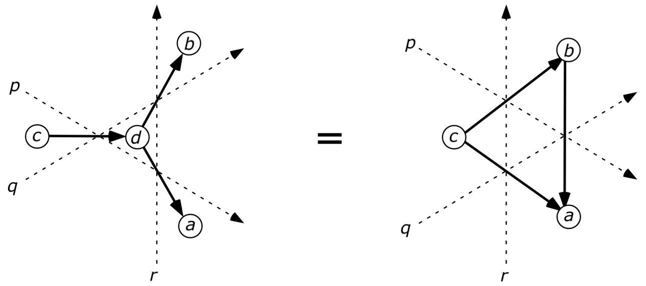


Figure 1.11: Star-triangle relation [150].

As an application, using the methods derived in solving the zero-field eight-vertex model, Baxter solves the hard hexagon model [20, Chapter 14]. This model consists of a two-dimensional triangular lattice where no two particles are adjacent or at the same place. By coloring the six adjacent surfaces, none of the colored hexagons overlap, i.e.

it is a gas of hard or non-overlapping molecules. In order to solve the model, Baxter generalizes the model to the hard-square model with diagonal interaction. He solves this model using the star-triangle relation.

1.2 Other applications

1.2.1 Knot theory

Knot theory studies when two links are equivalent, where a link is a finite union of pairwise disjoint knots, i.e. closed ropes. Two knots (or links) are said to be equivalent if their diagrams are equivalent, where the associated diagram is its two-dimensional projection with knowledge of which line is above the other in each intersection. Furthermore, two diagrams are equivalent if it is possible to go from one diagram to the other via finite, well-known, Reidemeister moves [157]. In particular, the Yang-Baxter equation matches with the third Reidemeister move, see for example Figure 1.12.

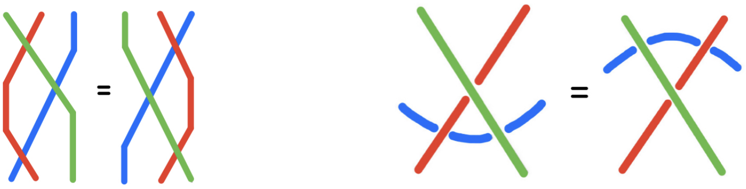


Figure 1.12: On the left a graphical interpretation of the Yang-Baxter equation (1.1), where a crossing means that R is applied, and on the right the third Reidemeister move. The colors indicate the lines that agree.

Since checking all possible sequences of the Reidemeister moves to prove that two diagrams are equivalent is impossible, another strategy is used via link invariants. A link invariant is a map, say ϕ, that maps the set of links (resp. their diagrams) to another set, such that ϕ is constant on equivalence classes of links (resp. invariant under the Reidemeister moves).

The Yang-Baxter equation is sometimes also called the braid relation as it relates to Artin's definition of the braid group [5]. The n-strand braid group is defined as

$$B_n = \mathrm{gr}(\sigma_1, \dots, \sigma_{n-1} \mid \sigma_i\sigma_j = \sigma_j\sigma_i \text{ for } |i-j| \geq 2,\ \sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}),$$

where each σ_i denotes the interchangement of two consecutive braids (the i-th and $(i+1)$-th braid). The left equality of braidings in Figure 1.12 reads as $\sigma_1\sigma_2\sigma_1 = \sigma_2\sigma_1\sigma_2$. In particular, the Yang-Baxter equation can be used to describe braids and their representations. Given a bijective solution $R \in \mathrm{Aut}(V \otimes V)$, $\rho_R : B_n \to \mathrm{Aut}(V^{\otimes n}) : \sigma_i \mapsto \mathrm{id}_V^{i-1} \otimes R \otimes \mathrm{id}_V^{n-i-1}$ is a representation of the braid group B_n. These representations can be used to construct link invariants. For more information on links, braids, and the Yang-Baxter equation, see for example [137, 186]. In [109, 179], it is shown that solutions to the Yang-Baxter equation $R : V \otimes V \to V \otimes V$, satisfying $R^2 = aR + b$, with a and

b scalars, give polynomial invariants of oriented links. These include involutive solutions, i.e. where $R^2 = \mathrm{id}_{V\otimes V}$, and idempotent solutions, i.e. where $R^2 = R$. In [110], certain statistical mechanics models are used to construct link invariants. The Yang-Baxter equation or star-triangle relations plays a prominent role in these studies [183].

An interesting link invariant is that of tricoloring. A diagram of a link is tricolored if we can color it using three colors such that at every crossing there is either one color, or all three colors. For this, we consider three edges at each crossing: the line on top of the crossing and two lines that coincide under the crossing (but can have a different color). See for example Figure 1.13.

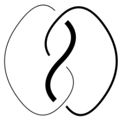


Figure 1.13: An example of a tricoloring where each thickness of the line indicates its color [156].

In Figure 1.13, the three lines either all have the same color or they all have a different color. Tricoloring, i.e. $\phi(D)$ is equal to the number of tricolorings of a diagram D, is a link invariant because the number of different tricolorings is preserved under the Reidemeister moves. Mathematically, we can denote the tricoloring via the introduction of a binary operation $\triangleleft$ on the set $X = \mathbb{Z}/3\mathbb{Z}$, by $x \triangleleft y = 2x - y$, for all $x, y \in X$, where $\mathbb{Z}$ denotes the set of all integers. The pair $(X, \triangleleft)$ satisfies

- For any $x \in X$, $x \triangleleft x = x$,
- For any $x \in X$, the map $y \mapsto y \triangleleft x$ is bijective, with inverse given by $\overline{\triangleleft}$,
- For any $x, y, z \in X$, $(x \triangleleft y) \triangleleft z = (x \triangleleft z) \triangleleft (y \triangleleft z)$.

A pair $(X, \triangleleft)$ satisfying the above three conditions is called a quandle [78, 112]. Using this $\triangleleft$-map, the coloring given in Figure 1.14 is a tricoloring. For more information on quandle colorings and knots, see for example [56]. The invariance under the third Reidemeister move is satisfied because of the third condition of a quandle. Note that this third condition is also equivalent with $r : X \times X \to X \times X : (x, y) \mapsto (y, x \triangleleft y)$ being a set-theoretic solution of the Yang-Baxter equation, i.e. a solution defined on sets instead of vector spaces (see Section 1.3). The map r satisfies $r_1 r_2 r_1 = r_2 r_1 r_2$, where $r_1 = r \times \mathrm{id}_X$ and $r_2 = \mathrm{id}_X \times r$.

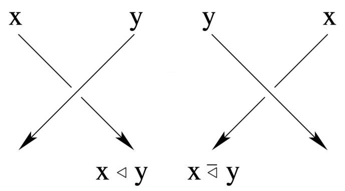


Figure 1.14: A tricoloring given by a quandle [56, Figure 1].

1.2.2 Quantum computation

In this part, we discuss the application of the Yang-Baxter equation in quantum computation. We follow [190], and recommend this book for the interested reader who wants more information on the topic.

Similar to classical mechanics, there is a quantum version of classical computation. In classical computing, information is stored in bits, denoted by 0 (off/false) and 1 (on/true). On the other hand, in quantum computing data is represented by quantum bits, also called qubits, and denoted by $|0\rangle$ and $|1\rangle$. A qubit, in comparison with a bit, can be true and false at the same time, which is called superposition. A qubit state is a superposition of the basis states $|0\rangle$ and $|1\rangle$, i.e. it is a linear combination $|\psi\rangle = c_1 |0\rangle + c_2 |1\rangle$, where c_1 and c_2 are complex numbers related to the probability outcome of the basis states. The qubit state does not have a value between 0 and 1, but rather a probability $|c_1|^2$ of value 0 and $|c_2|^2$ of value 1, with $|c_1|^2 + |c_2|^2 = 1$.

Qubit states have a matrix representation in the following sense,

$$|0\rangle \leftrightarrow \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle \leftrightarrow \begin{pmatrix} 0 \\ 1 \end{pmatrix},$$

and

$$|\psi\rangle = c_1 |0\rangle + c_2 |1\rangle \leftrightarrow c_1 \begin{pmatrix} 1 \\ 0 \end{pmatrix} + c_2 \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} c_1 \\ c_2 \end{pmatrix}.$$

In quantum computation, a computation is performed by assembling a series of quantum gates. Resembling classical logic gates, like AND, OR, XOR, etc., a quantum (logic) gate is an operator between qubit states that has to be reversible or even unitary. Note that reversibility is not always true for classical logic gates. A set of quantum gates is said to be universal if they generate all quantum gates, i.e. they can be used as the building blocks.

A quantum gate also has a matrix representation. So applying a quantum gate on a qubit state can be seen as a multiplication of matrices. Take, for example, the Pauli-X operator σ_X, with matrix representation

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Applying this operator on the qubit state $|0\rangle$, denoted $\sigma_x |0\rangle$, gives the qubit state $|1\rangle$. Indeed, we have

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

Let V be a two-dimensional vector space with basis qubit states $|0\rangle$ and $|1\rangle$. Then, $V \otimes V$ has basis qubit states $|0\rangle \otimes |0\rangle, |0\rangle \otimes |1\rangle, |1\rangle \otimes |0\rangle$, and $|1\rangle \otimes |1\rangle$. They are denoted by respectively

$$|00\rangle, |01\rangle, |10\rangle, |11\rangle,$$

and are respectively expressed by the matrix columns

$$\begin{pmatrix}1\\0\\0\\0\end{pmatrix}, \begin{pmatrix}0\\1\\0\\0\end{pmatrix}, \begin{pmatrix}0\\0\\1\\0\end{pmatrix}, \begin{pmatrix}0\\0\\0\\1\end{pmatrix}.$$

Consequently, a quantum gate or unitary operator U on $V \otimes V$ can be expressed as a 4×4 matrix.

By using its action on the basis qubit states of $V \otimes V$, a solution R of the Yang-Baxter equation has a matrix representation

$$\mathbf{R} = \begin{pmatrix} R_{00}^{00} & R_{01}^{00} & R_{10}^{00} & R_{11}^{00} \\ R_{00}^{01} & R_{01}^{01} & R_{10}^{01} & R_{11}^{01} \\ R_{00}^{10} & R_{01}^{10} & R_{10}^{10} & R_{11}^{10} \\ R_{00}^{11} & R_{01}^{11} & R_{10}^{11} & R_{11}^{11} \end{pmatrix},$$

where $R|xy\rangle = \sum_{a,b\in\{0,1\}} R_{xy}^{ab} |ab\rangle$, for $x, y \in \{0,1\}$.

In [113], it is shown that several unitary solutions to the Yang-Baxter equation, i.e. solutions where $R_{21}R_{12} = \mathrm{id}_{V\otimes V}$, together with local unitary two-dimensional operators form a universal set of quantum gates. So, unitary solutions to the Yang-Baxter equation on a two-dimensional complex vector space V, or unitary 4×4 R-matrices are of enormous importance in quantum computation. In [73], all unitary 4×4 matrices that are R-matrices and also quantum operators are classified. Unitary solutions are also studied in [90].

1.2.3 Factorizable S-matrices

High energy particle physics and connected subfields of physics are concerned with the scattering of particles. In certain models, small particles interact when colliding. These interactions can transform the particles into other types of particles. This process is called scattering and the probabilities of different outcomes are all contained in the so-called S-matrix or scattering matrix. The S-matrix can also be seen as an operator that maps the initial quantum state of the particles to the quantum state of the particles after scattering. The goal is to find the S-matrix of different types of models in physics.

In an attempt to find the S-matrix of some many-body quantum systems, it was discovered that the S-matrix can be factorized into S-matrices of two-body quantum systems [21, 140, 185]. So roughly said the transformation of interacting particles comes down to how two particles interact, assuming the other particles are at a distance so that they do not influence the two interacting particles. This simplifies the construction of the S-matrix of the total quantum system, one only needs to calculate the two-body S-matrices explicitly.

There are some necessary conditions to be able to factorize an S-matrix, called factorization equations [189]. The factorization of the S-matrix of a three-body quantum system can be done in two ways, which should not differ from each other. Following

[189, Fig. 2], one way the S-matrix of a three-body model with particles P_1, P_2 and P_3, denoted S_{123}, can be factorized, is by consecutively looking at the interaction between the particles P_1 and P_2, then between P_1 and P_3, and finally between P_2 and P_3. The other way is to first look at the interaction between particles P_2 and P_3, then between P_1 and P_3, and finally P_1 and P_2. Denoting the corresponding two-body S-matrix by S_{ij} for the particles P_i and P_j, we obtain

$$S_{123} = S_{12}S_{13}S_{23} = S_{23}S_{13}S_{12},$$

which corresponds to the quantum Yang-Baxter equation (1.2). This equation also needs to be satisfied for the factorization of S-matrices associated to quantum systems with more particles. So the Yang-Baxter equation (or its quantum version) again pops out as a condition that needs to be satisfied to determine the S-matrix and solve problems in many parts of physics.

1.2.4 Quantum groups

The Yang-Baxter equation appears in the theory of Hopf algebras. A Hopf algebra $\mathcal{A}$ with basis $\{e_i\}$, $i = 1, 2, \dots$, is called quasi-triangular [71], if there exists an invertible element $\mathcal{R} \in \mathcal{A} \otimes \mathcal{A}$, called the universal R-matrix, satisfying among other things $\mathcal{R}\Delta(a) = \tau\Delta(a)\mathcal{R}$, for any $a \in A$, where τ is the twist map, i.e. $\tau(x \otimes y) = y \otimes x$. The R-matrix of any quasi-triangular Hopf algebra satisfies the quantum Yang-Baxter equation (1.2), or equivalently $\tau\mathcal{R}$ is a solution of the Yang-Baxter equation (1.1).

Examples of Hopf algebras are given by the enveloping algebra of Lie algebras. As these algebras are still cocommutative, they only give trivial solutions of the Yang-Baxter equation. Motivated by the work of Jimbo [107, 108], Drinfeld constructed Hopf algebras, via quantum enveloping algebras (i.e. deformations of enveloping algebras) of Lie algebras, that are no longer cocommutative, via a Drinfeld double. These are examples of quantum groups. So, quantum groups are non commutative non cocommutative Hopf algebras, and they produce highly non-trivial solutions of the quantum Yang-Baxter equation. For more information on the topic, see for example [71, 143].

1.3 Drinfeld's problem and set-theoretic solutions

The importance of the Yang-Baxter equation is clear from Section 1.1 and Section 1.2. The impossibly difficult problem is to classify all solutions (on vector spaces) of the Yang-Baxter equation. With regard to this problem, Drinfeld [72] urged to focus on the so-called set-theoretic solutions of the Yang-Baxter equation, as they form solutions on vector spaces by linearly extending them. For a non-empty set X and a map $r : X \times X \to X \times X$, the pair (X, r) is called a *set-theoretic solution of the Yang-Baxter equation* if, in $\mathrm{Map}(X^3, X^3)$,

$$r_{12}r_{23}r_{12} = r_{23}r_{12}r_{23}, \tag{1.15}$$

where $r_{12} = r \times \mathrm{id}_X$ and $r_{23} = \mathrm{id}_X \times r$. We shall write

$$r(x, y) = (\lambda_x(y), \rho_y(x)), \tag{1.16}$$

for $x, y \in X$, and briefly call a set-theoretic solution of the Yang-Baxter equation a *solution of the Yang-Baxter equation* or a *solution.*

In general, (X, r) is a set-theoretic solution of the Yang-Baxter equation (1.15) if and only if

$$\begin{aligned} r_{12}r_{23}r_{12}(x,y,z) &= r_{12}r_{23}(\lambda_x(y), \rho_y(x), z) \\ &= r_{12}(\lambda_x(y), \lambda_{\rho_y(x)}(z), \rho_z(\rho_y(x))) \\ &= (\lambda_{\lambda_x(y)}(\lambda_{\rho_y(x)}(z)), \rho_{\lambda_{\rho_y(x)}(z)}(\lambda_x(y)), \rho_z(\rho_y(x))), \end{aligned}$$

equals

$$\begin{aligned} r_{23}r_{12}r_{23}(x,y,z) &= r_{23}r_{12}(x, \lambda_y(z), \rho_z(y)) \\ &= r_{23}(\lambda_x(\lambda_y(z)), \rho_{\lambda_y(z)}(x), \rho_z(y)) \\ &= (\lambda_x(\lambda_y(z)), \lambda_{\rho_{\lambda_y(z)}(x)}(\rho_z(y)), \rho_{\rho_z(y)}(\rho_{\lambda_y(z)}(x))), \end{aligned}$$

or equivalently, the following conditions need to be satisfied,

$$\lambda_{\lambda_x(y)}(\lambda_{\rho_y(x)}(z)) = \lambda_x(\lambda_y(z)), \tag{1.17}$$

$$\rho_{\lambda_{\rho_y(x)}(z)}(\lambda_x(y)) = \lambda_{\rho_{\lambda_y(z)}(x)}(\rho_z(y)), \tag{1.18}$$

$$\rho_z(\rho_y(x)) = \rho_{\rho_z(y)}(\rho_{\lambda_y(z)}(x)), \tag{1.19}$$

for all $x, y, z \in X$.

A solution of the Yang-Baxter equation (X, r) is said to be *involutive* if $r^2 = \mathrm{id}_{X^2}$. It is called *bijective* if the map r is bijective. In particular, involutive solutions of the Yang-Baxter equation are bijective. A solution is said to be *left* (resp. *right*) *non-degenerate* if the map λ_x (resp. ρ_x) is bijective, for any $x \in X$. A left and right non-degenerate solution of the Yang-Baxter equation is simply called *non-degenerate*. If a solution is not left nor right non-degenerate, then it is said to be a *degenerate* solution. A solution is called *idempotent* if $r^2 = r$ and *cubic* if $r^3 = r$. Furthermore, a solution (X, r) is called *square-free* if $r(x, x) = (x, x)$, for all $x \in X$. Finally, we say that a solution (X, r) is *finite* if the set X is finite.

For any bijective set-theoretic solution (X, r), with $r(x, y) = (\lambda_x(y), \rho_y(x))$, its inverse (X, r^{-1}) is also a (bijective) set-theoretic solution of the Yang-Baxter equation. We denote, for any $x, y \in X$,

$$r^{-1}(x,y) = (\hat{\lambda}_x(y), \hat{\rho}_y(x)). \tag{1.20}$$

In case X is a group with multiplication of $x, y \in X$ denoted by xy, and $\lambda : X \to \mathrm{Sym}(X) : x \mapsto \lambda_x$ is a group homomorphism and $\rho : X \to \mathrm{Sym}(X) : x \mapsto \rho_x$ is a group anti-homomorphism satisfying $xy = \lambda_x(y)\rho_y(x)$, for all $x, y \in X$, then an exact description of r^{-1} is given in the proof of [135, Theorem 1]. Namely, $r^{-1}(x, y) = ((\rho_{x^{-1}}(y^{-1}))^{-1}, (\lambda_{y^{-1}}(x^{-1}))^{-1})$, for all $x, y \in X$, where x^{-1} denotes the inverse of x in the group X. Note that in this case, the map $\hat{\lambda} : X \to \mathrm{Sym}(X) : x \to \hat{\lambda}_x$ defined by

$\hat{\lambda}_x(y) = (\rho_{x^{-1}}(y^{-1}))^{-1}$ is a group homomorphism, and the map $\hat{\rho} : X \to \mathrm{Sym}(X) : x \to \hat{\rho}_x$ defined by $\hat{\rho}_x(y) = (\lambda_{x^{-1}}(y^{-1}))^{-1}$ is a group anti-homomorphism.

A *homomorphism* between two set-theoretic solutions (X, r_X) and (Y, r_Y) is a map $f : X \to Y$ (sometimes also denoted $f : (X, r_X) \to (Y, r_Y)$) that satisfies $(f \times f)r_X = r_Y(f \times f)$. If f is injective, then (X, r_X) can be embedded in (Y, r_Y), and f is called a *monomorphism* of solutions. If f is surjective, then (Y, r_Y) is called an *epimorphic image* of (X, r_X), and f is said to be an *epimorphism* of solutions. If f is bijective, then the solutions are called *isomorphic*. If $Y \subseteq X$, $r_X(Y \times Y) \subseteq (Y \times Y)$, and $r_Y = r_X|_{Y \times Y}$, then (Y, r_Y) is called a *subsolution* of (X, r_X).

To find all set-theoretic solutions of the Yang-Baxter equation (1.15), the idea is to construct solutions using known algebraic structures or to define new algebraic structures that provide (all) solutions of a certain type. Some known examples are solutions defined on a non-empty set X, by putting for all $x, y \in X$,

$$\begin{aligned} &r(x,y) = (x,y), \qquad && r(x,y) = (c,x), \qquad && r(x,y) = (y,c), \\ &r(x,y) = (x,c), && r(x,y) = (c,y), && r(x,y) = (c,c), \end{aligned}$$

for a fixed element $c \in X$. The solution (X, r), with $r(x,y) = (y,x)$, for all $x, y \in X$, is called the *trivial solution* on the set X. Given mappings $f, g : X \to X$, we obtain solutions with $r(x,y) = (f(y), g(x))$ (resp. $r(x,y) = (f(x), f(y))$ if and only if $fg = gf$ (resp. $f^2 = f$). The solution defined by $r(x,y) = (f(y), g(x))$ is called a *Lyubashenko solution*, or a *solution of Lyubashenko type* [72]. Given a monoid M with identity element 1, we obtain solutions by putting $r(a,b) = (ab, 1)$ or $r(a,b) = (1, ab)$ for all $a, b \in M$. Finally, given a band S, i.e. a semigroup with $xx = x$, for all $x \in S$, then $r(x,y) = (xy, y)$ and $r(x,y) = (x, xy)$ define set-theoretic solutions of the Yang-Baxter equation.

Many other algebraic structures have been connected to the Yang-Baxter equation in order to find and classify its set-theoretic solutions. Some of them were known long before being connected to the Yang-Baxter equation, while others were introduced for this purpose. In the remaining of this chapter, we give an overview of several algebraic structures and examine how they provide solutions. In particular we consider cycle sets [161, 166], braces [37, 40, 42, 49, 92, 105, 142, 163, 166], quandles [78, 112] (see also [62, Section 3.1] and references therein), and some of their generalizations. This section aims to give a brief overview with many references for the interested reader.

1.3.1 Braces and its generalizations

In [163], Rump introduces braces as a tool to classify all non-degenerate involutive set-theoretic solutions of the Yang-Baxter equation. Later in [49], an equivalent definition of a left brace was given by Cedó, Jespers, and Okniński, which was generalized to the definition of a skew left brace by Guarnieri and Vendramin [92]. For a survey on braces, we refer to [43, 181].

Definition 1.3.1. *A* skew (left) brace *is a set B with two binary operations denoted by $+$ and $\circ$ such that both $(B, +)$ and $(B, \circ)$ are groups, and the brace relation*

$$a \circ (b + c) = (a \circ b) - a + (a \circ c), \tag{1.21}$$

is satisfied, for any $a, b, c \in B$. It is denoted by $(B, +, \circ)$ and $(B, +)$ (resp. $(B, \circ)$) is called its additive (resp. multiplicative) group. The inverse of a in $(B, +)$ is naturally denoted by $-a$, while its inverse in $(B, \circ)$ is denoted by $\overline{a}$. If the additive group $(B, +)$ is abelian, then $(B, +, \circ)$ is called a (left) brace*.*

There is also a notion of a right brace (see for example [49]), where (1.21) is replaced by $(a + b) \circ c = (a \circ c) - c + (b \circ c)$. There is a bijective correspondence between left and right braces, hence it is not important which one is considered. Unless specifically mentioned, we only use left braces in what follows. Note that the identity element of $(B, +)$ and $(B, \circ)$ of a (skew) left brace $(B, +, \circ)$ coincide (see for example [92, Lemma 1.7]).

The inspiration for the introduction of braces comes from Jacobson radical rings. In [163], it is shown that two-sided braces $(B, +, \circ)$, i.e. left braces that are also right braces, correspond to Jacobson radical rings $(B, +, \cdot)$, by putting $a \cdot b = -a + (a \circ b) - b$, where $\cdot$ denotes the product of the ring. Furthermore, skew braces arise from special near-rings [167]. As a consequence, many terms and theorems from group and ring theory have been translated to (skew) brace theory, see for example [1, 44, 55, 99, 100, 118, 123, 124, 162, 164, 173].

Given a (skew) left brace $(B, +, \circ)$, the map $\lambda : (B, \circ) \to \mathrm{Aut}(B, +) : a \mapsto \lambda_a$ with $\lambda_a(b) = a \circ (\overline{a} + b) = -a + (a \circ b)$ is a group homomorphism and the map $\rho : (B, \circ) \to \mathrm{Sym}(B) : a \mapsto \rho_a$ with $\rho_a(b) = \overline{(\overline{b} + a)} \circ a$ is a group anti-homomorphism. Note that, for any $a, b \in B$, $a \circ b = \lambda_a(b) \circ \rho_b(a)$. With this notation, the pair (B, r_B) with $r_B : B \times B \to B \times B : (a, b) \mapsto (\lambda_a(b), \rho_b(a))$ is a non-degenerate bijective set-theoretic solution of the Yang-Baxter equation, for any skew brace $(B, +, \circ)$ [92]. Given a brace, the solution is also involutive [163, 49]. In fact, there is more. In [49], it is shown that given a brace $(B, +, \circ)$, there exists a non-degenerate involutive set-theoretic solution of the Yang-Baxter equation (X, r) with r denoted by $r(x, y) = (\lambda_x(y), \rho_y(x))$ such that the group generated by the λ-maps, $\mathcal{G}(X, r) = \mathrm{gr}(\lambda_x \mid x \in X)$, is isomorphic to the multiplicative group of the left brace B. In [9], an explicit construction is provided to, given a left brace $(B, +, \circ)$, construct all non-degenerate involutive set-theoretic solutions (X, r) such that $\mathcal{G}(X, r)$ and $(B, +, \circ)$ are isomorphic as braces. This means firstly that one can find an addition on $\mathcal{G}(X, r)$ such that it has a left brace structure, and secondly that this left brace is isomorphic to $(B, +, \circ)$ in the sense that there exists a bijective map $f : \mathcal{G}(X, r) \to B$ that is a homomorphism for both operations $+$ and $\circ$. So, the classification of all non-degenerate involutive set-theoretic solutions of the Yang-Baxter equation can be reduced to classifying all left braces. To read more on this topic, we refer to [43] or to the master's thesis [181]. In a similar fashion, skew left braces are used to study non-degenerate bijective solutions [8].

An *ideal* of a skew left brace $(B, +, \circ)$ is a normal subgroup I of $(B, \circ)$ such that $I + a = a + I$, and $\lambda_a(I) \subseteq I$, for all $a \in B$, first defined in [92] (and in [49] for braces). Ideals of skew left braces are precisely the kernels of skew left brace homomorphisms (see [105]). In [55] (see also [173] and [6, Proposition 1.1.12]), the *socle* of a skew left brace $(B,+,\circ)$ is defined as

$$\operatorname{Soc}(B) = \{a \in B \mid a \circ b = a + b = b + a, \text{ for all } b \in B\} = Z(B,+) \cap \operatorname{Ker}(\lambda),$$

the intersection of the center of the additive group of B and the kernel of its λ-map. Since $\lambda_a(b) = -a + a \circ b$ and $\rho_a(b) = \overline{(\overline{b} + a)} \circ a$, for $a, b \in B$, it follows that

$$\operatorname{Soc}(B) = \{a \in B \mid \lambda_a = \mathrm{id}_B \text{ and } \rho_a = \mathrm{id}_B\}.$$

The socle $\operatorname{Soc}(B)$ is an ideal of the skew left brace $(B,+,\circ)$, and both its additive and multiplicative groups are abelian (see for example [92]). In particular it is a left brace.

To find all (finite) left braces, a two-step method is used. First, one needs to find and classify the building blocks, called simple braces, i.e. braces that have no non-trivial ideals. After that, there is a need for ways to construct new braces given two or more (simple) left braces. Also, extensions and the study of homology and cohomology of left braces can be used for this purpose. Plenty in this area has been done in [7, 11, 12, 50, 51, 123, 124]. In [180], the number of non-isomorphic (skew) left braces is given up to size 133 (with several numbers missing in between).

Semi-braces and other generalizations

A *(left) semi-brace* is introduced in [105] as a set B with with two operations $+$ and $\circ$ such that $(B,+)$ is a semigroup, $(B,\circ)$ is a group, and for any $a, b, c \in B$,

$$a \circ (b + c) = (a \circ b) + a \circ (\overline{a} + c), \tag{1.22}$$

assuming that $\circ$ has higher precedence than $+$. If $(B,+)$ is a left cancellative semigroup, i.e. $a + b = a + c$ implies $b = c$, for all $a, b, c \in B$, then the left semi-brace is called a *left cancellative (left) semi-brace*, introduced in [37], and later generalized to several other structures (see for example [40, 41, 42, 142]). Left braces and skew left braces are examples of (left cancellative) left semi-braces. Similarly as for (skew) left braces, one can define the λ-map of a left semi-brace as $\lambda : (B,\circ) \to \operatorname{End}(B,+) : a \mapsto \lambda_a$ with $\lambda_a(b) = a \circ (\overline{a} + b)$, which is a homomorphism. For a left cancellative left semi-brace $(B,+,\circ)$, we obtain $\lambda_a \in \operatorname{Aut}(B,+)$, for any $a \in B$. The ρ-map associated to a left semi-brace $(B,+,\circ)$ is defined as $\rho : (B,\circ) \to \operatorname{Map}(B,B) : a \mapsto \rho_a$ with $\rho_a(b) = \overline{(\overline{b} + a)} \circ a$. If $(B,+)$ is left cancellative, then ρ is an anti-homomorphism. If for a given semi-brace the ρ-map is an anti-homomorphism, then (B, r_B), where r_B is defined identical to the (skew) brace case, is a set-theoretic solution of the Yang-Baxter equation. Note that this solution can be degenerate. For left cancellative left semi-braces, the associated solution is left non-degenerate (as $\lambda_a \in \operatorname{Aut}(B,+)$, for any $a \in B$).

Recently, in [169], Rump introduced an algebraic structure called a *strong semi-brace* to deal with involutive solutions that are not necessarily non-degenerate. It is defined as a monoid $(A,\circ)$ with neutral element 0 and an additional binary operation $\cdot$ such that, for any $a, b, c \in A$,

$$\begin{aligned} &(a \circ b) \cdot c = a \cdot (b \cdot c), & 0 \cdot a = a, \\ &a \cdot (b \circ c) = ((c \cdot a) \cdot b) \circ (a \cdot c), & a \cdot 0 = 0, \\ &(a \cdot b) \circ a = (b \cdot a) \circ b. & \end{aligned}$$

If in addition to being a strong semi-brace $(A, \circ, \cdot)$, for any $a \in A$, the left multiplication map $\ell_a : A \to A : b \mapsto a \cdot b$ is bijective, then $(A, \cdot)$ is a cycle set (see Subsection 1.3.2) with associated left non-degenerate involutive solution $r(a, b) = (\ell_a^{-1}(b), \ell_{\ell_a^{-1}(b)}(a))$.

1.3.2 Cycle sets and its generalizations

In [161], a *cycle set* is introduced as a set X with a binary operation $\cdot : X \times X \to X$ such that the map $\ell_x : X \to X : y \mapsto x \cdot y$ is bijective, for all $x \in X$, and

$$(x \cdot y) \cdot (x \cdot z) = (y \cdot x) \cdot (y \cdot z), \tag{1.23}$$

holds, for all $x, y, z \in X$. It is shown that there is a bijective correspondence between cycle sets and right non-degenerate involutive solutions by defining $r(x, y) = (\ell_y^{-1}(x) \cdot y, \ell_y^{-1}(x))$ given a cycle set $(X, \cdot)$, and conversely by defining $\ell_x(\rho_x(y)) = y$ given a right non-degenerate involutive solution defined by $r(x, y) = (\lambda_x(y), \rho_y(x))$. Note that this also implies a bijective correspondence between cycle sets and left non-degenerate involutive solutions by defining $r(x, y) = (\ell_x^{-1}(y), \ell_x^{-1}(y) \cdot x)$; and by defining $x \cdot y = \lambda_x^{-1}(y)$ given a left non-degenerate involutive solution defined by $r(x, y) = (\lambda_x(y), \rho_y(x))$. Under this correspondence, non-degenerate involutive set-theoretic solutions are equivalent to cycle sets $(X, \cdot)$ with $x \mapsto x \cdot x$ bijective. Cycle sets are studied in [30, 31, 32, 35, 70, 161, 162, 168]. In [163], a bijective correspondence is proven between right braces and linear cycle sets, i.e. cycle sets with an additional operation $+$ that makes $(X, +)$ into an abelian group and satisfying several relations between both operations. With the machinery of cycle sets it is shown, in [161, Theorem 2] (and independently in [101, Corollary 2.3] using monoids of I-type), that any finite left non-degenerate involutive set-theoretic solution of the Yang-Baxter equation is also right non-degenerate.

In [166], a "non-commutative" or "q-version" of a cycle set is introduced as a *q-cycle set*. More precisely, a q-cycle set is a set X with two binary operations $\cdot$ and $:$ such that $\ell_x : X \to X : y \mapsto x \cdot y$ is bijective, for all $x \in X$, and

$$\begin{aligned} (x \cdot y) \cdot (x \cdot z) &= (y : x) \cdot (y \cdot z), \\ (x : y) : (x : z) &= (y \cdot x) : (y : z), \\ (x \cdot y) : (x \cdot z) &= (y : x) \cdot (y : z), \end{aligned}$$

holds for all $x, y, z \in X$. A q-cycle set $(X, \cdot, :)$ is called *regular* if, for any $x \in X$, the map $y \mapsto x : y$ is bijective. In the same paper, a bijective correspondence is proven between q-cycle sets and left non-degenerate solutions, by defining the map r of the solution as $r(x, y) = (\ell_x^{-1}(y), \ell_x^{-1}(y) : x)$ given a q-cycle set $(X, \cdot, :)$; and given a left non-degenerate solution $r(x,y) = (\lambda_x(y), \rho_y(x))$, by defining $x \cdot y = \lambda_x^{-1}(y)$ and $x : y = \rho_{\lambda_y^{-1}(x)}(y)$. Under this correspondence, regular q-cycle sets correspond to bijective left non-degenerate solutions. In [34], the structure of q-cycle sets is used to prove that finite bijective left non-degenerate solutions are also right non-degenerate.

1.3.3 Quandles and its generalizations

The Reidemeister moves are crucial in the study of equivalent knots, see Subsection 1.2.1. These three moves can algebraically be described as follows (see [121]). For a set X with binary operation $\triangleleft$ as defined in Figure 1.14, the Reidemeister moves translated in terms of $(X, \triangleleft)$ are

(R1) $x \triangleleft x = x$, for all $x \in X$,

(R2) $x \mapsto x \triangleleft y$ is bijective, for all $y \in X$

(R3) $(x \triangleleft y) \triangleleft z = (x \triangleleft z) \triangleleft (y \triangleleft z)$, for all $x, y, z \in X$.

A pair $(X, \triangleleft)$ satisfying (R3) is called a *shelf* [62]. A shelf satisfying (R2) is called a *rack* [78]. Finally, a *quandle* is a rack that satisfies (R1) [112].

Given a shelf $(X, \triangleleft)$, the map r defined by $r(x,y) = (y, x \triangleleft y)$ defines a left non-degenerate set-theoretic solution of the Yang-Baxter equation. Similarly, the map $r'(x,y) = (y \triangleleft x, x)$ is a right non-degenerate solution. In case the shelf is a rack, both solutions are non-degenerate (and bijective, see [97, Proposition 2.2]). The study of racks is motivated by the problem to classify finite-dimensional pointed Hopf algebras [4]. If the shelf is a quandle, then both solutions are square-free. These types of solutions seem to have better structural properties and have therefore properly been investigated in, for example, [81, 82, 83, 101, 161]. Shelves, racks, quandles, and their link with the Yang-Baxter equation have been studied in [14, 24, 62, 74, 182, 124, 122].

Remark 1.3.2. *An important result is that to any left non-degenerate set-theoretic solution of the Yang-Baxter equation (X, r) with r defined by $r(x,y) = (\lambda_x(y), \rho_y(x))$, for $x, y \in X$, one can associate a left non-degenerate solution (X, s) with $s : X \times X \to X \times X : (x,y) \mapsto (y, \sigma_y(x))$, where $\sigma_y(x) = \lambda_y(\rho_{\lambda_x^{-1}(y)}(x))$, for all $x, y \in X$ [97, 125]. Furthermore, $(X, \triangleleft)$, with $x \triangleleft y = \sigma_y(x)$, for all $x, y \in X$, is a shelf. If $(X, \triangleleft)$ is a rack, i.e. σ_y is bijective, for all $y \in X$, then (X, s) is right non-degenerate, which is equivalent with (X, s) being a bijective solution, and also with (X, r) being a bijective left non-degenerate solution (see [97, Proposition 2.2] or [124, Proposition 5.7]).*

Similarly, if (X, r) is a right non-degenerate solution, then (X, s') with $s' : X \times X \to X \times X : (x,y) \mapsto (\tau_x(y), x)$, where $\tau_y(x) = \rho_x(\lambda_{\rho_y^{-1}(x)}(y))$, for all $x, y \in X$, is a right non-degenerate solution, and $(X, \triangleleft)$, with $y \triangleleft x = \tau_x(y)$, for all $x, y \in X$, is a shelf. If $(X, \triangleleft)$ is a rack, i.e. τ_x is bijective, for all $x \in X$, then (X, s') is right non-degenerate, which is equivalent with (X, s') being a bijective solution, and also with (X, r) being a bijective right non-degenerate solution.

Chapter 2

Set-theoretic solutions and structure monoids

Simplicity does not precede complexity, but follows it.

Alan Perlis

The study of set-theoretic solutions of the Yang-Baxter equation and associated algebraic structures pioneered in the work of Gateva-Ivanova and Van den Bergh [88], and Etingof, Schedler and Soloviev [75], where specific classes of solutions were translated into monoids and groups respectively, the so-called structure monoid $M(X,r)$ and structure group $G(X,r)$ associated to a solution (X,r). These papers focused on (finite) non-degenerate involutive set-theoretic solutions. It turns out that the structure monoid associated to such a solution is a monoid of I-type (see also [101]) and the structure group is solvable and Bieberbach, i.e. finitely generated, torsion-free and abelian-by-finite. As a consequence, the associated group algebra $K[G(X,r)]$, where K is any field, is a Noetherian domain satisfying a polynomial identity (PI) [103, Theorem 3.6.4].

The structure monoids and groups of non-degenerate bijective set-theoretic solutions of the Yang-Baxter equation are investigated in [97, 98, 125, 135]. In particular, there exists a bijective 1-cocycle from the structure group $G(X,r)$ to the structure group of the associated rack solution (X,s). This rack solution is also called the derived solution, and its structure group $G(X,s)$ is called the (left) derived structure group and is denoted by $A_{\mathrm{gr}}(X,r)$. For non-degenerate involutive solutions, the derived structure group is a free abelian group, and the previously mentioned result was already proven in [75, Proposition 2.5]. The monoid with the same (monoid) presentation as the (left) derived structure group is called the left derived (structure) monoid and is denoted by $A(X,r)$. The left derived monoid and its associated monoid algebra $K[A(X,r)]$, where K is a field, have been studied in [97, 98]. It is shown that the structure monoid of a left non-degenerate solution (X,r) is a regular submonoid of the semidirect product of the left derived monoid and the symmetric group on the set X. A similar result was shown in [125, 135, 174] for groups and is used to prove that the structure group of any finite bijective non-degenerate solution is abelian-by-finite [135, Proposition 10]. All these investigations resulted in a profound connection between non-degenerate bijective set-theoretic solutions of the Yang-Baxter equation and monoid and (semi)group theory.

In this chapter, we study the connection between the structure monoid and the left and right derived structure monoid for arbitrary set-theoretic solutions of the Yang-Baxter equation, and focus on the results stated in Section 2 and Section 3 of [52] (Cedó, Jespers, and Verwimp). In the first section we recall an important result of Gateva-Ivanova and Majid [86], namely that, given a set-theoretic solution of the Yang-Baxter equation (X,r), defined by $r(x,y)=(\lambda_x(y),\rho_y(x))$, for all $x,y\in X$, there exists a unique set-theoretic solution (M,r_M) associated to the structure monoid $M=M(X,r)$ such that r_M extends r, and for any $a,b\in M$, $a\circ b=\lambda_a(b)\circ\rho_b(a)$, where $\circ$ denotes the multiplication in M and $r_M(a,b)=(\lambda_a(b),\rho_b(a))$. In fact $\lambda : M\to \mathrm{Map}(M,M)$ is a homomorphism extending the λ-map of r, and $\rho : M\to\mathrm{Map}(M,M)$ is an anti-homomorphism extending the ρ-map of r. In the second section we introduce the left (resp. right) derived (structure) monoid $(A(X,r),+)$ (resp. $(A'(X,r),\oplus)$) associated to a solution (X,r). We prove that there exists a unique 1-cocycle $\pi : M(X,r)\to A(X,r)$, with respect to the natural left action $\lambda' : M(X,r)\to\mathrm{End}(A(X,r),+)$, such that $\pi(x)=x$ and $\lambda'_x(y)=\lambda_x(y)$, for all $x,y\in X$. Similarly, there is a unique 1-cocycle $\pi' : M(X,r)\to A'(X,r)$, with respect to natural right action $\rho' : M(X,r)\to\mathrm{End}(A'(X,r),\oplus)$ such that $\pi'(x)=x$ and $\rho'_x(y)=\rho_x(y)$, for all $x,y\in X$. This yields the existence of a monoid homomorphism $f : M(X,r)\to A(X,r)\rtimes\mathrm{Im}(\lambda') : a\mapsto(\pi(a),\lambda'_a)$ and a monoid anti-homomorphism $f' : M(X,r)\to A'(X,r)^{op}\rtimes\mathrm{Im}(\rho') : a\mapsto(\pi'(a),\rho'_a)$. We investigate when the 1-cocycles are injective or surjective. In general they are not bijective, but if (X,r) is a finite solution, the bijectiveness of π (resp. π') is equivalent with the solution being left (resp. right) non-degenerate.

2.1 Solution associated with the structure monoid

In [86, Section 3.2], Gateva-Ivanova and Majid prove that any bijective set-theoretic solution (X,r) of the Yang-Baxter equation can be extended to a bijective set-theoretic solution on its structure monoid $M(X,r)$, satisfying a certain condition. Without this condition, the extension is not necessarily unique, which will be made clear by an example. The result in [86] is stated for bijective solutions, nevertheless the proof remains valid without this assumption. Hence, we will restate their result, but the proof remains the same. For completeness' sake, we recall the construction of the solution on $M(X,r)$.

Recall from Section 1.3, that (X,r) is a set-theoretic solution of the Yang-Baxter equation (1.15), with

$$r(x,y)=(\lambda_x(y),\rho_y(x)),$$

for all $x, y \in X$, if and only if the following three conditions are satisfied,

$$\begin{aligned}
\lambda_{\lambda_x(y)}(\lambda_{\rho_y(x)}(z)) &= \lambda_x(\lambda_y(z)),\\
\rho_{\lambda_{\rho_y(x)}(z)}(\lambda_x(y)) &= \lambda_{\rho_{\lambda_y(z)}(x)}(\rho_z(y)),\\
\rho_z(\rho_y(x)) &= \rho_{\rho_z(y)}(\rho_{\lambda_y(z)}(x)),
\end{aligned}$$

i.e. (1.17), (1.18), and (1.19) are satisfied, for all $x, y, z \in X$.

In this thesis, we will use the following notation. For a semigroup, monoid or group A and a subset B of A we denote by $\langle B\rangle$, $\langle B\rangle^1$ and $\mathrm{gr}(B)$ the subsemigroup, submonoid and subgroup of A generated by B, respectively. For a set X, we denote the free monoid generated by the set X by $\mathrm{FM}(X)$. In case $(S, \cdot)$ is a semigroup, then we denote by S^1 the smallest monoid containing S, by $Z(S)$ the center of S, and define $(S, \cdot^{\mathrm{op}})$ as the *opposite semigroup* of $(S, \cdot)$, i.e. $a \cdot^{\mathrm{op}} b = b \cdot a$, for all $a, b \in S$. By $\langle X \mid R\rangle$, $\langle X \mid R\rangle^1$ or $\mathrm{gr}(X \mid R)$ we denote the semigroup, monoid or group, respectively, presented with set of generators X and with set of relations R. For a set X, $\mathrm{Sym}(X)$ is the group of all permutations on X, $\mathrm{Map}(X, X)$ is the set of all maps $X \to X$. For an algebraic structure S, $\mathrm{End}(S)$ is the set of all endomorphism of S, i.e. all homomorphisms $S \to S$, and $\mathrm{Aut}(S)$ is the set of all bijective endomorphisms of S. Finally, by $\mathbb{N}$ we denote the set of non-negative integers.

The *structure semigroup* of a set-theoretic solution of the Yang-Baxter equation (X, r) is the semigroup

$$S = S(X, r) = \langle X \mid x \circ y = \lambda_x(y) \circ \rho_y(x), \text{ for all } x, y \in X\rangle,$$

with operation denoted by $\circ$. The *structure monoid* of a set-theoretic solution of the Yang-Baxter equation (X, r) is the monoid $M(X, r)$ with operation $\circ$, defined by the following presentation,

$$M = M(X, r) = \langle X \mid x \circ y = \lambda_x(y) \circ \rho_y(x), \text{ for all } x, y \in X\rangle^1.$$

The *structure group* of (X, r) is the group with the same (group) presentation as $M(X, r)$, i.e.

$$G = G(X, r) = \mathrm{gr}(X \mid x \circ y = \lambda_x(y) \circ \rho_y(x), \text{ for all } x, y \in X).$$

Note that S and M have a natural *length function*, mapping an element a of S or M to a non-negative integer n if $a = x_1 \circ \cdots \circ x_n$, for some generators $x_1, \ldots, x_n \in X$, and to 0 if a is the identity element. We say that a has *length* n, and denote $\mathrm{length}(a) = n$. Also on G one has a length function, but its values are integers, with $\mathrm{length}(x) = 1$ and $\mathrm{length}(\overline{x}) = -1$, for all $x \in X$, with $\overline{x}$ the inverse of x in G.

One can extend the λ-map of the solution (X, r) to a “left action”

$$\lambda : M \to \mathrm{Map}(M, M) : a \mapsto \lambda_a,$$

on the structure monoid, with $\lambda_1 = \mathrm{id}_M$, the identity map on M, and for any $x_1, \ldots, x_m$, $y_1, \ldots, y_n \in X$ and $n > 1$, $\lambda_{x_1}(1) = 1$, and

$$\lambda_{x_1}(y_1 \circ \cdots \circ y_n) = \lambda_{x_1}(y_1) \circ \lambda_{\rho_{y_1}(x_1)}(y_2 \circ \cdots \circ y_n), \tag{2.1}$$

and for $m > 1$,

$$\lambda_{x_1 \circ \cdots \circ x_m} = \lambda_{x_1} \cdots \lambda_{x_m}. \tag{2.2}$$

Similarly, one can extend the ρ-map of the solution (X, r) to a "right action"

$$\rho : M \to \mathrm{Map}(M, M) : a \mapsto \rho_a,$$

on the structure monoid, with $\rho_1 = \mathrm{id}_M$, and for $x_1, \ldots, x_m, y_1, \ldots, y_n \in X$ and $n > 1$, $\rho_{x_1}(1) = 1$, and

$$\rho_{x_1}(y_1 \circ \cdots \circ y_n) = \rho_{\lambda_{y_n}(x_1)}(y_1 \circ \cdots \circ y_{n-1}) \circ \rho_{x_1}(y_n), \tag{2.3}$$

and for $m > 1$,

$$\rho_{x_1 \circ \cdots \circ x_m} = \rho_{x_m} \cdots \rho_{x_1}. \tag{2.4}$$

It is proven in [86] that λ and ρ are well-defined "actions" on $M(X, r)$. Furthermore, it is then shown that every set-theoretic solution of the Yang-Baxter equation (X, r) is the restriction of a set-theoretic solution defined on the structure monoid $M(X, r)$.

Theorem 2.1.1 (Gateva-Ivanova and Majid [86, Theorem 3.6])**.** *Let (X, r) be a set-theoretic solution of the Yang-Baxter equation. Then, the mapping λ is a monoid homomorphism and the mapping ρ is a monoid anti-homomorphism such that, for any $a, b, c \in M = M(X, r)$,*

$$\rho_b(c \circ a) = \rho_{\lambda_a(b)}(c) \circ \rho_b(a), \tag{2.5}$$
$$\lambda_b(a \circ c) = \lambda_b(a) \circ \lambda_{\rho_a(b)}(c). \tag{2.6}$$

Furthermore, for $a, b \in M$,

$$a \circ b = \lambda_a(b) \circ \rho_b(a). \tag{2.7}$$

Define $r_M : M \times M \to M \times M$ by $r_M(a, b) = (\lambda_a(b), \rho_b(a))$, for all $a, b \in M$. Then, (M, r_M) is a set-theoretic solution of the Yang-Baxter equation. Obviously, r_M extends the solution r.

Note that the previous result also holds for the structure semigroup $S(X, r)$. In [86, Theorem 3.14] it is furthermore proven that the solution (M, r_M) is non-degenerate if and only if (X, r) is non-degenerate, and (M, r_M) being involutive is equivalent with (X, r) being involutive.

Without (2.5) and (2.6), or without (2.7), the extension of the previous theorem is not necessarily unique.

Example 2.1.2. *Consider the solution (X, r), with r defined by $r(x, y) = (y, t)$, for a fixed element $t \in X$. The extension of Theorem 2.1.1 yields a solution (M, r_M) on the structure monoid $M = M(X, r) = \langle X \mid x \circ y = y \circ t = t \circ t \rangle^1$, with r_M defined by $r(a, b) = (b, t \circ \cdots \circ t)$, where the length of the second component equals the length of a. It is possible to define other solutions (M, r'_M) on $M(X, r)$, with $r'_M|_{X \times X} = r$. For example, define $r'_M(x, y) = (y, t)$, for all $x, y \in X$, and $r'_M(a, b) = (t \circ t, t \circ t)$ for all*

$a, b \in M$ with $(a,b) \notin X \times X$. Then, (M, r'_M) is a solution, but (2.5), (2.6) *and* (2.7) *are not satisfied for the λ-map and ρ-map of the solution (M, r'_M). Indeed, take for example $x, x_1, x_2, x_3, x_4 \in X$, then $\rho_x((x_1 \circ x_2) \circ (x_3 \circ x_4)) = t \circ t$, but $\rho_{\lambda_{x_3 \circ x_4}(x)}(x_1 \circ x_2) \circ \rho_x(x_3 \circ x_4) = (t \circ t) \circ (t \circ t)$, which are not equal in $M(X,r)$. Also, $x_1 \circ (x_2 \circ x_3) = t \circ t \circ t$ in $M(X,r)$ is not equal to $\lambda_{x_1}(x_2 \circ x_3) \circ \rho_{x_2 \circ x_3}(x_1) = (t \circ t) \circ (t \circ t)$ in $M(X,r)$.*

Unless mentioned otherwise, we will assume in what follows that $(M(X,r), r_{M(X,r)})$ is the extended solution of (X,r) as defined in Theorem 2.1.1, and call it the *solution associated to* $M(X,r)$.

The existence of an extension to the structure group was proven in [135, Theorem 9] for bijective non-degenerate set-theoretic solutions (X,r) of the Yang-Baxter equation. In this case, the λ-map and ρ-map induce actual left and right actions on the structure group $G = G(X,r)$, say $\lambda^e : G \to \mathrm{Sym}(G)$ and $\rho^e : G \to \mathrm{Sym}(G)$. Furthermore, the mapping $r_G(a,b) = (\lambda^e_a(b), \rho^e_b(a))$, for $a, b \in G$, defines a set-theoretic solution on G. We denote this solution by $(G(X,r), r_{G(X,r)})$ and call it *the extended solution of* (X,r) *on* $G(X,r)$. In case the solution is also involutive, the natural map $\iota : X \to G$ is injective [88, 135]. However, in general, ι is not necessarily injective, which was already noticed in [135] and confirmed in [174] by an example. One obtains that r_G is an extension of the induced set-theoretic solution $\mathrm{Inj}(X,r) = (\iota(X), r_{\iota(X)}) = (\iota(X), r_G|_{\iota(X)^2})$, called the *injectivization* of (X,r), and $G(X,r) \cong G(\iota(X), r_{\iota(X)}) = G(\mathrm{Inj}(X,r))$ [125, Proposition 7.6]. If $\iota : X \to G$ is injective, the solution (X,r) is called *injective*. Injective solutions are introduced and studied by Soloviev in [174]. In particular, it was shown that Lyubashenko solutions, defined by $r(x,y) = (f(y), g(x))$, with $f, g \in \mathrm{Sym}(X)$ such that $fg = gf$, is injective if and only if it is involutive, which is equivalent to fg being the identity map on X. On the other hand, the map $\iota : X \to M$ is always injective. So, one does not lose any information on the solution (X,r), when studying the structure monoid and its associated solution.

A natural question is whether the result in [135, Theorem 9] can be extended to any solution (X,r). This, however, is not possible in general as shown by the following example.

Example 2.1.3. *Let X be a set with more than one element and consider the solution (X, id_{X^2}). Obviously, each λ_x and ρ_x is the constant mapping with image $\{x\}$. Hence, the structure monoid is the free monoid on the set X and the structure group is the free group on X. However, since the maps λ_x are not injective, one can not define $\lambda_{x^{-1}}$ such that $\lambda_x \lambda_{x^{-1}} = \lambda_{x^{-1}} \lambda_x = \mathrm{id}_G$. Thus, the map $\lambda : X \to \mathrm{Map}(X,X)$ can not be extended to a monoid homomorphism $\lambda : G \to \mathrm{Map}(G,G)$.*

A surprising fact is that if the mappings λ_x and ρ_x of a set-theoretic solution (X,r) can be extended to left and right actions on the structure group $G(X,r)$, then the induced set-theoretic solution on $G(X,r)$ is always bijective [135].

2.2 Derived monoids

Let (X,r) be a set-theoretic solution of the Yang-Baxter equation. If (X,r) is left non-degenerate, then, using the notation (1.16), the *(left) derived solution* (X,s) of (X,r) is defined by

$$s(x,y) = (y, \lambda_y \rho_{\lambda_x^{-1}(y)}(x)) = (y, \sigma_y(x)), \tag{2.8}$$

for all $x,y \in X$. This solution was first defined by Soloviev in [174] for non-degenerate bijective solutions (X,r), but it can be defined for any left non-degenerate solution (X,r), see [97, Proposition 2.2]. In general, it is not always possible to define the derived solution, namely one needs that all λ-maps of the solution are bijective. Similarly, if (X,r) is right non-degenerate, then one can define the *right derived solution* as (X,s') with

$$s'(x,y) = (\rho_x \lambda_{\rho_y^{-1}(x)}(y), x) = (\tau_x(y), x),$$

for all $x,y \in X$. For non-degenerate involutive solutions (X,r), both the left and right derived solutions are equal to the trivial solution. Left and right derived solutions correspond to shelves (see Remark 1.3.2).

Let (X,r) be an arbitrary set-theoretic solution of the Yang-Baxter equation. In [97], the derived monoids of (X,r) are defined as

$$A(X,r) = \langle X \mid x + \lambda_x(y) = \lambda_x(y) + \lambda_{\lambda_x(y)}\rho_y(x), \text{ for all } x,y \in X\rangle^1,$$

and

$$A'(X,r) = \langle X \mid \rho_y(x) \oplus y = \rho_{\rho_y(x)}\lambda_x(y) \oplus \rho_y(x), \text{ for all } x,y \in X\rangle^1.$$

The zero element of $A(X,r)$ is denoted by 0, while the zero element of $A'(X,r)$ is denoted by $0'$. We will call $A(X,r)$ the *left derived (structure) monoid* of (X,r) and $A'(X,r)$ the *right derived (structure) monoid* of (X,r). Note that the left (resp. right) derived structure monoid of (X,r) is determined by the first (resp. second) components of $r(x,y)$ and $r^2(x,y)$, see Fig. 2.1.

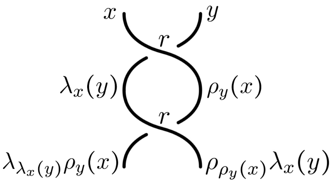

x
y
r
$\lambda_x(y)$
$\rho_y(x)$
r
$\lambda_{\lambda_x(y)}\rho_y(x)$
$\rho_{\rho_y(x)}\lambda_x(y)$

Figure 2.1: Graphical interpretation of applying r and r^2 on (x,y).

Furthermore, it is clear that $X \subseteq M(X,r)$, $X \subseteq A(X,r)$ and $X \subseteq A'(X,r)$, because the defining relations of these three monoids are homogeneous of degree 2.

The *left or right derived (structure) group* of (X,r) is the group with the same (group) presentation as the left or right derived structure monoid, and will be denoted by $A_{\mathrm{gr}}(X,r)$ or $A'_{\mathrm{gr}}(X,r)$ respectively, i.e.

$$A_{\mathrm{gr}}(X,r) = \mathrm{gr}(X \mid x + \lambda_x(y) = \lambda_x(y) + \lambda_{\lambda_x(y)}\rho_y(x), \text{ for all } x,y \in X),$$

and

$$A'_{\mathrm{gr}}(X,r) = \mathrm{gr}(X \mid \rho_y(x) \oplus y = \rho_{\rho_y(x)}\lambda_x(y) \oplus \rho_y(x), \text{ for all } x,y \in X).$$

Similar to $S(X,r)$, $M(X,r)$ and $G(X,r)$, there is a natural length function on $A(X,r)$, $A'(X,r)$, $A_{\mathrm{gr}}(X,r)$, and $A'_{\mathrm{gr}}(X,r)$. In [174], Soloviev proves that for non-degenerate bijective solutions, the structure group of the left (resp. right) derived solution is equal to the left (resp. right) derived structure group of the solution, i.e. $G(X,s) = A_{\mathrm{gr}}(X,r)$ and $G(X,s') = A'_{\mathrm{gr}}(X,r)$. In a similar fashion, the left derived structure monoid of a left non-degenerate solution (X,r) is equal to the structure monoid of the left derived solution (X,s), i.e. $A(X,r) = M(X,s)$, while the right derived structure monoid of a right non-degenerate solution (X,r) equals the structure monoid of the right derived solution (X,s'), i.e. $A'(X,r) = M(X,s')$.

Proposition 2.2.1. *Let (X,r) be a set-theoretic solution of the Yang-Baxter equation, where $r(x,y) = (\lambda_x(y),\rho_y(x))$, for all $x,y \in X$. Then, there exists a unique monoid homomorphism $\lambda' : M(X,r) \to \mathrm{End}(A(X,r),+)$ such that, $\lambda'(x)(y) = \lambda_x(y)$, for all $x,y \in X$, and there exists a unique monoid anti-homomorphism $\rho' : M(X,r) \to \mathrm{End}(A'(X,r),\oplus)$ such that, $\rho'(x)(y) = \rho_x(y)$, for all $x,y \in X$. Furthermore, if (X,r) is left (resp. right) non-degenerate, then $\mathrm{Im}(\lambda') \subseteq \mathrm{Aut}(A(X,r),+)$ (resp. $\mathrm{Im}(\rho') \subseteq \mathrm{Aut}(A'(X,r),\oplus)$).*

Proof. Write $\lambda'(a) = \lambda'_a$ and $\rho'(a) = \rho'_a$, for all $a \in M(X,r)$. Denote by $1, 0, 0'$ the identity elements of the monoids $M(X,r)$, $A(X,r)$, $A'(X,r)$, respectively, and define $\lambda'_1 = \mathrm{id}_{A(X,r)}$, $\rho'_1 = \mathrm{id}_{A'(X,r)}$, $\lambda'_a(0) = 0$, $\rho'_a(0') = 0'$, for all $a \in M(X,r)$.

Let $x_1,\dots,x_m,y_1,\dots,y_n \in X$. Define

$$\lambda'_{x_1\circ\cdots\circ x_m}(y_1 + \cdots + y_n) = \lambda_{x_1}\dots\lambda_{x_m}(y_1) + \cdots + \lambda_{x_1}\dots\lambda_{x_m}(y_n),$$

and

$$\rho'_{x_1\circ\cdots\circ x_m}(y_1 \oplus \cdots \oplus y_n) = \rho_{x_m}\dots\rho_{x_1}(y_1) \oplus \cdots \oplus \rho_{x_m}\dots\rho_{x_1}(y_n),$$

To prove that λ' and ρ' are well-defined, it is enough to prove that the following equalities hold,

$$\lambda'_{x_1\circ x_2}(y_1 + \cdots + y_n) = \lambda'_{\lambda_{x_1}(x_2)\circ\rho_{x_2}(x_1)}(y_1 + \cdots + y_n), \tag{2.9}$$

$$\lambda'_{x_1\circ\cdots\circ x_m}(y_1 + \lambda_{y_1}(y_2)) = \lambda'_{x_1\circ\cdots\circ x_m}(\lambda_{y_1}(y_2) + \lambda_{\lambda_{y_1}(y_2)}(\rho_{y_2}(y_1))), \tag{2.10}$$

$$\rho'_{x_1\circ x_2}(y_1 \oplus \cdots \oplus y_n) = \rho'_{\lambda_{x_1}(x_2)\circ\rho_{x_2}(x_1)}(y_1 \oplus \cdots \oplus y_n), \tag{2.11}$$

$$\rho'_{x_1\circ\cdots\circ x_m}(\rho_{y_2}(y_1) \oplus y_2) = \rho'_{x_1\circ\cdots\circ x_m}(\rho_{\rho_{y_2}(y_1)}(\lambda_{y_1}(y_2)) \oplus \rho_{y_2}(y_1)). \tag{2.12}$$

Using relations (1.17) and (1.19), equations (2.9) and (2.11) are easily verified. Indeed,

$$\begin{aligned}
\lambda'_{x_1\circ x_2}(y_1+\cdots+y_n) &= \lambda_{x_1}\lambda_{x_2}(y_1)+\cdots+\lambda_{x_1}\lambda_{x_2}(y_n)\\
&= \lambda_{\lambda_{x_1}(x_2)}\lambda_{\rho_{x_2}(x_1)}(y_1)+\cdots+\lambda_{\lambda_{x_1}(x_2)}\lambda_{\rho_{x_2}(x_1)}(y_n)\\
&= \lambda'_{\lambda_{x_1}(x_2)\circ\rho_{x_2}(x_1)}(y_1+\cdots+y_n),\\
\rho'_{x_1\circ x_2}(y_1\oplus\cdots\oplus y_n) &= \rho_{x_2}\rho_{x_1}(y_1)\oplus\cdots\oplus\rho_{x_2}\rho_{x_1}(y_n)\\
&= \rho_{\rho_{x_2}(x_1)}\rho_{\lambda_{x_1}(x_2)}(y_1)\oplus\cdots\oplus\rho_{\rho_{x_2}(x_1)}\rho_{\lambda_{x_1}(x_2)}(y_n)\\
&= \rho'_{\lambda_{x_1}(x_2)\circ\rho_{x_2}(x_1)}(y_1\oplus\cdots\oplus y_n).
\end{aligned}$$

We will prove equations (2.10) and (2.12) by induction on m. For $m=0$, (2.10) and (2.12) follow by the defining relations of $A(X,r)$ and $A'(X,r)$. Suppose that $m>0$ and assume that $\lambda'_{x_1\circ\cdots\circ x_k}(y_1+\lambda_{y_1}(y_2)) = \lambda'_{x_1\circ\cdots\circ x_k}(\lambda_{y_1}(y_2)+\lambda_{\lambda_{y_1}(y_2)}(\rho_{y_2}(y_1)))$ and $\rho'_{x_1\circ\cdots\circ x_k}(\rho_{y_2}(y_1)\oplus y_2) = \rho'_{x_1\circ\cdots\circ x_k}(\rho_{\rho_{y_2}(y_1)}(\lambda_{y_1}(y_2))\oplus\rho_{y_2}(y_1))$ hold for $k<m$. Then, using (1.17), (1.18) and (1.19),

$$\begin{aligned}
&\lambda'_{x_1\circ\cdots\circ x_m}(y_1+\lambda_{y_1}(y_2))\\
&= \lambda_{x_1}\cdots\lambda_{x_m}(y_1)+\lambda_{x_1}\cdots\lambda_{x_m}(\lambda_{y_1}(y_2))\\
&= \lambda'_{x_1\circ\cdots\circ x_{m-1}}(\lambda_{x_m}(y_1)+\lambda_{x_m}(\lambda_{y_1}(y_2)))\\
&= \lambda'_{x_1\circ\cdots\circ x_{m-1}}(\lambda_{x_m}(y_1)+\lambda_{\lambda_{x_m}(y_1)}(\lambda_{\rho_{y_1}(x_m)}(y_2)))\\
&= \lambda'_{x_1\circ\cdots\circ x_{m-1}}(\lambda_{\lambda_{x_m}(y_1)}(\lambda_{\rho_{y_1}(x_m)}(y_2))+\lambda_{\lambda_{\lambda_{x_m}(y_1)}(\lambda_{\rho_{y_1}(x_m)}(y_2))}(\rho_{\lambda_{\rho_{y_1}(x_m)}(y_2)}(\lambda_{x_m}(y_1))))\\
&= \lambda'_{x_1\circ\cdots\circ x_{m-1}}(\lambda_{x_m}(\lambda_{y_1}(y_2))+\lambda_{\lambda_{x_m}(\lambda_{y_1}(y_2))}(\rho_{\lambda_{\rho_{y_1}(x_m)}(y_2)}(\lambda_{x_m}(y_1))))\\
&= \lambda'_{x_1\circ\cdots\circ x_{m-1}}(\lambda_{x_m}(\lambda_{y_1}(y_2))+\lambda_{\lambda_{x_m}(\lambda_{y_1}(y_2))}(\lambda_{\rho_{\lambda_{y_1}(y_2)}(x_m)}(\rho_{y_2}(y_1))))\\
&= \lambda'_{x_1\circ\cdots\circ x_{m-1}}(\lambda_{x_m}(\lambda_{y_1}(y_2))+\lambda_{x_m}(\lambda_{\lambda_{y_1}(y_2)}(\rho_{y_2}(y_1))))\\
&= \lambda_{x_1}\cdots\lambda_{x_m}(\lambda_{y_1}(y_2))+\lambda_{x_1}\cdots\lambda_{x_m}(\lambda_{\lambda_{y_1}(y_2)}(\rho_{y_2}(y_1)))\\
&= \lambda'_{x_1\circ\cdots\circ x_m}(\lambda_{y_1}(y_2)+\lambda_{\lambda_{y_1}(y_2)}(\rho_{y_2}(y_1))),
\end{aligned}$$

and

$$\begin{aligned}
&\rho'_{x_1\circ\cdots\circ x_m}(\rho_{y_2}(y_1)\oplus y_2)\\
&= \rho'_{x_2\circ\cdots\circ x_m}(\rho_{x_1}(\rho_{y_2}(y_1))\oplus\rho_{x_1}(y_2))\\
&= \rho'_{x_2\circ\cdots\circ x_m}(\rho_{\rho_{x_1}(y_2)}(\rho_{\lambda_{y_2}(x_1)}(y_1))\oplus\rho_{x_1}(y_2))\\
&= \rho'_{x_2\circ\cdots\circ x_m}(\rho_{\rho_{\rho_{x_1}(y_2)}(\rho_{\lambda_{y_2}(x_1)}(y_1))}(\lambda_{\rho_{\lambda_{y_2}(x_1)}(y_1)}(\rho_{x_1}(y_2)))\oplus\rho_{\rho_{x_1}(y_2)}(\rho_{\lambda_{y_2}(x_1)}(y_1)))\\
&= \rho'_{x_2\circ\cdots\circ x_m}(\rho_{\rho_{x_1}(\rho_{y_2}(y_1))}(\lambda_{\rho_{\lambda_{y_2}(x_1)}(y_1)}(\rho_{x_1}(y_2)))\oplus\rho_{x_1}(\rho_{y_2}(y_1)))\\
&= \rho'_{x_2\circ\cdots\circ x_m}(\rho_{\rho_{x_1}(\rho_{y_2}(y_1))}(\rho_{\lambda_{\rho_{y_2}(y_1)}(x_1)}(\lambda_{y_1}(y_2)))\oplus\rho_{x_1}(\rho_{y_2}(y_1)))\\
&= \rho'_{x_2\circ\cdots\circ x_m}(\rho_{x_1}(\rho_{\rho_{y_2}(y_1)}(\lambda_{y_1}(y_2)))\oplus\rho_{x_1}(\rho_{y_2}(y_1)))\\
&= \rho_{x_m}\cdots\rho_{x_1}(\rho_{\rho_{y_2}(y_1)}(\lambda_{y_1}(y_2)))\oplus\rho_{x_m}\cdots\rho_{x_1}(\rho_{y_2}(y_1))\\
&= \rho'_{x_1\circ\cdots\circ x_m}(\rho_{\rho_{y_2}(y_1)}(\lambda_{y_1}(y_2))\oplus\rho_{y_2}(y_1)).
\end{aligned}$$

So λ'_a and ρ'_a are indeed well-defined and by definition $\lambda'_a \in \mathrm{End}(A(X,r),+)$ and $\rho'_a \in \mathrm{End}(A'(X,r),\oplus)$, for all $a \in M(X,r)$. Thus λ' and ρ' are well-defined. Furthermore, it is clear that λ' is a monoid homomorphism and that it is unique for the condition $\lambda'_x(y) = \lambda_x(y)$, for all $x, y \in X$. It is also easy to see that ρ' is a monoid anti-homomorphism and that it is unique with respect to the condition $\rho'_x(y) = \rho_x(y)$, for all $x, y \in X$.

Assume now that (X,r) is left non-degenerate, i.e. $\lambda_x : X \to X$ is bijective, for all $x \in X$. We will prove that $\lambda'_a \in \mathrm{Aut}(A(X,r),+)$, for all $a \in M(X,r)$, by showing there exists $\alpha_a \in \mathrm{End}(A(X,r),+)$, such that $\alpha_a\lambda'_a = \lambda'_a\alpha_a = \mathrm{id}_{A(X,r)}$. Let $x, x_1, \dots, x_m, y_1, \dots, y_n \in X$ and define $\alpha_x \in \mathrm{End}(A(X,r),+)$ by

$$\alpha_x(y_1 + \dots + y_n) = \lambda_x^{-1}(y_1) + \dots + \lambda_x^{-1}(y_n),$$

and $\alpha_{x_1\circ\dots\circ x_m} = \alpha_{x_m}\cdots\alpha_{x_1}$. To see that α_a, for $a \in M(X,r)$, is well-defined, it is enough to prove that the following pair of equations are satisfied, for all $x_1, \dots, x_m, y_1, \dots, y_n \in X$,

$$\alpha_{x_1\circ x_2}(y_1 + \dots + y_n) = \alpha_{\lambda_{x_1}(x_2)\circ\rho_{x_2}(x_1)}(y_1 + \dots + y_n), \tag{2.13}$$

$$\alpha_{x_1\circ\dots\circ x_m}(y_1 + \lambda_{y_1}(y_2)) = \alpha_{x_1\circ\dots\circ x_m}(\lambda_{y_1}(y_2) + \lambda_{\lambda_{y_1}(y_2)}(\rho_{y_2}(y_1))). \tag{2.14}$$

The former is clear since, using (1.17),

$$\begin{aligned}
\alpha_{x_1\circ x_2}(y_1 + \dots + y_n) &= \alpha_{x_2}\alpha_{x_1}(y_1 + \dots + y_n)\\
&= \alpha_{x_2}(\lambda_{x_1}^{-1}(y_1) + \dots + \lambda_{x_1}^{-1}(y_n))\\
&= \lambda_{x_2}^{-1}\lambda_{x_1}^{-1}(y_1) + \dots + \lambda_{x_2}^{-1}\lambda_{x_1}^{-1}(y_n)\\
&= (\lambda_{x_1}\lambda_{x_2})^{-1}(y_1) + \dots + (\lambda_{x_1}\lambda_{x_2})^{-1}(y_n)\\
&= (\lambda_{\lambda_{x_1}(x_2)}\lambda_{\rho_{x_2}(x_1)})^{-1}(y_1) + \dots + (\lambda_{\lambda_{x_1}(x_2)}\lambda_{\rho_{x_2}(x_1)})^{-1}(y_n)\\
&= \lambda_{\rho_{x_2}(x_1)}^{-1}\lambda_{\lambda_{x_1}(x_2)}^{-1}(y_1) + \dots + \lambda_{\rho_{x_2}(x_1)}^{-1}\lambda_{\lambda_{x_1}(x_2)}^{-1}(y_n)\\
&= \alpha_{\rho_{x_2}(x_1)}\alpha_{\lambda_{x_1}(x_2)}(y_1 + \dots + y_n)\\
&= \alpha_{\lambda_{x_1}(x_2)\circ\rho_{x_2}(x_1)}(y_1 + \dots + y_n).
\end{aligned}$$

Let $x, y_1, y_2 \in X$. Note that, from (1.17),

$$\lambda_x^{-1}\lambda_{y_1}(y_2) = \lambda_{\lambda_x^{-1}(y_1)}\lambda^{-1}_{\rho_{\lambda_x^{-1}(y_1)}(x)}(y_2), \tag{2.15}$$

and thus, also using (1.18), we get that

$$\begin{aligned}
&\lambda_{\rho_{\lambda_x^{-1}\lambda_{y_1}(y_2)}(x)}\rho_{\lambda^{-1}_{\rho_{\lambda_x^{-1}(y_1)}(x)}(y_2)}(\lambda_x^{-1}(y_1)) \qquad (2.16)\\
&= \lambda_{\rho_{\lambda_{\lambda_x^{-1}(y_1)}\lambda^{-1}_{\rho_{\lambda_x^{-1}(y_1)}(x)}(y_2)}(x)}\rho_{\lambda^{-1}_{\rho_{\lambda_x^{-1}(y_1)}(x)}(y_2)}(\lambda_x^{-1}(y_1))\\
&= \rho_{\lambda_{\rho_{\lambda_x^{-1}(y_1)}(x)}(\lambda^{-1}_{\rho_{\lambda_x^{-1}(y_1)}(x)}(y_2))}\lambda_x(\lambda_x^{-1}(y_1))\\
&= \rho_{y_2}(y_1).
\end{aligned}$$

We will prove that (2.14) holds by induction on m. For $m = 0$, (2.14) follows by the defining relations of $A(X,r)$. Let $x_1,\dots,x_m,y_1,y_2 \in X$. Suppose that $m > 0$ and that $\alpha_{x_1\circ\cdots\circ x_k}(y_1+\lambda_{y_1}(y_2)) = \alpha_{x_1\circ\cdots\circ x_k}(\lambda_{y_1}(y_2)+\lambda_{\lambda_{y_1}(y_2)}(\rho_{y_2}(y_1)))$ holds for $k < m$. Using the previously obtained relations, we get

$$\begin{aligned}
&\alpha_{x_1\circ\cdots\circ x_m}(y_1+\lambda_{y_1}(y_2))\\
&= \alpha_{x_2\circ\cdots\circ x_m}(\lambda_{x_1}^{-1}(y_1)+\lambda_{x_1}^{-1}(\lambda_{y_1}(y_2)))\\
&\overset{(2.15)}{=} \alpha_{x_2\circ\cdots\circ x_m}(\lambda_{x_1}^{-1}(y_1)+\lambda_{\lambda_{x_1}^{-1}(y_1)}(\lambda^{-1}_{\rho_{\lambda_{x}^{-1}(y_1)}(x_1)}(y_2)))\\
&= \alpha_{x_2\circ\cdots\circ x_m}(\lambda_{\lambda_{x_1}^{-1}(y_1)}(\lambda^{-1}_{\rho_{\lambda_{x_1}^{-1}(y_1)}(x_1)}(y_2))\\
&\quad + \lambda_{\lambda_{\lambda_{x_1}^{-1}(y_1)}(\lambda^{-1}_{\rho_{\lambda_{x_1}^{-1}(y_1)}(x_1)}(y_2))}(\rho_{\lambda^{-1}_{\rho_{\lambda_{x_1}^{-1}(y_1)}(x_1)}(y_2)}(\lambda_{x_1}^{-1}(y_1))))\\
&\overset{(2.15)}{=} \alpha_{x_2\circ\cdots\circ x_m}(\lambda_{x_1}^{-1}(\lambda_{y_1}(y_2))+\lambda_{\lambda_{x_1}^{-1}(\lambda_{y_1}(y_2))}(\rho_{\lambda^{-1}_{\rho_{\lambda_{x_1}^{-1}(y_1)}(x_1)}(y_2)}(\lambda_{x_1}^{-1}(y_1))))\\
&\overset{(2.16)}{=} \alpha_{x_2\circ\cdots\circ x_m}(\lambda_{x_1}^{-1}(\lambda_{y_1}(y_2))+\lambda_{\lambda_{x_1}^{-1}(\lambda_{y_1}(y_2))}(\lambda^{-1}_{\rho_{\lambda_{x_1}^{-1}\lambda_{y_1}(y_2)}(x_1)}(\rho_{y_2}(y_1))))\\
&\overset{(2.15)}{=} \alpha_{x_2\circ\cdots\circ x_m}(\lambda_{x_1}^{-1}(\lambda_{y_1}(y_2))+\lambda_{x_1}^{-1}(\lambda_{\lambda_{y_1}(y_2)}(\rho_{y_2}(y_1))))\\
&= \alpha_{x_2\circ\cdots\circ x_m}(\alpha_{x_1}(\lambda_{y_1}(y_2)+\lambda_{\lambda_{y_1}(y_2)}(\rho_{y_2}(y_1))))\\
&= \alpha_{x_1\circ\cdots\circ x_m}(\lambda_{y_1}(y_2)+\lambda_{\lambda_{y_1}(y_2)}(\rho_{y_2}(y_1))),
\end{aligned}$$

where the third equality follows from the defining relations in $A(X,r)$. So α_a, for $a \in M(X,r)$, is well-defined. Furthermore, $\alpha_a\lambda'_a = \lambda'_a\alpha_a = \mathrm{id}_{A(X,r)}$ and thus $\lambda'_a \in \mathrm{Aut}(A(X,r),+)$, for all $a \in M(X,r)$. We conclude that $\mathrm{Im}(\lambda') \subseteq \mathrm{Aut}(A(X,r),+)$.

Similarly, one can prove that for right non-degenerate solutions (X,r), we have $\mathrm{Im}(\rho') \subseteq \mathrm{Aut}(A'(X,r),\oplus)$. □

The maps λ' and ρ' defined in the previous proposition yield a connection between the structure monoid and the derived monoids of a set-theoretic solution of the Yang-Baxter equation.

Theorem 2.2.2. *Let (X,r) be a set-theoretic solution of the Yang-Baxter equation. Then, there exists a unique 1-cocycle $\pi : M(X,r) \to A(X,r)$ with respect to the "left action" λ' such that $\pi(x) = x$, for all $x \in X$, and*

$$\pi(a\circ b) = \pi(a) + \lambda'_a(\pi(b)), \tag{2.17}$$

for all $a,b \in M(X,r)$. Moreover, there exists a unique 1-cocycle $\pi' : M(X,r) \to A'(X,r)$ with respect to the "right action" ρ' such that $\pi'(x) = x$, for all $x \in X$, and

$$\pi'(a\circ b) = \rho'_b(\pi'(a)) \oplus \pi'(b), \tag{2.18}$$

for all $a,b \in M(X,r)$. Furthermore, the mapping

$$f : M(X,r) \to A(X,r) \rtimes \mathrm{Im}(\lambda') : a \mapsto (\pi(a),\lambda'_a),$$

is a monoid homomorphism, and the mapping

$$f' : M(X,r) \to A'(X,r)^{op} \rtimes \operatorname{Im}(\rho') : a \mapsto (\pi'(a), \rho'_a),$$

is a monoid anti-homomorphism.

Proof. We define for $x_1, \dots, x_m \in X$, $\pi(1) = 0, \pi'(1) = 0', \pi(x_1) = x_1, \pi'(x_1) = x_1$, where $1, 0, 0'$ are the identity elements of the monoids $M(X,r)$, $A(X,r)$, $A'(X,r)$, respectively. For $m > 1$, define

$$\pi(x_1 \circ \cdots \circ x_m) = x_1 + \lambda'_{x_1}(\pi(x_2 \circ \cdots \circ x_m)), \tag{2.19}$$

$$\pi'(x_1 \circ \cdots \circ x_m) = \rho'_{x_m}(\pi'(x_1 \circ \cdots \circ x_{m-1})) \oplus x_m. \tag{2.20}$$

We prove that $\pi(x_1 \circ \cdots \circ x_m)$ and $\pi'(x_1 \circ \cdots \circ x_m)$ are well-defined by induction on m. For $m = 1$ it is clear. Let $m > 1$ and assume that $\pi(x_1 \circ \cdots \circ x_{m-1})$ and $\pi'(x_1 \circ \cdots \circ x_{m-1})$ are well-defined, for all $x_1, \dots, x_m \in X$. To prove that $\pi(x_1 \circ \cdots \circ x_m)$ and $\pi'(x_1 \circ \cdots \circ x_m)$ are well-defined, we need to show that

$$\pi(x_1 \circ \cdots \circ x_i \circ x_{i+1} \circ \cdots \circ x_m) = \pi(x_1 \circ \cdots \circ \lambda_{x_i}(x_{i+1}) \circ \rho_{x_{i+1}}(x_i) \circ \cdots \circ x_m),$$

and

$$\pi'(x_1 \circ \cdots \circ x_i \circ x_{i+1} \circ \cdots \circ x_m) = \pi'(x_1 \circ \cdots \circ \lambda_{x_i}(x_{i+1}) \circ \rho_{x_{i+1}}(x_i) \circ \cdots \circ x_m),$$

for all $1 \le i \le m-1$. If $i > 1$, we get by (2.19) and the induction hypothesis

$$\begin{aligned}
\pi(x_1 \circ \cdots \circ x_m) &= x_1 + \lambda'_{x_1}(\pi(x_2 \circ \cdots \circ x_m)) \\
&= x_1 + \lambda'_{x_1}(\pi(x_2 \circ \cdots \circ x_i \circ x_{i+1} \circ \cdots \circ x_m)) \\
&= x_1 + \lambda'_{x_1}(\pi(x_2 \circ \cdots \circ \lambda_{x_i}(x_{i+1}) \circ \rho_{x_{i+1}}(x_i) \circ \cdots \circ x_m)) \\
&= \pi(x_1 \circ \cdots \circ \lambda_{x_i}(x_{i+1}) \circ \rho_{x_{i+1}}(x_i) \circ \cdots \circ x_m),
\end{aligned}$$

and if $i < m-1$, using (2.20) and the induction hypothesis,

$$\begin{aligned}
\pi'(x_1 \circ \cdots \circ x_m) &= \rho'_{x_m}(\pi'(x_1 \circ \cdots \circ x_i \circ x_{i+1} \circ \cdots \circ x_{m-1})) \oplus x_m \\
&= \rho'_{x_m}(\pi'(x_1 \circ \cdots \circ \lambda_{x_i}(x_{i+1}) \circ \rho_{x_{i+1}}(x_i) \circ \cdots \circ x_{m-1})) \oplus x_m \\
&= \pi'(x_1 \circ \cdots \circ \lambda_{x_i}(x_{i+1}) \circ \rho_{x_{i+1}}(x_i) \circ \cdots \circ x_m).
\end{aligned}$$

Hence, we are left to prove that

$$\pi(x_1 \circ x_2 \circ \cdots \circ x_m) = \pi(\lambda_{x_1}(x_2) \circ \rho_{x_2}(x_1) \circ \cdots \circ x_m),$$

and

$$\pi'(x_1 \circ \cdots \circ x_{m-1} \circ x_m) = \pi'(x_1 \circ \cdots \circ \lambda_{x_{m-1}}(x_m) \circ \rho_{x_m}(x_{m-1})).$$

By relations (2.19), (2.9), and the defining relations in $(A(X,r),+)$, we get that

$$\begin{aligned}
&\pi(\lambda_{x_1}(x_2)\circ\rho_{x_2}(x_1)\circ x_3\circ\cdots\circ x_m)\\
&=\lambda_{x_1}(x_2)+\lambda'_{\lambda_{x_1}(x_2)}(\pi(\rho_{x_2}(x_1)\circ x_3\circ\cdots\circ x_m))\\
&=\lambda_{x_1}(x_2)+\lambda'_{\lambda_{x_1}(x_2)}(\rho_{x_2}(x_1)+\lambda'_{\rho_{x_2}(x_1)}(\pi(x_3\circ\cdots\circ x_m)))\\
&=\lambda_{x_1}(x_2)+\lambda_{\lambda_{x_1}(x_2)}(\rho_{x_2}(x_1))+\lambda'_{\lambda_{x_1}(x_2)}(\lambda'_{\rho_{x_2}(x_1)}(\pi(x_3\circ\cdots\circ x_m)))\\
&=x_1+\lambda_{x_1}(x_2)+\lambda'_{\lambda_{x_1}(x_2)\circ\rho_{x_2}(x_1)}(\pi(x_3\circ\cdots\circ x_m))\\
&=x_1+\lambda_{x_1}(x_2)+\lambda'_{x_1\circ x_2}(\pi(x_3\circ\cdots\circ x_m))\\
&=x_1+\lambda_{x_1}(x_2)+\lambda'_{x_1}(\lambda'_{x_2}(\pi(x_3\circ\cdots\circ x_m)))\\
&=x_1+\lambda'_{x_1}(x_2+\lambda'_{x_2}(\pi(x_3\circ\cdots\circ x_m)))\\
&=x_1+\lambda'_{x_1}(\pi(x_2\circ\cdots\circ x_m))\\
&=\pi(x_1\circ x_2\circ\cdots\circ x_m),
\end{aligned}$$

and, by (2.20), (2.11), and the defining relations in $(A'(X,r),\oplus)$,

$$\begin{aligned}
&\pi'(x_1\circ\cdots\circ x_{m-2}\circ\lambda_{x_{m-1}}(x_m)\circ\rho_{x_m}(x_{m-1}))\\
&=\rho'_{\rho_{x_m}(x_{m-1})}(\pi'(x_1\circ\cdots\circ x_{m-2}\circ\lambda_{x_{m-1}}(x_m)))\oplus\rho_{x_m}(x_{m-1})\\
&=\rho'_{\rho_{x_m}(x_{m-1})}(\rho'_{\lambda_{x_{m-1}}(x_m)}(\pi'(x_1\circ\cdots\circ x_{m-2}))\oplus\lambda_{x_{m-1}}(x_m))\oplus\rho_{x_m}(x_{m-1})\\
&=\rho'_{\rho_{x_m}(x_{m-1})}(\rho'_{\lambda_{x_{m-1}}(x_m)}(\pi'(x_1\circ\cdots\circ x_{m-2})))\oplus\rho_{\rho_{x_m}(x_{m-1})}(\lambda_{x_{m-1}}(x_m))\oplus\rho_{x_m}(x_{m-1})\\
&=\rho'_{\lambda_{x_{m-1}}(x_m)\circ\rho_{x_m}(x_{m-1})}(\pi'(x_1\circ\cdots\circ x_{m-2}))\oplus\rho_{x_m}(x_{m-1})\oplus x_m\\
&=\rho'_{x_{m-1}\circ x_m}(\pi'(x_1\circ\cdots\circ x_{m-2}))\oplus\rho_{x_m}(x_{m-1})\oplus x_m\\
&=\rho'_{x_m}(\rho'_{x_{m-1}}(\pi'(x_1\circ\cdots\circ x_{m-2})))\oplus\rho_{x_m}(x_{m-1})\oplus x_m\\
&=\rho'_{x_m}(\rho'_{x_{m-1}}(\pi'(x_1\circ\cdots\circ x_{m-2}))\oplus x_{m-1})\oplus x_m\\
&=\rho'_{x_m}(\pi'(x_1\circ\cdots\circ x_{m-1}))\oplus x_m\\
&=\pi'(x_1\circ\cdots\circ x_{m-1}\circ x_m).
\end{aligned}$$

Thus, indeed, π and π' are well-defined.

We will prove that equations (2.17) and (2.18) are satisfied, for all $a,b\in M(X,r)$, by induction on length(a)+length(b). If either length$(a)=0$, or length$(b)=0$, or length$(a)=$ length$(b)=1$, then (2.17) and (2.18) follow by definition. Let $a,b\in M(X,r)\setminus\{1\}$ such that length$(a)+$length$(b)>2$ and assume that, for any $a',b'\in M(X,r)$ with length$(a')+$length$(b')<$length$(a)+$length(b), $\pi(a'\circ b')=\pi(a')+\lambda'_{a'}(\pi(b'))$ and $\pi'(a'\circ b')=\rho'_{b'}(\pi'(a'))\oplus\pi'(b')$ hold. Write $a=x\circ a'$ and $b=b'\circ y$ for some $x,y\in X$ and

$a', b' \in M(X,r)$. By (2.19) and the induction hypothesis,

$$\begin{aligned}\pi(a\circ b) &= \pi(x\circ a'\circ b)\\ &= x+\lambda'_x(\pi(a'\circ b))\\ &= x+\lambda'_x(\pi(a')+\lambda'_{a'}(\pi(b)))\\ &= x+\lambda'_x(\pi(a'))+\lambda'_x(\lambda'_{a'}(\pi(b)))\\ &= \pi(x\circ a')+\lambda'_{x\circ a'}(\pi(b))\\ &= \pi(a)+\lambda'_a(\pi(b)),\end{aligned}$$

and by (2.20) and the induction hypothesis,

$$\begin{aligned}\pi'(a\circ b) &= \pi'(a\circ b'\circ y)\\ &= \rho'_y(\pi'(a\circ b'))\oplus y\\ &= \rho'_y(\rho'_{b'}(\pi'(a))\oplus\pi'(b'))\oplus y\\ &= \rho'_y(\rho'_{b'}(\pi'(a)))\oplus\rho'_y(\pi'(b'))\oplus y\\ &= \rho'_{b'\circ y}(\pi'(a))\oplus\pi'(b'\circ y)\\ &= \rho'_b(\pi'(a))\oplus\pi'(b).\end{aligned}$$

Hence, (2.17) and (2.18) follow by induction. It is clear that π and π' are the unique 1-cocycles satisfying the hypothesis. Therefore, the result follows. □

The question whether this connection between the structure monoid and the derived monoids is bijective follows naturally.

Question 2.2.3. *When are the 1-cocycles π and π' bijective?*

In general, the 1-cocycles π and π' are not bijective. We provide an example where π is injective but not surjective, followed by an example where π and π' are neither injective nor surjective.

Example 2.2.4. *Let (X,r) be a set-theoretic solution of the Yang-Baxter equation, where $|X|>1$ and $r: X\times X\to X\times X$ is a map defined by $r(x,y)=(x,x)$, for all $x,y\in X$. The associated (derived) structure monoids are*

$$\begin{aligned}M(X,r)&=\langle X\mid x\circ y=x\circ x,\ \textit{for all } x,y\in X\rangle^1,\\ A(X,r)&=\langle X\mid x+x=x+x,\ \textit{for all } x,y\in X\rangle^1,\\ A'(X,r)&=\langle X\mid x\oplus y=x\oplus x,\ \textit{for all } x,y\in X\rangle^1.\end{aligned}$$

It is clear that the 1-cocycle $\pi'=M(X,r)\to A'(X,r)$ is bijective. Since $\pi(x\circ y)=x+x$, for all $x,y\in X$, it follows that the 1-cocycle $\pi: M(X,r)\to A(X,r)$ is not surjective, and hence not bijective. Note that π is still injective. The set-theoretic solution (X,r) with $r: X\times X\to X\times X$ defined by $r(x,y)=(y,y)$ is an example where π' is not surjective, and thus not bijective. In this example, π' is still injective.

Example 2.2.5. *Consider the distributive and cancellative skew lattice from Example 5.4.4, i.e. $S = \{0,1,2\}$, and the operation $\wedge$ and $\vee$ are defined by*

$$\begin{array}{c|ccc} \wedge & 0 & 1 & 2 \\ \hline 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 2 \\ 2 & 0 & 1 & 2 \end{array}, \qquad \begin{array}{c|ccc} \vee & 0 & 1 & 2 \\ \hline 0 & 0 & 1 & 2 \\ 1 & 1 & 1 & 1 \\ 2 & 2 & 2 & 2 \end{array}.$$

In Proposition 5.5.4 we prove that (S,r), where $r : S \times S \to S \times S$ is defined by $r(x,y) = (x \wedge y, y \vee x)$, for all $x, y \in S$, is a set-theoretic solution of the Yang-Baxter equation. The associated (derived) structure monoids are

$$\begin{aligned} M(X,r) &= \langle 0,1,2 \mid 1 \circ 0 = 0 \circ 1, 2 \circ 0 = 0 \circ 2, 1 \circ 2 = 2 \circ 2, 2 \circ 1 = 1 \circ 1 \rangle^1, \\ A(X,r) &= \langle 0,1,2 \mid 1 + 0 = 0 + 0 = 2 + 0, 1 + 2 = 2 + 2, 2 + 1 = 1 + 1 \rangle^1, \\ A'(X,r) &= \langle 0,1,2 \mid 1 \oplus 0 = 1 \oplus 1, 2 \oplus 0 = 2 \oplus 2 \rangle^1. \end{aligned}$$

Since $\pi(2 \circ 0) = 2 + 0 = 0 + 0 = \pi(0 \circ 0)$ and $\pi'(2 \circ 0) = 2 \oplus 0 = 2 \oplus 2 = \pi'(2 \circ 2)$, but $2 \circ 0 \neq 0 \circ 0$ and $2 \circ 0 \neq 2 \circ 2$ in $M(X,r)$, both π and π' are not injective. Furthermore, π is not surjective because $0 + 2$ is not in the image of π, while π' is not surjective since $0 \oplus 2$ is not in the image of π'.

Proposition 2.2.6. *Let (X,r) be a set-theoretic solution of the Yang-Baxter equation and $\pi : M(X,r) \to A(X,r)$ and $\pi' : M(X,r) \to A'(X,r)$ be the 1-cocycles of Theorem 2.2.2. Then,*

(1) π is surjective if and only if λ_x is surjective for all $x \in X$,

(2) π' is surjective if and only if ρ_x is surjective for all $x \in X$.

Proof. Suppose first that π is surjective. Let $x, y \in X$. We will show that there exists $y' \in X$ such that $\lambda_x(y') = y$, i.e. λ_x is surjective. Since $x + y \in A(X,r)$ and π is surjective (and it preserves the degree), there exist $z, t \in X$ such that $\pi(z \circ t) = x + y$. So, $z + \lambda_z(t) = x + y$ in $A(X,r)$. By the defining relations of $A(X,r)$, this equality implies that there exists $y' \in X$ such that $\lambda_x(y') = y$. Hence, λ_x is surjective for all $x \in X$.

Assume now that λ_x is surjective for all $x \in X$. First, we show that this implies that λ'_x is surjective, for all $x \in X$. Let $x, x_1, \dots, x_n \in X$, for an arbitrary positive integer n, such that $x_1 + \dots + x_n \in A(X,r)$. Since λ_x is surjective, there exist $y_1, \dots, y_n \in X$ such that $\lambda_x(y_i) = x_i$, for all $i \in \{1, \dots, n\}$. Thus, $\lambda'_x(y_1 + \dots + y_n) = \lambda_x(y_1) + \dots + \lambda_x(y_n) = x_1 + \dots + x_n$, which shows that λ'_x is surjective.

Next, we prove that π is surjective by induction on the length n of the elements in $A(X,r)$. For elements of length 1, the result follows by definition. Assume now that $n > 1$ and that for any $x_1, \dots, x_{n-1} \in X$, there exist $y_1, \dots, y_{n-1} \in X$ such that $\pi(y_1 \circ \dots \circ y_{n-1}) = x_1 + \dots + x_{n-1}$. Let $x_1, \dots, x_n \in X$. Since λ_{x_1} being surjective implies that λ'_{x_1} is surjective, there exists $z_2, \dots, z_n \in X$ such that $\lambda'_{x_1}(z_2 + \dots + z_n) = x_2 + \dots + x_n$. Using the induction hypotheses, there exists $y_2, \dots, y_n \in X$ such that $\pi(y_2 \circ \cdots \circ y_n) = z_2 + \cdots + z_n$. This yields

$$\begin{aligned} x_1 + \cdots + x_n &= x_1 + \lambda'_{x_1}(z_2 + \cdots + z_n) \\ &= \pi(x_1) + \lambda'_{x_1}(\pi(y_2 \circ \cdots \circ y_n)) \\ &= \pi(x_1 \circ y_2 \circ \cdots \circ y_n), \end{aligned}$$

and π is surjective.

The proof for π' is similar. □

The following result shows when the 1-cocycles π and π' of Theorem 2.2.2 are injective, namely when λ_x (resp. ρ_x) is injective, for all $x \in X$. Note that, in contrast to the previous result, the converse is not true. The set-theoretic solution of Example 2.2.4 provides a counterexample. In this solution, $\lambda_x(y) = x$ for all $x, y \in X$, so λ_x is not injective. Nevertheless, π is injective. Similarly, (X, r) with $r : X \times X \to X \times X$ defined by $r(x, y) = (y, y)$ is a set-theoretic solution of the Yang-Baxter equation with ρ_y not injective ($\rho_y(x) = y$ for all $x, y \in X$), but where π' is injective (see Example 2.2.4).

Let $w_1, w_2 \in \operatorname{FM}(X)$ be two elements of degree n, where $\operatorname{FM}(X)$ denotes the (multiplicative) free monoid on X. Suppose that $w_1 = z_1 \cdots z_n$ and $w_2 = t_1 \cdots t_n$, for some $z_i, t_i \in X$. We say that

$$w_1 \approx w_2,$$

if there exist $1 \le i \le n-1$ and $z \in X$ such that $z_j = t_j$, for all $j \in \{1, 2, \dots, n\} \setminus \{i, i+1\}$ and either $z_{i+1} = \lambda_{z_i}(z) = t_i$ and $t_{i+1} = \lambda_{\lambda_{z_i}(z)}\rho_z(z_i) = \lambda_{t_i}\rho_z(z_i)$, or $t_{i+1} = \lambda_{t_i}(z) = z_i$ and $z_{i+1} = \lambda_{\lambda_{t_i}(z)}\rho_z(t_i) = \lambda_{z_i}\rho_z(t_i)$. Note that $z_1 + \cdots + z_n = t_1 + \cdots + t_n$ in $A(X, r)$ if and only if $z_i = t_i$, for all $1 \le i \le n$, or there exist $w'_1, \dots, w'_m \in \operatorname{FM}(X)$ of degree n such that

$$w_1 = w'_1 \approx w'_2 \approx \cdots \approx w'_m = w_2,$$

with $w_1 = z_1 \cdots z_n, w_2 = t_1 \cdots t_n \in \operatorname{FM}(X)$.

Proposition 2.2.7. *Let (X, r) be a set-theoretic solution of the Yang-Baxter equation, and $\pi : M(X, r) \to A(X, r)$ and $\pi' : M(X, r) \to A'(X, r)$ be the 1-cocycles of Theorem 2.2.2.*

(1) If λ_x is injective for all $x \in X$, then π is injective.

(2) If ρ_x is injective for all $x \in X$, then π' is injective.

Proof. Assume that λ_x is injective, for all $x \in X$. Since $\pi(x) = x$ for all $x \in X$, the restriction of π to elements of length 1 in $M(X, r)$ is injective. Let $n > 1$, and $x_1, \dots, x_n, y_1, \dots, y_n \in X$ be elements such that $\pi(x_1 \circ \cdots \circ x_n) = \pi(y_1 \circ \cdots \circ y_n)$. Thus, in $A(X, r)$, we have that

$$x_1 + \lambda_{x_1}(x_2) + \cdots + \lambda_{x_1} \cdots \lambda_{x_{n-1}}(x_n) = y_1 + \lambda_{y_1}(y_2) + \cdots + \lambda_{y_1} \cdots \lambda_{y_{n-1}}(y_n).$$

So either $\lambda_{x_1}\cdots\lambda_{x_{i-1}}(x_i) = \lambda_{y_1}\cdots\lambda_{y_{i-1}}(y_i)$, for all $1 \leq i \leq n$, or there exist $w'_1,\dots,w'_m \in \mathrm{FM}(X)$ of degree n such that

$$w_1 = w'_1 \approx w'_2 \approx \cdots \approx w'_m = w_2,$$

with $w_1 = x_1\lambda_{x_1}(x_2)\cdots\lambda_{x_1}\cdots\lambda_{x_{n-1}}(x_n)$ and $w_2 = y_1\lambda_{y_1}(y_2)\cdots\lambda_{y_1}\cdots\lambda_{y_{n-1}}(y_n)$ elements of $\mathrm{FM}(X)$.

In the former case, using the injectivity of λ_x, for $x \in X$, we obtain $x_i = y_i$, for all $1 \leq i \leq n$.

It is enough to prove the latter case for $m = 2$, as the process can recursively be continued for $m > 2$. So assume $w_1 \approx w_2$, with $w_1, w_2 \in \mathrm{FM}(X)$ defined above. Thus, there exist $1 \leq i \leq n-1$ and $z \in X$ such that $\lambda_{x_1}\cdots\lambda_{x_{j-1}}(x_j) = \lambda_{y_1}\cdots\lambda_{y_{j-1}}(y_j)$, for all $j \in \{1,2,\dots,n\} \smallsetminus \{i,i+1\}$, and also

$$\lambda_{x_1}\cdots\lambda_{x_i}(x_{i+1}) = \lambda_{\lambda_{x_1}\cdots\lambda_{x_{i-1}}(x_i)}(z) = \lambda_{y_1}\cdots\lambda_{y_{i-1}}(y_i), \tag{2.21}$$

$$\lambda_{y_1}\cdots\lambda_{y_i}(y_{i+1}) = \lambda_{\lambda_{y_1}\cdots\lambda_{y_{i-1}}(y_i)}\rho_z(\lambda_{x_1}\cdots\lambda_{x_{i-1}}(x_i)). \tag{2.22}$$

The case where $\lambda_{y_1}\cdots\lambda_{y_i}(y_{i+1}) = \lambda_{\lambda_{y_1}\cdots\lambda_{y_{i-1}}(y_i)}(z) = \lambda_{x_1}\cdots\lambda_{x_{i-1}}(x_i)$ and $\lambda_{x_1}\cdots\lambda_{x_i}(x_{i+1}) = \lambda_{\lambda_{x_1}\cdots\lambda_{x_{i-1}}(x_i)}\rho_z(\lambda_{y_1}\cdots\lambda_{y_{i-1}}(y_i))$ is handled in a similar fashion.

Since $\lambda_{x_1}\cdots\lambda_{x_{j-1}}(x_j) = \lambda_{y_1}\cdots\lambda_{y_{j-1}}(y_j)$, for all $j \in \{1,2,\dots,n\} \smallsetminus \{i,i+1\}$, and λ_x is injective for all $x \in X$, we have that $x_j = y_j$, for all $j \in \{1,\dots,i-1\}$. Hence, as λ_x is injective for all $x \in X$, equation (2.21) implies that $y_i = \lambda_{x_i}(x_{i+1})$. Now, we have that

$$\begin{aligned}
\lambda_{\lambda_{x_1}\cdots\lambda_{x_{i-1}}(x_i)}(z) &= \lambda_{x_1}\cdots\lambda_{x_i}(x_{i+1}) \\
&= \lambda_{x_1\circ\cdots\circ x_i}(x_{i+1}) \\
&= \lambda_{\lambda_{x_1\circ\cdots\circ x_{i-1}}(x_i)\circ\rho_{x_i}(x_1\circ\cdots\circ x_{i-1})}(x_{i+1}) \\
&= \lambda_{\lambda_{x_1}\cdots\lambda_{x_{i-1}}(x_i)}\lambda_{\rho_{x_i}(x_1\circ\cdots\circ x_{i-1})}(x_{i+1}),
\end{aligned}$$

where the third equality follows by (2.7) and the fact that, by Theorem 2.1.1, the mapping $\lambda : M(X,r) \to \mathrm{Map}(M(X,r),M(X,r))$ is well-defined.

Hence, since λ_x is injective for all $x \in X$, we have that

$$z = \lambda_{\rho_{x_i}(x_1\circ\cdots\circ x_{i-1})}(x_{i+1}).$$

This yields, by using equations (2.22), (2.21), (1.18), Theorem 2.1.1, and the fact shown earlier that $x_j = y_j$, for all $j \in \{1,\dots,i-1\}$ and $y_i = \lambda_{x_i}(x_{i+1})$,

$$\begin{aligned}
\lambda_{y_1}\cdots\lambda_{y_i}(y_{i+1}) &= \lambda_{\lambda_{y_1}\cdots\lambda_{y_{i-1}}(y_i)}\rho_z(\lambda_{x_1}\cdots\lambda_{x_{i-1}}(x_i)) \\
&= \lambda_{\lambda_{x_1}\cdots\lambda_{x_{i-1}}(\lambda_{x_i}(x_{i+1}))}\rho_z(\lambda_{x_1}\cdots\lambda_{x_{i-1}}(x_i)) \\
&= \lambda_{\lambda_{x_1\circ\cdots\circ x_{i-1}}(\lambda_{x_i}(x_{i+1}))}\rho_{\lambda_{\rho_{x_i}(x_1\circ\cdots\circ x_{i-1})}(x_{i+1})}(\lambda_{x_1\circ\cdots\circ x_{i-1}}(x_i)) \\
&= \lambda_{\lambda_{x_1\circ\cdots\circ x_{i-1}}(\lambda_{x_i}(x_{i+1}))}\lambda_{\rho_{\lambda_{x_i}(x_{i+1})}(x_1\circ\cdots\circ x_{i-1})}(\rho_{x_{i+1}}(x_i)) \\
&= \lambda_{x_1\circ\cdots\circ x_{i-1}}\lambda_{\lambda_{x_i}(x_{i+1})}(\rho_{x_{i+1}}(x_i)) \\
&= \lambda_{y_1\circ\cdots\circ y_{i-1}}\lambda_{y_i}(\rho_{x_{i+1}}(x_i)) \\
&= \lambda_{y_1}\cdots\lambda_{y_{i-1}}\lambda_{y_i}(\rho_{x_{i+1}}(x_i)).
\end{aligned}$$

Since λ_x is injective for all $x \in X$, we have that $y_{i+1} = \rho_{x_{i+1}}(x_i)$. Thus,

$$y_i \circ y_{i+1} = \lambda_{x_i}(x_{i+1}) \circ \rho_{x_{i+1}}(x_i) = x_i \circ x_{i+1}.$$

Since $\lambda_{x_1} \cdots \lambda_{x_{j-1}}(x_j) = \lambda_{y_1} \cdots \lambda_{y_{j-1}}(y_j)$, for all $j \in \{1, 2, \dots, n\} \smallsetminus \{i, i+1\}$, and λ_x is injective for all $x \in X$, we have that $x_j = y_j$, for all $j \in \{i+2, \dots, n\}$. Hence $x_1 \circ \cdots \circ x_n = y_1 \circ \cdots \circ y_n$, and therefore, π is injective.

The proof of part (2) is similar. □

If π (resp. π') is injective, then it is clear that the map f (resp. f'), defined in Theorem 2.2.2, is an embedding. The latter is proven in [97] under the assumption that (X, r) is a left non-degenerate solution. In this case π is bijective and $M(X, r)$ is a regular submonoid of the semidirect product $A(X, r) \rtimes \mathrm{gr}(\lambda_x \mid x \in X)$. A similar result to Theorem 2.2.2 for groups was shown in [75, 101] for non-degenerate involutive solutions, and in [125, 135, 174] for bijective non-degenerate solutions. So for any bijective non-degenerate solution (X, r), we have that $G(X, r)$ is a regular subgroup of the semidirect product $A_{\mathrm{gr}}(X, r) \rtimes \mathrm{gr}(\lambda_x \mid x \in X)$.

The following result answers Question 2.2.3 for finite solutions.

Corollary 2.2.8 (Jespers, Kubat, and Van Antwerpen [97, Proposition 1.4])**.** *Let (X, r) be a set-theoretic solution of the Yang-Baxter equation, λ' (resp. ρ') the left (resp. right) action as defined before, π (resp. π') the unique 1-cocycle with respect to λ' (resp. ρ'). Then, π (resp. π') is bijective if (X, r) is left non-degenerate (resp. right non-degenerate). The converse holds if X is finite.*

Proof. Assume first that (X, r) is a left non-degenerate set-theoretic solution of the Yang-Baxter equation. Then, by Proposition 2.2.6 and Proposition 2.2.7, π is bijective. Similarly, one can prove that (X, r) being a right non-degenerate solution implies that π' is bijective.

Assume now that $\pi : M(X, r) \to A(X, r)$ is bijective and X is finite. By Proposition 2.2.6, λ_x is surjective for all $x \in X$. Since X is finite, λ_x is bijective for all $x \in X$, that is (X, r) is left non-degenerate. Similarly, one shows that if π' is bijective and X is finite, then (X, r) is right non-degenerate. □

The next example shows the difficulty of Question 2.2.3 for infinite solutions.

Example 2.2.9. *Let $r : \mathbb{N} \times \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ be the map defined by $r(x, y) = (f(y), f(x))$, for all $x, y \in \mathbb{N}$, where $f(x) = \max\{0, x - 1\}$, for all $x \in \mathbb{N}$. Then $(\mathbb{N}, r)$ is a set-theoretic solution of the Yang-Baxter equation. Indeed, it is easy to see that $(\mathbb{N}, r)$ is a solution, as for any $x, y, z \in X$,*

$$r_{12} r_{23} r_{12}(x, y, z) = (f^2(z), f^2(y), f^2(x)) = r_{23} r_{12} r_{23}(x, y, z).$$

Note that, for every $x \in \mathbb{N}$, $f^x(x) = 0$. Hence, the associated (derived) structure monoids *are*

$$\begin{aligned} M(\mathbb{N},r) &= \langle \mathbb{N} \mid x \circ y = 0 \circ 0 \rangle^1, \\ A(\mathbb{N},r) &= \langle \mathbb{N} \mid x + y = 0 + 0 \rangle^1, \\ A'(\mathbb{N},r) &= \langle \mathbb{N} \mid x \oplus y = 0 \oplus 0 \rangle^1. \end{aligned}$$

Therefore, for every integer $n > 1$, the monoids $M(\mathbb{N},r)$, $A(\mathbb{N},r)$ and $A'(\mathbb{N},r)$ have only one element of degree n. Since π and π' preserve the degree and $\pi(x) = x$ and $\pi'(x) = x$, for all $x \in \mathbb{N}$, we have that π and π' are bijective. However, for any $x \in \mathbb{N}$, $\lambda_x = \rho_x = f$ is not injective, because $f(0) = f(1)$.

Given a solution (X,r), the following proposition clarifies the link between the maps $\lambda' : M(X,r) \to \operatorname{Aut}(A(X,r),+)$ and $\lambda : M(X,r) \to \operatorname{Map}(M(X,r),M(X,r))$ as well as between the maps $\rho' : M(X,r) \to \operatorname{Aut}(A'(X,r),\oplus)$ and $\rho : M(X,r) \to \operatorname{Map}(M(X,r),M(X,r))$.

Proposition 2.2.10. *Let (X,r) be a set-theoretic solution of the Yang-Baxter equation. Then,*

$$\pi(\lambda_a(b)) = \lambda'_a(\pi(b)) \quad \textit{and} \quad \pi'(\rho_a(b)) = \rho'_a(\pi'(b)),$$

for all $a,b \in M(X,r)$.

Proof. Let $a,b \in M(X,r)$. First, we show for any $x \in X$ and $b \in M(X,r)$,

$$\pi(\lambda_x(b)) = \lambda'_x(\pi(b)), \tag{2.23}$$

by induction on the length of b. If $\operatorname{length}(b) = 1$, then

$$\pi(\lambda_x(b)) = \lambda_x(b) = \lambda_x(\pi(b)) = \lambda'_x(\pi(b)).$$

Assume that (2.23) holds for all elements $b \in M(X,r)$ of length at most n, with n a non-negative integer, and let $b \in M(X,r)$ be an element of length $n+1$. Write $b = y \circ b'$, where $y \in X$ and $b' \in M(X,r)$ is an element of length n. Then, by (2.1), Proposition 2.2.1, Theorem 2.2.2, and the induction hypothesis,

$$\begin{aligned} \pi(\lambda_x(b)) &= \pi(\lambda_x(y \circ b')) \\ &= \pi(\lambda_x(y) \circ \lambda_{\rho_y(x)}(b')) \\ &= \pi(\lambda_x(y)) + \lambda'_{\lambda_x(y)}(\pi(\lambda_{\rho_y(x)}(b'))) \\ &= \lambda'_x(\pi(y)) + \lambda'_{\lambda_x(y)}(\lambda'_{\rho_y(x)}(\pi(b'))) \\ &= \lambda'_x(\pi(y)) + \lambda'_x(\lambda'_y(\pi(b'))) \\ &= \lambda'_x(\pi(y) + \lambda'_y(\pi(b'))) \\ &= \lambda'_x(\pi(y \circ b')) \\ &= \lambda'_x(\pi(b)). \end{aligned}$$

Since both λ and λ' are homomorphisms, we obtain $\pi(\lambda_a(b)) = \lambda'_a(\pi(b))$, for all $a,b \in M(X,r)$, and the first claim follows. The second part can be proven similarly, hence the result. □

We end this chapter with an important remark on left and right non-degenerate solutions. This observation will be used frequently in the upcoming chapters.

Remark 2.2.11. *If (X, r) is a left non-degenerate set-theoretic solution of the Yang-Baxter equation, then Proposition 2.2.6 and Proposition 2.2.7 imply that $\pi : M(X, r) \to A(X, r)$ is bijective. This allows us to identify $M(X, r)$ and $A(X, r)$ via π, i.e. $a = \pi(a)$, for all $a \in M(X, r)$. Note also that with this identification, by Proposition 2.2.10, $\lambda'_a = \lambda_a$, for all $a \in M(X, r)$. Hence, $(M(X, r), +)$ is a semigroup, with $a \circ b = a + \lambda_a(b)$.*

Similarly, if (X, r) is a right non-degenerate set-theoretic solution of the Yang-Baxter equation, then Proposition 2.2.6 and Proposition 2.2.7 imply that $\pi' : M(X, r) \to A'(X, r)$ is bijective. Hence, one can identify $M(X, r)$ and $A'(X, r)$ via π', i.e. $a = \pi'(a)$, for all $a \in M(X, r)$. With this identification, by Proposition 2.2.10, $\rho'_a = \rho_a$, for all $a \in M(X, r)$. Thus, $(M(X, r), \oplus)$ is a semigroup, with $a \circ b = \rho_b(a) \oplus b$.

In case (X, r) is a non-degenerate set-theoretic solution of the Yang-Baxter equation, by the above, we get two semigroups $(M(X, r), +)$ and $(M(X, r), \oplus)$, a monoid homomorphism $\lambda = \lambda' : M(X, r) \to \operatorname{Map}(M(X, r), M(X, r))$, and a monoid anti-homomorphism $\rho = \rho' : M(X, r) \to \operatorname{Map}(M(X, r), M(X, r))$, with $\operatorname{Im}(\lambda) \subseteq \operatorname{Aut}(M(X, r), +)$ and $\operatorname{Im}(\rho) \subseteq \operatorname{Aut}(M(X, r), \oplus)$, satisfying (2.5), (2.6), and (2.7).

Chapter 3

Left non-degenerate solutions and YB-semitrusses

> My methods are really methods of working and thinking; this is why they have crept in everywhere anonymously.
>
> *Emmy Noether*

The study of set-theoretic solutions of the Yang-Baxter equation that are left non-degenerate but not necessarily right non-degenerate, involutive or bijective was initiated by Jespers, Kubat and Van Antwerpen in [97]. They prove among others the bijectiveness between the structure monoid and the left derived monoid, discussed in the previous chapter. Additionally, for some results, they focus on solutions that are also bijective and sometimes also finite. We will see later in this chapter that finite bijective left non-degenerate solutions are actually also right non-degenerate, and thus some results (for example [97, Theorem 2.7, Theorem 2.8, Proposition 4.2, Theorem 4.5] and [98, Theorem 3]) are proven for finite bijective non-degenerate solutions.

From Section 1.3, we know that left cancellative left semi-braces, q-cycle sets and shelves provide left non-degenerate set-theoretic solutions of the Yang-Baxter equation. In fact, q-cycle sets are in a bijective correspondence with left non-degenerate solutions (see Subsection 1.3.2). In [60] (Colazzo, Jespers, Van Antwerpen, and Verwimp), another algebraic structure is introduced to determine and analyze left non-degenerate set-theoretic solutions of the Yang-Baxter equation. In contrast to q-cycle sets, this algebraic structure, called a YB-semitruss, is an associative structure, so that structure monoids of left non-degenerate solutions are natural examples of YB-semitrusses.

To link braces and rings, Brzeziński introduced (skew) trusses and left semitrusses [26, 27]. The latter consists of two semigroup structures on a set with a relation between both operations. This relation interpolates between the left brace relation and the left distributivity law for rings. Natural examples of left semitrusses are structure monoids of left non-degenerate solutions [52, Example 5.2] (Cedó, Jespers, and Verwimp). In general, left semitrusses do not yield set-theoretic solutions of the Yang-Baxter equation. Following [60, Section 2] (Colazzo, Jespers, Van Antwerpen, and Verwimp), in the first section of this chapter, we give sufficient conditions for a left semitruss to produce a left non-degenerate set-theoretic solution of the Yang-Baxter equation, and we call such structures YB-semitrusses. It is also proven that all left non-degenerate solutions are restrictions of solutions associated to a YB-semitruss, and thus YB-semitrusses actually determine all left non-degenerate solutions.

The second section concerns the question, posed in [52] (Cedó, Jespers, and Verwimp), whether any finite non-degenerate set-theoretic solution of the Yang-Baxter equation is bijective. We will prove the affirmative answer, shown first in [60] (Colazzo, Jespers, Van Antwerpen, and Verwimp). For λ-irretractable solutions, i.e. solutions (X, r) where $\lambda_x = \lambda_y$ implies $x = y$, for all $x, y \in X$, the result was proven in [52, Theorem 4.5] (Cedó, Jespers, and Verwimp). The converse, whether finite bijective left non-degenerate set-theoretic solutions of the Yang-Baxter equation are also right non-degenerate, is proven to be true in [34], by Castelli, Catino, and Stefanelli. The latter was already shown for finite involutive left non-degenerate solutions, in [101, 161], but a counterexample was given for infinite involutive left non-degenerate solutions. The infinite bijective case remains an open question in the other direction (see [52, Question 4.3] (Cedó, Jespers, and Verwimp)).

Question 3.0.1. *Is any (infinite) non-degenerate set-theoretic solution of the Yang-Baxter equation bijective (or even involutive)?*

For bijective non-degenerate set-theoretic solutions of the Yang-Baxter equation (X, r), with r denoted by (1.16), one can naturally define an equivalence relation on X by

$$x \sim y \text{ if and only if } \lambda_x = \lambda_y \text{ and } \rho_x = \rho_y.$$

This relation induces a solution $\mathrm{Ret}(X, r) = (X/\sim, \overline{r})$, called the retract solution of (X, r). This has first been shown for non-degenerate involutive solutions [75], and later generalized to (finite) bijective non-degenerate solutions [125, 47], see also Section 4.4. In Section 3.3, we introduce the retract relation for arbitrary non-degenerate set-theoretic solutions of the Yang-Baxter equation, following [60, Section 4] (Colazzo, Jespers, Van Antwerpen, and Verwimp).

The final section of this chapter is devoted to the algebraic structure of unital YB-semitrusses, following [60, Section 5] (Colazzo, Jespers, Van Antwerpen, and Verwimp). More precisely, we study the structure algebra $K[(M(X, r), +)]$ for finite left non-degenerate solutions, where the addition comes from the YB-semitruss structure on $M(X, r)$. In particular, we prove that the structure algebra is left Noetherian PI of finite Gelfand-Kirillov dimension. Furthermore, we give an application to $K[(M(X, r), \circ)]$ in case (X, r) is a finite left non-degenerate solution with bijective diagonal map $\mathfrak{q} : X \to X : x \mapsto \lambda_x^{-1}(x)$. For finite bijective non-degenerate solutions, these results are proven in [97, 98]. We end this section by studying a specific case of a YB-semitruss and show that its derived solution is determined by bijective non-degenerate solutions.

3.1 Left non-degenerate solutions and YB-semitrusses

Since braces were introduced as a generalization of Jacobson radical rings, and consist of a specific brace relation between the two group operations, the natural question arises how the brace relation and distributive law of rings are connected. Therefore, in [27], Brzeziński introduced the notion of a skew truss as a set with a group and semigroup structure that are connected via a particular law that interpolates between the brace relation and the distributivity law. More precisely, a *skew left truss* is a set A with two binary operations $+$ and $\circ$, such that $(A,+)$ is a group, $(A,\circ)$ is a semigroup, and

$$a\circ(b+c)=(a\circ b)-\alpha(a)+(a\circ c),$$

for all $a,b,c\in A$, where $\alpha : A\to A$ is a function. By taking $\alpha=\mathrm{id}_A$, one recovers the brace relation, and choosing $\alpha : A\to A : a\mapsto 0$, with 0 the neutral element of $(A,+)$, one retrieves the left distributivity law. If $(A,\circ)$ is a group, it is possible to define a bijective non-degenerate solution of the Yang-Baxter equation, via skew braces [27].

Generalizing this idea, Brzeziński introduced a *left semitruss* [26] as a set A with two semigroup structures $(A,\circ)$ and $(A,+)$, and a function $\lambda : A\to \mathrm{Map}(A,A) : a\mapsto \lambda_a$, such that

$$a\circ(b+c)=(a\circ b)+\lambda_a(c), \tag{3.1}$$

for all $a,b,c\in A$. The semigroup $(A,+)$ is called the additive semigroup and $(A,\circ)$ the multiplicative semigroup of the left semitruss, and the relation (3.1) is called the left semitruss identity. We denote the left semitruss by $(A,+,\circ,\lambda)$. Taking $\lambda_a(c)=a\circ c$ we obtain the left distributivity law, and by putting $\lambda_a(c)=a\circ(\overline{a}+c)$, with $\overline{a}$ the inverse of a in $(A,\circ)$ if one assumes it is a group, one recovers the (semi-)brace relation (1.22), providing us some first examples of left semitrusses.

Natural examples of left semitrusses arise from semigroups $(A,+)$ with a map $\lambda : A\to \mathrm{End}(A,+) : a\mapsto\lambda_a$ such that $\lambda_a\lambda_b=\lambda_{a+\lambda_a(b)}$, for all $a,b\in A$. Then $(A,+,\circ,\lambda)$ is a left semitruss if we define $a\circ b=a+\lambda_a(b)$, for all $a,b\in A$. In this case, one can define the semigroup monomorphism $f:(A,\circ)\to(A,+)\rtimes\mathrm{End}(A,+) : a\mapsto(a,\lambda_a)$, with $(a,\lambda_a)\circ(b,\lambda_b):=(a+\lambda_a(b),\lambda_a\lambda_b)=(a\circ b,\lambda_{a+\lambda_a(b)})=(a\circ b,\lambda_{a\circ b})$. The left semitruss structure of $(A,+,\circ,\lambda)$ can be translated into the set $\{(a,\lambda_a)\mid a\in A\}$, by defining $(a,\lambda_a)+(b,\lambda_b):=(a+b,\lambda_{a+b})$ and $\lambda_{(a,\lambda_a)}(b,\lambda_b):=(\lambda_a(b),\lambda_{\lambda_a(b)})$. Then f becomes a homomorphism between the two left semitrusses, i.e. $f(a+b)=f(a)+f(b), f(a\circ b)=f(a)\circ f(b)$ and $f(\lambda_a(b))=\lambda_{f(a)}(f(b))$. Again we get $(a,\lambda_a)\circ(b,\lambda_b)=(a,\lambda_a)+\lambda_{(a,\lambda_a)}(b,\lambda_b)$. Note that these special semigroups of $(A,+)\rtimes\mathrm{End}(A,+)$ have a similar flavor to regular subgroups of the holomorph of a group (see before Corollary 2.2.8).

Other natural examples of left semitrusses come from left non-degenerate set-theoretic solutions of the Yang-Baxter equation.

Example 3.1.1. *Let (X,r) be a left non-degenerate set-theoretic solution of the Yang-Baxter equation. Recall from Remark 2.2.11 that we can identify $M(X,r)$ and $A(X,r)$ via the bijective 1-cocycle π, that is $a=\pi(a)$ for all $a\in M(X,r)$, such that $\lambda_a=\lambda'_a$, for all $a\in M(X,r)$. With this identification, we obtain a semigroup operation $+$ on*

$M(X,r)$, defined by $a+b=a\circ\lambda_a^{-1}(b)$, for all $a,b\in M(X,r)$, and $\lambda_a\in\mathrm{Aut}(M(X,r),+)$, for all $a\in M(X,r)$. Now, we claim that $(M(X,r),+,\circ,\lambda)$ is a left semitruss. Let $a,b,c\in M(X,r)$. Then,

$$a\circ(b+c)=a+\lambda_a(b+c)=a+\lambda_a(b)+\lambda_a(c)=(a\circ b)+\lambda_a(c).$$

So, (3.1) holds, and $(M(X,r),+,\circ,\lambda)$ is indeed a left semitruss. Furthermore, $M(X,r)+a\subseteq a+M(X,r)$, for all $a\in M(X,r)$. Note that if, moreover, r is bijective then, by Remark 2.2.11, the left derived solution (X,s) is also right non-degenerate, and thus $M(X,r)+a=a+M(X,r)$, for all $a\in M(X,r)$, i.e. $(M(X,r),+)$ consists of normal elements. As shown in [97], this property is fundamental in the study of the associated structure algebra $K[M(X,r),+]$, where K is a field.

In general, left semitrusses do not necessarily yield set-theoretic solutions of the Yang-Baxter equation, in the sense of (skew) left braces or left cancellative left semi-braces (see Subsection 1.3.1). In this section, we determine sufficient conditions for a left semitruss to produce a left non-degenerate set-theoretic solution of the Yang-Baxter equation, and call the structure a YB-semitruss. We also show that all left non-degenerate set-theoretic solutions of the Yang-Baxter equation are determined by YB-semitrusses, by showing that the structure monoid of a left non-degenerate solutions is a natural example of a YB-semitruss. After that, we study YB-semitrusses with a left cancellative additive semigroup and provide several examples, such as left cancellative semi-braces, skew left braces, and, given a left non-degenerate solution, a left cancellative image of its structure monoid. We investigate idempotents in YB-semitrusses and provide a sufficient assumption for a YB-semitruss to be a skew left brace and hence provide a bijective non-degenerate solution of the Yang-Baxter equation. We finish this section by defining the matched product of YB-semitrusses and their solutions.

In [26, 52, 61], specific subclasses of left semitrusses are studied that yield left non-degenerate set-theoretic solutions of the Yang-Baxter equation. However, not every left non-degenerate solution can be obtained in this way. To resolve this for all left non-degenerate solutions, we define the following subclass of left semitrusses. Strictly speaking these should be called left non-degenerate YB-left semitrusses, but for simplicity reasons we call them YB-semitrusses. In Subsection 3.1.1 we show that they determine all left non-degenerate solutions.

Definition 3.1.2. *A tuple $(A,+,\circ,\lambda,\sigma)$ is said to be a* YB-semitruss *if $(A,+,\circ,\lambda)$ is a left semitruss and $\sigma: A\to\mathrm{Map}(A,A): a\mapsto\sigma_a$ is map such that, for any $a,b,c\in A$,*

$$\lambda_a\in\mathrm{Aut}(A,+)\ \text{and}\ \lambda_a\lambda_b=\lambda_{a\circ b}, \tag{3.2}$$
$$a+\lambda_a(b)=a\circ b, \tag{3.3}$$
$$a+b=b+\sigma_b(a), \tag{3.4}$$
$$\sigma_a\in\mathrm{End}(A,+)\ \text{and}\ \sigma_{a+b}=\sigma_b\,\sigma_a, \tag{3.5}$$
$$\sigma_{\lambda_a(c)}\,\lambda_a(b)=\lambda_a\,\sigma_c(b). \tag{3.6}$$

The map $\lambda : (A, \circ) \to \mathrm{Aut}(A, +) : a \mapsto \lambda_a$ is thus a semigroup homomorphism, called the λ-map *of the YB-semitruss, and the map $\sigma : (A, +) \to \mathrm{End}(A, +) : a \mapsto \sigma_a$ is a semigroup anti-homomorphism, called the* σ-map *of the YB-semitruss.*

Let $(A, +)$ be a semigroup such that there exists a map $\sigma : A \to \mathrm{Map}(A, A) : a \mapsto \sigma_a$ satisfying (3.4) and (3.5). Then, $(A, +, +, \iota, \sigma)$ with $\iota : A \to \mathrm{Aut}(A, +) : a \mapsto \mathrm{id}_A$ is a YB-semitruss called the *trivial YB-semitruss* on $(A, +)$. If, for example, $(A, +)$ is an abelian semigroup, then we can take $\sigma_a = \mathrm{id}_A$, for all $a \in A$. If $(A, +, \circ, \lambda, \sigma)$ and $(B, +', \circ', \lambda', \sigma')$ are YB-semitrusses with B a subset of A, and $a +' b = a + b$, $a \circ' b = a \circ b$, $\lambda'_a = \lambda_a$, and $\sigma'_a = \sigma_a$, for all $a, b \in B$, then B is called a *sub-YB-semitruss* of A.

Previously, we saw that for a semigroup $(A, +)$, certain λ-maps, and $a \circ b = a + \lambda_a(b)$, a regular subsemigroup of $(A, +) \rtimes \mathrm{End}(A, +)$ of the type $\{(a, \lambda_a) \mid a \in A\}$ gives an example of a left semitrusses, where $(a, \lambda_a) \circ (b, \lambda_b) := (a + \lambda_a(b), \lambda_a \lambda_b)$, $(a, \lambda_a) + (b, \lambda_b) := (a + b, \lambda_{a+b})$ and $\lambda_{(a,\lambda_a)}(b, \lambda_b) := (\lambda_a(b), \lambda_{\lambda_a(b)})$. In case $(A, +)$ is an abelian semigroup and $\lambda_a \in \mathrm{Aut}(A, +)$, for all $a \in A$, we can put $\sigma_a = \mathrm{id}_A$, and obtain examples of YB-semitrusses. Specific examples in this context are semigroups of I-type, an algebraic structure that describes non-degenerate involutive set-theoretic solutions, studied in [88, 101]. In this case, the semigroup of I-type plays the roll of $(A, \circ)$ and $(A, +)$ is a free abelian semigroup.

Another example comes from strong semi-braces [169], see also Subsection 1.3.1. A strong semi-brace with $(A, \cdot)$ a cycle set yields an example of a YB-semitruss, by taking $(A, +, \circ^{op}, \lambda, \iota)$, with $a + b = (a \cdot b) \circ a$, the λ-map is the inverse of the left multiplication and $\iota_a = \mathrm{id}_A$ (so $(A, +)$ is abelian). Later, we will provide other natural examples of YB-semitrusses by looking at the structure monoid of left non-degenerate set-theoretic solutions of the Yang-Baxter equation.

Condition (3.3) links the additive structure of a YB-semitruss with its multiplicative structure. Furthermore, for a YB-semitruss $(A, +, \circ, \lambda, \sigma)$, (3.4) implies that $A + b \subseteq b + A$, so right ideals in the semigroup $(A, +)$ are two-sided ideals. If, moreover, each σ_b is bijective, then $A + b = b + A$, i.e. every element of A is a normal element. The latter is an essential property to describe the structure monoids of bijective non-degenerate solutions, see for example [97].

Later, in Proposition 3.1.3, we will show how to associate a left non-degenerate set-theoretic solution to a YB-semitruss. It will be clear that the first part of condition (3.5) is not really needed to prove this result. However, in Theorem 3.1.13 we will show that, without loss of generality, to deal with an arbitrary left non-degenerate we may assume that (3.5) holds.

Recall from Chapter 2 that for a set X and a map $r : X \times X \to X \times X : (x, y) \mapsto (\lambda_x(y), \rho_y(x))$, the pair (X, r) is a set-theoretic solution of the Yang-Baxter equation if and only if equations (1.17), (1.18), and (1.19) are satisfied, i.e. for all $x, y, z \in X$,

$$\begin{aligned} \lambda_x \lambda_y(z) &= \lambda_{\lambda_x(y)} \lambda_{\rho_y(x)}(z), \\ \lambda_{\rho_{\lambda_y(z)}(x)} \rho_z(y) &= \rho_{\lambda_{\rho_y(x)}(z)} \lambda_x(y), \\ \rho_z \rho_y(x) &= \rho_{\rho_z(y)} \rho_{\lambda_y(z)}(x). \end{aligned}$$

Given a YB-semitruss $(A,+,\circ,\lambda,\sigma)$, by condition (3.4) and the second part of (3.5), we obtain, for all $a,b\in A$,

$$\sigma_a\,\sigma_b=\sigma_{b+a}=\sigma_{a+\sigma_a(b)}=\sigma_{\sigma_a(b)}\,\sigma_a\,. \tag{3.7}$$

Because of the equations (1.17), (1.18) and (1.19), equation (3.7) is equivalent to saying that the map

$$s_A:A\times A\to A\times A:(a,b)\mapsto(b,\sigma_b(a)), \tag{3.8}$$

is a (left non-degenerate) set-theoretic solution of the Yang-Baxter equation. We call it the *associated (left) derived solution of the YB-semitruss A* in accordance with the definition of a left derived solution in Section 2.2.

The other requirements in Definition 3.1.2 are justified in the following proposition. Let $(A,+,\circ,\lambda)$ be a left semitruss such that $\lambda:(A,\circ)\to\operatorname{Aut}(A,+):a\mapsto\lambda_a$ is a homomorphism, and with an additional map $\sigma:A\to\operatorname{Map}(A,A)$ satisfying $a+b=b+\sigma_b(a)$, for all $a,b\in A$ (i.e. condition (3.4) holds). An example of such a left semitruss is a YB-semitruss. Define the *ρ-map* of A as the map

$$\rho:A\to\operatorname{Map}(A,A):a\mapsto\rho_a,$$

with, for all $a,b\in A$,

$$\rho_b(a)=\lambda^{-1}_{\lambda_a(b)}\,\sigma_{\lambda_a(b)}(a). \tag{3.9}$$

In [52, Proposition 5.4] (Cedó, Jespers, and Verwimp), it was shown that a left semitruss $(A,+,\circ,\lambda)$ satisfying (3.2), and such that for any $a,b\in A$, $\sigma_b(a)\in A$ is unique, yields a left non-degenerate set-theoretic solution of the Yang-Baxter equation. We will now generalize this result, not assuming that $\sigma_b(a)$ is unique, for all $a,b\in A$. The proof follows the same main idea as the proofs of [97, Proposition 2.2] and [174, Theorem 2.3].

Proposition 3.1.3. *Let $(A,+,\circ,\lambda)$ be a left semitruss with $\lambda:(A,\circ)\to\operatorname{Aut}(A,+):a\mapsto\lambda_a$ a homomorphism satisfying (3.3). Let $\sigma:A\to\operatorname{Map}(A,A):a\mapsto\sigma_a$ be a map satisfying condition (3.4) and the second part of (3.5), i.e. $a+b=b+\sigma_b(a)$ and $\sigma_{a+b}=\sigma_b\,\sigma_a$, for all $a,b\in A$. Then,*

$$r_A:A\times A\to A\times A:(a,b)\mapsto(\lambda_a(b),\rho_b(a)), \tag{3.10}$$

with ρ-map defined by (3.9), is a (left non-degenerate) solution if and only if condition (3.6) holds, i.e. $\sigma_{\lambda_a(b)}\,\lambda_a=\lambda_a\,\sigma_b$, for all $a,b\in A$.

Furthermore, if $(A,+,\circ,\lambda,\sigma)$ is a YB-semitruss, then $r_A=\varphi^{-1}s_A\varphi$, where $\varphi:A\times A\to A\times A:(a,b)\mapsto(a,\lambda_a(b))$. In particular, r_A is bijective if and only if s_A is bijective, or equivalently s_A is (right) non-degenerate (i.e. all maps σ_a are bijective).

Proof. Let $J:A\times A\times A\to A\times A\times A$ be the map defined by $J(a,b,c)=(a,\lambda_a(b),\lambda_a\lambda_b(c))$. Clearly J is bijective and $J^{-1}(a,b,c)=(a,\lambda_a^{-1}(b),\lambda^{-1}_{\lambda_a^{-1}(b)}\lambda_a^{-1}(c))$, for all $a,b,c\in A$. By

(3.3) and (3.4), $\lambda_a(b) \circ \lambda^{-1}_{\lambda_a(b)}\,\sigma_{\lambda_a(b)}(a) = \lambda_a(b) + \sigma_{\lambda_a(b)}(a) = a + \lambda_a(b) = a \circ b$, and we get

$$\begin{aligned}
J^{-1}(s_A \times \mathrm{id}_A)J(a,b,c) &= J^{-1}(s_A \times \mathrm{id}_A)(a, \lambda_a(b), \lambda_a\lambda_b(c)) \\
&= J^{-1}(\lambda_a(b), \sigma_{\lambda_a(b)}(a), \lambda_a\lambda_b(c)) \\
&= (\lambda_a(b), \lambda^{-1}_{\lambda_a(b)}\,\sigma_{\lambda_a(b)}(a), \lambda^{-1}_{\lambda^{-1}_{\lambda_a(b)}\,\sigma_{\lambda_a(b)}(a)}\lambda^{-1}_{\lambda_a(b)}\lambda_a\lambda_b(c)) \\
&= (\lambda_a(b), \lambda^{-1}_{\lambda_a(b)}\,\sigma_{\lambda_a(b)}(a), \lambda^{-1}_{\lambda_a(b)\circ\lambda^{-1}_{\lambda_a(b)}\,\sigma_{\lambda_a(b)}(a)}\lambda_{a\circ b}(c)) \\
&= (\lambda_a(b), \lambda^{-1}_{\lambda_a(b)}\,\sigma_{\lambda_a(b)}(a), \lambda^{-1}_{a\circ b}\lambda_{a\circ b}(c)) \\
&= (\lambda_a(b), \lambda^{-1}_{\lambda_a(b)}\,\sigma_{\lambda_a(b)}(a), c) \\
&= (\lambda_a(b), \rho_b(a), c).
\end{aligned}$$

Hence, $J^{-1}(s_A \times \mathrm{id}_A)J = r_A \times \mathrm{id}_A$. Moreover, if condition (3.6) holds, then

$$\begin{aligned}
J^{-1}(\mathrm{id}_A \times s_A)J(a,b,c) &= J^{-1}(\mathrm{id}_A \times s_A)(a, \lambda_a(b), \lambda_a\lambda_b(c)) \\
&= J^{-1}(a, \lambda_a\lambda_b(c), \sigma_{\lambda_a\lambda_b(c)}\,\lambda_a(b)) \\
&= (a, \lambda_a^{-1}\lambda_a\lambda_b(c), \lambda^{-1}_{\lambda_a^{-1}\lambda_a\lambda_b(c)}\lambda_a^{-1}\,\sigma_{\lambda_a\lambda_b(c)}\,\lambda_a(b)) \\
&= (a, \lambda_b(c), \lambda^{-1}_{\lambda_b(c)}\lambda_a^{-1}\lambda_a\,\sigma_{\lambda_b(c)}(b)) \\
&= (a, \lambda_b(c), \lambda^{-1}_{\lambda_b(c)}\,\sigma_{\lambda_b(c)}(b)) \\
&= (a, \lambda_b(c), \rho_c(b)),
\end{aligned}$$

yields $J^{-1}(\mathrm{id}_A \times s_A)J = \mathrm{id}_A \times r_A$. As mentioned earlier, by (3.4) and the second part of (3.5), condition (3.7) holds, and we get that (A, s_A) is a solution, and thus also (A, r_A) is a solution.

Conversely, assume that (A, r_A) is a left non-degenerate solution. By definition of the ρ-map we obtain that $\sigma_b(a) = \lambda_b\rho_{\lambda_a^{-1}(b)}(a)$ and

$$\begin{aligned}
\sigma_{\lambda_a(b)}(\lambda_a(c)) &= \lambda_{\lambda_a(b)}\rho_{\lambda^{-1}_{\lambda_a(c)}\lambda_a(b)}\lambda_a(c) \\
&= \lambda_{\lambda_a(b)}\rho_{\lambda_{\rho_c(a)}\lambda_c^{-1}(b)}\lambda_a(c) && \text{by (1.17)} \\
&= \lambda_{\lambda_a(b)}\lambda_{\rho_{\lambda_c\lambda_c^{-1}(b)}(a)}\rho_{\lambda_c^{-1}(b)}(c) && \text{by (1.18)} \\
&= \lambda_{\lambda_a(b)}\lambda_{\rho_b(a)}\rho_{\lambda_c^{-1}(b)}(c) \\
&= \lambda_a\lambda_b\rho_{\lambda_c^{-1}(b)}(c) && \text{by (1.17)} \\
&= \lambda_a\,\sigma_b(c).
\end{aligned}$$

Hence, condition (3.6) holds.

Finally, observe that $s_A = \varphi r_A \varphi^{-1}$ with $\varphi : A \times A \to A \times A : (a,b) \mapsto (a, \lambda_a(b))$ and the other claims follow. □

The previous proposition states that a left non-degenerate solution r_A can be determined by a conjugate of the derived solution s_A, by a mapping say φ. However,

φ is not an arbitrary permutation of $A \times A$. For bijective non-degenerate solutions it is called a Drinfeld twist [89]. More precisely, a Drinfeld twist on a bijective non-degenerate solution (X, r) is a triple (F, Φ, Ψ) of bijective maps $F : X \times X \to X \times X$ and $\Phi, \Psi : X \times X \times X \to X \times X \times X$ satisfying

$$\begin{aligned}(F \times \mathrm{id}_X)\Psi &= (\mathrm{id}_X \times F)\Phi,\\ \Phi(\mathrm{id}_X \times r) &= (\mathrm{id}_X \times r)\Phi,\\ \Psi(r \times \mathrm{id}_X) &= (r \times \mathrm{id}_X)\Psi.\end{aligned}$$

Given a Drinfeld twist (F, Φ, Ψ) on a bijective non-degenerate solution (X, r), there is another solution defined on X by FrF^{-1}, see [89, Theorem 2.1]. Furthermore, in the same paper, they show that there exists a Drinfeld twist between any two non-degenerate involutive solutions, as there is a Drinfeld twist between any non-degenerate involutive solution and the trivial solution defined by $r(x, y) = (y, x)$, for all $x, y \in X$.

For a YB-semitruss A, we call (A, r_A) or r_A its *associated solution.* Given a YB-semitruss $(A, +, \circ, \lambda, \sigma)$, note that s_A, defined by (3.8), is the associated solution of the trivial YB-semitruss $(A, +, +, \iota, \sigma)$, where $\iota : A \to \mathrm{Aut}(A, +) : a \mapsto \mathrm{id}_A$.

It turns out that if an associated solution is bijective then its inverse is the associated solution of a well-described YB-semitruss.

Proposition 3.1.4. *Let $(A, +, \circ, \lambda, \sigma)$ be a YB-semitruss with σ_a bijective for any $a \in A$, or equivalently by Proposition 3.1.3, the associated solution (A, r_A) is bijective. Then, for any $a, b \in A$,*

$$r_A^{-1}(a, b) = (\sigma_a^{-1}\,\lambda_a(b), \lambda^{-1}_{\sigma_a^{-1}\,\lambda_a(b)}(a)),$$

and (A, r_A^{-1}) is the solution associated to the YB-semitruss $(A, +^{op}, \circ, \overline{\lambda}, \overline{\sigma})$, with $\overline{\lambda}_a = \sigma_a^{-1}\,\lambda_a$, and $\overline{\sigma}_a = \sigma_a^{-1}$, for all $a \in A$. We call $(A, +^{op}, \circ, \overline{\lambda}, \overline{\sigma})$ the opposite YB-semitruss *of the YB-semitruss $(A, +, \circ, \lambda, \sigma)$.*

In particular, for a YB-semitruss $(A, +, \circ, \lambda, \sigma)$, the associated solution (A, r_A) is involutive if and only if the associated derived solution (A, s_A) is trivial, i.e. all maps $\sigma_a = \mathrm{id}_A$.

Proof. Let $(A, +, \circ, \lambda, \sigma)$ be a YB-semitruss with σ_a bijective, for all $a \in A$. Its associated solution r_A is defined by, see (3.10), $r_A(a, b) = (\lambda_a(b), \lambda^{-1}_{\lambda_a(b)}\,\sigma_{\lambda_a(b)}(a))$. Define, for any $a, b \in A$, $r'(a, b) = (\sigma_a^{-1}\,\lambda_a(b), \lambda^{-1}_{\sigma_a^{-1}\,\lambda_a(b)}(a))$. Then, for any $a, b \in A$,

$$\begin{aligned}r_A r'(a, b) &= r(\sigma_a^{-1}\,\lambda_a(b), \lambda^{-1}_{\sigma_a^{-1}\,\lambda_a(b)}(a))\\ &= (\lambda_{\sigma_a^{-1}\,\lambda_a(b)}\lambda^{-1}_{\sigma_a^{-1}\,\lambda_a(b)}(a), \lambda^{-1}_{\lambda_{\sigma_a^{-1}\,\lambda_a(b)}\lambda^{-1}_{\sigma_a^{-1}\,\lambda_a(b)}(a)}\,\sigma_{\lambda_{\sigma_a^{-1}\,\lambda_a(b)}\lambda^{-1}_{\sigma_a^{-1}\,\lambda_a(b)}(a)}\,\sigma_a^{-1}\,\lambda_a(b))\\ &= (a, \lambda_a^{-1}\,\sigma_a\,\sigma_a^{-1}\,\lambda_a(b))\\ &= (a, b),\end{aligned}$$

and

$$\begin{aligned} r' r_A(a,b) &= r'(\lambda_a(b), \lambda^{-1}_{\lambda_a(b)}\, \sigma_{\lambda_a(b)}(a)) \\ &= (\sigma^{-1}_{\lambda_a(b)}\, \lambda_{\lambda_a(b)} \lambda^{-1}_{\lambda_a(b)}\, \sigma_{\lambda_a(b)}(a), \lambda^{-1}_{\sigma^{-1}_{\lambda_a(b)}\, \lambda_{\lambda_a(b)} \lambda^{-1}_{\lambda_a(b)}\, \sigma_{\lambda_a(b)}(a)} \lambda_a(b)) \\ &= (a,b). \end{aligned}$$

So indeed, $r' = r_A^{-1}$.

Now, assume that $(A, +^{\text{op}}, \circ, \overline{\lambda}, \overline{\sigma})$, with $\overline{\lambda}_a = \sigma_a^{-1}\, \lambda_a$ and $\overline{\sigma}_a = \sigma_a^{-1}$, is a YB-semitruss. Its associated solution, denoted by (A, r'_A), is given by

$$\begin{aligned} r'_A(a,b) &= (\overline{\lambda}_a(b), \overline{\lambda}^{-1}_{\overline{\lambda}_a(b)} \overline{\sigma}_{\overline{\lambda}_a(b)}(a)) \\ &= (\sigma_a^{-1}\, \lambda_a(b), \lambda^{-1}_{\sigma_a^{-1}\, \lambda_a(b)}\, \sigma_{\sigma_a^{-1}\, \lambda_a(b)}\, \sigma^{-1}_{\sigma_a^{-1}\, \lambda_a(b)}(a)) \\ &= (\sigma_a^{-1}\, \lambda_a(b), \lambda^{-1}_{\sigma_a^{-1}\, \lambda_a(b)}(a)) \\ &= r_A^{-1}(a,b). \end{aligned}$$

So, it remains to prove that $(A, +^{\text{op}}, \circ, \overline{\lambda}, \overline{\sigma})$ is a YB-semitruss. Clearly, $(A, +^{\text{op}})$ and $(A, \circ)$ are semigroups, and $\overline{\lambda}_a \in \operatorname{Aut}(A, +^{\text{op}})$, for all $a \in A$. Furthermore, for any $a, b, c \in A$,

$$\begin{aligned} \overline{\lambda}_a \overline{\lambda}_b(c) &= \sigma_a^{-1}\, \lambda_a\, \sigma_b^{-1}\, \lambda_b(c) \\ &= \sigma_a^{-1}\, \sigma^{-1}_{\lambda_a(b)}\, \lambda_a \lambda_b(c) && \text{by (3.6)} \\ &= (\sigma_{\lambda_a(b)}\, \sigma_a)^{-1} \lambda_{a \circ b}(c) && \text{by (3.2)} \\ &= \sigma^{-1}_{a + \lambda_a(b)}\, \lambda_{a \circ b}(c) && \text{by (3.5)} \\ &= \sigma^{-1}_{a \circ b}\, \lambda_{a \circ b}(c) && \text{by (3.3)} \\ &= \overline{\lambda}_{a \circ b}(c), \end{aligned}$$

so $\overline{\lambda} : (A, \circ) \to \operatorname{Aut}(A, +^{\text{op}}) : a \mapsto \overline{\lambda}_a$ is a homomorphism. Also, for any $a \in A$, it is clear that $\overline{\sigma}_a \in \operatorname{Aut}(A, +^{\text{op}})$, and thus $\overline{\sigma} : (A, +^{\text{op}}) \to \operatorname{Map}(A, A) : a \mapsto \overline{\sigma}_a$ is a semigroup anti-homomorphism.

Since $(A, +, \circ, \lambda, \sigma)$ satisfies (3.4), we have that $a + b = b + \sigma_b(a)$, for all $a, b \in A$. Hence, also $\sigma_b^{-1}(a) + b = b + a$, or equivalently, $b +^{\text{op}} \sigma_b^{-1}(a) = a +^{\text{op}} b$, i.e. (3.4) holds for $(A, +^{\text{op}}, \circ, \overline{\lambda}, \overline{\sigma})$. Furthermore, as $(A, +, \circ, \lambda, \sigma)$ satisfies (3.3), and since (3.4) is satisfied for $(A, +^{\text{op}}, \circ, \overline{\lambda}, \overline{\sigma})$, we have, for any $a, b \in A$,

$$a +^{\text{op}} \overline{\lambda}_a(b) = a +^{\text{op}} \sigma_a^{-1}\, \lambda_a(b) = a +^{\text{op}} \overline{\sigma}_a \lambda_a(b) = \lambda_a(b) +^{\text{op}} a = a + \lambda_a(b) = a \circ b.$$

So, (3.3) holds for $(A,+^{\mathrm{op}},\circ,\overline{\lambda},\overline{\sigma})$. The previous computations yield

$$\begin{aligned}(a\circ b)+^{\mathrm{op}}\overline{\lambda}_a(c) &= (a\circ b)+^{\mathrm{op}}\overline{\lambda}_{a\circ b}\overline{\lambda}_b^{-1}(c)\\ &= (a\circ b)\circ\overline{\lambda}_b^{-1}(c)\\ &= a\circ(b\circ\overline{\lambda}_b^{-1}(c))\\ &= a\circ(b+^{\mathrm{op}}\overline{\lambda}_b\overline{\lambda}_b^{-1}(c))\\ &= a\circ(b+^{\mathrm{op}}c),\end{aligned}$$

thus the left semitruss identity (3.1) is satisfied. Finally, (3.6) yields $\sigma_{\lambda_a(b)}\,\lambda_a=\lambda_a\,\sigma_b$ and thus $\lambda_a\,\sigma_b^{-1}=\sigma^{-1}_{\lambda_a(b)}\,\lambda_a$. Hence, $\sigma_a^{-1}\,\lambda_a\,\sigma_b^{-1}=\sigma_a^{-1}\,\sigma^{-1}_{\lambda_a(b)}\,\lambda_a$. Equation (3.4) implies that $\sigma_a^{-1}(\lambda_a(b))+a=a+\lambda_a(b)$, and hence, by (3.7), we know that $\sigma_a^{-1}\,\sigma^{-1}_{\lambda_a(b)}=\sigma^{-1}_{\sigma_a^{-1}\,\lambda_a(b)}\,\sigma_a^{-1}$. Hence, $\overline{\lambda}_a\,\sigma_b^{-1}=\sigma^{-1}_{\overline{\lambda}_a(b)}\,\overline{\lambda}_a$. So, $(A,+^{\mathrm{op}},\circ,\overline{\lambda},\overline{\sigma})$ is a YB-semitruss, as desired. □

YB-semitrusses $(A,+,\circ,\lambda,\sigma)$ give some interesting relations, using their λ-map and ρ-map, on the semigroup $(A,\circ)$.

Proposition 3.1.5. *Let $(A,+,\circ,\lambda,\sigma)$ be a YB-semitruss, with ρ-map defined by (3.9). Then, for any $a,b,c\in A$,*

$$a\circ b=\lambda_a(b)\circ\rho_b(a), \tag{3.11}$$
$$\lambda_b(a\circ c)=\lambda_b(a)\circ\lambda_{\rho_a(b)}(c), \tag{3.12}$$
$$\rho_b(c\circ a)=\rho_{\lambda_a(b)}(c)\circ\rho_b(a). \tag{3.13}$$

Proof. Let $a,b,c\in A$. Then, by (3.3) and (3.4),

$$\lambda_a(b)\circ\rho_b(a)=\lambda_a(b)\circ\lambda^{-1}_{\lambda_a(b)}\,\sigma_{\lambda_a(b)}(a)=\lambda_a(b)+\sigma_{\lambda_a(b)}(a)=a+\lambda_a(b)=a\circ b.$$

Thus, by (3.2) and (3.3),

$$\begin{aligned}\lambda_b(a\circ c) &= \lambda_b(a+\lambda_a(c))=\lambda_b(a)+\lambda_b\lambda_a(c)\\ &= \lambda_b(a)+\lambda_{b\circ a}(c)=\lambda_b(a)+\lambda_{\lambda_b(a)\circ\rho_a(b)}(c)\\ &= \lambda_b(a)+\lambda_{\lambda_b(a)}\lambda_{\rho_a(b)}(c)\\ &= \lambda_b(a)\circ\lambda_{\rho_a(b)}(c).\end{aligned}$$

To prove (3.13), we first claim that

$$\rho_{\lambda^{-1}_{\lambda_a^{-1}(b)}\lambda_a^{-1}(c)}\lambda_a^{-1}(b)=\lambda^{-1}_{\rho_{\lambda_a^{-1}(c)}(a)}\rho_{\lambda_b^{-1}(c)}(b). \tag{3.14}$$

Indeed, by setting $x=\lambda_b^{-1}(c)$, $y=b$ and $z=a$ in (1.18), we obtain

$$\lambda_{\rho_{\lambda_b(\lambda_b^{-1}(c))}(a)}\rho_{\lambda_b^{-1}(c)}(b)=\rho_{\lambda_{\rho_b(a)}\lambda_b^{-1}(c)}\lambda_a(b).$$

Put $c = \lambda_a^{-1}(d)$ and $b = \lambda_a^{-1}(e)$. By (1.17), this yields

$$\begin{aligned}
\lambda_{\rho_{\lambda_a^{-1}(d)}(a)}\rho_{\lambda^{-1}_{\lambda_a^{-1}(e)}\lambda_a^{-1}(d)}\lambda_a^{-1}(e) &= \rho_{\lambda_{\rho_{\lambda_a^{-1}(e)}(a)}\lambda^{-1}_{\lambda_a^{-1}(e)}\lambda_a^{-1}(d)}\lambda_a\lambda_a^{-1}(e) \\
&= \rho_{\lambda^{-1}_{\lambda_a(\lambda_a^{-1}(e))}(d)}(e) \\
&= \rho_{\lambda_e^{-1}(d)}(e),
\end{aligned}$$

as desired.

Furthermore, using (3.3),

$$\sigma_a(b+c) = \lambda_a\rho_{\lambda^{-1}_{b+c}(a)}(b+c) = \lambda_a\rho_{\lambda^{-1}_{b\circ\lambda_b^{-1}(c)}(a)}(b\circ\lambda_b^{-1}(c)),$$

and,

$$\begin{aligned}
\sigma_a(b)+\sigma_a(c) &= \sigma_a(b)\circ\lambda^{-1}_{\sigma_a(b)}(\sigma_a(c)) \\
&= \lambda_a(\rho_{\lambda_b^{-1}(a)}(b))\circ\lambda^{-1}_{\lambda_a\rho_{\lambda_b^{-1}(a)}(b)}(\lambda_a(\rho_{\lambda_c^{-1}(a)}(c))) \\
&= \lambda_a(\rho_{\lambda_b^{-1}(a)}(b))\circ\lambda_{\rho_{\rho_{\lambda_b^{-1}(a)}(b)}(a)}(\lambda^{-1}_{\rho_{\lambda_b^{-1}(a)}(b)}(\rho_{\lambda_c^{-1}(a)}(c))) && \text{by (1.17)} \\
&= \lambda_a(\rho_{\lambda_b^{-1}(a)}(b))\circ\lambda_{\rho_{\rho_{\lambda_b^{-1}(a)}(b)}(a)}(\rho_{\lambda^{-1}_{\lambda_b^{-1}(c)}\lambda_b^{-1}(a)}(\lambda_b^{-1}(c))) && \text{by (3.14)} \\
&= \lambda_a(\rho_{\lambda_b^{-1}(a)}(b)\circ\rho_{\lambda^{-1}_{\lambda_b^{-1}(d)}\lambda_b^{-1}(a)}(\lambda_b^{-1}(c))) && \text{by (3.12)}.
\end{aligned}$$

Since σ_a is an additive homomorphism and λ_a is bijective, we get that

$$\rho_{\lambda^{-1}_{b\circ\lambda_b^{-1}(c)}(a)}(b\circ\lambda_b^{-1}(c)) = \rho_{\lambda_b^{-1}(a)}(b)\circ\rho_{\lambda^{-1}_{\lambda_b^{-1}(c)}\lambda_b^{-1}(a)}(\lambda_b^{-1}(c)).$$

Put $d = \lambda_b^{-1}(c)$ and $e = \lambda^{-1}_{b\circ d}(a)$. Then, the previous equality becomes, for arbitrary $b, d, e \in A$,

$$\rho_e(b\circ d) = \rho_{\lambda_b^{-1}\lambda_{b\circ d}(e)}(b)\circ\rho_e(d) = \rho_{\lambda_d(e)}(b)\circ\rho_e(d),$$

as desired. □

Using the previous result, we can prove that for any YB-semitruss its associated ρ-map, defined by (3.9), is an anti-homomorphism.

Lemma 3.1.6. *Let $(A,+,\circ,\lambda,\sigma)$ be a YB-semitruss with ρ-map defined by $\rho_b(a) = \lambda^{-1}_{\lambda_a(b)}\sigma_{\lambda_a(b)}(a)$, for all $a, b \in A$. Then, $\rho : (A,\circ) \to \mathrm{Map}(A,A) : a \mapsto \rho_a$ is an anti-homomorphism.*

Proof. Let $a, b, c \in A$. By (3.12), (3.5), (3.6), and (1.17),

$$\begin{aligned}
\rho_{b\circ a}(c) &= \lambda^{-1}_{\lambda_c(b\circ a)}\,\sigma_{\lambda_c(b\circ a)}(c)\\
&= \lambda^{-1}_{\lambda_c(b)\circ\lambda_{\rho_b(c)}(a)}\,\sigma_{\lambda_c(b+\lambda_b(a))}(c)\\
&= \lambda^{-1}_{\lambda_{\rho_b(c)}(a)}\lambda^{-1}_{\lambda_c(b)}\,\sigma_{\lambda_c(b)+\lambda_c\lambda_b(a)}(c)\\
&= \lambda^{-1}_{\lambda_{\rho_b(c)}(a)}\lambda^{-1}_{\lambda_c(b)}\,\sigma_{\lambda_c\lambda_b(a)}\,\sigma_{\lambda_c(b)}(c)\\
&= \lambda^{-1}_{\lambda_{\rho_b(c)}(a)}\,\sigma_{\lambda^{-1}_{\lambda_c(b)}\lambda_c\lambda_b(a)}\,\lambda^{-1}_{\lambda_c(b)}\,\sigma_{\lambda_c(b)}(c)\\
&= \lambda^{-1}_{\lambda_{\rho_b(c)}(a)}\,\sigma_{\lambda_{\rho_b(c)}(a)}\,\rho_b(c)\\
&= \rho_a\rho_b(c).
\end{aligned}$$

Hence, $\rho_{b\circ a}(c) = \rho_a\rho_b(c)$, as desired. □

In fact, the assumption that a YB-semitruss $(A, +, \circ, \lambda, \sigma)$ satisfies $\sigma_{a+b} = \sigma_b\,\sigma_a$, for all $a, b \in A$, also follows from the ρ-map being an anti-homomorphism. By the definition of the ρ-map of a YB-semitruss (3.9), we have $\sigma_b(a) = \lambda_b\rho_{\lambda_a^{-1}(b)}(a)$, for all $a, b \in A$. Hence, for any $a, b, c \in A$, using (1.17), (1.18) and that the ρ-map is an anti-homomorphism,

$$\begin{aligned}
\sigma_{a+b}(c) &= \lambda_{a+b}\rho_{\lambda_c^{-1}(a+b)}(c)\\
&= \lambda_a\lambda_{\lambda_a^{-1}(b)}\rho_{\lambda_c^{-1}(a)+\lambda_c^{-1}(b)}(c)\\
&= \lambda_b\lambda_{\rho_{\lambda_a^{-1}(b)}(a)}\rho_{\lambda_c^{-1}(a)\circ\lambda^{-1}_{\lambda_c^{-1}(a)}(\lambda_c^{-1}(b))}(c)\\
&= \lambda_b\lambda_{\rho_{\lambda_a^{-1}(b)}(a)}\rho_{\lambda^{-1}_{\lambda_c^{-1}(a)}(\lambda_c^{-1}(b))}\rho_{\lambda_c^{-1}(a)}(c)\\
&= \lambda_b\lambda_{\rho_{\lambda_a^{-1}(b)}(a)}\rho_{\lambda^{-1}_{\rho_{\lambda_c^{-1}(a)}(c)}(\lambda_a^{-1}(b))}\rho_{\lambda_c^{-1}(a)}(c)\\
&= \lambda_b\lambda_{\rho_{\lambda_{\rho_{\lambda_c^{-1}(a)}(c)}(\lambda^{-1}_{\rho_{\lambda_c^{-1}(a)}(c)}\lambda_a^{-1}(b))}(a)}\rho_{\lambda^{-1}_{\rho_{\lambda_c^{-1}(a)}(c)}\lambda_a^{-1}(b)}(\rho_{\lambda_c^{-1}(a)}(c))\\
&= \lambda_b\rho_{\lambda_{\rho_{\rho_{\lambda_c^{-1}(a)}(c)}(a)}(\lambda^{-1}_{\rho_{\lambda_c^{-1}(a)}(c)}\lambda_a^{-1}(b))}\lambda_a(\rho_{\lambda_c^{-1}(a)}(c))\\
&= \lambda_b\rho_{\lambda^{-1}_{\lambda_a\rho_{\lambda_c^{-1}(a)}(c)}(b)}\lambda_a(\rho_{\lambda_c^{-1}(a)}(c))\\
&= \sigma_b(\lambda_a\rho_{\lambda_c^{-1}(a)}(c))\\
&= \sigma_b\,\sigma_a(c). \qquad (3.15)
\end{aligned}$$

So indeed, the map $\sigma : (A, +) \to \mathrm{Map}(A, A) : a \mapsto \sigma_a$ is an anti-homomorphism.

In order to compare different YB-semitrusses, one needs to define a homomorphism between YB-semitrusses, which obviously needs to preserve both operations and should be compatible with the λ-map and the σ-map.

Definition 3.1.7. *Let $(A, +, \circ, \lambda, \sigma)$ and $(B, +', \circ', \lambda', \sigma')$ be YB-semitrusses. A homomorphism between the YB-semitrusses A and B is a map $f : A \to B$ satisfying, for any $a, b \in A$,* *(1)* $f(a+b) = f(a) +' f(b)$,

(2) $f(a \circ b) = f(a) \circ' f(b)$,

(3) $f(\lambda_a(b)) = \lambda'_{f(a)}(f(b))$,

(4) $f(\sigma_b(a)) = \sigma'_{f(b)}(f(a))$.

Let $(A, +, \circ, \lambda, \sigma)$ and $(B, +', \circ', \lambda', \sigma')$ be two YB-semitrusses. If f is a homomorphism between A and B, then f is also compatible with the inverses of the λ-maps, i.e. $(\lambda'_{f(a)})^{-1}(f(b)) = f(\lambda_a^{-1}(b))$, for all $a, b \in A$. The ρ-map is compatible with f if f is surjective.

Lemma 3.1.8. *Let $f : A \to B$ be an epimorphism between YB-semitrusses $(A, +, \circ, \lambda, \sigma)$ and $(B, +', \circ', \lambda', \sigma')$ with ρ-maps ρ and ρ' respectively. Then, $\rho'_{f(a)} f(b) = f\rho_a(b)$ for all $a, b \in A$. Furthermore, if, for all $a \in A$, ρ_a is surjective then, for all $x \in B$, ρ'_x is surjective. If, in addition, for all $a \in A$, ρ_a is also injective and the map $g_a : B \to B : f(b) \mapsto f\rho_a^{-1}(b)$ is well-defined, i.e. $f\rho_a^{-1}(b) = f\rho_{a'}^{-1}(b')$ for any $a, a', b, b' \in A$ such that $f(a) = f(a')$ and $f(b) = f(b')$, then all $\rho'_{f(a)}$ are also injective and $(\rho'_{f(a)})^{-1} f = f\rho_a^{-1}$.*

Proof. By definition (3.9), $\rho_b(a) = \lambda^{-1}_{\lambda_a(b)}\sigma_{\lambda_a(b)}(a)$ and $\rho'_y(x) = (\lambda')^{-1}_{\lambda'_x(y)}\sigma'_{\lambda'_x(y)}(x)$, for all $a, b \in A$, $x, y \in B$. Hence,

$$\begin{aligned}
\rho'_{f(b)} f(a) &= (\lambda'_{\lambda'_{f(a)} f(b)})^{-1}\sigma'_{\lambda'_{f(a)} f(b)} f(a) \\
&= (\lambda'_{f(\lambda_a(b))})^{-1}\sigma'_{f(\lambda_a(b))} f(a) \\
&= (\lambda'_{f(\lambda_a(b))})^{-1} f(\sigma_{\lambda_a(b)}(a)) \\
&= f(\lambda^{-1}_{\lambda_a(b)}\sigma_{\lambda_a(b)}(a)) \\
&= f\rho_b(a),
\end{aligned}$$

for any $a, b \in A$. This proves the first part.

Furthermore, this implies that $\rho'_{f(b)}$ is surjective if both f and ρ_b are surjective, and the second part follows as well.

For the final part, assume that ρ_a is bijective, for any $a \in A$, and that the mapping $g_a : B \to B : f(b) \mapsto f\rho_a^{-1}(b)$ is well-defined. Then, for any $a, b \in A$,

$$g_a \rho'_{f(a)} f(b) = g_a f\rho_a(b) = f\rho_a^{-1}\rho_a(b) = f(b),$$

and

$$\rho'_{f(a)} g_a f(b) = \rho'_{f(a)} f\rho_a^{-1}(b) = f\rho_a\rho_a^{-1}(b) = f(b).$$

Therefore $\rho'_{f(a)}$ is bijective with inverse g_a. □

Recall from Section 1.3 that (Y, r_Y) is an epimorphic (resp. isomorphic) image of (X, r_X) if there exists a surjective (resp. bijective) map $f : X \to Y$ satisfying $(f \times f)r_X = r_Y(f \times f)$.

Proposition 3.1.9. *Let $(A,+,\circ,\lambda,\sigma)$ and $(B,+',\circ',\lambda',\sigma')$ be YB-semitrusses with associated solutions (A,r_A) and (B,r_B) respectively. Then, (B,r_B) is an epimorphic (respectively isomorphic) image of (A,r_A) if and only if there exists a surjective (respectively bijective) map $f:A\to B$ such that $f\lambda_a=\lambda'_{f(a)}f$ and $f\sigma_a=\sigma'_{f(a)}f$, for any $a\in A$, i.e. conditions (3) and (4) of Definition 3.1.7 hold.*

Proof. Assume first that (B,r_B) is an epimorphic image of (A,r_A). Then, there exists a surjective map $f:A\to B$ such that $(f\times f)r_A=r_B(f\times f)$. This means that, for any $a,b\in A$,

$$(f\lambda_a(b), f\lambda^{-1}_{\lambda_a(b)}\sigma_{\lambda_a(b)}(a))=(\lambda'_{f(a)}f(b),(\lambda'_{\lambda'_{f(a)}f(b)})^{-1}\sigma'_{\lambda'_{f(a)}f(b)}(f(a))).$$

The first component yields, for any $a\in A$, that $f\lambda_a=\lambda'_{f(a)}f$, and as λ_a and $\lambda'_{f(a)}$ are bijective, $f\lambda_a^{-1}=(\lambda'_{f(a)})^{-1}f$. The second component then implies

$$\begin{aligned}(\lambda'_{\lambda'_{f(a)}f(b)})^{-1}\sigma'_{\lambda'_{f(a)}f(b)}(f(a)) &= f\lambda^{-1}_{\lambda_a(b)}\sigma_{\lambda_a(b)}(a)\\ &=(\lambda'_{f\lambda_a(b)})^{-1}f\sigma_{\lambda_a(b)}(a)\\ &=(\lambda'_{\lambda'_{f(a)}f(b)})^{-1}f\sigma_{\lambda_a(b)}(a).\end{aligned}$$

It follows that $f\sigma_{\lambda_a(b)}(a)=\sigma'_{\lambda'_{f(a)}f(b)}(f(a))=\sigma'_{f\lambda_a(b)}f(a)$, for every $a,b\in A$. Hence, $f\sigma_b(a)=\sigma'_{f(b)}f(a)$.

Conversely, if, for any $a\in A$, we have $f\lambda_a=\lambda'_{f(a)}f$ and $f\sigma_a=\sigma'_{f(a)}f$, then

$$\begin{aligned}r_B(f\times f)(a,b) &= (\lambda'_{f(a)}f(b),(\lambda'_{\lambda'_{f(a)}f(b)})^{-1}\sigma'_{\lambda'_{f(a)}f(b)}f(a))\\ &=(f\lambda_a(b),(\lambda'_{f\lambda_a(b)})^{-1}\sigma'_{f\lambda_a(b)}f(a))\\ &=(f\lambda_a(b),(\lambda'_{f\lambda_a(b)})^{-1}f\sigma_{\lambda_a(b)}(a))\\ &=(f\lambda_a(b),f\lambda^{-1}_{\lambda_a(b)}\sigma_{\lambda_a(b)}(a))\\ &=(f\times f)r_A(a,b).\end{aligned}$$

Thus, (B,r_B) is an epimorphic image of (A,r_A). □

As a corollary of the previous result, we get that isomorphic YB-semitrusses yield isomorphic associated solutions. The converse however is not true. Take for example two non-isomorphic abelian groups of the same size $(A,+)$ and $(B,+')$. Then, the trivial YB-semitrusses $(A,+,+,\iota,\sigma)$ with $\iota_a=\sigma_a=\mathrm{id}_A$ for all $a\in A$, and $(B,+',+',\iota',\sigma')$ with $\iota'_b=\sigma'_b=\mathrm{id}_B$ for all $b\in B$, are non-isomorphic YB-semitrusses with isomorphic associated solutions.

3.1.1 Structure monoids as YB-semitrusses

In this part we study the structure semigroup and monoid of left non-degenerate set-theoretic solutions of the Yang-Baxter equation and show that they are natural examples of YB-semitrusses. We use this result to prove that all left non-degenerate solutions are determined by YB-semitrusses, in the sense that for any left non-degenerate solution its structure semigroup and monoid are YB-semitrusses, and the solutions associated to these YB-semitrusses are extensions of the original left non-degenerate solution. Conversely, any YB-semitruss is an epimorphic image of the associated structure semigroup or monoid (considered as a YB-semitruss). Thus, left non-degenerate set-theoretic solutions of the Yang-Baxter equation are restrictions of solutions associated to YB-semitrusses. Finally, we prove that isomorphic solutions have isomorphic associated structure semigroups or monoids (considered as a YB-semitrusses) and vice versa.

Before going deeper into the main results of this part, we investigate YB-semitrusses where both semigroups are monoids, and show that their identity element must coincide, and denote it by 1. It follows that both λ_1 as σ_1 must be the identity map and, for any $a \in A$, $\lambda_a(1) = 1$. With the additional assumption that for any $a \in A$, $\sigma_a(1) = 1$, we will define this type of YB-semitrusses as unital YB-semitrusses.

Lemma 3.1.10. *Let $(A, +, \circ, \lambda, \sigma)$ be a YB-semitruss such that $(A, +)$ and $(A, \circ)$ are monoids with identity element 0 and 1 respectively. Then, condition (3.3) is equivalent to $0 = 1$. Furthermore, $\lambda_1 = \sigma_1 = \mathrm{id}_A$ and $\lambda_a(1) = 1$, for any $a \in A$.*

Proof. Assume that $(A, +, \circ, \lambda, \sigma)$ is a YB-semitruss such that both $(A, +)$ and $(A, \circ)$ are monoids, and denote their identity element by 0 and 1 respectively. By (3.2), $\lambda_1 = \lambda_{1\circ 1} = \lambda_1\lambda_1$ and thus, because λ_1 is bijective, $\lambda_1 = \mathrm{id}_A$. Hence, by (3.3), $0 = 1 \circ 0 = 1 + \lambda_1(0) = 1 + 0 = 1$. Conversely, assume that $(A, \circ)$ and $(A, +)$ share the same identity, say 1. It then follows from the left semitruss identity (3.1), for any $a, b \in A$, that $a + \lambda_a(b) = a \circ 1 + \lambda_a(b) = a \circ (1 + b) = a \circ b$.

Furthermore, for any $a \in A$, condition (3.4) implies $a = a + 1 = 1 + \sigma_1(a) = \sigma_1(a)$, i.e. $\sigma_1 = \mathrm{id}_A$. Also, for any $a, b \in A$, by condition (3.2), we have $b + \lambda_a(1) = \lambda_a(\lambda_a^{-1}(b)) + \lambda_a(1) = \lambda_a(\lambda_a^{-1}(b) + 1) = \lambda_a(\lambda_a^{-1}(b)) = b$. Taking $b = 1$, this yields $\lambda_a(1) = 1 + \lambda_a(1) = 1$. □

Definition 3.1.11. *A* unital YB-semitruss *is a YB-semitruss $(A, +, \circ, \lambda, \sigma)$ where both $(A, +)$ and $(A, \circ)$ are monoids and, for any $a \in A$,*

$$\sigma_a(1) = 1, \tag{3.16}$$

where 1 denotes the identity in $(A, +)$ (and also in $(A, \circ)$).

We will prove that structure monoids of left non-degenerate solutions have a natural unital YB-semitruss structure. First, we note that (3.16) is automatically satisfied for unital YB-semitruss where $(A, +)$ is a left cancellative monoid.

Remark 3.1.12. *If $(A, +, \circ, \lambda, \sigma)$ is a unital YB-semitruss such that $(A, +)$ is a left cancellative monoid, then (3.16) follows from (3.4). Indeed, for $a \in A$, $a + 1 = a = 1 + a = a + \sigma_a(1)$, and by left cancellativity, we get $1 = \sigma_a(1)$. However, (3.16) does not hold in general for any YB-semitruss with both semigroups $(A, +)$ and $(A, \circ)$ being monoids. For example, take the multiplicative monoid $A = \{0, 1\}$, and define $(A, +) = (A, \circ)$, $\lambda_1 = \lambda_0 = \mathrm{id}_A$, $\sigma_1 = \mathrm{id}_A$, and $\sigma_0(a) = 0$, for $a \in A$. Then, $(A, +, \circ, \lambda, \sigma)$ is a YB-semitruss with $\sigma_0(1) = 0 \neq 1$. So, (3.16) is not satisfied in A, and $(A, +, \circ, \lambda, \sigma)$ is not unital.*

In the following theorem, we show that the structure semigroup $S(X,r)$ and structure monoid $M(X,r)$ of a left non-degenerate set-theoretic solution of the Yang-Baxter equation (X,r) are YB-semitrusses. Furthermore, the associated solution of the unital YB-semitruss $M(X,r)$ is precisely the solution (M,r_M) from Theorem 2.1.1. This justifies the terminology in Section 3.1.

Theorem 3.1.13. *Let (X,r) be a left non-degenerate set-theoretic solution of the Yang-Baxter equation. The associated structure monoid $M = M(X,r)$ is a unital YB-semitruss and has the structure semigroup $S(X,r)$ as a sub-YB-semitruss (not unital). The associated solution (respectively left derived solution) of the unital YB-semitruss M, as defined in Proposition 3.1.3, is precisely the solution (M,r_M) (respectively the left derived solution (M,s_M) of (M,r_M)) from Theorem 2.1.1. Similar results hold for the YB-semitruss $S(X,r)$.*

Proof. Let (X,r) be a left non-degenerate solution. From Example 3.1.1, we know that $(M(X,r),+,\circ,\lambda)$ is a left semitruss with $\lambda : (M(X,r),\circ) \longrightarrow \operatorname{Aut}(M(X,r),+)$ a semigroup homomorphism and $a\circ b = a+\lambda_a(b)$, for all $a,b \in M(X,r)$. So (3.2) and (3.3) are satisfied.

By Theorem 2.1.1, we can extend the solution (X,r) to a left non-degenerate solution $(M(X,r),r_{M(X,r)})$. The left derived solution of $(M(X,r),r_{M(X,r)})$ is the solution $(M(X,r),s_{M(X,r)})$, defined by $s_{M(X,r)}(a,b) = (b,\sigma_b(a))$, where $\sigma_b(a) = \lambda_b\rho_{\lambda_a^{-1}(b)}(a)$, for all $a,b \in M(X,r)$. By the defining relations in $A(X,r)$ and the identification of $M(X,r)$ with $A(X,r)$, we have $a+b = b+\sigma_b(a)$, for all $a,b \in M(X,r)$, hence explaining the use of the notation σ in the definition of a YB-semitruss. Hence, (3.4) holds.

Moreover, since (3.13) is satisfied in $(M(X,r),\circ)$, see (2.5), one can show (with a reversed argument to that in the last part of the proof of Proposition 3.1.5) that $\sigma_a \in \operatorname{End}(M(X,r),+)$, for all $a \in M(X,r)$. Furthermore, using that the extension of ρ to $\rho : (M(X,r),\circ) \to \operatorname{Map}(M(X,r),M(X,r))$ is an anti-homomorphism (see Theorem 2.1.1), we proved in (3.15) that $\sigma_{a+b} = \sigma_b\sigma_a$, for all $a,b \in M(X,r)$. So, $\sigma : (M(X,r),+) \to \operatorname{End}(M(X,r),+) : a \mapsto \sigma_a$ is a semigroup anti-homomorphism, and (3.5) is satisfied.

For any $a,b,c \in M(X,r)$,

$$\begin{aligned}
\lambda_a\sigma_c(b) &= \lambda_a\lambda_c\rho_{\lambda_b^{-1}(c)}(b)\\
&= \lambda_{\lambda_a(c)}\lambda_{\rho_c(a)}\rho_{\lambda_b^{-1}(c)}(b)\\
&= \lambda_{\lambda_a(c)}\lambda_{\rho_{\lambda_b(\lambda_b^{-1}(c))}(a)}\rho_{\lambda_b^{-1}(c)}(b)\\
&= \lambda_{\lambda_a(c)}\rho_{\lambda_{\rho_b(a)}(\lambda_b^{-1}(c))}\lambda_a(b)\\
&= \lambda_{\lambda_a(c)}\rho_{\lambda^{-1}_{\lambda_a(b)}(\lambda_a(c))}\lambda_a(b)\\
&= \sigma_{\lambda_a(c)}\lambda_a(b).
\end{aligned}$$

So, equation (3.6) holds.

Similar results can be proven for the structure semigroup $S(X,r)$, and we obtain that both $(M(X,r),+,\circ,\lambda,\sigma)$ and $(S(X,r),+,\circ,\lambda,\sigma)$ are YB-semitrusses.

Finally, the extensions of λ and ρ to $M(X,r)$ satisfy $\lambda_x(1) = \rho_x(1) = 1$, for all $x \in X$ (see before Theorem 2.1.1), which yields $\sigma_a(1) = \lambda_a \rho_{\lambda_1^{-1}(a)}(1) = 1$, for all $a \in M(X,r)$. Thus, $(M(X,r), +, \circ, \lambda, \sigma)$ is a unital YB-semitruss.

To finish the claim, it is clear that the solution associated to the unital structure YB-semitruss $(M(X,r), +, \circ, \lambda, \sigma)$, defined in Proposition 3.1.3, is exactly the solution $(M(X,r), r_{M(X,r)})$ from Theorem 2.1.1. The same holds for the associated left derived solution and $(M(X,r), s_{M(X,r)})$. Similar results hold for the structure YB-semitruss $S(X,r)$. □

For a left non-degenerate set-theoretic solution (X,r), we refer to the YB-semitruss $(M(X,r), +, \circ, \lambda, \sigma)$ as the *unital structure YB-semitruss* associated to (X,r), and to the sub-YB-semitruss $S(X,r)$ as the *structure YB-semitruss* of (X,r).

For specific left non-degenerate solutions (X,r), the structure monoid $M(X,r)$ possibly can be made into a YB-semitruss in several manners. The following example shows that one can consider another σ-map. This indicates that on a set A with two operations $+$ and $\circ$, and a λ-map, it is possible to have more than one σ-map that makes $(A, +, \circ, \lambda, \sigma)$ into a YB-semitruss.

Example 3.1.14. *Let $X = \{1,2\}$. Consider the left non-degenerate solution $r : X \times X \to X \times X : (x,y) \mapsto (\lambda_x(y), \rho_y(x))$ defined by $\lambda_1 = \lambda_2 = \rho_2 = \mathrm{id}_X$ and $\rho_1 : X \to X : x \mapsto 1$. The associated left derived structure monoid is $A = A(X,r) = \langle X \mid 1+2 = 2+1 = 1+1 \rangle^1$. Note that the solution (X,r) is equal to its left derived solution, and thus the σ-map, defined by (3.9), is equal to the ρ-map of the solution, and $M = M(X,r) = A$. One can also consider another σ-map on X, denoted σ', and defined by σ'_1 the constant mapping onto 2 and $\sigma'_2 = \mathrm{id}_X$. This map yields a left non-degenerate solution $r' : X \times X \to X \times X : (x,y) \mapsto (\lambda'_x(y), \rho'_y(x))$ with $\lambda'_1 = \lambda'_2 = \mathrm{id}_X$, $\rho'_1 = \sigma'_1$ and $\rho'_2 = \sigma'_2$. We get that $M(X,r') = A(X,r') = A = M(X,r)$. However, it easily is verified that the solutions r and r' are not isomorphic and thus also r_M and r'_M are not isomorphic.*

The following result shows that (unital) YB-semitrusses are epimorphic images of (unital) structure YB-semitrusses. Together with the results from Theorem 3.1.13, this proves that YB-semitrusses determine all left non-degenerate set-theoretic solutions of the Yang-Baxter equation.

Theorem 3.1.15. *Let $(A, +, \circ, \lambda, \sigma)$ be a YB-semitruss with associated solution (A, r_A). Then, A is an epimorphic image of the structure YB-semitruss $S(A, r_A)$. If A is a unital YB-semitruss, then A is an epimorphic image of the unital structure YB-semitruss $M(A, r_A)$.*

Proof. Consider the natural map of the generating set A of $S(A, r_A)$ to A. Because of the equations (2.5), (2.6) and (2.7) in $S(A, r_A)$ and the relations (3.11), (3.12) and (3.13) in the YB-semitruss A, this map can be extended to a semigroup epimorphism $f : (S(A, r_A), \circ) \to (A, \circ)$. By relation (3.3), which holds in both YB-semitrusses, the latter yields a semigroup epimorphism $f : (S(A, r_A), +) \to (A, +)$. Finally, f is an epimorphism of YB-semitrusses since the λ-map and σ-map of $S(A, r_A)$ are extensions of those of A.

If $(A,+,\circ,\lambda,\sigma)$ is unital, we obtain that $\lambda_1 = \mathrm{id}_A$ in both YB-semitrusses A and $M(A,r_A)$, and also $\lambda_a(1) = 1$, for all $a \in A$, and thus also for all $a \in M(A,r_A)$. Thus, for unital YB-semitrusses, we can extend f to $M(A,r_A)$. □

For a left non-degenerate set-theoretic solution (X,r), the structure YB-semitruss $(S(X,r),+,\circ,\lambda,\sigma)$ and unital structure YB-semitruss $(M(X,r),+,\circ,\lambda,\sigma)$ have a natural strongly $\mathbb{N}$-gradation, via the length function on $S(X,r)$ and $M(X,r)$ respectively. Moreover, the λ-map and σ-map preserve the length of the elements. In general we say that a YB-semitruss $(A,+,\circ,\lambda,\sigma)$ is $\mathbb{N}$-*graded* (respectively *strongly* $\mathbb{N}$-*graded*) if

$$A = \bigcup_{n\in\mathbb{N}} A_n,$$

a disjoint union of subsets A_n indexed by the non-negative integers $n \in \mathbb{N}$, such that $A_n + A_m \subseteq A_{n+m}$ (respectively $A_n + A_m = A_{n+m}$) and all maps λ_a and σ_a are graded, i.e. degree preserving. In particular, if A is strongly $\mathbb{N}$-graded, then the subsemigroup $A \setminus A_0$ is additively (and thus also multiplicatively) generated by its elements of degree 1. Note that, since the λ-map and σ-map are degree preserving, the associated solution $r_A : A \times A \to A \times A$ restricts to solutions $r_{A_n} : A_n \times A_n \to A_n \times A_n$, for all $n \in \mathbb{N}$.

Because of the previous comment we can write the previous result within a graded context as well. The graded statements follow at once as A is generated by $A_1 \cup A_0$ and the mentioned natural map preserves degrees.

Corollary 3.1.16. *If $(A,+,\circ,\lambda,\sigma)$ is a strongly $\mathbb{N}$-graded YB-semitruss with $A_0 = \varnothing$, then A is a graded epimorphic image of the $\mathbb{N}$-graded structure YB-semitruss $S(A_1,r_{A_1})$. If, moreover, A is unital and $A_0 = \{1\}$, then A is a graded epimorphic image of the $\mathbb{N}$-graded unital structure YB-semitruss $M(A_1,r_{A_1})$.*

In Proposition 3.1.9 it was shown that isomorphic YB-semitrusses yield isomorphic associated solutions. The converse is however not true. Nonetheless, isomorphic left non-degenerate solutions have isomorphic (unital) structure YB-semitrusses and vice versa.

Proposition 3.1.17. *Two left non-degenerate set-theoretic solutions of the Yang-Baxter equation (X,r) and (Y,r') are isomorphic if and only if their associated (unital) structure YB-semitrusses $S(X,r)$ and $S(Y,r')$ ($M(X,r)$ and $M(Y,r')$) are isomorphic as YB-semitrusses.*

Proof. We prove the result for the unital structure YB-semitrusses. The proof for the structure YB-semitrusses is similar.

Let (X,r) and (Y,r') be two isomorphic left non-degenerate solutions and denote $r(x,y) = (\lambda_x(y),\rho_y(x))$, for all $x,y \in X$, and $r'(x',y') = (\lambda'_{x'}(y'),\rho'_{y'}(x'))$, for all $x',y' \in Y$. Then, there exists a bijective map $f : X \to Y$ such that $(f\times f)r = r'(f\times f)$, i.e. for any $x,y \in X$, $f(\lambda_x(y)) = \lambda'_{f(x)}(f(y))$ and $f(\rho_y(x)) = \rho'_{f(y)}(f(x))$. By replacing y by $\lambda_x^{-1}(y)$, we also get that $(\lambda'_{f(x)})^{-1}(f(y)) = f(\lambda_x^{-1}(y))$. Defining the σ-map and σ'-map according to the relation (3.9) for $M(X,r)$ and $M(Y,r')$ respectively, i.e. $\sigma_b(a) = \lambda_b\rho_{\lambda_a^{-1}(b)}(a)$, for all $a, b \in M(X,r)$, and $\sigma'_{b'}(a') = \lambda'_{b'}\rho'_{(\lambda'_{a'})^{-1}(b')}(a')$, for all $a', b' \in M(Y, r')$. Then, for any $x, y \in X$,

$$\begin{aligned}
f(\sigma_y(x)) &= f(\lambda_y(\rho_{\lambda_x^{-1}(y)}(x))) \\
&= \lambda'_{f(y)}(f(\rho_{\lambda_x^{-1}(y)}(x))) \\
&= \lambda'_{f(y)}(\rho'_{f(\lambda_x^{-1}(y))}(f(x))) \\
&= \lambda'_{f(y)}(\rho'_{(\lambda'_{f(x)})^{-1}(f(y))}(f(x))) \\
&= \sigma'_{f(y)}(f(x)).
\end{aligned}$$

We will prove that the associated unital structure YB-semitrusses $M = M(X,r)$ and $M' = M(Y,r')$ are isomorphic, by extending the map f to M. Define $f(1_M) = 1_{M'}$, and for any $x \in X, a \in M$, $f(x \circ a) = f(x) \circ' f(a)$. Hence, $f(a \circ b) = f(a) \circ' f(b)$, for all $a, b \in M$. To prove that it is well-defined, let $x, y \in X$. Then, by the defining relations in M',

$$\begin{aligned}
f(\lambda_x(y) \circ \rho_y(x)) &= f(\lambda_x(y)) \circ' f(\rho_y(x)) \\
&= \lambda'_{f(x)}(f(y)) \circ' \rho'_{f(y)}(f(x)) \\
&= f(x) \circ' f(y) \\
&= f(x \circ y),
\end{aligned}$$

and by induction on the length of the elements of M, $f(\lambda_a(b) \circ \rho_b(a)) = f(a \circ b)$, for all $a, b \in M$. Furthermore, by induction on the length of the elements of M, using relations (3.12) and (3.13) in both M and M', we get that $f(\lambda_a(b)) = \lambda'_{f(a)}(f(b))$ and $f(\sigma_b(a)) = \sigma'_{f(b)}(f(a))$, for all $a, b \in M$. Moreover, as $a + b = a \circ \lambda_a^{-1}(b)$ and $f(a) +' f(b) = f(a) \circ' (\lambda'_{f(a)})^{-1}(f(b))$, for all $a, b \in M$, we have that

$$\begin{aligned}
f(a + b) &= f(a \circ \lambda_a^{-1}(b)) \\
&= f(a) \circ' f(\lambda_a^{-1}(b)) \\
&= f(a) \circ' (\lambda'_{f(a)})^{-1}(f(b)) \\
&= f(a) +' f(b).
\end{aligned}$$

Finally, we check that $f : M \to M'$ is bijective. For any $a' = x'_1 \circ \cdots \circ x'_n \in M'$ with $x'_1, \cdots, x'_n \in Y$, there exist $x_1, \ldots, x_n \in X$ such that $f(x_i) = x'_i$, for all $i \in \{1, \ldots, n\}$. Hence, $f(x_1 \circ \cdots \circ x_n) = a'$. The injectivity of f naturally follows from the defining relations in both M and M' and the injectivity of $f : X \to Y$. Hence, by Definition 3.1.7, $(M(X,r), +, \circ, \lambda, \sigma) \cong (M(Y,r'), +', \circ', \lambda', \sigma')$ as YB-semitrusses.

Conversely, assume that $M = M(X,r)$ and $M' = M(Y,r')$ are isomorphic as YB-semitrusses, i.e. there exists a bijective YB-semitruss morphism $f : M \to M'$ such that $(f \times f)r_M = r_{M'}(f \times f)$. So, for any $a, b \in M$, $f(\lambda_a(b)) = \lambda'_{f(a)}(f(b))$ and $f(\rho_b(a)) = \rho'_{f(b)}(f(a))$, and thus the same equalities hold for all $x, y \in X$. Furthermore, since the set X is the unique minimal set of generators of the monoid $(M, \circ)$ and f is a monoid homomorphism, we get that $f(X) = Y$, the unique minimal set of generators of the monoid M'. Hence, $(X,r) \cong (Y,r')$. □

Two structure monoids that are isomorphic as monoids do not necessarily imply isomorphic solutions. In [97, Example 1.1], two non-isomorphic bijective non-degenerate solutions are given with the same structure monoid. In case both solutions are involutive non-degenerate one has a satisfactory answer. This already has been pointed out in [97, page 6]. If one of the solutions is bijective while the other is still involutive, not necessarily non-degenerate, the result is still true.

Proposition 3.1.18. *Let (X,r) be an involutive solution. Suppose (Y,r') is a bijective solution such that $M(X,r) \cong M(Y,r')$ as monoids. Then, $(X,r) \cong (Y,r')$ as solutions.*

Proof. Let f be a monoid isomorphism f between $M(X,r)$ and $M(Y,r')$. Since f maps the unique minimal generating set X of $M(X,r)$ to the unique minimal generating set Y of $M(Y,r')$, f can be restricted to a map $f : X \to Y$. Moreover, since r is involutive, one obtains that a word of length 2 can be equal in $M(X,r)$ to at most one other word of length 2 (in the alphabet X). Hence, the same can be said about words of length 2 (in the alphabet Y) in $M(Y,r')$. Since r' is bijective, it can not be idempotent except if $r^2 = \mathrm{id}_{Y\times Y}$, so r' is involutive. Let $x,y \in X$. Then, either $x \circ y$ can not be rewritten in $M(X,r)$ or $x \circ y = \lambda_x(y) \circ \rho_y(x)$ with $(x,y) \neq (\lambda_x(y), \rho_y(x))$. In the former case, as f is a monoid isomorphism, it follows that $f(x \circ y) = f(x) \circ f(y)$ can also not be rewritten in $M(Y,r')$, implying that $\lambda'_{f(x)}(f(y)) = f(x)$ and $\rho'_{f(y)}(f(x)) = f(y)$, where r' is defined by λ' and ρ'. In the latter case, $f(x) \circ f(y) = f(\lambda_x(y)) \circ f(\rho_y(x))$ are the two only ways to write this element in $M(Y,r')$. Considering the defining relation of $M(Y,r')$, it follows that $\lambda'_{f(x)}(f(y)) = f(\lambda_x(y))$ and $\rho'_{f(y)}(f(x)) = f(\rho_y(x))$. In general, we obtain that $f(\lambda_x(y)) = \lambda'_{f(x)}(f(y))$ and $f(\rho_x(y)) = \rho'_{f(x)}(f(y))$, for all $x,y \in X$, which shows that f is an isomorphism of solutions. □

The following example shows that the assumption that (Y,r') is bijective is essential. Let $X = \{1,2\}$ and (X,r) the trivial solution, i.e. $r(x,y) = (y,x)$, for $x,y \in X$. Its structure monoid is the free abelian monoid of rank 2, i.e. $M(X,r) = \langle X \mid 1 \circ 2 = 2 \circ 1\rangle^1$. On X we can also define a degenerate idempotent solution (X,r') with $r'(x,y) = (\lambda'_x(y), \rho'_y(x))$ and $\lambda'_1 : x \mapsto 1, \lambda'_2 = \rho'_1 = \mathrm{id}_X$ and $\rho'_2 : x \mapsto 2$, i.e. $r'(2,1) = (1,2)$ and the other pairs are fixed under r'. Then, $M(X,r') = \langle X \mid 2 \circ 1 = 1 \circ 2\rangle^1 = M(X,r)$. However, $(X,r) \ncong (X,r')$. Note that the example (X,r') is not left non-degenerate and that, because of Theorem 3.2.8 no counterexamples exists in case (Y,r') is finite non-degenerate.

We end this section with a class of examples that yield left non-degenerate idempotent solutions. Idempotent solutions will also come into the picture in Chapter 5.

Example 3.1.19. *If (X,r) is an idempotent set-theoretic solution of the Yang-Baxter equation, i.e. $r^2 = r$, then $\lambda_{\lambda_x(y)}(\rho_y(x)) = \lambda_x(y)$ and $\rho_{\rho_y(x)}(\lambda_x(y)) = \rho_y(x)$, for all $x,y \in X$. Moreover, if the solution is left non-degenerate, the σ-map of the unital structure YB-semitruss $M(X,r)$ satisfies $\sigma_b(a) = \lambda_b(\rho_{\lambda_a^{-1}(b)}(a)) = \lambda_{\lambda_a(t)}(\rho_t(a)) = \lambda_a(t) = \lambda_a(\lambda_a^{-1}(b)) =$*

b, with $t = \lambda_a^{-1}(b)$. Conversely, assume $(A,+,\circ,\lambda,\sigma)$ is a YB-semitruss, with $\sigma_b(a) = b$ for all $a, b \in A$. Then, one easily verifies that the solution (A, r_A) is idempotent, i.e. that $(r_A)^2 = r_A$. Hence, idempotent left non-degenerate solutions correspond to YB-semitrusses $(A,+,\circ,\lambda,\sigma)$ with σ_b the constant mapping onto b, for every $b \in A$.

3.1.2 Left cancellative YB-semitrusses

In this part, we focus on YB-semitrusses $(A,+,\circ,\lambda,\sigma)$ with $(A,+)$ a left cancellative semigroup, i.e. $a+b = a+c$ implies $b = c$, for all $a, b, c \in A$. We call such a YB-semitrusses a *left cancellative YB-semitruss*. In general, not every YB-semitruss is left cancellative. Take for example the trivial YB-semitruss $(A,+,+,\iota,\sigma)$, with $\sigma_a = \mathrm{id}_A$, for all $a \in A$, on an abelian semigroup $(A,+)$ that is not left cancellative. An example of such a semigroup is the subsemigroup $\{-1, 0, 1\}$ of the integers with its normal multiplication. For unital structure YB-semitrusses, the additive semigroup is also not necessarily left cancellative. We will define a left cancellative congruence μ on $(M(X,r),+)$ and prove that the left cancellative image $(M(X,r)/\mu,+)$ of $(M(X,r),+)$ has a YB-semitruss structure. Afterwards, we show that the known algebraic associative structures that determine left non-degenerate set-theoretic solution of the Yang-Baxter equation are examples of YB-semitrusses.

Lemma 3.1.20. *Let $(A,+,\circ,\lambda)$ be a left semitruss with λ_a bijective and $a+\lambda_a(b) = a\circ b$, for all $a, b \in A$. Then, $(A,+)$ being left cancellative is equivalent to $(A,\circ)$ being left cancellative.*

Proof. Let $(A,+,\circ,\lambda)$ be a left semitruss with λ_a bijective and $a + \lambda_a(b) = a \circ b$, for all $a, b \in A$. Take $a, b, c \in A$. If $(A,+)$ is left cancellative and $a \circ b = a \circ c$. Then, $a + \lambda_a(b) = a + \lambda_a(c)$, and since λ_a is bijective, $b = c$.

Conversely, if $(A,\circ)$ is left cancellative and $a+b = a+c$. Then, $a\circ\lambda_a^{-1}(b) = a\circ\lambda_a^{-1}(c)$, and since λ_a^{-1} is bijective, $b = c$. □

In general, the σ-map of a YB-semitruss is not necessarily unique, see Example 3.1.14. However, if $(A,+)$ is a left cancellative semigroup, then the map σ_a is uniquely determined, for any $a \in A$. Indeed, if $a + b = b + \sigma_b(a) = b + \sigma'_b(a)$, then $\sigma_b(a) = \sigma'_b(a)$, for any $a, b \in A$. Furthermore, by (3.11), for any YB-semitruss $(A,+,\circ,\lambda,\sigma)$ and for any $a, b \in A$, there exists $x \in A$ such that $a \circ b = \lambda_a(b) \circ x$. In case $(A,+)$ (and thus also $(A,\circ)$) is left cancellative, this element $x \in A$ is unique.

It turns out that several of the requirements to be a YB-semitruss are redundant in case $(A,+)$ is left cancellative.

Proposition 3.1.21. *Let $(A,+,\circ,\lambda)$ be a left semitruss with $(A,+)$ (and thus also $(A,\circ)$) left cancellative, and λ_a bijective, for any $a \in A$, such that for all $a, b \in A$, the equation*

$$a + \lambda_a(b) = a \circ b,$$

holds, and there exists an $x \in A$ such that

$$a \circ b = \lambda_a(b) \circ x.$$

We denote x by $\rho_b(a)$. Then, there exists a unique semigroup anti-morphism $\sigma : (A, +) \to \mathrm{End}(A, +) : a \mapsto \sigma_a$ such that $(A, +, \circ, \lambda, \sigma)$ is a YB-semitruss. For $a, b \in A$, we have $\sigma_b(a) = \lambda_b \rho_{\lambda_a^{-1}(b)}(a)$.

Proof. By [26, Proposition 2.1], we have that $\lambda : (A, \circ) \to \mathrm{Aut}(A, +) : a \mapsto \lambda_a$ is a semigroup morphism. By Lemma 3.1.20 and since (3.3) is satisfied by assumption, for any $a, b \in A$, there exists a unique element $x \in A$ such that $a \circ b = \lambda_a(b) \circ x$. We put $\rho_b(a) = x$. For any $a, b \in A$, define $\sigma_b(a) = \lambda_b \rho_{\lambda_a^{-1}(b)}(a)$. Then, by the assumption that (3.3) holds,

$$\begin{aligned}
b + \sigma_b(a) &= b + \lambda_b \rho_{\lambda_a^{-1}(b)}(a) \\
&= b \circ \rho_{\lambda_a^{-1}(b)}(a) \\
&= \lambda_a \lambda_a^{-1}(b) \circ \rho_{\lambda_a^{-1}(b)}(a) \\
&= a \circ \lambda_a^{-1}(b) \\
&= a + \lambda_a \lambda_a^{-1}(b) \\
&= a + b.
\end{aligned}$$

Hence, (3.4) holds. Furthermore, for any $a, b, c \in A$,

$$c + \sigma_c(a + b) = a + b + c = a + c + \sigma_c(b) = c + \sigma_c(a) + \sigma_c(b).$$

So, by left cancellativity, $\sigma_c(a + b) = \sigma_c(a) + \sigma_c(b)$. On the other hand,

$$b + a + \sigma_a \sigma_b(c) = b + \sigma_b(c) + a = c + b + a = b + a + \sigma_{b+a}(c),$$

and again by left cancellativity, $\sigma_a \sigma_b = \sigma_{b+a}$. Thus, $\sigma : (A, +) \to \mathrm{End}(A, +)$ is an anti-morphism and (3.5) holds. Finally, for any $a, b, c \in A$,

$$\lambda_a(b) + \sigma_{\lambda_a(b)} \lambda_a(c) = \lambda_a(c) + \lambda_a(b) = \lambda_a(c + b) = \lambda_a(b + \sigma_b(c)) = \lambda_a(b) + \lambda_a \sigma_b(c),$$

and, since $(A, +)$ is left cancellative, we get $\sigma_{\lambda_a(b)} \lambda_a(c) = \lambda_a \sigma_b(c)$, and condition (3.6) is satisfied. Hence, $(A, +, \circ, \lambda, \sigma)$ is a YB-semitruss. □

In [52, Proposition 5.4] (Cedó, Jespers, and Verwimp), the first part of Proposition 3.1.3 was proven for YB-semitrusses $(A, +, \circ, \lambda, \sigma)$ with a unique σ-map $\sigma : A \to \mathrm{Map}(A, A)$ satisfying $a + b = b + \sigma_b(a)$, for all $a, b \in A$. In order to obtain such a unique mapping on the unital structure YB-semitruss $M = M(X, r)$ of a left non-degenerate solution (X, r), a least left cancellative congruence η on $(M, +)$ is considered in [52, Section 5] (Cedó, Jespers, and Verwimp). We include a description of the elements in η. Let

$$\eta_0 = \{(a, b) \in M^2 \mid \exists c \in M \text{ such that } c + a = c + b\},$$

a reflexive and symmetric binary relation on M. Define η_1 as its transitive closure, i.e.

$$\eta_1 = \{(a,b) \in M^2 \mid \exists a_1, \dots, a_n \in M \text{ such that } (a,a_1),(a_1,a_2),\dots,(a_n,b) \in \eta_0\}.$$

Thus, η_1 is an equivalence relation on M. For every $m \geq 1$, define

$$\begin{aligned}\eta_{2m} =& \{(c+a, c+b) \in M^2 \mid c \in M \text{ and } (a,b) \in \eta_{2m-1}\}\\ &\cup \{(a,b) \in M^2 \mid \exists c \in M \text{ such that } (c+a,c+b) \in \eta_{2m-1}\},\\ \eta_{2m+1} =& \{(a,b) \in M^2 \mid \exists a_1, \dots, a_n \in M \text{ such that } (a,a_1),(a_1,a_2),\dots,(a_n,b) \in \eta_{2m}\}.\end{aligned}$$

Note that $\eta_n \subseteq \eta_{n+1} \subseteq \eta$, for all $n \geq 0$. Let $\eta' = \cup_{n=0}^{\infty} \eta_n$.

Lemma 3.1.22. *Let (X,r) be a left non-degenerate set-theoretic solution of the Yang-Baxter equation, and consider the unital structure YB-semitruss $(M,+,\circ,\lambda,\sigma)$ associated to (X,r), with $M = M(X,r)$. With the above notation we have that $\eta' = \eta$, and for all $z \in M$,*

$$\eta = \{(\lambda_z(a), \lambda_z(b)) \mid (a,b) \in \eta\} = \{(\lambda_z^{-1}(a), \lambda_z^{-1}(b)) \mid (a,b) \in \eta\}.$$

Proof. First, we show that η' is a congruence on $(M,+)$. Since η_n is reflexive and symmetric, for all n, so is η'. Assume that $(a,b),(b,c) \in \eta'$ for some $a,b,c \in M$. As $\eta_n \subseteq \eta_{n+1}$, for all n, there exists a positive integer m such that $(a,b),(b,c) \in \eta_{2m}$. Since η_{2m+1} is the transitive closure of η_{2m}, we obtain that $(a,c) \in \eta_{2m+1} \subseteq \eta'$. Thus, η' is an equivalence relation on M. Let $c \in M$. Since $(a,b) \in \eta_{2m+1}$, also $(a+c, b+c) \in \eta_{2m+1} \subseteq \eta'$ and $(c+a, c+b) \in \eta_{2m+2} \subseteq \eta'$. Hence, η' is a congruence.

We will now prove that $(M,+)/\eta'$ is a left cancellative monoid. Since $\eta' \subseteq \eta$ and η is the smallest left cancellative congruence, this implies that $\eta' = \eta$. Let $a,b,c \in M$ be elements such that $(c+a, c+b) \in \eta'$. There exists a positive integer m such that $(c+a, c+b) \in \eta_{2m+1}$. Thus, $(a,b) \in \eta_{2m+2} \subseteq \eta'$. So indeed, $(M,+)/\eta'$ is a left cancellative monoid and $\eta' = \eta$.

Let $(a,b) \in \eta_0$. Then, by definition of η_0, there exists $c \in M$ such that $c+a = c+b$. Let $z \in M$. By (3.2), $\lambda_z \in \operatorname{Aut}(M,+)$, so we get for any $\varepsilon = \pm 1$,

$$\lambda_z^\varepsilon(c) + \lambda_z^\varepsilon(a) = \lambda_z^\varepsilon(c+a) = \lambda_z^\varepsilon(c+b) = \lambda_z^\varepsilon(c) + \lambda_z^\varepsilon(b).$$

So, $\eta_0 = \{(\lambda_z(a), \lambda_z(b)) \mid (a,b) \in \eta_0\} = \{(\lambda_z^{-1}(a), \lambda_z^{-1}(b)) \mid (a,b) \in \eta_0\}$. It follows that its transitive closure is equal to

$$\eta_1 = \{(\lambda_z(a), \lambda_z(b)) \mid (a,b) \in \eta_1\} = \{(\lambda_z^{-1}(a), \lambda_z^{-1}(b)) \mid (a,b) \in \eta_1\}.$$

Let $(a,b) \in \eta_2$, then either $(a,b) = (c+a', c+b')$, for some $c, a', b' \in M$ with $(a',b') \in \eta_1$, or $(c+a, c+b) \in \eta_1$, for some $c \in M$. In the first case, $(a',b') \in \eta_1$, so also $(\lambda_z^\varepsilon(a'), \lambda_z^\varepsilon(b')) \in \eta_1$, for $\varepsilon = \pm 1$. Hence, for $\varepsilon = \pm 1$,

$$(\lambda_z^\varepsilon(a), \lambda_z^\varepsilon(b)) = (\lambda_z^\varepsilon(c) + \lambda_z^\varepsilon(a'), \lambda_z^\varepsilon(c) + \lambda_z^\varepsilon(b')) \in \eta_2.$$

In the second case, $(c+a,c+b)\in\eta_1$ implies that $(\lambda_z^\varepsilon(c)+\lambda_z^\varepsilon(a),\lambda_z^\varepsilon(c)+\lambda_z^\varepsilon(b))=(\lambda_z^\varepsilon(c+a),\lambda_z^\varepsilon(c+b))\in\eta_1$. So, $(\lambda_z^\varepsilon(a),\lambda_z^\varepsilon(b))\in\eta_2$, for $\varepsilon=\pm1$. Therefore,

$$\eta_2=\{(\lambda_z(a),\lambda_z(b))\mid(a,b)\in\eta_2\}=\{(\lambda_z^{-1}(a),\lambda_z^{-1}(b))\mid(a,b)\in\eta_2\}.$$

By induction on n, we obtain

$$\eta_n=\{(\lambda_z(a),\lambda_z(b))\mid(a,b)\in\eta_n\}=\{(\lambda_z^{-1}(a),\lambda_z^{-1}(b))\mid(a,b)\in\eta_n\},$$

and thus,

$$\eta=\{(\lambda_z(a),\lambda_z(b))\mid(a,b)\in\eta\}=\{(\lambda_z^{-1}(a),\lambda_z^{-1}(b))\mid(a,b)\in\eta\},$$

as desired. □

We do not know whether $\lambda_a=\lambda_b$, for all $(a,b)\in\eta$ and whether η is a congruence on $(M(X,r),\circ)$, for any left non-degenerate solution (X,r). In Subsection 4.1.1, we will show that for bijective non-degenerate solutions, η is equal to the least left cancellative congruence on $(M,\circ)$, and $\lambda_a=\lambda_b$, for all $(a,b)\in\eta$. This generalizes the first part of [97, Proposition 4.2].

Following [53, Section 2] (Cedó, Jespers, and Verwimp), we resolve this problem, by considering another congruence μ on $(M(X,r),+)$ such that $\overline{M}=M(X,r)/\mu$ is left cancellative, as follows. We will define μ as the least binary relation on $M=M(X,r)$ satisfying that μ is a congruence on $(M,+)$, it is also a congruence on $(M,\circ)$, $(M,+)/\mu$ is left cancellative and $(\lambda_c^\varepsilon(a),\lambda_d^\varepsilon(b))\in\mu$, for all $(a,b),(c,d)\in\mu$ and $\varepsilon\in\{-1,1\}$. Later, we will prove that $\overline{M}$ has a YB-semitruss structure. As a consequence, this YB-semitruss is a left cancellative YB-semitruss. We will give a description of the elements in μ. Let $\mu_0=\eta_0$, a reflexive and symmetric binary relation on M. For $m\geq0$, define

$$\begin{aligned}
\mu_{4m+1}=&\{(a,b)\in M^2\mid\exists\, a_1,\dots,a_n\in M\text{ such that }(a,a_1),(a_1,a_2),\dots,(a_n,b)\in\mu_{4m}\},\\
\mu_{4m+2}=&\{(\lambda_z^\varepsilon(a\circ c),\lambda_z^\varepsilon(b\circ c))\in M^2\mid z,c\in M,\ \varepsilon\in\{-1,1\}\text{ and }(a,b)\in\mu_{4m+1}\},\\
\mu_{4m+3}=&\{(a,b)\in M^2\mid\exists\, a_1,\dots,a_n\in M\text{ such that }(a,a_1),(a_1,a_2),\dots,(a_n,b)\in\mu_{4m+2}\},\\
\mu_{4(m+1)}=&\{(c+a+d,c+b+d)\in M^2\mid c,d\in M\text{ and }(a,b)\in\mu_{4m+3}\}\\
&\cup\{(a,b)\in M^2\mid\exists\, c\in M\text{ such that }(c+a,c+b)\in\mu_{4m+3}\}.
\end{aligned}$$

Note that $\mu_n\subseteq\mu_{n+1}$, for all $n\geq0$. Let $\mu=\cup_{n=0}^\infty\mu_n$.

Lemma 3.1.23. *Let (X,r) be a left non-degenerate set-theoretic solution of the Yang-Baxter equation, and consider the unital structure YB-semitruss $(M,+,\circ,\lambda,\sigma)$ associated to (X,r), with $M=M(X,r)$. With the above notation, μ is a congruence on $(M,+)$, and it is a congruence on $(M,\circ)$. Furthermore, both $(M,+)/\mu$ and $(M,\circ)/\mu$ are left cancellative monoids, and*

$$(\lambda_c(a),\lambda_d(b)),(\lambda_c^{-1}(a),\lambda_d^{-1}(b))\in\mu,$$

for all $(a,b),(c,d)\in\mu$.

Proof. First, we prove that μ is a congruence on $(M,+)$. Since each μ_n is reflexive and symmetric, so is μ. Let $a,b,c \in M$ with $(a,b),(b,c) \in \mu$. There exists a positive integer m such that $(a,b),(b,c) \in \mu_{2m}$. Since μ_{2m+1} is the transitive closure of μ_{2m}, we have that $(a,c) \in \mu_{2m+1} \subseteq \mu$. So, μ is an equivalence relation.

Let $(a,b) \in \mu$ and $c,d \in M$. There exists a positive integer m such that $(a,b) \in \mu_{4m+3}$. Thus, $(c+a+d, c+b+d) \in \mu_{4(m+1)} \subseteq \mu$. Hence, μ is a congruence on $(M,+)$.

Now, we prove that $(M,+)/\mu$ is a left cancellative monoid. Let $(c,d) \in \mu$ and $a,b \in M$ such that $(c+a, d+b) \in \mu$. Since μ is a congruence on $(M,+)$, we have that $(d+a, c+a) \in \mu$. So, using transitivity, $(d+a, d+b) \in \mu$. There exists a positive integer m such that $(d+a, d+b) \in \mu_{4m+3}$. Thus, $(a,b) \in \mu_{4(m+1)} \subseteq \mu$, as desired.

Let $(a,b) \in \mu$ and $c,d \in M$. There exists a positive integer m such that $(a,b) \in \mu_{4m+1}$. It follows that $(\lambda_d(a \circ c), \lambda_d(b \circ c)) \in \mu_{4m+2}$ and $(d \circ a \circ c, d \circ b \circ c) = (d + \lambda_d(a \circ c), d + \lambda_d(b \circ c)) \in \mu_{4(m+1)} \subseteq \mu$. Hence, μ is a congruence on $(M,\circ)$.

Next, we prove that $(M,\circ)/\mu$ is a left cancellative monoid. Let $(c,d) \in \mu$ and $a,b \in M$ such that $(c \circ a, d \circ b) \in \mu$. As μ is a congruence on $(M,\circ)$, we get that $(d \circ a, c \circ a) \in \mu$. So, using transitivity, $(d + \lambda_d(a), d + \lambda_d(b)) = (d \circ a, d \circ b) \in \mu$. Since $(M,+)/\mu$ is a left cancellative monoid we get that $(\lambda_d(a), \lambda_d(b)) \in \mu$. Now there exists a positive integer m such that $(\lambda_d(a), \lambda_d(b)) \in \mu_{4m+1}$, and thus $(a,b) \in \mu_{4m+2} \subseteq \mu$, as desired.

We are left to prove that, for any $(a,b),(c,d) \in \mu$,

$$(\lambda_c(a), \lambda_d(b)), (\lambda_c^{-1}(a), \lambda_d^{-1}(b)) \in \mu.$$

Let $(a,b),(c,d) \in \mu$. Since μ is a congruence on $(M,\circ)$, we have that

$$(c + \lambda_c(x), d + \lambda_d(x)) = (c \circ x, d \circ x) \in \mu,$$

for all $x \in M$. As $(M,+)/\mu$ is a left cancellative monoid, we obtain that $(\lambda_c(x), \lambda_d(x)) \in \mu$, for all $x \in M$. Put $x = \lambda_c^{-1}(y)$. Then,

$$(y, \lambda_d \lambda_c^{-1}(y)) \in \mu,$$

for all $y \in M$. So, there exists a positive integer m such that $(y, \lambda_d \lambda_c^{-1}(y)) \in \mu_{4m+1}$. Therefore, $(\lambda_d^{-1}(y), \lambda_c^{-1}(y)) \in \mu_{4m+2} \subseteq \mu$, for all $y \in M$. So, there exists a positive integer k such that

$$(\lambda_d^{-1}(a), \lambda_c^{-1}(a)), (\lambda_d(a), \lambda_c(a)), (a,b) \in \mu_{4k+1}.$$

Hence,

$$(\lambda_c^{-1}(a), \lambda_d^{-1}(a)), (\lambda_d^{-1}(a), \lambda_d^{-1}(b)), (\lambda_c(a), \lambda_d(a)), (\lambda_d(a), \lambda_d(b)) \in \mu_{4k+2},$$

which implies

$$(\lambda_c(a), \lambda_d(b)), (\lambda_c^{-1}(a), \lambda_d^{-1}(b)) \in \mu_{4k+3} \subseteq \mu,$$

as desired. □

Let (X,r) be a left non-degenerate solution, and consider the unital structure YB-semitruss $(M,+,\circ,\lambda,\sigma)$ associated to (X,r), with $M=M(X,r)$. With the above notation, let $\overline{M}=M/\mu$ and consider the natural map $M\to\overline{M}:a\mapsto\overline{a}$. Let $\overline{\lambda}:(\overline{M},\circ)\to\operatorname{Aut}(\overline{M},+):\overline{a}\mapsto\overline{\lambda}_{\overline{a}}$ defined by $\overline{\lambda}_{\overline{a}}(\overline{b})=\overline{\lambda_a(b)}$, for all $\overline{a},\overline{b}\in\overline{M}$.

Note that $\overline{\lambda}$ is well-defined, because if $\overline{c}=\overline{a}$ and $\overline{d}=\overline{b}$, then, by Lemma 3.1.23,

$$\overline{\lambda_a(b)}=\overline{\lambda_c(d)}.$$

Now it is easy to check that $\overline{\lambda}_{\overline{a}}\in\operatorname{Aut}(\overline{M},+)$, in fact $(\overline{\lambda}_{\overline{a}})^{-1}:\overline{M}\to\overline{M}$ is the map defined by $(\overline{\lambda}_{\overline{a}})^{-1}(\overline{b})=\overline{\lambda_a^{-1}(b)}$, which is well-defined by Lemma 3.1.23. Furthermore, by Lemma 3.1.23, $(\overline{M},\circ)$ is left cancellative and $\overline{\lambda}$ is a homomorphism such that $\overline{a}\circ\overline{b}=\overline{a}+\overline{\lambda}_{\overline{a}}(\overline{b})$, for all $\overline{a},\overline{b}\in\overline{M}$. Moreover, by Example 3.1.1, $(\overline{M},+,\circ,\overline{\lambda})$ is a left semitruss.

Define $\overline{\sigma}:(\overline{M},+)\to\operatorname{End}(\overline{M},+):\overline{a}\mapsto\overline{\sigma}_{\overline{a}}$ by $\overline{\sigma}_{\overline{a}}(\overline{b})=\overline{\sigma_a(b)}$, for all $\overline{a},\overline{b}\in\overline{M}$. Then, one shows that $\overline{\sigma}$ is well-defined as follows. Let $\overline{c}=\overline{a}$ and $\overline{d}=\overline{b}$. Then,

$$\overline{a}+\overline{\sigma}_{\overline{a}}(\overline{b})=\overline{a}+\overline{\sigma_a(b)}=\overline{b}+\overline{a}=\overline{d}+\overline{c}=\overline{c}+\overline{\sigma_c(d)}=\overline{c}+\overline{\sigma}_{\overline{c}}(\overline{d})=\overline{a}+\overline{\sigma}_{\overline{c}}(\overline{d}).$$

As $(\overline{M},+)$ is left cancellative, we get that $\overline{\sigma}_{\overline{a}}(\overline{b})=\overline{\sigma}_{\overline{c}}(\overline{d})$, as desired. Furthermore, it is clear that $\overline{\sigma}$ is an anti-homomorphism, and $\overline{\sigma}_{\overline{a}}\in\operatorname{End}(\overline{M},+)$, for all $\overline{a}\in\overline{M}$.

Example 3.1.24. *Let (X,r) be a left non-degenerate solution and let μ be the left cancellative congruence on $(M(X,r),+)$ from Lemma 3.1.23. Put $\overline{M}=M/\mu$. Then, $(\overline{M},+,\circ,\overline{\lambda})$ is a left semitruss. Furthermore, $\overline{\sigma}:(\overline{M},+)\to\operatorname{End}(\overline{M},+):\overline{a}\mapsto\overline{\sigma}_{\overline{a}}$ defined above satisfies $\overline{a}+\overline{b}=\overline{b}+\overline{\sigma}_{\overline{b}}(\overline{a})$, for all $\overline{a},\overline{b}\in\overline{M}$. We claim that $(\overline{M},+,\circ,\overline{\lambda},\overline{\sigma})$ is a left cancellative YB-semitruss. Indeed $(\overline{M},+)$ and $(\overline{M},\circ)$ are left cancellative and*

$$\overline{a}\circ\overline{b}=\overline{a}+\overline{\lambda}_{\overline{a}}(\overline{b})=\overline{\lambda}_{\overline{a}}(\overline{b})+\overline{\sigma}_{\overline{\lambda}_{\overline{a}}(\overline{b})}(\overline{a})=\overline{\lambda}_{\overline{a}}(\overline{b})\circ(\overline{\lambda}_{\overline{\lambda}_{\overline{a}}(\overline{b})})^{-1}\overline{\sigma}_{\overline{\lambda}_{\overline{a}}(\overline{b})}(\overline{a}),$$

for all $\overline{a},\overline{b}\in\overline{M}$. So, $(\overline{M},+,\circ,\overline{\lambda})$ is a left semitruss satisfying the assumptions of Proposition 3.1.21. Therefore, $(\overline{M},+,\circ,\overline{\lambda},\overline{\sigma})$ is a left cancellative YB-semitruss.

We end this subsection with some more examples of left cancellative YB-semitrusses. Left braces, skew left braces and left cancellative semi-braces are associative structures introduced to study left non-degenerate solutions. Recall from Subsection 1.3.1 that a left cancellative semi-brace is a triple $(A,+,\circ)$ with $(A,\circ)$ a group, $(A,+)$ a left cancellative semigroup, and such that the semi-brace relation $a\circ(b+c)=a\circ b+a\circ(\overline{a}+c)$ holds, for all $a,b,c\in A$, where $\overline{a}$ denotes the inverse of a in $(A,\circ)$. If $(A,+)$ is a group, the left cancellative semi-brace is called a skew (left) brace, and if $(A,+)$ is an abelian group, then the skew (left) brace is called a (left) brace. Note that for skew left braces, the semi-brace relation becomes $a\circ(b+c)=(a\circ b)-a+(a\circ c)$. We will now show that they all are examples of left cancellative YB-semitrusses.

Example 3.1.25. *A left cancellative semi-brace $(A,+,\circ)$ is a left cancellative YB-semitruss with $\lambda_a(b)=a\circ(\overline{a}+b)$ and $\sigma_b(a)=\lambda_b(\overline{b}\circ(a+b))=\lambda_b(\overline{b})+a+b$ for all $a,b\in A$. Conversely, a YB-semitruss with $(A,\circ)$ a group is a left cancellative semi-brace.*

Proof. Let $(A, +, \circ)$ be a left cancellative semi-brace and denote the identity of the group $(A, \circ)$ by 1. We will first show that 1 is a left identity of $(A, +)$. Since $1 + 1 = 1 \circ (1 + 1) = 1 \circ 1 + 1 \circ (\overline{1} + 1) = 1 + 1 + 1$, we get, by left cancellativity of $(A, +)$, that $1 = 1 + 1$. So, for any $a \in A$, $1 + a = 1 + 1 + a$ and thus $a = 1 + a$. By [37, Proposition 3], the map $\lambda : (A, \circ) \to \mathrm{Aut}(A, +) : a \mapsto \lambda_a$ with $\lambda_a(b) = a \circ (\overline{a} + b)$, for all $a, b \in A$, is a group homomorphism and for any $a, b, c \in A$, $a \circ (b + c) = a \circ b + a \circ (\overline{a} + c) = a \circ b + \lambda_a(c)$. Take $b = 1$, and we have $a \circ c = a + \lambda_a(c)$. So (3.2) and (3.3) are satisfied. Because $(A, \circ)$ is a group, for any $a, b \in A$, there exists a unique $x \in A$ such that $a \circ b = \lambda_a(b) \circ x$, namely $x = \rho_b(a) = \overline{\lambda_a(b)} \circ a \circ b$. Hence, by Proposition 3.1.21, $(A, +, \circ, \lambda, \sigma)$ is a YB-semitruss with $\sigma_b(a) = \lambda_b \rho_{\lambda_a^{-1}(b)}(a) = \lambda_b(\overline{\lambda_a(\lambda_a^{-1}(b))} \circ a \circ \lambda_a^{-1}(b)) = \lambda_b(\overline{b} \circ (a + b)) = \lambda_b(\overline{b} + \lambda_{\overline{b}}(a + b)) = \lambda_b(\overline{b}) + a + b$.

Conversely, let $(A, +, \circ, \lambda, \sigma)$ be a YB-semitruss with $(A, \circ)$ a group. Then, by Lemma 3.1.20, $(A, +)$ is a left cancellative semigroup. Furthermore, (3.2) yields $\lambda_{\overline{a}} = \lambda_a^{-1}$, for all $a \in A$. Thus, by (3.3), $\overline{a} \circ \lambda_a(b) = \overline{a} \circ \lambda_{\overline{a}}^{-1}(b) = \overline{a} + b$, and therefore, $\lambda_a(b) = a \circ (\overline{a} + b)$, for all $a, b \in A$. Finally, for any $a, b, c \in A$, $a \circ (b + c) = a + \lambda_a(b + c) = a + \lambda_a(b) + \lambda_a(c) = (a \circ b) + a \circ (\overline{a} + c)$. Therefore, $(A, +, \circ)$ is a left cancellative semi-brace. □

The last statement of the following example has been proven in [37]. For completeness' sake we include a short proof.

Example 3.1.26. *A skew left brace $(A, +, \circ)$ is a unital left cancellative YB-semitruss $(A, +, \circ, \lambda, \sigma)$ where both $(A, +)$ and $(A, \circ)$ are groups, $\lambda_a(b) = -a + a \circ b$ and $\sigma_b(a) = -b + a + b$, for all $a, b \in A$. Conversely, a YB-semitruss $(A, +, \circ, \lambda, \sigma)$ with both $(A, +)$ and $(A, \circ)$ groups is a skew left brace.*

Furthermore, a left cancellative semi-brace with ρ_a bijective, for any $a \in A$, is a skew left brace.

Proof. Since any skew left brace is a left cancellative semi-brace, the first part of the claim is clear by the previous example. Recall from Subsection 1.3.1 that the identity of $(A, +)$ and $(A, \circ)$ coincide, and denote it by 1. Hence, for any $a, b \in A$, $\lambda_a(b) = a \circ (\overline{a} + b) = -a + (a \circ 1) + (a \circ (\overline{a} + b)) = -a + a \circ (1 + b) = -a + (a \circ b)$, and since $1 = b \circ \overline{b} = b + \lambda_b(\overline{b})$, we have that $\sigma_b(a) = \lambda_b(\overline{b}) + a + b = -b + a + b$. Conversely, if $(A, +, \circ, \lambda, \sigma)$ is a YB-semitruss with $(A, +)$ and $(A, \circ)$ groups, by Example 3.1.25, $(A, +, \circ)$ it is a left cancellative semi-brace with $(A, +)$ a group. Hence, $(A, +, \circ)$ is a skew left brace.

Let $(A, +, \circ)$ be a left cancellative semi-brace and assume that ρ_a is bijective for any $a \in A$. By the previous example, we know that $(A, +, \circ, \lambda, \sigma)$ is a YB-semitruss. Hence, $\lambda : (A, \circ) \to \mathrm{Aut}(A, +)$ is a monoid homomorphism and, by Lemma 3.1.6, $\rho : (A, \circ) \to \mathrm{Map}(A, A) : a \mapsto \rho_a$ is a monoid anti-homomorphism. In particular, since λ_a and ρ_a are bijective for any $a \in A$, we get $\lambda_1 = \mathrm{id}_A$ and $\rho_1 = \mathrm{id}_A$, where 1 denotes the identity of $(A, \circ)$. Moreover, by (3.11) and since $(A, \circ)$ is a group, $\rho_b(a) = \overline{(\lambda_a(b))} \circ a \circ b = \overline{a \circ (\overline{a} + b)} \circ a \circ b = \overline{(\overline{a} + b)} \circ \overline{a} \circ a \circ b = \overline{(\overline{a} + b)} \circ b$, which yields

$$a + b = b \circ \overline{\rho_b(\overline{a})}. \tag{3.17}$$

For any $a \in A$, we have $1 + a = 1 + \lambda_1(a) = 1 \circ a = a$ and, by (3.17), $a + 1 = 1 \circ \overline{\rho_1(\overline{a})} = \overline{\overline{a}} = a$. Hence, 1 is also an identity for $(A, +)$. Furthermore, put $b = \lambda_a(\overline{a})$. Then

$a+b=a+\lambda_a(\overline{a})=a\circ\overline{a}=1$. Since $\overline{\rho_{\overline{a}}(a)}=\overline{\overline{(\overline{a}+\overline{a})}\circ\overline{a}}=a\circ(\overline{a}+\overline{a})=\lambda_a(\overline{a})=b$ we also obtain, by (3.17), that $b+a=a\circ\overline{\rho_a(\overline{b})}=a\circ\overline{\rho_a\rho_{\overline{a}}(a)}=a\circ\overline{\rho_{\overline{a}\circ a}(a)}=a\circ\overline{\rho_1(a)}=a\circ\overline{a}=1$. Therefore, $(A,+)$ is a group and $(A,+,\circ)$ is a skew left brace. □

Let (X,r) be a bijective non-degenerate set-theoretic solution. Then, $(G(X,r),+,\circ)$ is a skew left brace by a result of Guarnieri and Vendramin [92, Theorem 3.9]. Another way to show this is by proving (similar as the proof for Theorem 3.1.13) that $(G(X,r),+,\circ,\lambda,\sigma)$ is a YB-semitruss and then use Example 3.1.26.

Note that if $(B,+,\circ)$ is a skew left brace, the opposite YB-semitruss as defined in Proposition 3.1.4 is a skew left brace and the definition coincides with the definition of an opposite skew left brace given in [117, Proposition 3.1].

In order to deal with degenerate and non-bijective solutions the notion of a left semi-brace has been introduced in [105], see also Subsection 1.3.1. In general this is not a YB-semitruss as, for example, $A+b$ is not necessarily contained in $b+A$. It is easy to see that a left semi-brace is a YB-semitruss if and only if it is a left cancellative semi-brace. Furthermore, Catino, Colazzo and Stefanelli in [40] and Catino, Mazzotta and Stefanelli in [42] introduced a generalization of left semi-braces. In general these do not yield left non-degenerate solutions.

We conclude this section with an example of a left cancellative YB-semitruss that is finite but is not a left cancellative semi-brace. It is an example where $(A,\circ)$ is not a group.

Example 3.1.27. *Let $A=\{1,2,3,4\}$. Define for any $a,b\in A$, $a+b=b$, $\sigma_b(a)=b$ and $a\circ b=\lambda_a(b)$, where $\lambda_1=\lambda_2=\mathrm{id}_A$ and $\lambda_3=\lambda_4=(13)(24)$. Then $(A,+,\circ,\lambda,\sigma)$ is a YB-semitruss with $(A,+)$ left cancellative and the ρ-map is given by $\rho_1=\rho_3:t\mapsto 1$ and $\rho_2=\rho_4:t\mapsto 2$. In particular, $1\circ 1=2\circ 1$, so $(A,\circ)$ is not a group.*

3.1.3 Idempotents in YB-semitrusses

For a semigroup $(S,*)$, we denote by $E_*(S)$ its subset of idempotents. Let $(A,+,\circ,\lambda,\sigma)$ be a YB-semitruss, then we have two subsets of idempotents $E_+(A)$ and $E_\circ(A)$. In [37, Proposition 5], it is proven that if $(A,+,\circ)$ is a left cancellative semi-brace, then $E_+(A)$ is a right-zero semigroup, i.e. $e+f=f$, for all $e,f\in E_+(A)$, $E_+(A)$ is a subsemigroup of $(A,\circ)$, and $(E_+(A),+,\circ)$ is a left cancellative semi-brace. Furthermore, $(A,+)$ is the direct sum of the maximal subgroup $(A+1,+)$ and the right zero semigroup $(E_+(A),+)$, where $\{1\}=E_\circ(A)$. It is shown that $A+1$ is a subgroup of $(A,\circ)$ and $(A+1,+,\circ)$ is a skew left brace. We will prove that for an arbitrary YB-semitruss $(A,+,\circ,\lambda,\sigma)$, $(E_+(A),+)$ is subsemigroup of $(A,+)$ and $(E_\circ(A),\circ)$ is a subsemigroup of $(A,\circ)$. Actually, we will show that $(E_+(A),+,\circ,\lambda,\sigma)$ is a sub-YB-semitruss and $(E_\circ(A),+,\circ,\lambda)$ is a sub-semitruss of A. In the terminology of [2], $(A,+)$ and $(A,\circ)$ are E-semigroups and they thus both have a so-called E-unitary cover.

Proposition 3.1.28. *Let $(A,+,\circ,\lambda,\sigma)$ be a YB-semitruss. The following properties hold.*

(1) $\lambda_e = \mathrm{id}_A$*, for any* $e \in E_\circ(A)$*.*

(2) $\sigma_e^2 = \sigma_e$*, for any* $e \in E_+(A)$*.*

(3) $E_\circ(A) \subseteq E_+(A)$*.*

(4) $E_+(A)$ *is a sub-YB-semitruss of* A*.*

(5) $E_\circ(A)$ *is a sub-semitruss of* A*.*

(6) If the associated solution (A, r_A) *is bijective, then* $(E_+(A), +)$ *and* $(E_\circ(A), \circ)$ *are commutative semigroups.*

Proof. (1) Let $e \in E_\circ(A)$. Since λ_e is bijective and $\lambda_e^2 = \lambda_{e\circ e} = \lambda_e$, the first property is clear.

(2) Let $e \in E_+(A)$. By (3.5), $\sigma_e^2 = \sigma_e \sigma_e = \sigma_{e+e} = \sigma_e$.

(3) Let $e \in E_\circ(A)$. Then, by the first property, $e = e \circ e = e + \lambda_e(e) = e + e$, and thus $e \in E_+(A)$.

(4) Let $e, f \in E_+(A)$. By (3.4),

$$(e+f)+(e+f) = e+f+f+\sigma_f(e) = e+f+\sigma_f(e) = e+e+f = e+f,$$

so $e+f \in E_+(A)$. Thus, $(E_+(A), +)$ is a subsemigroup of $(A, +)$. Since both λ_a and σ_a are endomorphisms of $(A, +)$, for all $a \in A$, we get that $\lambda_e(f) \in E_+(A)$ and $\sigma_e(f) \in E_+(A)$. It follows that $e \circ f = e + \lambda_e(f) \in E_+(A)$, so $(E_+(A), \circ)$ is a subsemigroup of $(A, \circ)$. We conclude that $E_+(A)$ is a sub-YB-semitruss of A.

(5) Let $e, f \in E_\circ(A)$. Then, by the previous results, (3.2) and (3.3),

$$\begin{aligned}(e\circ f)\circ(e\circ f) &= (e\circ f) + \lambda_{e\circ f}(e\circ f) = e+f+\lambda_e\lambda_f(e+f)\\ &\overset{(1)}{=} e+f+e+f \overset{(4)}{=} e+f = e\circ\lambda_e^{-1}(f) \overset{(1)}{=} e\circ f.\end{aligned}$$

Thus, $e \circ f \in E_\circ(A)$. So, by (1), also $e + f = e \circ \lambda_e^{-1}(f) = e \circ f \in E_\circ(A)$. Finally, by (1), $\lambda_e(f) = f \in E_\circ(A)$. It follows that $(E_\circ(A), +, \circ, \lambda)$ is a sub-semitruss of A.

(6) Assume that r_A, defined by (3.10), is bijective. So, by Proposition 3.1.3, σ_a is bijective, for all $a \in A$. Hence, by the second property, we get that $\sigma_e = \mathrm{id}_A$ for any $e \in E_+(A)$. Therefore, for any $e, f \in E_+(A)$, by (3.4), $e + f = f + \sigma_f(e) = f + e$, and $(E_+(A), +)$ is commutative. For $e, f \in E_\circ(A) \subseteq E_+(A)$, by the first property, we obtain $e \circ f = e + \lambda_e(f) = e + f = f + e = f \circ \lambda_f^{-1}(e) = f \circ e$. So, also $(E_\circ(A), \circ)$ is commutative. □

Recall that if S is a left cancellative semigroup, then any idempotent is a left identity. It induces some additional information on a left cancellative YB-semitruss.

Proposition 3.1.29. *Let* $(A, +, \circ, \lambda, \sigma)$ *be a YB-semitruss. If* $e \in E_+(A)$ *is a left identity of* $(A, +)$*, then* $\sigma_e(a) = a + e$*, for all* $a \in A$*. In particular, if* $(A, +, \circ, \lambda, \sigma)$ *is left cancellative, then* $E_\circ(A)$ *is a sub-YB-semitruss.*

Proof. Let $e \in E_+(A)$ be a left identity of $(A,+)$ and $a \in A$. By (3.4), we have

$$\sigma_e(a) = e + \sigma_e(a) = a + e.$$

Assume now that $(A,+)$ is left cancellative and let $e, f \in E_\circ(A)$. By Proposition 3.1.28(3), $e, f \in E_+(A)$. Hence, $\sigma_e(f) = f + e = e \in E_\circ(A)$. So, by Proposition 3.1.28(5), $E_\circ(A)$ is a sub-YB-semitruss of A. □

In case the associated solution of a left cancellative YB-semitruss is bijective, we can say more.

Proposition 3.1.30. *Let $(A,+,\circ,\lambda,\sigma)$ be a left cancellative YB-semitruss. If the associated solution (A,r_A) is bijective, then*

(1) $|E_+(A)| \leq 1$,

(2) $(A,+)$ is right cancellative.

In particular, in this case, if furthermore A is finite, then $(A,+)$ is a group.

Proof. (1) Let $e, f \in E_+(A)$. Since $(A,+)$ is left cancellative, e and f are also left identities. Moreover, since r_A is bijective, by Proposition 3.1.3, we have that σ_e is bijective. By Proposition 3.1.28, σ_e is also idempotent, and thus $\sigma_e = \mathrm{id}_A$. It follows that $e = f + e = e + \sigma_e(f) = e + f = f$.

(2) Let $a, b, c \in A$ such that $a + c = b + c$. Then, (3.4) yields $c + \sigma_c(a) = c + \sigma_c(b)$. Since $(A,+)$ is left cancellative, it follows that $\sigma_c(a) = \sigma_c(b)$. By Proposition 3.1.3, σ_c is bijective, and thus $a = b$. So, $(A,+)$ is right cancellative, as desired. □

Proposition 3.1.31. *Let $(A,+,\circ,\lambda,\sigma)$ be a YB-semitruss. If $(A,+)$ is a group, then $(A,\circ)$ is a group.*

Proof. Let $(A,+,\circ,\lambda,\sigma)$ be a YB-semitruss where $(A,+)$ is a group. By Lemma 3.1.20, we have that $(A,\circ)$ is left cancellative. Let 0 denote the identity of $(A,+)$. We claim that $0 \in E_\circ(A)$ so in particular, 0 is a left identity in $(A,\circ)$. First note that $\lambda_0(0) = \lambda_0(0+0) = \lambda_0(0) + \lambda_0(0)$, i.e. $\lambda_0(0) = 0$. This implies, by (3.3), $0 \circ 0 = 0 + \lambda_0(0) = 0$, and thus indeed $0 \in E_\circ(A)$. Similarly, for $a \in A$, we get $\lambda_a(0) = \lambda_a(0+0) = \lambda_a(0) + \lambda_a(0)$, so $\lambda_a(0) = 0$. It follows that $a \circ 0 = a + \lambda_a(0) = a + 0 = a$. Hence, 0 is also a right identity in $(A,\circ)$, and $(A,\circ)$ is a monoid. Put $b = \lambda_a^{-1}(-a)$. Then, by (3.3), $a \circ b = a \circ \lambda_a^{-1}(-a) = a + (-a) = 0$. Therefore, any $a \in A$ has a right inverse in $(A,\circ)$. It follows that $(A,\circ)$ is a group. □

By Example 3.1.26, a YB-semitruss with $(A,+)$ and $(A,\circ)$ groups is a skew left brace. Hence, the following corollary follows naturally.

Corollary 3.1.32. *Let $(A,+,\circ,\lambda,\sigma)$ be a YB-semitruss. If $(A,+)$ is a group, then $(A,+,\circ)$ is a skew left brace and the associated solution (A,r_A) is bijective and non-degenerate.*

Recall (see for example [58]) that a regular semigroup S is a semigroup such that, for any $a \in S$, there exists $b \in S$, with $aba = a$. An element $a \in S$ with this property is called a regular element. If moreover any two idempotents in S commute, then S is called an inverse semigroup [58, Theorem 1.17].

Lemma 3.1.33. *Let $(A, +, \circ, \lambda, \sigma)$ be a YB-semitruss. If $a \in A$ is regular in $(A, \circ)$, then a is regular in $(A, +)$.*

Proof. Let $a \in A$ be regular in $(A, \circ)$, and $b \in A$ such that $a \circ b \circ a = a$. Then, by (3.2) and (3.3),

$$\begin{aligned} a &= a \circ b \circ a \\ &= a + \lambda_a(b + \lambda_b(a)) \\ &= a + \lambda_a(b) + \lambda_a\lambda_b(a) \\ &= a + \lambda_a(b) + \lambda_a\lambda_b\lambda_a\lambda_a^{-1}(a) \\ &= a + \lambda_a(b) + \lambda_{a\circ b\circ a}\lambda_a^{-1}(a) \\ &= a + \lambda_a(b) + \lambda_a\lambda_a^{-1}(a) \\ &= a + \lambda_a(b) + a. \end{aligned}$$

So, $a + \lambda_a(b) + a = a$, and a is regular in $(A, +)$, as desired. □

Proposition 3.1.34. *Let $(A, +, \circ, \lambda, \sigma)$ be a YB-semitruss. If $E_+(A) = E_\circ(A)$ and $(A, \circ)$ is an inverse semigroup, then $(A, +)$ is an inverse semigroup.*

Proof. By Proposition 3.1.28(1), $e \circ a = e + \lambda_e(a) = e + a$, for any $e \in E_\circ(A) = E_+(A)$ and $a \in A$. Hence, if $(A, \circ)$ is an inverse semigroup, then any two idempotents commute, and thus $e + f = e \circ f = f \circ e = f + e$, for all $e, f \in E_\circ(A) = E_+(A)$. Hence, $(E_+(A), +)$ is a commutative semigroup and thus, by Lemma 3.1.33, the result follows. □

3.1.4 Matched product of solutions and YB-semitrusses

One way to create new examples of algebraic structures is to built them from two given examples. For the associative examples of Subsection 3.1.2, many constructions have been defined and studied, such as the (semi-)direct product, the asymmetric product and the matched product, see for example [7, 11, 12, 36, 37, 43, 59, 173]. To define the matched product of two left cancellative semi-braces (or two (skew) left braces) A and B, one needs two actions satisfying certain conditions. Using these actions, one defines the operations $+$ and $\circ$ on $A \times B$ such that $(A \times B, +, \circ)$ becomes a left cancellative semi-brace. In particular, the multiplicative group $(A \times B, \circ)$ is the Zappa-Szép product of the groups $(A, \circ_A)$ and $(B, \circ_B)$ [38], i.e. $(A, \circ_A)$ and $(B, \circ_B)$ form a matched pair of groups [178]. We will generalize this idea and define the matched product of YB-semitrusses. In particular, the multiplicative structure of the matched product of two unital YB-semitrusses forms a matched pair of monoids. Matched pairs of monoids were successfully used by Gateva-Ivanova and Majid in [86] to construct new solutions, by defining the matched product of solutions. We end this section by proving that the solution associated to the matched product of two YB-semitrusses is equal to the matched product of the solutions associated to those two YB-semitrusses.

Definition 3.1.35. *Let $(A,+,\circ,\lambda,\sigma)$ and $(B,+',\circ',\lambda',\sigma')$ be YB-semitrusses, with $\alpha:(B,\circ')\to\operatorname{Aut}(A,+)$ and $\beta:(A,\circ)\to\operatorname{Aut}(B,+')$ semigroup morphisms such that*

$$\lambda_a\alpha_{\beta_a^{-1}(u)} = \alpha_u\lambda_{\alpha_u^{-1}(a)}, \qquad \lambda'_u\beta_{\alpha_u^{-1}(a)} = \beta_a\lambda'_{\beta_a^{-1}(u)}, \tag{3.18}$$

$$\alpha_u\,\sigma_a = \sigma_{\alpha_u(a)}\,\alpha_u, \qquad \beta_a\,\sigma'_u = \sigma'_{\beta_a(u)}\,\beta_a, \tag{3.19}$$

for all $a\in A$, $u\in B$. The quadruple (A,B,α,β) is called a matched product system of YB-semitrusses.

In order to show that the matched product of a matched product system of YB-semitrusses is again a YB-semitruss, the following lemma is needed. It provides sufficient conditions to define a left semitruss structure on a given semigroup with a given λ-map.

Lemma 3.1.36. *Let $(A,+)$ be a semigroup and $\lambda:A\to\operatorname{End}(A,+):a\mapsto\lambda_a$. Define, for any $a,b\in A$, $a\circ b=a+\lambda_a(b)$. If $\lambda_{a+\lambda_a(b)}=\lambda_a\lambda_b$ holds, for all $a,b\in A$, then $(A,+,\circ,\lambda)$ is a left semitruss.*

Proof. Define, for any $a,b\in A$, $a\circ b=a+\lambda_a(b)$. Let $a,b,c\in A$. Then,

$$\begin{aligned}(a\circ b)\circ c &= (a+\lambda_a(b))\circ c = a+\lambda_a(b)+\lambda_{a+\lambda_a(b)}(c)\\ &= a+\lambda_a(b)+\lambda_a\lambda_b(c) = a+\lambda_a(b+\lambda_b(c))\\ &= a\circ(b\circ c).\end{aligned}$$

Thus, $(A,\circ)$ is a semigroup. Moreover,

$$a\circ(b+c) = a+\lambda_a(b+c) = a+\lambda_a(b)+\lambda_a(c) = (a\circ b)+\lambda_a(c).$$

So, the left semitruss identity (3.1) is satisfied, and $(A,+,\circ,\lambda)$ is a left semitruss, as desired. □

We will now prove that any matched product system of YB-semitrusses (A,B,α,β) gives rise to a YB-semitruss structure on the set $A\times B$.

Theorem 3.1.37. *Let $(A,+,\circ,\lambda,\sigma)$ and $(B,+',\circ',\lambda',\sigma')$ be YB-semitrusses, and $\alpha:(B,\circ')\to\operatorname{Aut}(A,+)$ and $\beta:(A,\circ)\to\operatorname{Aut}(B,+')$ be semigroup morphisms, such that (A,B,α,β) is a matched product system of YB-semitrusses. Define*

$$(a,u)+(b,v) = (a+b,u+'v), \tag{3.20}$$

$$(a,u)\circ(b,v) = (\alpha_u(\alpha_u^{-1}(a)\circ b),\beta_a(\beta_a^{-1}(u)\circ' v)), \tag{3.21}$$

$$\lambda_{(a,u)}(b,v) = (\lambda_a\alpha_{\beta_a^{-1}(u)}(b),\lambda'_u\beta_{\alpha_u^{-1}(a)}(v)), \tag{3.22}$$

$$\sigma_{(a,u)}(b,v) = (\sigma_a(b),\sigma'_u(v)), \tag{3.23}$$

for all $(a,u),(b,v)\in A\times B$. Then, $(A\times B,+,\circ,\lambda,\sigma)$ is a YB-semitruss, called the matched product of A and B (via α and β), *and denote it by $A\bowtie B$.*

Proof. Let $a, b, c \in A$ and $u, v, w \in B$, and put $\tilde{a} = \alpha_u^{-1}(a)$, $\tilde{u} = \beta_a^{-1}(u)$, $\tilde{b} = \alpha_v^{-1}(b)$, $\tilde{v} = \beta_b^{-1}(v)$. First, note that, by (3.18),

$$\alpha_u(\tilde{a} \circ b) = \alpha_u(\tilde{a} + \lambda_{\tilde{a}}(b)) = \alpha_u(\tilde{a}) + \alpha_u\lambda_{\tilde{a}}(b)) = a + \lambda_a\alpha_{\tilde{u}}(b) = a \circ \alpha_{\tilde{u}}(b), \tag{3.24}$$

and

$$\beta_a(\tilde{u} \circ' v) = \beta_a(\tilde{u} +' \lambda'_{\tilde{u}}(v)) = \beta_a(\tilde{u}) +' \beta_a\lambda'_{\tilde{u}}(v)) = u +' \lambda'_u\beta_{\tilde{a}}(v) = u \circ' \beta_{\tilde{a}}(v). \tag{3.25}$$

Also, by (3.3) and (3.18),

$$\begin{aligned}
\alpha^{-1}_{\beta_{\tilde{a}}(v)}(\tilde{a} \circ b) &= \alpha^{-1}_{\beta_{\tilde{a}}(v)}(\tilde{a} + \lambda_{\tilde{a}}(b)) \\
&= \alpha^{-1}_{\beta_{\tilde{a}}(v)}(\tilde{a}) + \alpha^{-1}_{\beta_{\tilde{a}}(v)}(\lambda_{\tilde{a}}(b)) \\
&= \alpha^{-1}_{\beta_{\tilde{a}}(v)}(\tilde{a}) + \lambda_{\alpha^{-1}_{\beta_{\tilde{a}}(v)}(\tilde{a})}\alpha^{-1}_{\beta^{-1}_{\tilde{a}}(\beta_{\tilde{a}}(v))}(b) \\
&= \alpha^{-1}_{\beta_{\tilde{a}}(v)}(\tilde{a}) \circ \alpha_v^{-1}(b), \qquad (3.26)
\end{aligned}$$

and

$$\begin{aligned}
\beta^{-1}_{\alpha_{\tilde{u}}(b)}(\tilde{u} \circ' v) &= \beta^{-1}_{\alpha_{\tilde{u}}(b)}(\tilde{u} +' \lambda'_{\tilde{u}}(v)) \\
&= \beta^{-1}_{\alpha_{\tilde{u}}(b)}(\tilde{u}) +' \beta^{-1}_{\alpha_{\tilde{u}}(b)}(\lambda'_{\tilde{u}}(v)) \\
&= \beta^{-1}_{\alpha_{\tilde{u}}(b)}(\tilde{u}) +' \lambda'_{\beta^{-1}_{\alpha_{\tilde{u}}(b)}(\tilde{u})}\beta^{-1}_{\alpha^{-1}_{\tilde{u}}(\alpha_{\tilde{u}}(b))}(v) \\
&= \beta^{-1}_{\alpha_{\tilde{u}}(b)}(\tilde{u}) \circ' \beta_b^{-1}(v). \qquad (3.27)
\end{aligned}$$

It follows that, using (3.24), (3.27), and (3.18),

$$\begin{aligned}
\lambda_{\alpha_u(\tilde{a}\circ b)}\alpha_{\beta^{-1}_{\alpha_u(\tilde{a}\circ b)}\beta_a(\tilde{u}\circ' v)}(c) &= \lambda_{a\circ\alpha_{\tilde{u}}(b)}\alpha_{\beta^{-1}_{a\circ\alpha_{\tilde{u}}(b)}\beta_a(\tilde{u}\circ' v)}(c) \\
&= \lambda_a\lambda_{\alpha_{\tilde{u}}(b)}\alpha_{\beta^{-1}_{\alpha_{\tilde{u}}(b)}(\tilde{u}\circ' v)}(c) \\
&= \lambda_a\lambda_{\alpha_{\tilde{u}}(b)}\alpha_{\beta^{-1}_{\alpha_{\tilde{u}}(b)}(\tilde{u})\circ'\beta_b^{-1}(v)}(c) \\
&= \lambda_a\lambda_{\alpha_{\tilde{u}}(b)}\alpha_{\beta^{-1}_{\alpha_{\tilde{u}}(b)}(\tilde{u})}\alpha_{\beta_b^{-1}(v)}(c) \\
&= \lambda_a\alpha_{\tilde{u}}\lambda_{\alpha^{-1}_{\tilde{u}}\alpha_{\tilde{u}}(b)}\alpha_{\tilde{v}}(c) \\
&= \lambda_a\alpha_{\tilde{u}}\lambda_b\alpha_{\tilde{v}}(c).
\end{aligned}$$

Similarly, we have $\lambda'_{\beta_a(\tilde{u}\circ' v)}\beta_{\alpha^{-1}_{\beta_a(\tilde{u}\circ' v)}\alpha_u(\tilde{a}\circ b)}(w) = \lambda'_u\beta_{\tilde{a}}\lambda'_v\beta_{\tilde{b}}(w)$, using (3.25), (3.26), and (3.18). These yield, by (3.21), (3.22), and (3.18),

$$\begin{aligned}
\lambda_{(a,u)\circ(b,v)}(c, w) &= \lambda_{(\alpha_u(\tilde{a}\circ b),\beta_a(\tilde{u}\circ' v))}(c, w) \\
&= (\lambda_{\alpha_u(\tilde{a}\circ b)}\alpha_{\beta^{-1}_{\alpha_u(\tilde{a}\circ b)}(\beta_a(\tilde{u}\circ' v))}(c), \lambda'_{\beta_a(\tilde{u}\circ' v)}\beta_{\alpha^{-1}_{\beta_a(\tilde{u}\circ' v)}(\alpha_u(\tilde{a}\circ b))}(w)) \\
&= (\lambda_a\alpha_{\tilde{u}}\lambda_b\alpha_{\tilde{v}}(c), \lambda'_u\beta_{\tilde{a}}\lambda'_v\beta_{\tilde{b}}(w)) \\
&= \lambda_{(a,u)}(\lambda_b\alpha_{\tilde{v}}(c), \lambda'_v\beta_{\tilde{b}}(w)) \\
&= \lambda_{(a,u)}\lambda_{(b,v)}(c, w). \qquad (3.28)
\end{aligned}$$

Moreover, by (3.22),

$$\begin{aligned}\lambda_{(a,u)}(b,v)+\lambda_{(a,u)}(c,w)&=(\lambda_a\alpha_{\beta_a^{-1}(u)}(b),\lambda'_u\beta_{\alpha_u^{-1}(a)}(v))+(\lambda_a\alpha_{\beta_a^{-1}(u)}(c),\lambda'_u\beta_{\alpha_u^{-1}(a)}(w))\\&=(\lambda_a\alpha_{\beta_a^{-1}(u)}(b)+\lambda_a\alpha_{\beta_a^{-1}(u)}(c),\lambda'_u\beta_{\alpha_u^{-1}(a)}(v)+'\lambda'_u\beta_{\alpha_u^{-1}(a)}(w))\\&=(\lambda_a\alpha_{\beta_a^{-1}(u)}(b+c),\lambda'_u\beta_{\alpha_u^{-1}(a)}(v+'w))\\&=\lambda_{(a,u)}(b+c,v+'w),\end{aligned}$$

so $\lambda_{(a,u)}\in\mathrm{End}(A\times B,+)$. Furthermore, $\lambda_{(a,u)}$ is bijective and its inverse is given by $\lambda^{-1}_{(a,u)}(b,v)=(\alpha^{-1}_{\beta_a^{-1}(u)}\lambda_a^{-1}(b),\beta^{-1}_{\alpha_u^{-1}(a)}(\lambda'_u)^{-1}(v))$. Hence, $\lambda_{(a,u)}\in\mathrm{Aut}(A\times B,+)$, and condition (3.2) is satisfied.

Moreover, by (3.20), (3.22), (3.24), and (3.25), we have

$$(a,u)+\lambda_{(a,u)}(b,v)=(a+\lambda_a\alpha_{\tilde u}(b),u+'\lambda'_u\beta_{\tilde a}(v))=(\alpha_u(\tilde a\circ b),\beta_a(\tilde u\circ' v))=(a,u)\circ(b,v),$$

and $A\times B$ satisfies condition (3.3). It follows, using (3.28), that

$$\lambda_{(a,u)+\lambda_{(a,u)}(b,v)}=\lambda_{(a,u)\circ(b,v)}=\lambda_{(a,u)}\lambda_{(b,v)}.$$

Hence, by Lemma 3.1.36, we conclude that $(A\times B,+,\circ,\lambda)$ is a left semitruss. It remains to prove that conditions (3.4), (3.5) and (3.6) hold. Since the addition and the σ-map of $A\times B$ are defined componentwise, and (3.4) holds in both A and B, we get that $A\times B$ satisfies (3.4). With the same argument, (3.5) holds in $A\times B$ as it is satisfied in both A and B. By (3.22), (3.23), (3.6) and (3.19),

$$\begin{aligned}\sigma_{\lambda_{(a,u)}(c,w)}\,\lambda_{(a,u)}(b,v)&=\sigma_{(\lambda_a\alpha_{\beta_a^{-1}(u)}(c),\lambda'_u\beta_{\alpha_u^{-1}(a)}(w))}(\lambda_a\alpha_{\beta_a^{-1}(u)}(b),\lambda'_u\beta_{\alpha_u^{-1}(a)}(v))\\&=(\sigma_{\lambda_a\alpha_{\beta_a^{-1}(u)}(c)}(\lambda_a\alpha_{\beta_a^{-1}(u)}(b)),\sigma'_{\lambda'_u\beta_{\alpha_u^{-1}(a)}(w)}(\lambda'_u\beta_{\alpha_u^{-1}(a)}(v))\\&=(\lambda_a\,\sigma_{\alpha_{\beta_a^{-1}(u)}(c)}(\alpha_{\beta_a^{-1}(u)}(b)),\lambda'_u\,\sigma'_{\beta_{\alpha_u^{-1}(a)}(w)}(\beta_{\alpha_u^{-1}(a)}(v))\\&=(\lambda_a\alpha_{\beta_a^{-1}(u)}\,\sigma_c(b),\lambda'_u\beta_{\alpha_u^{-1}(a)}\,\sigma'_w(v))\\&=\lambda_{(a,u)}(\sigma_c(b),\sigma'_w(v))\\&=\lambda_{(a,u)}\,\sigma_{(c,w)}(b,v).\end{aligned}$$

Hence, (3.6) holds in $A\times B$. We conclude that $(A\times B,+,\circ,\lambda,\sigma)$ is a YB-semitruss. □

Via this construction we now give an example of a YB-semitruss that is not a left cancellative semi-brace, and such that the additive and multiplicative operations are different.

Example 3.1.38. *Let $A=\{1,\dots,n\}$ and define $a+b=a\circ b=b$, $\lambda_a=\mathrm{id}_A$ and $\sigma_a(b)=a$, for all $a,b\in A$. Then, $(A,+,\circ,\lambda,\sigma)$ is a YB-semitruss. Let $B=C_n=\mathrm{gr}(\xi)$, the cyclic group of n-elements, and consider the trivial left brace $(B,+,+)$ with $(B,+)=(B,\circ)=C_n$, i.e. a YB-semitruss with $\lambda_u=\sigma_u=\mathrm{id}_B$, for any $u\in B$. Define α as the natural action of C_n over A, i.e. $\alpha:B\to\mathrm{Map}(A,A)$ is defined by $\alpha(\xi^i)(a)=(1\ 2\ \dots n)^i(a)$. It is clear that $\alpha:(B,\circ)\to\mathrm{Aut}(A,+)$ is a semigroup homomorphism. Put $\beta_a=\mathrm{id}_B$, for* *all $a \in A$. Then,* (3.18) *and* (3.19) *are satisfied, and (A, B, α, β) is a matched product system of YB-semitrusses. The matched product of A and B becomes $(A \times B, +, \circ, \lambda, \sigma)$, defined in Theorem* 3.1.37*. In particular, for any $a, b \in A, \xi^i, \xi^j \in B$,*

$$(a, \xi^i) + (b, \xi^j) = (a + b, \xi^i + \xi^j) = (b, \xi^{i+j}),$$

and

$$(a, \xi^i) \circ (b, \xi^j) = (\alpha_{\xi^i}(\alpha_{\xi^i}^{-1}(a) \circ b), \xi^i \circ \xi^j) = ((1\ 2\ \dots n)^i(b), \xi^{i+j}).$$

To end this section, we establish a connection between the matched product of YB-semitrusses and the matched product of their solutions. This has already been done for left cancellative semi-braces in [37], and left braces in [7, 11].

For completeness' sake we recall the definition of a matched product of solutions given in [38]. Let (X, r_X) and (Y, r_Y) be set-theoretic solutions of the Yang-Baxter equation, and $\alpha : Y \to \mathrm{Sym}(X) : u \mapsto \alpha_u$ and $\beta : X \to \mathrm{Sym}(Y) : a \mapsto \beta_a$ are maps. Then, the quadruple $(r_X, r_Y, \alpha, \beta)$ is called a *matched product system of solutions* if the following conditions are satisfied

$$\alpha_u\alpha_v = \alpha_{\lambda_u(v)}\alpha_{\rho_v(u)}, \tag{3.29}$$

$$\beta_a\beta_b = \beta_{\lambda_a(b)}\beta_{\rho_b(a)}, \tag{3.30}$$

$$\rho_{\alpha_u^{-1}(b)}\alpha_{\beta_a(u)}^{-1}(a) = \alpha_{\beta_{\rho_b(a)}\beta_b^{-1}(u)}^{-1}\rho_b(a), \tag{3.31}$$

$$\rho_{\beta_a^{-1}(v)}\beta_{\alpha_u(a)}^{-1}(u) = \beta_{\alpha_{\rho_v(u)}\alpha_v^{-1}(a)}^{-1}\rho_v(u), \tag{3.32}$$

$$\lambda_a\alpha_{\beta_a^{-1}(u)} = \alpha_u\lambda_{\alpha_u^{-1}(a)}, \tag{3.33}$$

$$\lambda_u\beta_{\alpha_u^{-1}(a)} = \beta_a\lambda_{\beta_a^{-1}(u)}, \tag{3.34}$$

for all $a, b \in X$ and $u, v \in Y$.

As shown in [38, Theorem 1], any matched product system of solutions $(r_X, r_Y, \alpha, \beta)$ determines a new set-theoretic solution on the set $X \times Y$. More precisely, if $(r_X, r_Y, \alpha, \beta)$ is a matched product system of solutions, then the map $r : (X \times Y) \times (X \times Y) \to (X \times Y) \times (X \times Y)$ defined by

$$r((a, u), (b, v)) = ((\alpha_u\lambda_{\tilde{a}}(b),\ \beta_a\lambda_{\tilde{u}}(v)),\ (\alpha_{\tilde{U}}^{-1}\rho_{\alpha_{\tilde{u}}(b)}(a),\ \beta_{\tilde{A}}^{-1}\rho_{\beta_{\tilde{a}}(v)}(u))),$$

where

$$\tilde{a} = \alpha_u^{-1}(a),\ \tilde{u} = \beta_a^{-1}(u),\ A = \alpha_u\lambda_{\tilde{a}}(b),\ U = \beta_a\lambda_{\tilde{u}}(v),\ \tilde{A} = \alpha_U^{-1}(A),\ \tilde{U} = \beta_A^{-1}(U),$$

for all $(a, u), (b, v) \in X \times Y$, is a set-theoretic solution of the Yang-Baxter equation. This solution is called the *matched product* of the solutions r_X and r_Y (via α and β) and it is denoted by $r_X \bowtie r_Y$.

The proof of the following result is strongly based on [38, Theorem 9] and [39, Theorem 6].

Proposition 3.1.39. *Let $(A, +, \circ, \lambda, \sigma)$ and $(B, +', \circ', \lambda', \sigma')$ be YB-semitrusses such that (A, B, α, β) is a matched product system of YB-semitrusses. Then, $r_{A \bowtie B} = r_A \bowtie r_B$.*

Proof. Recall that if $(A, +, \circ, \lambda, \sigma)$ is a YB-semitruss, then

$$r_A(x, y) = (\lambda_x(y), \rho_y(x)) = (\lambda_x(y), \lambda^{-1}_{\lambda_x(y)}\, \sigma_{\lambda_x(y)}(x)),$$

is its associated solution. The λ-map and ρ-map of B are denoted by λ' and ρ' respectively. First, note that (3.18) is equivalent to (3.33) and (3.34). Let $a, b \in A$ and $u, v \in B$. Since α and β are semigroup morphism and since Proposition 3.1.5 holds for A and B, we get

$$\alpha_u \alpha_v = \alpha_{u \circ' v} = \alpha_{\lambda'_u(v) \circ' \rho'_v(u)} = \alpha_{\lambda'_u(v)} \alpha_{\rho'_v(u)},$$

i.e. (3.29) holds and with similar computations (3.30) holds as well. Moreover,

$$\begin{aligned}
\alpha^{-1}_{\beta_{\rho_b(a)}\beta^{-1}_b(u)} \rho_b(a) &= \alpha^{-1}_{\beta^{-1}_{\lambda_a(b)}\beta_a(u)} \rho_b(a) && \text{by (3.30)}\\
&= \alpha^{-1}_{\beta^{-1}_{\lambda_a(b)}\beta_a(u)} \lambda^{-1}_{\lambda_a(b)}\, \sigma_{\lambda_a(b)}(a) &&\\
&= \lambda^{-1}_{\alpha^{-1}_{\beta_a(u)}\lambda_a(b)} \alpha^{-1}_{\beta_a(u)}\, \sigma_{\lambda_a(b)}(a) && \text{by (3.18)}\\
&= \lambda^{-1}_{\alpha^{-1}_{\beta_a(u)}\lambda_a(b)}\, \sigma_{\alpha^{-1}_{\beta_a(u)}\lambda_a(b)}\, \alpha^{-1}_{\beta_a(u)}(a) && \text{by (3.19)}\\
&= \lambda^{-1}_{\lambda_{\alpha^{-1}_{\beta_a(u)}(a)}\alpha^{-1}_u(b)}\, \sigma_{\lambda_{\alpha^{-1}_{\beta_a(u)}(a)}\alpha^{-1}_u(b)}\, \alpha^{-1}_{\beta_a(u)}(a) && \text{by (3.18)}\\
&= \rho_{\alpha^{-1}_u(a)} \alpha^{-1}_{\beta_a(u)}(a), &&
\end{aligned}$$

Hence, (3.31) holds. With similar computations, we have that (3.32) holds. Therefore, $(r_A, r_B, \alpha, \beta)$ is a matched product of solutions. Now, we compare $r_A \bowtie r_B$ with $r_{A \bowtie B}$. The first component of $r_A \bowtie r_B$ is given by $(\alpha_u \lambda_{\alpha^{-1}_u(a)}(b), \beta_a \lambda'_{\beta^{-1}_a(u)}(v))$, which coincides with $\lambda_{(a,u)}(b, v)$ in $A \bowtie B$. Now, put

$$\begin{aligned}
\tilde{a} = \alpha^{-1}_u(a), &\quad \tilde{u} = \beta^{-1}_a(u),\\
A = \alpha_u \lambda_{\tilde{a}}(b) = \lambda_a \alpha_{\tilde{u}}(b), &\quad U = \beta_a \lambda'_{\tilde{u}}(v) = \lambda'_u \beta_{\tilde{a}}(v),\\
\tilde{A} = \alpha^{-1}_U(A), &\quad \tilde{U} = \beta^{-1}_A(U).
\end{aligned}$$

Then, the second component of $r_{A \bowtie B}$ is given by

$$\begin{aligned}
\lambda^{-1}_{\lambda_{(a,u)}(b,v)}\, \sigma_{\lambda_{(a,u)}(b,v)}(a, u) &= \lambda^{-1}_{(A,U)}\, \sigma_{(A,U)}(a, u)\\
&= (\lambda^{-1}_{\tilde{A}} \alpha^{-1}_U\, \sigma_A(a), (\lambda'_{\tilde{U}})^{-1} \beta^{-1}_A\, \sigma'_U(u))\\
&= (\alpha^{-1}_{\tilde{U}} \lambda^{-1}_A\, \sigma_A(a), \beta^{-1}_{\tilde{A}} (\lambda'_U)^{-1}\, \sigma'_U(u))\\
&= (\alpha^{-1}_{\tilde{U}} \lambda^{-1}_{\lambda_a \alpha_{\tilde{u}}(b)}\, \sigma_{\lambda_a \alpha_{\tilde{u}}(b)}(a), \beta^{-1}_{\tilde{A}} (\lambda'_{\lambda'_u \beta_{\tilde{a}}(v)})^{-1}\, \sigma'_{\lambda'_u \beta_{\tilde{a}}(v)}(u))\\
&= (\alpha^{-1}_{\tilde{U}} \rho_{\alpha_{\tilde{u}}(b)}(a), \beta^{-1}_{\tilde{A}} \rho'_{\beta_{\tilde{a}}(v)}(u)),
\end{aligned}$$

which coincides with the second component of $r_A \bowtie r_B$. Therefore, $r_{A \bowtie B} = r_A \bowtie r_B$, which concludes the proof. □

3.2 YB-semitrusses with associated bijective solutions

In [161, Theorem 2] (and independently in [101, Corollary 2.3]), it is shown that any finite involutive left non-degenerate set-theoretic solution of the Yang-Baxter equation is right non-degenerate. In [161], the following example is provided to show that the latter is no longer true in the infinite case.

Example 3.2.1. *Let X be the set of the integers, and define*

$$r : X \times X \to X \times X : (x, y) \mapsto (\lambda_x(y), \lambda^{-1}_{\lambda_x(y)}(x)),$$

with $\lambda_x(y) = y + \min(x, 0)$, for all $x, y \in X$. The inverse of λ_x is given by $\lambda_x^{-1}(y) = y - \min(x, 0)$, for all $y \in X$. Then, (X, r) is an involutive left non-degenerate solution. The solution is, however, not right non-degenerate. To see this, take $a < 0$. Then, $\rho_a(b) = \lambda^{-1}_{\lambda_b(a)}(b) = b - \min(a + \min(b, 0), 0) = b - (a + b) = -a$, for all $b < 0$. Hence, ρ_a is not bijective for $a < 0$.

At that point, it was unknown whether the result remained true for finite bijective left non-degenerate solutions. The following natural questions were posed in [52, Question 4.2, Question 4.3] (Cedó, Jespers, and Verwimp).

Question 3.2.2. *Is any finite bijective left non-degenerate set-theoretic solution of the Yang-Baxter equation right non-degenerate?*

Question 3.2.3. *Are non-degenerate solutions of the Yang-Baxter equation always bijective?*

The former is positively answered in [34, Corollary 6], using q-cycle sets (see Subsection 1.3.2) as a tool to prove the result. The aim of this section is to use the structure of YB-semitrusses to prove that both questions are true in the finite case. Later, we will show that Question 3.2.3 is true for λ-irretractable non-degenerate solutions. We say that a left non-degenerate solution (X, r) of the Yang-Baxter equation is *λ-irretractable* if $\lambda_x = \lambda_y$ implies $x = y$, for all $x, y \in X$. Note that if (X, r) is non-degenerate and involutive, then this notion corresponds with the one introduced by Etingof, Schedler and Soloviev in [75].

Recall that the solution (A, r_A) associated to a YB-semitruss $(A, +, \circ, \lambda, \sigma)$ is always left non-degenerate. If the solution is also right non-degenerate, i.e. ρ_a defined by (3.9) is bijective, for all $a \in A$, we call the YB-semitruss a *non-degenerate YB-semitruss*. An example is the structure YB-semitruss $S(X, r)$ associated to a non-degenerate solution (X, r).

Define the *diagonal map* of a YB-semitruss $(A, +, \circ, \lambda, \sigma)$ as

$$\mathfrak{q} : A \to A : a \mapsto \lambda_a^{-1}(a).$$

Note that $\mathfrak{q}$ is degree preserving.

Lemma 3.2.4. *Let $(A,+,\circ,\lambda,\sigma)$ be a non-degenerate YB-semitruss. Then, the diagonal map $\mathfrak{q}$ is injective. Moreover, if A is finite or $\mathbb{N}$-graded with all homogeneous components A_n finite, then $\mathfrak{q}$ is bijective.*

Proof. Let $a, b \in A$ such that $\mathfrak{q}(a) = \mathfrak{q}(b)$. Put $c = \mathfrak{q}(a)$. Then, by (3.6),

$$\rho_c(a) = \lambda^{-1}_{\lambda_a(c)}\,\sigma_{\lambda_a(c)}(a) = \lambda^{-1}_{\lambda_a\lambda_a^{-1}(a)}\,\sigma_{\lambda_a(c)}(a) = \lambda_a^{-1}\,\sigma_{\lambda_a(c)}(a) = \sigma_c\,\lambda_a^{-1}(a) = \sigma_c(c).$$

Similarly, $\rho_c(b) = \sigma_c(c)$. Hence, $\rho_c(a) = \sigma_c(c) = \rho_c(b)$. Since, by assumption, ρ_c is bijective, it follows that $a = b$. So indeed, $\mathfrak{q}$ is injective. If A is finite, the last statement is an easy consequence. Let A be an $\mathbb{N}$-graded YB-semitruss with all homogeneous components A_n finite. Since $\mathfrak{q}$ is degree preserving, it follows that $\mathfrak{q}$ is bijective on each A_n, and thus also on A. □

In [166, Corollary 2 of Proposition 8], Rump proved a stronger result for bijective left non-degenerate solutions. Namely, for any bijective left non-degenerate solution (X,r), $\mathfrak{q}$ is bijective if and only if (X,r) is non-degenerate. The assumption that (X,r) is bijective is essential here. Take for example X a set with two or more elements, and (X,r) the idempotent left non-degenerate solution defined by $r(x,y) = (y,y)$, for all $x, y \in X$, see Example 3.1.19. Then, (X,r) is not bijective nor right non-degenerate, but $\mathfrak{q}$ is bijective because $\mathfrak{q}(x) = \lambda_x^{-1}(x) = x$, for all $x \in X$. So, for an arbitrary solution (X,r) it is possible that $\mathfrak{q}$ is bijective even if r is neither bijective nor right non-degenerate.

The following lemma shows the importance of the bijectiveness of $\mathfrak{q}$ to prove that the solution is bijective.

Lemma 3.2.5. *Let $(A,+,\circ,\lambda,\sigma)$ be a non-degenerate YB-semitruss. If the diagonal map $\mathfrak{q}$ is bijective, then the associated solution (A,r_A) is bijective.*

Proof. By Proposition 3.1.3, r_A is bijective if and only if σ_a is bijective, for all $a \in A$. Let $a, b \in A$. From (3.9), (3.6), and (1.17), we obtain

$$\rho_b(a) = \lambda^{-1}_{\lambda_a(b)}\,\sigma_{\lambda_a(b)}(a) = \lambda^{-1}_{\lambda_a(b)}\lambda_a\,\sigma_b\,\lambda_a^{-1}(a) = \lambda_{\rho_b(a)}\lambda_b^{-1}\,\sigma_b\,\mathfrak{q}(a).$$

Put $c = \rho_b(a)$. Since ρ_b is bijective, we get $c = \lambda_c\lambda_b^{-1}\,\sigma_b\,\mathfrak{q}\rho_b^{-1}(c)$, for all $b, c \in A$. Hence,

$$\mathfrak{q}(c) = \lambda_b^{-1}\,\sigma_b\,\mathfrak{q}\rho_b^{-1}(c).$$

Since $\mathfrak{q}$ is bijective, we have that

$$\sigma_b(c) = \lambda_b\mathfrak{q}\rho_b\mathfrak{q}^{-1}(c),$$

for all $b, c \in A$. Hence, σ_b is bijective and (A,r_A) is bijective. □

To reprove the result of Castelli, Catino and Stefanelli [34, Corollary 6], using the tools of YB-semitrusses, the following lemma is needed.

Lemma 3.2.6. *Let $(A,+,\circ,\lambda,\sigma)$ be a YB-semitruss, with diagonal map $\mathfrak{q}$ and such that σ_a is bijective, for all $a\in A$. For any $a,b\in A$, the following equality is satisfied,*

$$\lambda_b^{-1}\mathfrak{q}(a)=\mathfrak{q}(\lambda^{-1}_{\sigma_a^{-1}\lambda_a(b)}(a)).$$

Proof. Let $a,b\in A$. From (1.17), it follows that

$$\lambda^{-1}_{\rho_{\lambda_a^{-1}(b)}(a)}\lambda_b^{-1}=\lambda^{-1}_{\rho_{\lambda_a^{-1}(b)}(a)}\lambda^{-1}_{\lambda_a(\lambda_a^{-1}(b))}=\lambda^{-1}_{\lambda_a^{-1}(b)}\lambda_a^{-1}.$$

Putting $a=\sigma_b^{-1}\lambda_b(c)$, we get, for any $b,c\in A$,

$$\lambda^{-1}_{\rho_{\lambda^{-1}_{\sigma_b^{-1}\lambda_b(c)}(b)}(\sigma_b^{-1}\lambda_b(c))}\lambda_b^{-1}(b)=\lambda^{-1}_{\lambda^{-1}_{\sigma_b^{-1}\lambda_b(c)}(b)}\lambda^{-1}_{\sigma_b^{-1}\lambda_b(c)}(b). \tag{3.35}$$

By definition (3.9), $\rho_b(a)=\lambda^{-1}_{\lambda_a(b)}\sigma_{\lambda_a(b)}(a)$, and thus

$$\rho_{\lambda^{-1}_{\sigma_b^{-1}\lambda_b(c)}(b)}(\sigma_b^{-1}\lambda_b(c))=\lambda_b^{-1}\sigma_b(\sigma_b^{-1}\lambda_b(c))=c.$$

Hence, (3.35) is equivalent to

$$\lambda_c^{-1}\mathfrak{q}(b)=\mathfrak{q}(\lambda^{-1}_{\sigma_b^{-1}\lambda_b(c)}(b)),$$

as desired. □

The sufficiency of the next result was first proven by Castelli, Catino and Stefanelli in [34, Corollary 6] in case the associated solution is finite. We translate their proof in the language of YB-semitrusses and add it for completeness' sake. We generalize their result to not only finite solutions, but to solutions associated to $\mathbb{N}$-graded YB-semitrusses with all homogeneous components A_n finite.

Proposition 3.2.7. *Let $(A,+,\circ,\lambda,\sigma)$ be a finite or $\mathbb{N}$-graded YB-semitruss with all homogeneous components A_n finite and with (A,r_A) its associated left non-degenerate solution. Then, (A,r_A) is right non-degenerate if and only if r_A is bijective.*

Proof. Assume first that the solution (A,r_A) is non-degenerate, i.e. $(A,+,\circ,\lambda,\sigma)$ is a non-degenerate YB-semitruss. By Lemma 3.2.4, the diagonal map $\mathfrak{q}$ is bijective and, by Lemma 3.2.5, we conclude that r_A is bijective.

To prove the converse, let $(A,+,\circ,\lambda,\sigma)$ be an $\mathbb{N}$-graded YB-semitruss with all homogeneous components A_n finite and such that (A,r_A) is bijective, i.e. σ_a is bijective, for all $a\in A$. First, we prove that the diagonal map $\mathfrak{q}$ is bijective. Let $n\in\mathbb{N}$. Since $\mathfrak{q}$ is degree preserving, it is enough to prove the bijectivity of $\mathfrak{q}$ on A_n. Without loss of generality, we consider the restrictions of λ,ρ,σ to A_n. Since A_n is finite, there exists $m\in\mathbb{N}$ such that $(\lambda_z^{-1})^m=\mathrm{id}_{A_n}$, for all $z\in A_n$. If $m=1$, then $\mathfrak{q}=\mathrm{id}_{A_n}$ and in particular,

$\mathfrak{q}$ is bijective. If $m \geq 2$, then by Lemma 3.2.6, for any $a \in A_n$,

$$\begin{aligned}
a &= (\lambda_a^{-1})^m(a) \\
&= (\lambda_a^{-1})^{m-2}\lambda_a^{-1}\mathfrak{q}(a) \\
&= (\lambda_a^{-1})^{m-2}\mathfrak{q}\lambda^{-1}_{\sigma_a^{-1}\lambda_a(a)}(a) \\
&= (\lambda_a^{-1})^{m-3}\lambda_a^{-1}\mathfrak{q}\lambda^{-1}_{\sigma_a^{-1}\lambda_a(a)}(a) \\
&= (\lambda_a^{-1})^{m-3}\mathfrak{q}\lambda_{\sigma^{-1}_{\lambda^{-1}_{\sigma_a^{-1}\lambda_a(a)}(a)}\lambda_{\lambda^{-1}_{\sigma_a^{-1}\lambda_a(a)}(a)}(a)}\lambda^{-1}_{\sigma_a^{-1}\lambda_a(a)}(a),
\end{aligned}$$

and so on. So, in the end, there exists $t \in A_n$ such that $a = \mathfrak{q}(t)$. Therefore, $\mathfrak{q}$ is surjective on A_n, and since A_n is finite, $\mathfrak{q}$ is bijective on A_n. Hence, $\mathfrak{q}$ is bijective on A. Now, we will prove that (A, r_A) is right non-degenerate. As the ρ-map is degree preserving, it is enough to prove, for any $a \in A$, that $\rho_a(b) = \rho_a(c)$ implies $b = c$, for $b, c \in A_n$, and some $n \in \mathbb{N}$. Assume for some $n \in \mathbb{N}$ and $b, c \in A_n$ that $\rho_a(b) = \rho_a(c)$. By definition (3.9), this means that $\lambda^{-1}_{\lambda_b(a)}\sigma_{\lambda_b(a)}(b) = \lambda^{-1}_{\lambda_c(a)}\sigma_{\lambda_c(a)}(c)$. Therefore, (3.6) yields

$$\begin{aligned}
\lambda^{-1}_{\lambda_b(a)}\lambda_b\,\sigma_a\,\mathfrak{q}(b) &= \lambda^{-1}_{\lambda_b(a)}\lambda_b\,\sigma_a\,\lambda_b^{-1}(b) \\
&= \lambda^{-1}_{\lambda_b(a)}\,\sigma_{\lambda_b(a)}(b) \\
&= \lambda^{-1}_{\lambda_c(a)}\,\sigma_{\lambda_c(a)}(c) \\
&= \lambda^{-1}_{\lambda_c(a)}\lambda_c\,\sigma_a\,\lambda_c^{-1}(c) \\
&= \lambda^{-1}_{\lambda_c(a)}\lambda_c\,\sigma_a\,\mathfrak{q}(c).
\end{aligned}$$

By (1.17), $\lambda^{-1}_{\lambda_b(a)}\lambda_b = \lambda_{\rho_a(b)}\lambda_a^{-1} = \lambda_{\rho_a(c)}\lambda_a^{-1} = \lambda^{-1}_{\lambda_c(a)}\lambda_c$. Thus, we obtain $\sigma_a\,\mathfrak{q}(b) = \sigma_a\,\mathfrak{q}(c)$. Finally, since σ_a is bijective, this implies $\mathfrak{q}(b) = \mathfrak{q}(c)$. So, $b = c$ and ρ_a is injective on A_n. Since A_n is finite, ρ_a is bijective on A_n, for all $n \in \mathbb{N}$, and thus ρ_a is bijective on A.

A similar proof shows that a finite YB-semitruss $(A, +, \circ, \lambda, \sigma)$ with (A, r_A) is bijective is a non-degenerate YB-semitruss, i.e. (A, r_A) is also right non-degenerate. □

We are now in a position to prove the main result of this section.

Theorem 3.2.8. *Let (X, r) be a finite left non-degenerate set-theoretic solution of the Yang-Baxter equation. Then, r is bijective if and only if (X, r) is right non-degenerate.*

Proof. Let (X, r) be a finite left non-degenerate solution, and put $M = M(X, r)$. From Theorem 3.1.13, we know that one can associate to (X, r) its unital structure YB-semitruss $(M, +, \circ, \lambda, \sigma)$ and a left non-degenerate solution (M, r_M). Furthermore, M is an $\mathbb{N}$-graded YB-semitruss with all homogeneous components finite. From Proposition 3.2.7, it follows that (M, r_M) is right non-degenerate if and only if r_M is bijective. Since (M, r_M) being right non-degenerate is equivalent to (X, r) being right non-degenerate, and r_M being bijective is equivalent to r being bijective, we get that (X, r) is right non-degenerate if and only if r is bijective. □

In Lemma 3.2.5, it was shown that the bijectiveness of $\mathfrak{q}$ is an important property to prove that r is bijective. In [52, Lemma 4.4] (Cedó, Jespers, and Verwimp), the bijectiveness of $\mathfrak{q}$ is proven in case a non-degenerate solution is λ-irretractable. Hence, Question 3.2.3 is true for λ-irretractable non-degenerate solutions. This result was first shown in [52, Theorem 4.5] (Cedó, Jespers, and Verwimp). The following proposition slightly extends this result and the proof follows the same lines.

Proposition 3.2.9. *Let $(A,+,\circ,\lambda,\sigma)$ be a non-degenerate YB-semitruss satisfying, for any $a,b\in A$, $(\lambda_a,\rho_a)=(\lambda_b,\rho_b)$ implies $a=b$. Then, the diagonal map $\mathfrak{q}$ is bijective and its inverse is given by $a\mapsto\rho_a^{-1}(a)$. As a consequence, (A,r_A) is a bijective non-degenerate set-theoretic solution of the Yang-Baxter equation.*

Proof. Let $a\in A$. By (1.17),

$$\lambda_{\lambda_{\rho_a^{-1}(a)}(a)}\lambda_a = \lambda_{\lambda_{\rho_a^{-1}(a)}(a)}\lambda_{\rho_a(\rho_a^{-1}(a))} = \lambda_{\rho_a^{-1}(a)}\lambda_a.$$

Since λ_a is bijective, we obtain

$$\lambda_{\lambda_{\rho_a^{-1}(a)}(a)} = \lambda_{\rho_a^{-1}(a)}. \tag{3.36}$$

Furthermore, by (1.19),

$$\rho_a\rho_{\lambda_{\rho_a^{-1}(a)}(a)} = \rho_{\rho_a(\rho_a^{-1}(a))}\rho_{\lambda_{\rho_a^{-1}(a)}(a)} = \rho_a\rho_{\rho_a^{-1}(a)}.$$

Thus, as ρ_a is bijective by assumption,

$$\rho_{\lambda_{\rho_a^{-1}(a)}(a)} = \rho_{\rho_a^{-1}(a)}. \tag{3.37}$$

Relations (3.36), (3.37), and the assumption imply $\lambda_{\rho_a^{-1}(a)}(a)=\rho_a^{-1}(a)$, and therefore $a=\lambda^{-1}_{\rho_a^{-1}(a)}(\rho_a^{-1}(a))=\mathfrak{q}(\rho_a^{-1}(a))$. With similar computations, we get that

$$\lambda_{\rho_{\lambda_a^{-1}(a)}(a)} = \lambda_{\lambda_a^{-1}(a)}, \tag{3.38}$$

and

$$\rho_{\rho_{\lambda_a^{-1}(a)}(a)} = \rho_{\lambda_a^{-1}(a)}, \tag{3.39}$$

which implies, by the assumption, $\rho_{\lambda_a^{-1}(a)}(a)=\lambda_a^{-1}(a)$. Thus, also $a=\rho^{-1}_{\lambda_a^{-1}(a)}(\lambda_a^{-1}(a))=\rho^{-1}_{\mathfrak{q}(a)}(\mathfrak{q}(a))$. It follows that the diagonal map $\mathfrak{q}$ is bijective and its inverse is given by $a\mapsto\rho_a^{-1}(a)$. □

3.3 Non-degenerate YB-semitrusses and the retract relation

For a non-degenerate involutive set-theoretic solution of the Yang-Baxter equation, the permutation group $\mathcal{G}(X,r)$, defined as

$$\mathcal{G}(X,r) = \mathrm{gr}(\lambda_x \mid x \in X),$$

is studied in [83]. For non-degenerate bijective solutions, various equivalent definitions of the permutation group are given, see for example [8, 47] or Subsection 4.1.2. In analogy to this, we define a set $\mathcal{G}(A)$ for a YB-semitruss $(A,+,\circ,\lambda,\sigma)$, and use this to prove the main result of the previous section, i.e. the bijectiveness of finite non-degenerate solutions, for a much wider class of non-degenerate solutions.

Let $(A,+,\circ,\lambda,\sigma)$ be a YB-semitruss and consider the following set

$$\mathcal{G}(A) = \{f(a) := (\sigma_a, \lambda_a, \rho_a) \mid a \in A\}, \tag{3.40}$$

with ρ_a defined by (3.9). Note that by Proposition 3.1.3, conditions (1.17), (1.18), and (1.19) are satisfied for the λ-map and the ρ-map of a YB-semitruss $(A,+,\circ,\lambda,\sigma)$.

Define additive and multiplicative operations on $\mathcal{G}(A)$ by

$$f(a) + f(b) := (\sigma_{a+b}, \lambda_{a+b}, \rho_{a+b}) = f(a+b),$$

and

$$f(a) \circ f(b) := (\sigma_{a\circ b}, \lambda_{a\circ b}, \rho_{a\circ b}) = f(a\circ b),$$

for all $a,b \in A$. The following lemma shows that both operations are well-defined on $\mathcal{G}(A)$, in the sense that $f(a) = f(a')$ and $f(b) = f(b')$ imply both $f(a)+f(b) = f(a')+f(b')$ and $f(a)\circ f(b) = f(a')\circ f(b')$, for all $a,a',b,b' \in A$.

Lemma 3.3.1. *Let $a,a',b,b' \in A$.*

(1) If $f(a) = f(a')$ then $\sigma_{a\circ b} = \sigma_{a'\circ b}$, $\lambda_{a\circ b} = \lambda_{a'\circ b}$, $\rho_{a\circ b} = \rho_{a'\circ b}$, and $\lambda_{a+b} = \lambda_{a'+b}$, $\rho_{a+b} = \rho_{a'+b}$, $\sigma_{a+b} = \sigma_{a'+b}$.

(2) if $f(b) = f(b')$ then $\lambda_{a\circ b} = \lambda_{a\circ b'}$, $\rho_{a\circ b} = \rho_{a\circ b'}$, $\sigma_{a\circ b} = \sigma_{a\circ b'}$, and $\lambda_{a+b} = \lambda_{a+b'}$, $\rho_{a+b} = \rho_{a+b'}$, $\sigma_{a+b} = \sigma_{a+b'}$.

Proof. (1) Assume that $f(a) = f(a')$, i.e. $\sigma_a = \sigma_{a'}, \lambda_a = \lambda_{a'}$ and $\rho_a = \rho_{a'}$. By (3.2), $\lambda_{a\circ b} = \lambda_a\lambda_b = \lambda_{a'}\lambda_b = \lambda_{a'\circ b}$ and, by Lemma 3.1.6, $\rho_{a\circ b} = \rho_b\rho_a = \rho_b\rho_{a'} = \rho_{a'\circ b}$. Moreover,

$$\sigma_{a\circ b} = \sigma_{a+\lambda_a(b)} = \sigma_{\lambda_a(b)}\,\sigma_a = \sigma_{\lambda_{a'}(b)}\,\sigma_{a'} = \sigma_{a'\circ b}\,.$$

On the other hand, we get that $\lambda_{a+b} = \lambda_{a\circ\lambda_a^{-1}(b)} = \lambda_a\lambda_{\lambda_a^{-1}(b)} = \lambda_{a'}\lambda_{\lambda_{a'}^{-1}(b)} = \lambda_{a'+b}$, $\rho_{a+b} = \rho_{a\circ\lambda_a^{-1}(b)} = \rho_{\lambda_a^{-1}(b)}\rho_a = \rho_{\lambda_{a'}^{-1}(b)}\rho_{a'} = \rho_{a'+b}$, and finally, $\sigma_{a+b} = \sigma_b\,\sigma_a = \sigma_b\,\sigma_{a'} = \sigma_{a'+b}$.

(2) Assume that $f(b) = f(b')$, i.e. $\sigma_b = \sigma_{b'}, \lambda_b = \lambda_{b'}$ and $\rho_b = \rho_{b'}$. By (3.2), $\lambda_{a\circ b} = \lambda_{a\circ b'}$, and since ρ is an anti-homomorphism by Lemma 3.1.6, we have that $\rho_{a\circ b} = \rho_{a\circ b'}$. Further, by (3.6), $\sigma_{\lambda_a(b)} = \lambda_a\, \sigma_b\, \lambda_a^{-1} = \lambda_a\, \sigma_{b'}\, \lambda_a^{-1} = \sigma_{\lambda_a(b')}$, which yields

$$\sigma_{a\circ b} = \sigma_{a+\lambda_a(b)} = \sigma_{\lambda_a(b)}\, \sigma_a = \sigma_{\lambda_a(b')}\, \sigma_a = \sigma_{a\circ b'}\,.$$

Moreover, $a + b = b + \sigma_b(a) = b \circ \lambda_b^{-1}\, \sigma_b(a)$ implies $\lambda_{a+b} = \lambda_{b\circ\lambda_b^{-1}\sigma_b(a)} = \lambda_b\lambda_{\lambda_b^{-1}\sigma_b(a)} = \lambda_{b'}\lambda_{\lambda_{b'}\sigma_{b'}(a)} = \lambda_{a+b'}$. With the same computations, we obtain $\rho_{a+b} = \rho_{a+b'}$. Finally, $\sigma_{a+b} = \sigma_b\, \sigma_a = \sigma_{b'}\, \sigma_a = \sigma_{a+b'}$. □

By the previous result,

$$f : A \to \mathcal{G}(A) : a \mapsto f(a) = (\sigma_a, \lambda_a, \rho_a),$$

is a semigroup homomorphism for both the additive and multiplicative operations. We will show that $\mathcal{G}(A)$ is a YB-semitruss provided A is non-degenerate. First, we introduce a λ-map on $\mathcal{G}(A)$.

Lemma 3.3.2. *Let $(A, +, \circ, \lambda, \sigma)$ be a YB-semitruss and $\mathcal{G}(A)$ the set defined by (3.40). The map $\lambda : \mathcal{G}(A) \to \mathrm{Map}(\mathcal{G}(A), \mathcal{G}(A)) : f(a) \mapsto \lambda_{f(a)}$, given by $\lambda_{f(a)}(f(b)) = f(\lambda_a(b))$, is well-defined. Furthermore, for any $f(a) \in \mathcal{G}(A)$, the map $\lambda_{f(a)}$ is surjective.*

Proof. First, we prove that the map λ is well-defined. If $f(a) = f(a')$, then $\lambda_{f(a)}(f(b)) = f(\lambda_a(b)) = (\sigma_{\lambda_a(b)}, \lambda_{\lambda_a(b)}, \rho_{\lambda_a(b)}) = (\sigma_{\lambda_{a'}(b)}, \lambda_{\lambda_{a'}(b)}, \rho_{\lambda_{a'}(b)}) = \lambda_{f(a')}(f(b))$. Next, assume that $f(b) = f(b')$, i.e. $\sigma_b = \sigma_{b'}, \lambda_b = \lambda_{b'}$ and $\rho_b = \rho_{b'}$. By (1.17), $\lambda_{\lambda_a(b)} = \lambda_a\lambda_b\lambda_{\rho_b(a)}^{-1} = \lambda_a\lambda_{b'}\lambda_{\rho_{b'}(a)}^{-1} = \lambda_{\lambda_a(b')}$. By (3.6), $\sigma_{\lambda_a(b)} = \lambda_a\, \sigma_b\, \lambda_a^{-1} = \lambda_a\, \sigma_{b'}\, \lambda_a^{-1} = \sigma_{\lambda_a(b')}$, and because of (3.6) and (1.17), we get for any $c \in A$,

$$\begin{aligned}
\rho_{\lambda_a(b)}(c) &= \lambda_{\lambda_c\lambda_a(b)}^{-1}\, \sigma_{\lambda_c\lambda_a(b)}(c)\\
&= \lambda_{\lambda_{c\circ a}(b)}^{-1}\lambda_c\lambda_a\, \sigma_b\, \lambda_a^{-1}\lambda_c^{-1}(c)\\
&= \lambda_{\rho_b(c\circ a)}\lambda_b^{-1}\lambda_{c\circ a}^{-1}\lambda_c\lambda_a\, \sigma_b\, \lambda_a^{-1}\lambda_c^{-1}(c)\\
&= \lambda_{\rho_{b'}(c\circ a)}\lambda_{b'}^{-1}\lambda_{c\circ a}^{-1}\lambda_c\lambda_a\, \sigma_{b'}\, \lambda_a^{-1}\lambda_c^{-1}(c)\\
&= \rho_{\lambda_a(b')}(c).
\end{aligned}$$

Hence, $\lambda_{f(a)}(f(b)) = f(\lambda_a(b)) = f(\lambda_a(b')) = \lambda_{f(a)}(f(b'))$, and the map λ is well-defined.

To prove that $\lambda_{f(a)}$ is surjective, for any $f(a) \in \mathcal{G}(A)$, let $f(c) \in \mathcal{G}(A)$. Then, there exists $b \in A$ such that $\lambda_a(b) = c$. Hence, $\lambda_{f(a)}(f(b)) = (\sigma_{\lambda_a(b)}, \lambda_{\lambda_a(b)}, \rho_{\lambda_a(b)}) = (\sigma_c, \lambda_c, \rho_c) = f(c)$, as desired. □

Now, we define a σ-map on $\mathcal{G}(A)$ in the following way

$$\sigma : \mathcal{G}(A) \to \mathrm{Map}(\mathcal{G}(A), \mathcal{G}(A)) : f(a) \mapsto \sigma_{f(a)},$$

with

$$\sigma_{f(a)}(f(b)) = f(\sigma_a(b)).$$

The well-definedness of this map will follow from Lemma 3.3.4, but first we prove another useful result of the σ-map of a non-degenerate YB-semitrusses.

Proposition 3.3.3. *Let $(A, +, \circ, \lambda, \sigma)$ be a non-degenerate YB-semitruss. Let $a, b \in A$. If $\lambda_a = \lambda_b$ and $\rho_a = \rho_b$, then $\sigma_a = \sigma_b$. Furthermore, if $\lambda_a = \rho_a = \mathrm{id}_A$, then $\sigma_a = \mathrm{id}_A$.*

Proof. First note that, for any $x, y, z \in A$, using (1.18),

$$\begin{aligned}\lambda_{\rho_{\lambda_y \lambda_x^{-1}(z)}\rho_y^{-1}(x)}\rho_{\lambda_x^{-1}(z)}(y) &= \rho_{\lambda_{\rho_y \rho_y^{-1}(x)}\lambda_x^{-1}(z)}\lambda_{\rho_y^{-1}(x)}(y)\\ &= \rho_z \lambda_{\rho_y^{-1}(x)}(y),\end{aligned}$$

where the non-degeneracy of A explains the bijectiveness of ρ_y. This implies

$$\rho_{\lambda_x^{-1}(z)}(y) = \lambda^{-1}_{\rho_{\lambda_y \lambda_x^{-1}(z)}\rho_y^{-1}(x)}\rho_z \lambda_{\rho_y^{-1}(x)}(y). \tag{3.41}$$

Now, assume that $\lambda_a = \lambda_b$ and $\rho_a = \rho_b$, for some $a, b \in A$. Let $c \in A$. Using (3.41) with $c = x = y$, $a = z$, and later with $c = x = y$, $b = z$, it follows that

$$\begin{aligned}\rho_{\lambda_c^{-1}(a)}(c) &= \lambda^{-1}_{\rho_{\lambda_c \lambda_c^{-1}(a)}\rho_c^{-1}(c)}\rho_a \lambda_{\rho_c^{-1}(c)}(c)\\ &= \lambda^{-1}_{\rho_a \rho_c^{-1}(c)}\rho_a \lambda_{\rho_c^{-1}(c)}(c)\\ &= \lambda^{-1}_{\rho_b \rho_c^{-1}(c)}\rho_b \lambda_{\rho_c^{-1}(c)}(c)\\ &= \rho_{\lambda_c^{-1}(b)}(c).\end{aligned}$$

So,

$$\sigma_a(c) = \lambda_a \rho_{\lambda_c^{-1}(a)}(c) = \lambda_b \rho_{\lambda_c^{-1}(b)}(c) = \sigma_b(c). \tag{3.42}$$

This proves the first part of the statement.

Finally, assume that $\lambda_a = \rho_a = \mathrm{id}_A$, for some $a \in A$. By (3.41), for any $c \in A$,

$$\begin{aligned}\rho_{\lambda_c^{-1}(a)}(c) &= \lambda^{-1}_{\rho_{\lambda_c \lambda_c^{-1}(a)}\rho_c^{-1}(c)}\rho_a \lambda_{\rho_c^{-1}(c)}(c)\\ &= \lambda^{-1}_{\rho_a \rho_c^{-1}(c)}\lambda_{\rho_c^{-1}(c)}(c)\\ &= \lambda^{-1}_{\rho_c^{-1}(c)}\lambda_{\rho_c^{-1}(c)}(c)\\ &= c.\end{aligned}$$

Hence, $\sigma_a(c) = \lambda_a \rho_{\lambda_c^{-1}(a)}(c) = \lambda_a(c) = c$, as desired. □

In order to prove that $\mathcal{G}(A)$ has a YB-semitruss structure, we need some more properties of the λ-map and the ρ-map of a YB-semitruss.

Lemma 3.3.4. *Let $(A, +, \circ, \lambda, \sigma)$ be a YB-semitruss and $a, b, c \in A$.*

(1) If $\lambda_a = \lambda_b$, then $\lambda_{\rho_c(a)} = \lambda_{\rho_c(b)}$.

(2) If $\lambda_a = \lambda_b$ and $\rho_a = \rho_b$, then $\lambda_{\lambda_c(a)} = \lambda_{\lambda_c(b)}$.

If, furthermore, A is non-degenerate, then $\lambda_a = \lambda_b$ and $\rho_a = \rho_b$ implies

(3) $\lambda_{\lambda_c^{-1}(a)} = \lambda_{\lambda_c^{-1}(b)}$ *and* $\rho_{\lambda_c^{-1}(a)} = \rho_{\lambda_c^{-1}(b)}$.

(4) $\rho_{\rho_c(a)} = \rho_{\rho_c(b)}$ *and* $\rho_{\lambda_c(a)} = \rho_{\lambda_c(b)}$.

(5) $\lambda_{\sigma_c(a)} = \lambda_{\sigma_c(b)}$ *and* $\rho_{\sigma_c(a)} = \rho_{\sigma_c(b)}$.

(6) $\sigma_{\sigma_c(a)} = \sigma_{\sigma_c(b)}$.

Proof. (1) By (1.17), $\lambda_{\lambda_a(c)}\lambda_{\rho_c(a)} = \lambda_a\lambda_c = \lambda_b\lambda_c = \lambda_{\lambda_b(c)}\lambda_{\rho_c(b)} = \lambda_{\lambda_a(c)}\lambda_{\rho_c(b)}$. The bijectiveness of $\lambda_{\lambda_a(c)}$ implies that $\lambda_{\rho_c(a)} = \lambda_{\rho_c(b)}$, as desired.

(2) Again by (1.17), $\lambda_{\lambda_c(a)}\lambda_{\rho_a(c)} = \lambda_c\lambda_a = \lambda_c\lambda_b = \lambda_{\lambda_c(b)}\lambda_{\rho_b(c)} = \lambda_{\lambda_c(b)}\lambda_{\rho_a(c)}$ and, since $\lambda_{\rho_a(c)}$ is bijective, this yields $\lambda_{\lambda_c(a)} = \lambda_{\lambda_c(b)}$.

Let $(A, +, \circ, \lambda, \sigma)$ be a non-degenerate YB-semitruss, and assume furthermore that $\lambda_a = \lambda_b$ and $\rho_a = \rho_b$, for some $a, b \in A$.

(3) First, note that by (1.17),

$$\lambda_c\lambda_{\lambda_c^{-1}(a)} = \lambda_{\lambda_c(\lambda_c^{-1}(a))}\lambda_{\rho_{\lambda_c^{-1}(a)}(c)} = \lambda_a\lambda_{\rho_{\lambda_c^{-1}(a)}(c)}. \tag{3.43}$$

Using (1.18), we obtain

$$\begin{aligned}\lambda_{\rho_a\rho_c^{-1}(c)}\rho_{\lambda_c^{-1}(a)}(c) &= \lambda_{\rho_{\lambda_c(\lambda_c^{-1}(a))}\rho_c^{-1}(c)}\rho_{\lambda_c^{-1}(a)}(c)\\ &= \rho_{\lambda_{\rho_c(\rho_c^{-1}(c))}\lambda_c^{-1}(a)}\lambda_{\rho_c^{-1}(c)}(c)\\ &= \rho_{\lambda_c\lambda_c^{-1}(a)}\lambda_{\rho_c^{-1}(c)}(c)\\ &= \rho_a\lambda_{\rho_c^{-1}(c)}(c).\end{aligned}$$

Since $\rho_a = \rho_b$, this yields

$$\begin{aligned}\rho_{\lambda_c^{-1}(a)}(c) &= \lambda^{-1}_{\rho_a\rho_c^{-1}(c)}\rho_a\lambda_{\rho_c^{-1}(c)}(c)\\ &= \lambda^{-1}_{\rho_b\rho_c^{-1}(c)}\rho_b\lambda_{\rho_c^{-1}(c)}(c)\\ &= \rho_{\lambda_c^{-1}(b)}(c).\end{aligned} \tag{3.44}$$

Hence, using (3.43), (3.44), and that $\lambda_a = \lambda_b$,

$$\lambda_c\lambda_{\lambda_c^{-1}(a)} = \lambda_a\lambda_{\rho_{\lambda_c^{-1}(a)}(c)} = \lambda_b\lambda_{\rho_{\lambda_c^{-1}(b)}(c)} = \lambda_c\lambda_{\lambda_c^{-1}(b)}.$$

As λ_c is bijective, we conclude that $\lambda_{\lambda_c^{-1}(a)} = \lambda_{\lambda_c^{-1}(b)}$. Similarly, using (1.19), (3.44), and that $\rho_a = \rho_b$,

$$\rho_{\lambda_c^{-1}(a)}\rho_c = \rho_{\rho_{\lambda_c^{-1}(a)}(c)}\rho_a = \rho_{\rho_{\lambda_c^{-1}(b)}(c)}\rho_b = \rho_{\lambda_c^{-1}(b)}\rho_c,$$

so, as ρ_c is bijective, $\rho_{\lambda_c^{-1}(a)} = \rho_{\lambda_c^{-1}(b)}$, as desired.

(4) By (1.19), $\rho_{\rho_c(a)}\rho_{\lambda_a(c)} = \rho_c\rho_a = \rho_c\rho_b = \rho_{\rho_c(b)}\rho_{\lambda_b(c)} = \rho_{\rho_c(b)}\rho_{\lambda_a(c)}$. So, because of the assumption that $\rho_{\lambda_a(c)}$ is bijective, we get that $\rho_{\rho_c(a)} = \rho_{\rho_c(b)}$.

Similarly, $\rho_{\rho_a(c)}\rho_{\lambda_c(a)} = \rho_a\rho_c = \rho_b\rho_c = \rho_{\rho_b(c)}\rho_{\lambda_c(b)} = \rho_{\rho_a(c)}\rho_{\lambda_c(b)}$ implies that $\rho_{\lambda_c(a)} = \rho_{\lambda_c(b)}$.

(5) Recall that $\sigma_c(a) = \lambda_c \rho_{\lambda_a^{-1}(c)}(a)$, and thus, $\lambda_{\sigma_c(a)} = \lambda_{\lambda_c \rho_{\lambda_a^{-1}(c)}(a)}$. Substitute $d = \lambda_a^{-1}(c) = \lambda_b^{-1}(c)$, then we get $\lambda_{\sigma_c(a)} = \lambda_{\lambda_{\lambda_a(d)} \rho_d(a)}$. Hence, the fifth statement is equivalent with $\lambda_{\lambda_{\lambda_a(d)} \rho_d(a)} = \lambda_{\lambda_{\lambda_b(d)} \rho_d(b)} = \lambda_{\lambda_{\lambda_a(d)} \rho_d(b)}$, for all $d \in A$. Now, from (1), we know that $\lambda_{\rho_d(a)} = \lambda_{\rho_d(b)}$ and from (4), we also get that $\rho_{\rho_d(a)} = \rho_{\rho_d(b)}$. Therefore, by (2), $\lambda_{\lambda_{\lambda_a(d)} \rho_d(a)} = \lambda_{\lambda_{\lambda_a(d)} \rho_d(b)}$, as desired.

Repeat the steps in the previous part, but replace in the last step (2) with (4), implying that $\rho_{\lambda_{\lambda_a(d)} \rho_d(a)} = \rho_{\lambda_{\lambda_a(d)} \rho_d(b)}$, for all $d \in A$, and thus $\rho_{\sigma_c(a)} = \rho_{\sigma_c(b)}$, for all $c \in A$.

(6) Because of (5) and Proposition 3.3.3, we immediately obtain that $\sigma_{\sigma_c(a)} = \sigma_{\sigma_c(b)}$.

□

Theorem 3.3.5. *Let $(A, +, \circ, \lambda, \sigma)$ be a non-degenerate YB-semitruss. Then, $\mathcal{G}(A) = \{f(a) = (\sigma_a, \lambda_a, \rho_a) \mid a \in A\}$ is a YB-semitruss for the operations*

$$f(a) \circ f(b) = (\sigma_{a \circ b}, \lambda_{a \circ b}, \rho_{a \circ b}),$$
$$f(a) + f(b) = (\sigma_{a+b}, \lambda_{a+b}, \rho_{a+b}),$$

λ-map $\lambda : \mathcal{G}(A) \to \mathrm{Map}(\mathcal{G}(A), \mathcal{G}(A)) : f(a) \mapsto \lambda_{f(a)}$ defined by

$$\lambda_{f(a)} f(b) = (\sigma_{\lambda_a(b)}, \lambda_{\lambda_a(b)}, \rho_{\lambda_a(b)}) = f(\lambda_a(b)),$$

and σ-map $\sigma : \mathcal{G}(A) \to \mathrm{Map}(\mathcal{G}(A), \mathcal{G}(A)) : f(b) \mapsto \sigma_{f(b)}$ defined by

$$\sigma_{f(b)}\, f(a) = (\sigma_{\sigma_b(a)}, \lambda_{\sigma_b(a)}, \rho_{\sigma_b(a)}) = f(\sigma_b(a)).$$

The map $f : A \to \mathcal{G}(A) : a \mapsto f(a)$ is a YB-semitruss epimorphism and the associated solution of $\mathcal{G}(A)$ is non-degenerate, where the ρ-map $\rho : \mathcal{G}(A) \to \mathrm{Map}(\mathcal{G}(A), \mathcal{G}(A)) : f(b) \mapsto \rho_{f(b)}$ of $\mathcal{G}(A)$ is defined by

$$\rho_{f(b)} f(a) = (\sigma_{\rho_b(a)}, \lambda_{\rho_b(a)}, \rho_{\rho_b(a)}) = f(\rho_b(a)). \tag{3.45}$$

Note that because of Proposition 3.3.3, the natural mapping $\mathcal{G}(A) \to \{(\lambda_a, \rho_a) \mid a \in A\}$ is bijective, and the latter can be considered as a YB-semitruss.

Proof. That the mentioned operations are well-defined has been proven in Lemma 3.3.1. That the λ-map is well-defined follows from Lemma 3.3.2, and that the σ-map is well-defined follows from Lemma 3.3.4.

Let $a \in A$. We will prove the bijectivity of $\lambda_{f(a)}$. Note that from Lemma 3.3.2, we know that $\lambda_{f(a)}$ is surjective. Next, assume that $\lambda_{f(a)}(f(b)) = \lambda_{f(a)}(f(b'))$, for some $f(b), f(b') \in \mathcal{G}(A)$. Then, $\lambda_{\lambda_a(b)} = \lambda_{\lambda_a(b')}$ and $\rho_{\lambda_a(b)} = \rho_{\lambda_a(b')}$, and thus it follows from Lemma 3.3.4(3) that $\lambda_b = \lambda_{\lambda_a^{-1} \lambda_a(b)} = \lambda_{\lambda_a^{-1} \lambda_a(b')} = \lambda_{b'}$. Similarly, we get that $\rho_b = \rho_{b'}$. By Proposition 3.3.3, it then follows that $\sigma_b = \sigma_{b'}$. So, $f(b) = f(b')$. Finally, it is clear that $\lambda_{f(a) \circ f(b)} = \lambda_{f(a)} \lambda_{f(b)}$. Hence, $\lambda : (\mathcal{G}(A), \circ) \to \mathrm{Aut}(\mathcal{G}(A), +)$ is a homomorphism.

Some straightforward computations show that the other requirements for $\mathcal{G}(A)$ to be a YB-semitruss are also satisfied. So $(\mathcal{G}(A), +, \circ, \lambda, \sigma)$ is a YB-semitruss and $f : A \to \mathcal{G}(A) : a \mapsto f(a)$ is an epimorphism of YB-semitrusses.

It remains to show that the associated solution of $\mathcal{G}(A)$ is right non-degenerate, i.e. $\rho_{f(a)}$ defined by (3.9) (or equivalently by (3.45)) is bijective, for all $f(a) \in \mathcal{G}(A)$. We prove this via Lemma 3.1.8, i.e. we need to prove that the map $g_a : \mathcal{G}(A) \to \mathcal{G}(A) : f(b) \mapsto f(\rho_a^{-1}(b))$ is well-defined, for all $a \in A$. By Proposition 3.3.3, it is enough to prove that $f(a) = f(a')$, $f(b) = f(b')$ yields $\lambda_{\rho_a^{-1}(b)} = \lambda_{\rho_{a'}^{-1}(b')}$ and $\rho_{\rho_a^{-1}(b)} = \rho_{\rho_{a'}^{-1}(b')}$. Clearly, without loss of generality, we may assume that $a = a'$. So, we need to prove Lemma 3.3.4(3) for ρ and λ interchanged. For this notice that if $r : X \times X \to X \times X : (x,y) \mapsto (\lambda_x(y), \rho_y(x))$ is a solution then so is $\tau r \tau : X^2 \times X^2 : (x,y) \mapsto (\rho_x(y), \lambda_y(x))$, where $\tau(x,y) = (y,x)$. Indeed, $r_{12}r_{23}r_{12} = r_{23}r_{12}r_{23}$ if and only if $(\tau r_{12}\tau)(\tau r_{23}\tau)(\tau r_{12}\tau) = (\tau r_{23}\tau)(\tau r_{12}\tau)(\tau r_{23}\tau)$. Hence, we indeed may interchange λ and ρ and the result follows. □

We are now in a position to define the retract relation for arbitrary non-degenerate set-theoretic solutions of the Yang-Baxter equation (X,r). Put $M = M(X,r)$. By Theorem 3.1.13, $(M,+,\circ,\lambda,\circ)$ is a YB-semitruss with associated non-degenerate solution (M,r_M). So, by Theorem 3.3.5, we obtain a YB-semitruss epimorphism

$$f : M \to \mathcal{G}(M) : a \mapsto (\sigma_a, \lambda_a, \rho_a).$$

By restricting f to X, $f|_X$ provides the retract relation on X, i.e.

$$x \sim y \;\text{ if and only if }\; \sigma_x = \sigma_y,\; \lambda_x = \lambda_y,\; \text{and}\; \rho_x = \rho_y.$$

Put $\overline{X} = X/\sim$. By Theorem 3.3.5, the map r induces a non-degenerate set-theoretic solution

$$\overline{r} : \overline{X}^2 \to \overline{X}^2 : (\overline{x},\overline{y}) \mapsto (\overline{\lambda_x(y)}, \overline{\rho_y(x)}),$$

where $\overline{x}$ denotes the $\sim$-class of $x \in X$. So, $(\overline{X},\overline{r}) = \mathrm{Ret}(X,r)$.

Corollary 3.3.6. *Let $(A,+,\circ,\lambda,\sigma)$ be a non-degenerate YB-semitruss. The semigroup $(\mathcal{G}(A),\circ)$ of the YB-semitruss $(\mathcal{G}(A),+,\circ,\lambda,\sigma)$ is cancellative (and thus also $(\mathcal{G}(A),+)$ is left cancellative), and satisfies the left and right Ore condition.*

Moreover, if there exists $a \in A$ such that $\lambda_a = \rho_a = \mathrm{id}_A$ (for example if A is unital), then $(\mathcal{G}(A),\circ)$ is a cancellative monoid.

Proof. To prove left cancellativity of $(\mathcal{G}(A),\circ)$, suppose $f(a)\circ f(b) = f(a)\circ f(b')$. Then, $\lambda_a\lambda_b = \lambda_{a\circ b} = \lambda_{a\circ b'} = \lambda_a\lambda_{b'}$ and $\rho_b\rho_a = \rho_{a\circ b} = \rho_{a\circ b'} = \rho_{b'}\rho_a$. As λ_a and ρ_a are bijective, we obtain that $\lambda_b = \lambda_{b'}$ and $\rho_b = \rho_{b'}$. By Proposition 3.3.3, it follows that $\sigma_b = \sigma_{b'}$, and $f(b) = f(b')$, as desired. So both semigroups $(\mathcal{G}(A),\circ)$ and $(\mathcal{G}(A),+)$ are left cancellative. Now, assume $f(a)\circ f(b) = f(a')\circ f(b)$. Then, $\lambda_a\lambda_b = \lambda_{a\circ b} = \lambda_{a'\circ b} = \lambda_{a'}\lambda_b$ and $\rho_b\rho_a = \rho_{a\circ b} = \rho_{a'\circ b} = \rho_b\rho_{a'}$. Again, by bijectivity of λ_b and ρ_b, we get that $\lambda_a = \lambda_{a'}$ and $\rho_a = \rho_{a'}$. Hence, also $\sigma_a = \sigma_{a'}$, by Proposition 3.3.3, and thus $f(a) = f(a')$. So, $(\mathcal{G}(A),\circ)$ is a cancellative semigroup. Since $\mathcal{G}(A)$ is a non-degenerate YB-semitruss, we obtain from Proposition 3.1.5 that $f(a)\circ f(b) = \lambda_{f(a)}(f(b))\circ\rho_{f(b)}(f(a))$, where ρ denotes the ρ-map for $\mathcal{G}(A)$. As each $\lambda_{f(a)}$ and $\rho_{f(b)}$ is bijective, the left and right Ore condition follow at once.

Moreover, if there exists $a \in A$ such that $\lambda_a = \rho_a = \mathrm{id}_A$, then, by Proposition 3.3.3, $\sigma_a = \mathrm{id}_A$ and $f(a) = (\mathrm{id}_A,\mathrm{id}_A,\mathrm{id}_A) = 1_{\mathcal{G}(A)} \in \mathcal{G}(A)$. So, $(\mathcal{G}(A),\circ)$ is a cancellative monoid. □

Proposition 3.2.7 can now be extended to a larger class of solutions. To do so, in the non-degenerate case, we consider $\{(\lambda_a, \rho_a) \mid a \in A\}$ as a subsemigroup of the direct product of $(\mathrm{Sym}(A), \circ)$ and its opposite group $(\mathrm{Sym}(A), \circ^{op})$, where $\circ$ denotes the composition of functions.

Corollary 3.3.7. *Let $(A, +, \circ, \lambda, \sigma)$ be a non-degenerate YB-semitruss. If, for any $a \in A$, there exists $b \in A$ such that $\lambda_a \lambda_b = \mathrm{id}_A$ and $\rho_{a\circ b} = \rho_b \rho_a = \mathrm{id}_A$ (for example if all λ_a and ρ_a are of finite order), then the associated solution r_A is bijective and $\mathcal{G}(\mathcal{A})$ is a skew left brace.*

Proof. We will first show that the assumptions imply that $(\mathcal{G}(A), \circ)$ is a group. Let $a \in A$, and take $b \in A$ such that $(\lambda_a, \rho_a)(\lambda_b, \rho_b) = (\lambda_a \lambda_b, \rho_b \rho_a) = (\mathrm{id}_A, \mathrm{id}_A)$. Thus, $\lambda_{a\circ b} = \rho_{a\circ b} = \mathrm{id}_A$. So, by Proposition 3.3.3, $\sigma_{a\circ b} = \mathrm{id}_A$, and $f(a) \circ f(b) = f(a \circ b) = (\mathrm{id}_A, \mathrm{id}_A, \mathrm{id}_A) = 1_{\mathcal{G}(A)}$. By Corollary 3.3.6, it follows that $(\mathcal{G}(A), \circ)$ is a cancellative monoid. Also, every element $f(a)$ of $\mathcal{G}(A)$ has a right inverse $f(b)$, for some $b \in A$. Hence, $(\mathcal{G}(A), \circ)$ is a group. In particular, all maps σ_a have a left inverse and are therefore bijective maps. Thus, by Proposition 3.1.3, r_A is bijective.

Finally, by the previous and Example 3.1.25, $(\mathcal{G}(A), +, \circ)$ is a left cancellative semibrace. By Theorem 3.3.5, $\rho_{f(a)}$ bijective, for all $f(a) \in \mathcal{G}(A)$, and it follows by Example 3.1.26 that $(\mathcal{G}(A), +, \circ)$ is a skew left brace. □

Corollary 3.3.8. *Let (X, r) be a non-degenerate solution. If the subsemigroup $\langle (\lambda_x, \rho_x) \mid x \in X\rangle$ of the group $(\mathrm{Sym}(X), \circ) \times (\mathrm{Sym}(X), \circ^{op})$ is a group itself, then r is bijective.*

Proof. Since (X, r) is a non-degenerate solution, the structure semigroup $S(X, r)$ is a non-degenerate YB-semitruss. By the assumptions and Corollary 3.3.7, $(\mathcal{G}(S(X, r)), \circ)$ is a group, and $r_{S(X,r)}$ is bijective. Since this map, restricted to $X \times X$ is equal to r, we obtain that r is bijective. □

3.4 Algebraic structure of YB-semitrusses

The final section of this chapter concerns the algebraic structure of YB-semitrusses. In the first part, for a field K and any finite left non-degenerate set-theoretic solution of the Yang-Baxter equation (X, r), we show that $K[A(X, r)]$ is a left Noetherian PI-algebra of finite Gelfand-Kirillov dimension. As a corollary, provided that the diagonal map $\mathfrak{q} : X \to X$ is bijective, we deduce that the algebras $K[M(X, r)]$ and $K[(A, \circ)]$ are connected $\mathbb{N}$-graded left Noetherian representable algebras, where A is a unital strongly $\mathbb{N}$-graded YB-semitruss, with A_1 finite, $A_0 = \{1\}$, and diagonal map $\mathfrak{q} : A \to A$ bijective. In the second and final part, we study YB-semitrusses $(A, +, \circ, \lambda, \sigma)$ such that the subsemigroup $\{\sigma_a \mid a \in A\}$ of $\mathrm{End}(A, +)$ is a finite left simple semigroup.

3.4.1 Additive structure of YB-semitrusses and the structure algebra

The structure algebra $K[(M(X, r), \circ)]$ of a set-theoretic solution (X, r) is a K-algebra defined by homogeneous quadratic relations. Such algebras have been studied thoroughly, for example in context of its Gröbner bases, classification of regular algebras of global dimension four, Artin-Shelter regular algebras, and constructions of Noetherian algebras (see for example [15, 54, 79, 103, 106]). For finite involutive non-degenerate solutions, in [88], it was shown that homologically $K[(M(X,r),\circ)]$ has many common points with polynomial algebras in commuting variables. In [97, 98], the structure algebra of finite bijective non-degenerate solutions was proven to be Noetherian and PI (satisfying a polynomial identity), by first proving the same result for the derived structure algebra $K[(A(X,r),+)]$. This idea of studying a solution via its derived solution, has also been applied in [125] to study the structure group of finite bijective non-degenerate solutions.

In this subsection, we study $K[(M(X,r),+)] = K[(A(X,r),+)]$, and show that it is a left Noetherian PI-algebra of finite Gelfand-Kirillov dimension, for any finite left non-degenerate solution (X,r). If furthermore, the diagonal map $\mathfrak{q}$ (see Section 3.2) is bijective, then we show that $K[(M(X,r),\circ)]$ is left Noetherian and satisfies a polynomial identity. As a consequence, for any unital strongly $\mathbb{N}$-graded YB-semitruss $(A,+,\circ,\lambda,\sigma)$, with A_1 finite, $A_0 = \{1\}$, and with diagonal map bijective, the algebra $K[(A,\circ)]$ is left Noetherian and PI.

Let (X,r) be a left non-degenerate set-theoretic solution of the Yang-Baxter equation and put

$$A = A(X,r) = \langle x \in X \mid x+y = y+\sigma_y(x), \text{ for all } x,y \in X\rangle^1,$$

the additive monoid of the unital structure YB-semitruss $M(X,r)$. From Lemma 3.1.10, recall that for a unital YB-semitruss the identity elements of the additive and the multiplicative monoid coincide, i.e. $0 = 1$. Furthermore, note that (3.4) implies that any right ideal $b+A$ of $(A,+)$ is a two-sided ideal of $(A,+)$. An element $a \in A$ is said to be *left divisible* by $b \in A$ if $a = b+c$ for some $c \in A$. Note that, by (3.4), this is equivalent with $a = d+b+c$, for some $c,d \in A$.

Consider the submonoid

$$\mathcal{C} = \mathcal{C}(A) = \{\sigma_a \mid a \in A\} = \langle \sigma_x \mid x \in X\rangle^1,$$

of $\operatorname{End}(A,+)$, with identity element $\sigma_0 = \mathrm{id}_A$. Furthermore, recall from (3.7) that, for $a,b \in A$,

$$\sigma_a\,\sigma_b = \sigma_{b+a} = \sigma_{a+\sigma_a(b)} = \sigma_{\sigma_a(b)}\,\sigma_a, \tag{3.46}$$

and thus

$$\sigma_a\,\mathcal{C} \subseteq \mathcal{C}\,\sigma_a\,. \tag{3.47}$$

So, every left ideal of the monoid $\mathcal{C}$ is a two-sided ideal. If $\mathcal{C}$ is finite (for example if X is finite), there exists a positive integer, say v, so that

$$\sigma_x^v = \sigma_{vx} = \sigma_{vx}^2,$$

is an idempotent, for all $x \in X$, where vx denotes $x+\cdots+x$ and x appears v times.

From now on $X = \{x_1,\dots,x_n\}$ is a finite set and thus any element of $A = A(X,r)$ is left divisible by only finitely many elements. Let $a \in A = \langle x_1,\dots,x_n \mid x_i+x_j = x_j+\sigma_{x_j}(x_i), \text{ for all } i,j \in \{1,\dots,n\}\rangle^1$, and let m_1 be the maximal non-negative integer so that a is left divisible by m_1x_1, that is $a = m_1x_1+b$ and $b \in A$ can not be written as

x_1+d, for some $d \in A$. Repeat this argument on b and consider the maximal non-negative integer m_2 so that $b = m_2x_2 + c$, for some $c \in A$. After at most n steps we get that

$$a = m_1x_1 + m_2x_2 + \cdots + m_nx_n,$$

for some non-negative integers m_i. Notice that $vx_i + vx_j = vx_j + \sigma_{vx_j}(vx_i) = vx_j + v\,\sigma_{vx_j}(x_i)$, and $\sigma_{vx_j}(x_i) \in X$. Hence,

$$B(v) = \{m_1vx_1 + \cdots + m_nvx_n \mid m_1, \dots, m_n \geq 0\}, \tag{3.48}$$

is a submonoid of $(A,+)$. Furthermore,

$$A = B(v) + F(v), \quad \text{with } F(v) = \{m_1x_1 + \cdots + m_nx_n \mid 0 \leq m_1, \dots, m_n < v\}. \tag{3.49}$$

Thus, A is a finitely generated module over the finitely generated submonoid $B(v)$. For $1 \leq i \leq n$, put

$$y_i = vx_i \quad \text{and} \quad X(v) = \{y_1, \dots, y_n\}.$$

So, $B(v) = \{m_1y_1 + \cdots + m_ny_n \mid m_1, \dots, m_n \geq 0\}$. The left derived solution $s : X \times X \to X \times X : (x,y) \mapsto (y, \sigma_y(x))$ of (X,r) induces a solution $s_{X(v)} : X(v) \times X(v) \to X(v) \times X(v) : (y_i, y_j) \mapsto (y_j, \sigma_{y_j}(y_i))$. Hence,

$$B(v) = A(X(v), s_{X(v)}) = \langle y_i \mid 1 \leq i \leq n \rangle^1.$$

For $1 \leq j \leq n$, put

$$\sigma_j = \sigma_{y_j} = \sigma_{vx_j}.$$

Because of (3.46) and since, for any $y \in X(v)$, σ_y is idempotent, any non-identity element of $\mathcal{C}(B(v)) = \{\sigma_a \mid a \in B(v)\}$ can be written as $\sigma_{j_1} \cdots \sigma_{j_k}$, for some $j_1, \dots, j_k$ and some $k \leq n$.

Let $\sigma_{j_1}\sigma_{j_2} \cdots \sigma_{j_k} \in \mathcal{C}(B(v))$, with $J = \{j_1, \cdots, j_k\}$ a subset of $\{1, \dots, n\}$. Then, for any $j_l \in J$, by (3.46),

$$\begin{aligned}\sigma_{j_l}\sigma_{j_{l+1}} \cdots \sigma_{j_k} &= \sigma_{\sigma_{j_l}(y_{j_{l+1}})}\sigma_{j_l}\sigma_{j_{l+2}} \cdots \sigma_{j_k}\\ &= \sigma_{\sigma_{j_l}(y_{j_{l+1}})}\sigma_{\sigma_{j_l}(y_{j_{l+2}})} \cdots \sigma_{\sigma_{j_l}(y_{j_k})}\sigma_{j_l}.\end{aligned}$$

Since σ_{j_l} is idempotent, we obtain

$$\begin{aligned}\sigma_{j_l} \cdots \sigma_{j_k}\sigma_{j_l} &= \sigma_{\sigma_{j_l}(y_{j_{l+1}})}\sigma_{\sigma_{j_l}(y_{j_{l+2}})} \cdots \sigma_{\sigma_{j_l}(y_{j_k})}\sigma_{j_l}\sigma_{j_l}\\ &= \sigma_{\sigma_{j_l}(y_{j_{l+1}})}\sigma_{\sigma_{j_l}(y_{j_{l+2}})} \cdots \sigma_{\sigma_{j_l}(y_{j_k})}\sigma_{j_l}\\ &= \sigma_{j_l} \cdots \sigma_{j_k}.\end{aligned} \tag{3.50}$$

From (3.50), it follows that each $\sigma_{j_1} \cdots \sigma_{j_k}$ is an idempotent. So, we have shown the following property. Recall that $\sigma_0 = \mathrm{id}_A$.

Lemma 3.4.1. *The submonoid $\mathcal{C}(B(v)) = \{\sigma_{j_1}\sigma_{j_2} \cdots \sigma_{j_k} \mid 1 \leq j_1, \cdots, j_k \leq n, 1 \leq k \leq n\} \cup \{\sigma_0\} = \{\sigma_{j_1}\sigma_{j_2} \cdots \sigma_{j_k} \mid 1 \leq j_1, \cdots, j_k \leq n \text{ all distinct}, 1 \leq k \leq n\} \cup \{\sigma_0\}$ of $\mathcal{C}(A)$ is a band, i.e. every element of $\mathcal{C}(B(v))$ is an idempotent.*

For $1 \leq k \leq n$ and $\kappa \in \mathrm{Sym}_n$, put

$$t_k = y_1 + \cdots + y_k,$$
$$\kappa(t_k) = y_{\kappa(1)} + \cdots + y_{\kappa(k)},$$
$$B_{\kappa(t_k)} = \langle y_{\kappa(i)} \mid 1 \leq i \leq k\rangle^1,$$

and

$$T = \{\kappa(t_k) \mid 1 \leq k \leq n,\ \kappa \in \mathrm{Sym}_n\},$$

all elements or subsets of $B(v)$, and thus also of A. Note that $B_{t_n} = B_{\kappa(t_n)} = B(v)$, for all $\kappa \in \mathrm{Sym}_n$. Let $0 \neq w \in B(v)$. Assume $w = w' + y_k$, for some $1 \leq k \leq n$. Let m be the maximal non-negative integer so that w' is left divisible by my_k. Then, $w = my_k + w'' + y_k$, for some $w'' \in B(v)$ that is not left divisible by y_k. If $0 \neq w''$, then we repeat the argument on w'' and after at most n steps we get that

$$w = w_t + t,$$

for some $t \in T$ and $w_t \in B_t$. By (3.50), we have

$$\sigma_w = \sigma_{w_t + t} = \sigma_t \sigma_{w_t} = \sigma_t \,.$$

Similarly, $\sigma_{a+t} = \sigma_t \sigma_a = \sigma_t$, for all $a \in B_t$, and thus

$$a + b + t = a + t + \sigma_t(b) = a + t + \sigma_{a+t}(b) = b + a + t, \tag{3.51}$$

for all $a, b \in B_t$. In particular, as $t \in B_t$,

$$a + t + b + t = b + t + a + t,$$

for all $a, b \in B_t$, so each $B_t + t$ is an abelian semigroup. Hence, with the above notation, we obtain the following result.

Lemma 3.4.2. *Let (X, r) be a finite left non-degenerate solution, and put $A = A(X, r)$. With the above notation, $A = B(v) + F(v)$, and $B(v) = \{0\} \cup \bigcup_{t \in T}(B_t + t)$ is a finite union of abelian subsemigroups.*

Furthermore, for $\kappa \in \mathrm{Sym}_n$, $1 \leq k \leq n$, and $1 \leq l \leq k$,

$$\kappa(t_k) + y_{\kappa(l)} = y_{\eta(l')} + \eta(t_k), \tag{3.52}$$

for some $\eta \in \mathrm{Sym}_n$, and $1 \leq l' \leq k$.

To prove this, it is sufficient to deal with the case that κ is the identity map, so $\kappa(i) = i$ for $1 \leq i \leq n$. Hence, we need to show that, for any $1 \leq l \leq k \leq n$, one can rewrite $t_k + y_l = y_1 + y_2 + \cdots + y_k + y_l$ as $y_{\eta(l')} + \eta(t_k)$, for some $\eta \in \mathrm{Sym}_n$ and $1 \leq l' \leq k$. If $l = 1$, then this is obvious. Assume $k > l > 1$. Then,

$$t_k + y_l = y_l + \cdots + y_k + y_l + \sigma_{y_l + \cdots + y_k + y_l}(y_1 + \cdots + y_{l-1}).$$

Hence, since σ is an anti-homomorphism and because of (3.50),

$$\begin{aligned} t_k + y_l &= y_l + y_{l+1} + \cdots + y_k + y_l + \sigma_{y_{l+1}+\cdots+y_k+y_l}(y_1 + \cdots + y_{l-1}) \\ &= y_l + y_1 + \cdots + y_{l-1} + y_{l+1} + \cdots + y_k + y_l \\ &= y_l + \eta(t_k) \\ &= y_{\eta(l')} + \eta(t_k), \end{aligned}$$

for some η and $l' = k$, as desired. It remains to deal with the case $k = l$. Since σ_{y_k} is an idempotent and σ is an anti-homomorphism,

$$\begin{aligned} t_k + y_k &= y_k + y_k + \sigma_{y_k+y_k}(y_1 + \cdots + y_{k-1}) \\ &= y_k + y_k + \sigma_{y_k}(y_1 + \cdots + y_{k-1}) \\ &= y_k + y_1 + \cdots + y_{k-1} + y_k \\ &= y_k + t_k, \end{aligned}$$

again as desired.

Let K be a field. For any $t \in T$, $K[B_t+t]$ is a left $K[B_t]$-module for the module action $K[B_t] \times K[B_t + t] \to K[B_t + t]$ defined by the linear extension of $(a, b + t) \mapsto a + b + t$, where $a, b \in B_t$ and $t \in T$. By (3.51), $a + b + t = b + a + t$, for all $a, b \in B_t$. Hence, $K[B_t + t] = K[B_t]^{ab} + t$, with $K[B_t]^{ab} = K[B_t]/[K[B_t], K[B_t]]$ the abelianization of the algebra $K[B_t]$. As the finitely generated commutative K-algebra $K[B_t]^{ab}$ is Noetherian (via Hilbert's basis theorem) and $K[B_t + t]$ is a cyclic (and thus finitely generated) left $K[B_t]^{ab}$-module, we get that the commutative (non-unital) algebra $K[B_t + t]$ is a Noetherian left $K[B_t]$-module.

Let $\kappa \in \mathrm{Sym}_n$. Since $B_{t_n} = B_{\kappa(t_n)} = B(v)$, the previous paragraph implies that $K[B_{\kappa(t_n)} + \kappa(t_n)]$ is a Noetherian left $K[B(v)]$-module, and, as ring, it is commutative. Put

$$R_n = \sum_{\kappa\in\mathrm{Sym}_n} K[B_{\kappa(t_n)} + \kappa(t_n)].$$

Clearly, this is a Noetherian left $K[B(v)]$-module. Furthermore, from (3.52) it follows that R_n is an ideal of $K[B(v)]$. As a ring it is a sum of left ideals that are PI-algebras (actually each of the left ideals is commutative as a ring) and thus, by a result of Rowen [159] (or more general a result of Kępczyk [114], which states that a ring which is a sum of two PI-rings is again a PI-ring), R_n is a PI-algebra.

Next consider the K-algebra $K[B(v)]/R_n$. For any $\kappa \in \mathrm{Sym}_n$, it easily is verified that $(K[B_{\kappa(t_{n-1})} + \kappa(t_{n-1})] + R_n)/R_n$ is a left $K[B(v)]/R_n$-submodule of $K[B(v)]/R_n$. With a similar reasoning as above, we obtain that $K[B_{\kappa(t_{n-1})} + \kappa(t_{n-1})]$ is a Noetherian cyclic left $K[B_{\kappa(t_{n-1})}]$-module, and thus $(K[B_{\kappa(t_{n-1})} + \kappa(t_{n-1})] + R_n)/R_n$ is a Noetherian left module over $K[B(v)]/R_n$. Furthermore, as a ring it is commutative. Put

$$R_{n-1} = \sum_{\kappa\in\mathrm{Sym}_n} K[B_{\kappa(t_{n-1})} + \kappa(t_{n-1})].$$

By (3.52), $R_{n-1}+R_n/R_n$ is an ideal in $K[B(v)]/R_n$, and a Noetherian left $K[B(v)]/R_n$-module. Consequently, $R_{n-1}+R_n$ is a Noetherian left $K[B(v)]$-module. One can repeat this process in an obvious manner, making use of the sets

$$R_k = \sum_{\kappa \in \mathrm{Sym}_n} K[B_{\kappa(t_k)} + \kappa(t_k)],$$

where $1 \leq k \leq n$. Put $R_0 = K$. It follows, in particular, that the algebra $K[B(v)] = R_0 + R_1 + \cdots + R_n$ is left Noetherian. Since a K-algebra V is PI if it has an ideal I so that both algebras I and V/I are PI, we obtain that $K[B(v)]$ is also a PI-algebra. Indeed, we get that R_n, $R_{n-1}+R_n/R_n$, $R_{n-2}+R_{n-1}+R_n/R_{n-1}+R_n$, and so on, are PI, and thus $R_0+\cdots+R_n = K[B(v)]$ is a PI-algebra. By (3.49), $K[A] = \sum_{f \in F(v)} K[B(v)]+f$. So, the K-algebra $K[A]$ is a finitely generated module over the subalgebra $K[B(v)]$, and thus, see for example [160, Section 0.2], $K[A]$ is also a left Noetherian PI-algebra (actually it is a Noetherian left $K[B(v)]$-module).

By definition (3.48) of $B(v)$, we get that the Gelfand-Kirillov dimension of $K[B(v)]$ is bounded by n. Since $K[A]$ is a finitely generated module over $K[B(v)]$, its Gelfand-Kirillov dimension is also bounded by n. We thus have proven the following result.

Theorem 3.4.3. *Let (X,r) be a finite left non-degenerate set-theoretic solution of the Yang-Baxter equation. Put $X = \{x_1, \ldots, x_n\}$, and let v be a positive integer so that σ_x^v is an idempotent endomorphism, for all $x \in X$. Then, with the notation introduced above, the left derived monoid $A(X,r)$ satisfies the following properties.*

(1) $A(X,r) = B(v) + F(v)$, i.e. $A(X,r)$ is a finitely generated module over $B(v) = A(X(v), s_{X(v)}) = \langle y_1 = vx_1, \ldots, y_n = vx_n\rangle^1$.

(2) $\mathcal{C}(B(v))$ is a band.

(3) For $1 \leq k \leq n$, $t_k = y_1 + \cdots + y_k \in B(v)$, and $\kappa \in \mathrm{Sym}_n$, each $B_{\kappa(t_k)} + \kappa(t_k)$ is a commutative semigroup, where $B_{\kappa(t_k)} = \langle y_{\kappa(i)} \mid 1 \leq i \leq k\rangle^1$.

(4) For $1 \leq k \leq n$ and $B_k = \bigcup_{\kappa \in \mathrm{Sym}_n} B_{\kappa(t_k)} + \kappa(t_k)$,

$$B_n \subseteq B_n \cup B_{n-1} \subseteq \cdots \subseteq B_n \cup \cdots \cup B_2 \cup B_1 \subseteq B(v),$$

is an ideal chain of $B(v)$.

(5) Each Rees factor semigroup of the ideal chain is a finite union of left ideals

$$(B_n \cup B_{n-1} \cup \cdots \cup B_{i+1} \cup B_{\kappa(t_i)} + \kappa(t_i))/(B_n \cup B_{n-1} \cup \cdots \cup B_{i+1}),$$

with $\kappa \in \mathrm{Sym}_n$.

(6) $A(X,r)$ satisfies the ascending chain condition on left ideals.

(7) *For any field K, each factor of the ideal chain*

$$\{0\} \subseteq K[B_n] \subseteq K[B_n] + K[B_{n-1}] \subseteq \cdots \subseteq K[B_n] + \cdots + K[B_1] \subseteq K[B(v)],$$

of $K[B(v)]$ is a Noetherian left $K[B(v)]$-module that is a finite sum of finitely generated commutative rings.

In particular, $K[A(X,r)]$ is a Noetherian left $K[B(v)]$-module, and $K[A(X,r)]$ is a left Noetherian PI-algebra of finite Gelfand-Kirillov dimension bounded by n.

In general the algebra $K[A(X,r)]$ is not right Noetherian. Indeed, consider the solution from Example 3.1.19, i.e. (X,r) with $r(x,y) = (y,y)$, for all $x,y \in X$. So, r is idempotent and left non-degenerate. For simplicity, take $X = \{x,y\}$. To avoid confusion of the operations in the structure algebra, we will write $A(X,r)$ multiplicatively, i.e. $A(X,r) = \langle x,y \mid xy = yy,\ yx = xx\rangle^1 = \{x^n, y^n \mid n \geq 0\}$. In $K[A(X,r)]$ we have $(x^n - y^n)a = 0$, for all $a \in A(X,r) \setminus \{0\}$. Hence, $\sum_{n>0} K(x^n - y^n)$ is a right ideal of $K[A(X,r)]$ that obviously is not finitely generated as a right ideal.

As an application of Theorem 3.4.3 we claim that the structure algebra $K[M(X,r)]$ is left Noetherian in case (X,r) is a finite left non-degenerate solution such that the diagonal map $\mathfrak{q}$ is bijective (i.e. $\mathfrak{q} : X \to X : x \mapsto \lambda_x^{-1}(x)$ is bijective). With a standard length and induction argument one can easily show that the latter is equivalent with the diagonal map $\mathfrak{q} : M(X,r) \to M(X,r) : a \mapsto \lambda_a^{-1}(a)$ being bijective.

From Theorem 2.2.2, it follows that for finite left non-degenerate solutions (X,r), the structure monoid $M(X,r)$ is a submonoid of the semidirect product $A(X,r) \rtimes \mathrm{Im}(\lambda)$, with $\mathrm{Im}(\lambda) = \{\lambda_a \mid a \in M(X,r)\}$ a finite group, and $\lambda'_a = \lambda_a$, for all $a \in M(X,r)$ (see Remark 2.2.11). From Theorem 3.4.3, we know that the algebra $K[A(X,r) \rtimes \mathrm{Im}(\lambda)]$ is a Noetherian left $K[B(v)]$-module. Hence, to prove that $K[M(X,r)]$ is left Noetherian, it is sufficient to show that $M(X,r)$ is a finitely generated module over $B(v)$. To prove this, we will show that one can choose the positive integer v in the statement of Theorem 3.4.3 so that $B(v) \subseteq M(X,r)$, i.e. for all $x \in X$ we may also assume that $\lambda_{vx} = \mathrm{id}_{M(X,r)}$. This is what will be shown in the following result.

Recall that an algebra over a field is called *representable* if it can be embedded into a matrix algebra over some field. A well-known result of Ananin [3] states that any finitely generated left Noetherian PI-algebra over a field is representable. Conversely, any representable algebra is a PI-algebra. Furthermore, an $\mathbb{N}$-graded K-algebra is called connected if its degree 0 component is equal to K.

Corollary 3.4.4. *Let (X,r) be a finite left non-degenerate solution and let K be a field. If the diagonal map $\mathfrak{q} : X \to X$ is bijective (for example if (X,r) is also bijective Proposition 3.2.7), then there exists a positive integer v so that σ_x^v is an idempotent endomorphism, for all $x \in X$, and $B(v) \subseteq M(X,r)$.*

Consequently, $M(X,r) = B(v)+F$, for some finite subset F of $M(X,r)$ and the structure algebra $K[M(X,r)]$ is a connected $\mathbb{N}$-graded left Noetherian representable algebra. In particular, so is the algebra $K[(A,\circ)]$, for any unital strongly $\mathbb{N}$-graded YB-semitruss $(A,+,\circ,\lambda,\sigma)$ with A_1 finite, $A_0 = \{1\}$, and with diagonal map $\mathfrak{q}$ bijective.

Proof. From Theorem 3.4.3, we know that $A = A(X,r)$ is a finitely generated module over the left Noetherian ring $K[B(v)]$, where v is any positive integer so that each σ_x^v is an idempotent, for $x \in X$. Without loss of generality, replacing v by a multiple, we may also assume, since X is finite, that $(\lambda_a|_X)^v = \mathrm{id}_X$, for all $a \in M(X,r)$. As $\lambda_a \in \mathrm{Aut}(M(X,r),+)$, it follows that $\lambda_a^v = \mathrm{id}_{M(X,r)}$, for all $a \in M(X,r)$.

Define, for any $x \in X$, $x^{(1)} = x$ and recursively $x^{(i+1)} = \mathfrak{q}(x^{(i)}) = \lambda^{-1}_{x^{(i)}}(x^{(i)})$. Since, by assumption, X is finite and $\mathfrak{q}$ is a bijective map, we get that the latter is of finite order, i.e. $\mathfrak{q}^m = \mathrm{id}_X$, for some positive integer m. So, for any $x \in X$, $x^{(m+1)} = \mathfrak{q}^m(x^{(1)}) = x^{(1)} = x$. Since, for any positive integer k, we have that $kx = x \circ \lambda_x^{-1}((k-1)x) = x \circ ((k-1)(\lambda_x^{-1}(x))) = x^{(1)} \circ x^{(2)} \circ \cdots \circ x^{(k)}$, we obtain that

$$vmx = (x^{(1)} \circ x^{(2)} \circ \cdots \circ x^{(m)})^v,$$

where a^v denotes $a \circ \cdots \circ a$, with a appearing v times, for all $a \in M(X,r)$. Thus, $\lambda_{vmx} = (\lambda_{x^{(1)}} \cdots \lambda_{x^{(m)}})^v = \mathrm{id}_{M(X,r)}$, for all $x \in X$. So, for any $x,y \in X$, we get that $vmx \in M(X,r)$, and $vmx \circ vmy = vmx \circ \lambda^{-1}_{vmx}(vmy) = vmx + vmy \in B(vm)$. Hence, $B(vm) \subseteq M(X,r)$, and $M(X,r) = B(vm) + F$ is a finitely generated left module over $B(vm)$, with $F = \{x_1^{m_1} \circ \cdots \circ x_n^{m_n} \mid 0 \le m_1, \ldots, m_n < vm\}$ a finite subset of $M(X,r)$.

Because of Corollary 3.1.16, for any unital YB-semitruss $(A,+,\circ,\lambda,\sigma)$ with bijective diagonal map, that is strongly $\mathbb{N}$-graded, with A_1 finite and $A_0 = \{1\}$, we have that the algebra $K[(A,\circ)]$ is a graded epimorphic image of the structure algebra $K[M(A_1, r_{A_1})]$ for the finite left non-degenerate solution (A_1, r_{A_1}) with bijective diagonal map. So, the last statement of the result follows from the first one. □

In [97, 98], it is proven that if (X,r) is a finite left non-degenerate bijective solution (so a finite non-degenerate bijective solution, by Theorem 3.2.8), then $M = M(X,r)$ is a finitely generated (left and right) module over an abelian normal submonoid T of M (which may be embedded in $A(X,r)$), i.e. $M = \bigcup_{f\in F} Tf = \bigcup_{f \in F} fT$, for some finite subset F of M. Hence, $G(X,r)$ is (finitely generated) abelian-by-finite (see also Chapter 2). Put $A = A(X,r)$. Then, $\mathcal{C}(A)$ is a group with the identity map $\mathrm{id}_A = \sigma_0$ as the only idempotent. Furthermore, by (3.4), any element of A is a normal element. Also, for an appropriate choice of v we get that, for any $x \in X$, $\lambda_x^v = \mathrm{id}_M$, and σ_x^v is an idempotent, thus $\sigma_x^v = \mathrm{id}_A$. Hence, $B(v) \subseteq (Z(A) \cap M)$. Since $B(v)$ is invariant under the λ-map, i.e. $\lambda_a(B(v)) = B(v)$, for all $a \in M$, it follows that $a \circ B(v) = B(v) \circ a$, for all $a \in M$. So, one obtains [98, Theorem 3]. More precisely, $K[(M,\circ)]$ is a module-finite normal extension of the commutative affine subalgebra $K[B(v)]$, and thus $K[(M,\circ)]$ is a left and right Noetherian PI-algebra. Note that the finite bijective left non-degenerate assumption implies that the diagonal map is bijective, because of Theorem 3.2.8 and Lemma 3.2.4.

3.4.2 YB-semitrusses with a left simple semigroup of endomorphisms and their solutions

Let $A = (A,+,\circ,\lambda,\sigma)$ be a YB-semitruss and assume that $\mathcal{C} = \mathcal{C}(A) = \{\sigma_a \mid a \in A\}$ is a finite subsemigroup of $\mathrm{End}(A,+)$. From (3.47), it follows that every left ideal of $\mathcal{C}$ is a two-sided ideal. Then, $\mathcal{C}$ has an ideal chain

$$C_0 \subseteq C_1 \cdots \subseteq C_{n-1} \subseteq C_n = \mathcal{C}, \tag{3.53}$$

with $C_0 = \{\theta\}$ or C_0 is the empty set, and all principal factors C_i/C_{i-1} are either a null semigroup or completely (θ)-simple. For more background on semigroup theory, we refer to [58]. In case C_i/C_{i-1} is completely (θ)-simple, it is of the form $\mathcal{M}^0(G,k,l,P)$, with G a maximal subgroup of $\mathcal{C}$ and P a regular sandwich matrix (no row or column of P consists wholly of zeros). Elements in this semigroup are $k \times l$ matrices with at most one nonzero entry, usually denoted by (g,i,j), with $g \in G^0 = G \cup \{\theta\}$, $1 \leq i \leq k$, $1 \leq j \leq l$. So, (g,i,j) is the $k \times l$ matrix with element g at position (i,j) and zero elsewhere. All elements (θ,i,j) are identified with the zero element θ. The multiplication of two elements $(a,i,j),(b,i',j') \in \mathcal{M}^0(G,k,l,P)$ is given by $(a,i,j)(b,i',j') = (ap_{ji'}b,i,j')$, where $P = (p_{xy})$, an $l \times k$ matrix over G^0. For any element $x = (a,i,j)$ in $\mathcal{M}^0(G,k,l,P)$, there exist nonzero idempotents e,f such that $exf = x$, which implies that any element has an idempotent as left identity. Indeed, $ex = e(exf) = e^2xf = exf = x$. Hence, as $R \cup C_{i-1}$ is a left ideal of $\mathcal{M}^0(G,k,l,P) \cup C_{i-1}$, for a "column" R of this semigroup $\mathcal{M}^0(G,k,l,P)$, we get that $R \cup C_{i-1}$ is a left ideal of $\mathcal{C}$. Since any left ideal of $\mathcal{C}$ must be a two-sided ideal, we get that, by the definition of the multiplication, there can only be one column in $\mathcal{M}^0(G,k,l,P)$, i.e. $l = 1$.

So the principal factors that are completely (θ)-simple (or possibly simple in case of C_1, if C_0 is the empty set) are of the form $\mathcal{M}^0(G,k,1,P)$. Furthermore, two matrix semigroups $\mathcal{M}^0(G,k,1,P)$ and $\mathcal{M}^0(G,k,1,P')$ are isomorphic if there exist an element u and a $k \times k$ matrix V such that $P' = uPV$. Thus, without loss of generality, we can normalize the $1 \times k$ row matrix P and assume that all its entries are the identity element of the group G, say 1. So,

$$\mathcal{M}^0(G,k,1,P) = G_1 \cup \cdots \cup G_k,$$

a finite union of finite groups, with $G_iG_j \subseteq G_i$, for all $1 \leq i,j \leq k$. Furthermore, the identity elements $e_i \in G_i$ are of the form $e_i = (1,i,1)$, and are the nonzero idempotents of $\mathcal{M}^0(G,k,1,P)$. They form a subsemigroup of $\mathcal{M}^0(G,k,1,P)$ such that $e_ie_j = e_i$, for any two nonzero idempotents e_i and e_j.

In this subsection we will deal with the case that $\mathcal{C}$ is a finite left simple semigroup, i.e. the only left ideal of $\mathcal{C}$ is $\mathcal{C}$ itself. This happens for example if $(A,+)$ is a right simple semigroup, because a left ideal L of $\mathcal{C}$ yields a right ideal $I = \{a \mid \sigma_a \in L\}$ of $(A,+)$. So, the ideal chain (3.53) becomes

$$C_0 \subseteq C_1 = \mathcal{C},$$

where C_0 is the empty set, and by definition, $\mathcal{C} = C_1/C_0$ is not null. So, $\mathcal{C}$ is a completely simple semigroup, and from what we know from before, $\mathcal{C}$ is of the form

$$\mathcal{C} = G_1 \cup \cdots \cup G_k,$$

a disjoint union of finite groups with respective identities $e_1,\ldots,e_k$. Moreover, we have

$$G_iG_j \subseteq G_i \quad \text{and} \quad e_ie_j = e_i. \tag{3.54}$$

Consider the anti-homomorphism $\sigma : (A, +) \to \mathrm{End}(A, +)$ and define the following subsemigroups of $(A, +)$, for $1 \le i \le n$,

$$A_i = \sigma^{-1}(G_i) = \{a \in A \mid \sigma_a \in G_i\}.$$

Note that they are left ideals of $(A, +)$ by (3.54). Denote, for $1 \le i \le n$,

$$G_i(A) := \{\sigma_b(a) \mid \sigma_b \in G_i,\ a \in A\} = \{\sigma_b(a) \mid b \in A_i,\ a \in A\}.$$

Let $a \in A_j$ and $b \in A_i$ (or $\sigma_b \in G_i$). Since $\sigma_b \sigma_a = \sigma_{\sigma_b(a)} \sigma_b$ by (3.7), we get, using (3.54), that $\sigma_{\sigma_b(a)} \in G_i$. So, $G_i(A) \subseteq A_i$. As e_i is the identity element of G_i, we have that $e_i\sigma_b = \sigma_b$ and $G_i(A)$ is a subsemigroup of $(A, +)$. For a subset T of A, we denote by $G_i(T)$ the set $\{\sigma_b(t) \mid \sigma_b \in G_i,\ t \in T\}$. Note that, since $e_i \in G_i$, we have $e_i(A) \subseteq A_i$, and $G_i(A_i) \subseteq G_i(A) = G_i(e_i(A)) \subseteq G_i(A_i)$. Thus,

$$G_i(A) = G_i(A_i).$$

We also have that

$$a + b = b + \sigma_b(a) = \sigma_b(a) + \sigma_{\sigma_b(a)}(b). \tag{3.55}$$

So, $a + b \in G_i(A) = G_i(A_i)$, for any $a \in A_j$, $b \in A_i$, and $G_i(A_i)$ is a left ideal of the semigroup $(A, +)$. Furthermore, we can consider the following restrictions of the derived solution (A, s_A) of A,

$$s_{j,i} : A_j \times A_i \to A_i \times A_i : (a, b) \mapsto (b, \sigma_b(a)).$$

In particular, the restriction

$$s_{i,i} : A_i \times A_i \to A_i \times A_i : (a, b) \mapsto (b, \sigma_b(a)),$$

is a solution.

Let $b \in A_i$. Since for every element of a finite semigroup, there is a power of that element which is idempotent, we get that there exists a positive integer, say v, so that $\sigma_b^v = \sigma_b^v \sigma_b^v$. Hence, $\sigma_b^v = e_i \in G_i$. As a consequence, using (3.7),

$$\sigma_b = e_i\, \sigma_b = \sigma_{vb}\, \sigma_b = \sigma_{\sigma_{vb}(b)}\, \sigma_{vb} = \sigma_{\sigma_b^v(b)}\, \sigma_b^v = \sigma_{e_i(b)}\, e_i = \sigma_{e_i(b)}\,. \tag{3.56}$$

So, for any $a \in A_j, b \in A_i$,

$$s_{j,i}(a, b) = (b, \sigma_{e_i(b)}(a)) = (b, \sigma_{e_i(b)}(e_i(a))) = s_{i,i}(e_i(a), b).$$

Hence, as $A = \cup_{i=1}^n A_i$, the map s_A is determined by all maps $s_{i,i}$, and the projections e_i, for $1 \le i \le n$.

Let $\sigma_b(a), \sigma_d(c) \in G_i(A_i)$. Then, $\sigma_{\sigma_d(c)} \in G_i$ and using that $G_i(A_i) = G_i(A) \subseteq A_i$, we have that $\sigma_{\sigma_d(c)}(\sigma_b(a)) \in G_i(A_i)$. Hence, the map $s_{i,i}$ restricts to a solution

$$\widetilde{s}_{i,i} : G_i(A_i) \times G_i(A_i) \to G_i(A_i) \times G_i(A_i) : (\sigma_b(a), \sigma_d(c)) \mapsto (\sigma_d(c), \sigma_{\sigma_d(c)}(\sigma_b(a))).$$

Furthermore, e_i acts as the identity on $G_i(A_i)$, i.e. $e_i(\sigma_b(a)) = \sigma_b(a)$, for any $\sigma_b(a) \in G_i(A_i)$. As G_i is a group we get that, for any $\sigma_d(c) \in G_i(A_i)$, the map $\sigma_{\sigma_d(c)} : G_i(A_i) \to G_i(A_i)$ is bijective (and of finite order, as $\mathcal{C}$ is finite). Therefore, the restriction

$$\widetilde{s}_{i,i} : G_i(A_i) \times G_i(A_i) \to G_i(A_i) \times G_i(A_i),$$

is a bijective non-degenerate solution (see Remark 1.3.2), and thus $G_i(A_i)$ is a normalizing subsemigroup of A_i, i.e. $G_i(A_i) + a = a + G_i(A_i)$ for all $a \in A_i$. To conclude, the solution $s_{i,i}$ on A_i satisfies, for any $a, b \in A_i$,

$$s_{i,i}(a,b) = (b, \sigma_b(a)) = (b, \sigma_{e_i(b)}(e_i(a)),$$

and, as both $e_i(a), e_i(b) \in G_i(A_i)$, $s_{i,i}$ is determined by its bijective non-degenerate subsolution on $G_i(A_i)$ and the projections e_i. Hence, we proved the first part of the following result.

Theorem 3.4.5. *Let $A = (A, +, \circ, \lambda, \sigma)$ be a YB-semitruss such that $\mathcal{C} = \{\sigma_a \mid a \in A\}$ is a finite left simple semigroup. Let $E = E(\mathcal{C})$ be the subsemigroup consisting of the idempotents, and G_e the maximal subgroup of $\mathcal{C}$ containing $e \in E$. Then, $A = \cup_{e\in E} A_e$, a disjoint union of left ideals $A_e = \sigma^{-1}(G_e)$, so that the derived solution s_A associated to A is determined by subsolutions, say s_{A_e}, and the idempotents $e \in E$, and for any $a_e \in A_e$, $a_f \in A_f$, with $e, f \in E$, we have $s_A(a_e, a_f) = (a_f, \sigma_{f(a_f)}(f(a_e))) = s_{A_f}(f(a_e), a_f)$. Furthermore, each s_{A_e} is determined by its bijective non-degenerate subsolution on $G_e(A_e)$ and the idempotent e.*

If, furthermore, A is strongly $\mathbb{N}$-graded with A_1 finite if $A_0 = \varnothing$, then, for any $e \in E(\mathcal{C})$, $A_e \setminus G_e(A_e)$ is finite and $G_e(A_e)$ is also strongly $\mathbb{N}$-graded.

Proof. It only remains to prove the second part of the statement. So, assume A is strongly $\mathbb{N}$-graded with A_1 finite if $A_0 = \varnothing$. Let $e \in E$. Because of (3.55), $A_e \setminus G_e(A_e)$ contains elements of length at most 1, and each element of $A_e \setminus (A_0 \cup A_1)$ belongs to $G_e(A_e)$, as A is strongly $\mathbb{N}$-graded. If $A_0 = \varnothing$, then A_1 is finite and so is $A_e \setminus G_e(A_e)$. If $A_0 \neq \varnothing$, then $A_0 \cap A_e = (A_0 + A_0) \cap A_e \subseteq G_e(A_e)$ and $A_1 \cap A_e = (A_1 + A_0) \cap A_e \subseteq G_e(A_e)$, as A is strongly $\mathbb{N}$-graded and using (3.55). So again, $A_e \setminus G_e(A_e)$ is finite, as desired. Clearly, A_e is strongly $\mathbb{N}$-graded and since the σ-maps are degree preserving, it follows that $G_e(A_e)$ is strongly $\mathbb{N}$-graded. Hence the result follows. □

Chapter 4

Bijective non-degenerate solutions and various types of nilpotency of the structure monoid and group

> Bad ideas is good, good ideas is terrific, no ideas is terrible.
>
> *Leonard Baum*

In this chapter, we study bijective non-degenerate set-theoretic solutions of the Yang-Baxter equation, following [47] (Cedó, Jespers, Kubat, Van Antwerpen, and Verwimp). In the first section, we generalize a result of Jespers, Kubat, and Van Antwerpen [97, Proposition 4.2]. In particular, given a left non-degenerate set-theoretic solution (X,r), we define the least cancellative congruence on $(M(X,r),\circ)$, and show that it is equal to the congruence η of Subsection 3.1.2, in case the solution is bijective and non-degenerate. For this, we follow [53, Section 3] (Cedó, Jespers, and Verwimp). Furthermore, we define various types of permutation groups discuss how they are related.

In [122], Lebed and Mortier described finite quandles whose structure group is abelian. This corresponds to describing all finite bijective non-degenerate solutions (X,r) with $\lambda_x = \mathrm{id}_X$ and $\rho_x(x) = x$, for all $x \in X$, such that its associated structure group $G(X,r)$ is abelian. In [122, Theorem 4.2], they show that such quandles $(X,\triangleleft)$ are abelian, i.e. $(x \triangleleft y) \triangleleft z = (x \triangleleft z) \triangleleft y$, for all $x,y,z \in X$, meaning that the group $\mathrm{gr}(\rho_x \mid x \in X)$ with $\rho_y(x) = x \triangleleft y$, for all $x,y \in X$, is abelian. Note that this result can also be translated for all finite bijective non-degenerate solutions (X,r) with $\rho_x = \mathrm{id}_X$, $\lambda_x(x) = x$ for all $x \in X$, and with abelian structure monoid $G(X,r)$. In this case, the result would be that the group $\mathrm{gr}(\lambda_x \mid x \in X)$ with $\lambda_x(y) = y \triangleleft x$, for all $x,y \in X$, is abelian. The reason for this is that for a quandle, rack or shelf $(X,\triangleleft)$, both $r(x,y) = (y, x \triangleleft y)$ and $r'(x,y) = (y \triangleleft x, x)$ define set-theoretic solutions of the Yang-Baxter equation (see Subsection 1.3.3).

In Section 4.2, we rediscover the above mentioned result of Lebed and Mortier by proving necessary and sufficient conditions for the structure monoid of a finite bijective non-degenerate solution to be Malcev nilpotent, in the sense of [136]. First, we handle the case where $M(X,r) = A(X,r)$ or $M(X,r) = A'(X,r)$, using the notation of Section 2.2, i.e. assuming the solution is equal to its left or right derived solution. These are exactly the solutions that are obtained by racks. In Section 4.3, we then characterize when the structure monoid $M(X,r)$ of a finite bijective non-degenerate solution is Malcev nilpotent. The proof contains the description of a concrete ideal chain that is based on the divisibility properties by the natural generators X of $M(X,r)$ and $A(X,r)$. In case (X,r) is a multipermutation solution of level 1, i.e. the solution is of Lyubashenko type, we give a description of all solutions with Malcev nilpotent structure monoid $M(X,r)$.

In Chapter 3, we defined the retract relation for arbitrary non-degenerate set-theoretic solutions of the Yang-Baxter equation, building on the definition of [125, 75] for finite bijective non-degenerate solutions. We start Section 4.4 by showing that the retract relation defined in [125] for finite bijective non-degenerate solutions also defines a retract relation if the solution is no longer finite. The remaining of Section 4.4 is devoted to bijective non-degenerate multipermutation solutions, i.e. solutions that are of size one after applying the retract multiple times. In particular, we show that for a bijective non-degenerate solution (X,r) of finite multipermutation level m, the solutions associated to $M(X,r)$ and $G(X,r)$ are of finite multipermutation level, bounded by $m+1$. If, moreover, (X,r) is square-free, then $m-1 \leq \operatorname{mpl}(G(X,r), r_{G(X,r)}) \leq m$. A similar result was shown in [80] for non-degenerate involutive set-theoretic solutions of the Yang-Baxter equation.

In [83, Theorem 6.10], Gateva-Ivanova and Cameron prove that for a non-degenerate involutive square-free solution (X,r) of arbitrary cardinality that is a finite multipermutation solution of level m, its associated structure group $G(X,r)$ and permutation group $\mathcal{G}(X,r)$ are solvable of derived length bounded by m. For finite non-degenerate involutive solutions (X,r), Bachiller, Cedó and Vendramin prove, in [13], that (X,r) is a multipermutation solution if and only if its structure group is poly-$\mathbb{Z}$, meaning it has a subnormal series with all quotient groups isomorphic to $\mathbb{Z}$. We extend these results and show that for bijective non-degenerate multipermutation solutions (X,r) of level m, the structure group $G(X,r)$ is solvable of derived length bounded by $m+1$. If furthermore, the solution is square-free, then its derived length is bounded by m.

4.1 Bijective non-degenerate solutions

In Subsection 3.1.2, a least left cancellative congruence η is defined on $(M(X,r),+)$, for a left non-degenerate set-theoretic solution (X,r). In the first part of this section, we define (completely analogue) a least left congruence ν on $(M(X,r),\circ)$, and we show that $\nu = \eta$ for bijective non-degenerate solutions.

In the second part, we deal with various types of permutation groups defined on a bijective non-degenerate solution (X,r), and study how they are related. These include the permutation groups defined in [8, 49, 75, 88, 135, 174], also known as an involutive Yang-Baxter group in case the solution is involutive [46].

4.1.1 Left cancellative congruences on $M(X, r)$

Let (X, r) be a left non-degenerate set-theoretic solution of the Yang-Baxter equation, and put $M = M(X, r)$. From Remark 2.2.11, we know that M and $A(X, r)$ can be identified via π, so that $\lambda_a = \lambda'_a \in \operatorname{Aut}(M, +)$, for all $a \in M$, and $a \circ b = a + \lambda_a(b)$, for all $a, b \in M$. If furthermore, r is bijective, then by Example 3.1.1, we obtain that $a + M = M + a$, for all $a \in M$.

Lemma 4.1.1. *Let (X, r) be a bijective left non-degenerate set-theoretic solution of the Yang-Baxter equation, and put $M = M(X, r)$. Let $a, b, y \in M$. Then, there exists $z \in M$ such that $z + a = a + y$, and*

$$\lambda_z^{-1}(a \circ b) = \lambda_z^{-1}(a) \circ \lambda^{-1}_{\lambda_a^{-1}(y)}(b). \tag{4.1}$$

Proof. Let $a, b, y \in M$. Since r is bijective, $a + M = M + a$, so there exists $z \in M$ such that $z + a = a + y$. Using that $a \circ b = a + \lambda_a(b)$, for all $a, b \in M$, it follows that

$$\begin{aligned}
\lambda_z^{-1}(a \circ b) =& \lambda_z^{-1}(a + \lambda_a(b)) \\
=& \lambda_z^{-1}(a) + \lambda_z^{-1}\lambda_a(b) \\
=& \lambda_z^{-1}(a) \circ \lambda^{-1}_{\lambda_z^{-1}(a)}\lambda_z^{-1}\lambda_a(b) \\
=& \lambda_z^{-1}(a) \circ \lambda^{-1}_{z \circ \lambda_z^{-1}(a)}\lambda_a(b) \\
=& \lambda_z^{-1}(a) \circ \lambda^{-1}_{z+a}\lambda_a(b) \\
=& \lambda_z^{-1}(a) \circ \lambda^{-1}_{a+y}\lambda_a(b) \\
=& \lambda_z^{-1}(a) \circ \lambda^{-1}_{a \circ \lambda_a^{-1}(y)}\lambda_a(b) \\
=& \lambda_z^{-1}(a) \circ \lambda^{-1}_{\lambda_a^{-1}(y)}\lambda_a^{-1}\lambda_a(b) \\
=& \lambda_z^{-1}(a) \circ \lambda^{-1}_{\lambda_a^{-1}(y)}(b).
\end{aligned}$$

□

We define ν as the smallest congruence on $(M, \circ)$, such that $(M, \circ)/\nu$ is a left cancellative monoid. In case the solution is bijective, we will show that ν is a congruence on $(M, +)$. A complete description of ν is given, as follows. Let

$$\nu_0 = \{(a, b) \in M^2 \mid \exists c \in M \text{ such that } c \circ a = c \circ b\},$$

a reflexive and symmetric binary relation on M. For every $m \geq 0$, put

$$\begin{aligned}
\nu_{2m+1} =& \{(a, b) \in M^2 \mid \exists a_1, \dots, a_n \in M \text{ such that } (a, a_1), (a_1, a_2), \dots, (a_n, b) \in \nu_{2m}\}, \\
\nu_{2m+2} =& \{(c \circ a, c \circ b) \in M^2 \mid c \in M \text{ and } (a, b) \in \nu_{2m+1}\} \\
& \cup \{(a, b) \in M^2 \mid \exists c \in M \text{ such that } (c \circ a, c \circ b) \in \nu_{2m+1}\}.
\end{aligned}$$

Clearly, $\nu_n \subseteq \nu_{n+1} \subseteq \nu$, for all $n \geq 0$. Let $\nu' = \cup_{n=0}^{\infty}\nu_n$.

Lemma 4.1.2. *Let (X, r) be a left non-degenerate set-theoretic solution of the Yang-Baxter equation. With the above notation, $\nu' = \nu$ is the least left cancellative congruence on $(M, \circ)$, and $\lambda_a = \lambda_b$, for all $(a, b) \in \nu$. Furthermore, if r is bijective, then for all $z \in M$,*

$$\nu \supseteq \{(\lambda_z^{-1}(a), \lambda_z^{-1}(b)) \mid (a, b) \in \nu\}, \tag{4.2}$$

and ν is also a congruence on $(M, +)$.

Proof. As each ν_n is reflexive and symmetric, it is clear that ν' is reflexive and symmetric as well. Let $a, b, c \in M$, with $(a, b), (b, c) \in \nu'$. Then, there exists a positive integer m such that $(a, b), (b, c) \in \nu_{2m}$. Since ν_{2m+1} is the transitive closure of ν_{2m}, we get that $(a, c) \in \nu_{2m+1} \subseteq \nu'$. So, ν' is an equivalence relation. Furthermore, each ν_n satisfies that $(x \circ z, y \circ z) \in \nu_n$ if $(x, y) \in \nu_n$, for all $z \in M$. Hence, $(a \circ d, b \circ d) \in \nu_{2m} \subseteq \nu'$, for all $d \in M$. Since $(a, b) \in \nu_{2m} \subseteq \nu_{2m+1}$, it follows that $(d \circ a, d \circ b) \in \nu_{2m+2} \subseteq \nu'$, for all $d \in M$. So, ν' is a congruence.

We will now show that $\nu' = \nu$. Let $a, b, c, d \in M$ with $(c, d), (c \circ a, d \circ b) \in \nu'$. As ν' is a congruence on $(M, \circ)$, it follows that $(d \circ b, c \circ b) \in \nu'$. So, $(c \circ a, c \circ b) \in \nu'$. There exists a positive integer m such that $(c \circ a, c \circ b) \in \nu_{2m+1}$. Thus $(a, b) \in \nu_{2m+2} \subseteq \nu'$. Hence $(M, \circ)/\nu'$ is a left cancellative monoid. Since $\nu' \subseteq \nu$, and ν is the smallest congruence on $(M, \circ)$, such that $(M, \circ)/\nu$ is a left cancellative monoid, we conclude that $\nu' = \nu$, as desired.

By induction on n, we will prove that $\lambda_a = \lambda_b$, for all $(a, b) \in \nu_n$. Let $(a, b) \in \nu_0$. Then, there exists $c \in M$ such that $c \circ a = c \circ b$. So,

$$\lambda_c \lambda_a = \lambda_c \lambda_b,$$

and as λ_c is bijective, $\lambda_a = \lambda_b$, as desired. Let $n > 0$ and suppose that $\lambda_a = \lambda_b$, for all $(a, b) \in \nu_{n-1}$. Let $(a, b) \in \nu_n$. If n is odd, then there exist $(a, c_1), (c_1, c_2), \dots, (c_k, b) \in \nu_{n-1}$, and by the induction hypothesis,

$$\lambda_a = \lambda_{c_1} = \cdots = \lambda_{c_k} = \lambda_b.$$

If n is even, then either $(a, b) = (c \circ a', c \circ b')$, for some $c \in M$ and $(a', b') \in \nu_{n-1}$, or there exists $c \in M$ such that $(c \circ a, c \circ b) \in \nu_{n-1}$. In the former case, by the induction hypothesis,

$$\lambda_a = \lambda_{c \circ a'} = \lambda_c \lambda_{a'} = \lambda_c \lambda_{b'} = \lambda_{c \circ b'} = \lambda_b.$$

In the second case, we obtain

$$\lambda_c \lambda_a = \lambda_{c \circ a} = \lambda_{c \circ b} = \lambda_c \lambda_b,$$

by the induction hypothesis, and hence $\lambda_a = \lambda_b$, as λ_c is bijective. So, we get that $\lambda_a = \lambda_b$, for all $(a, b) \in \nu_n$. By induction, we conclude that $\lambda_a = \lambda_b$, for all $(a, b) \in \nu$.

Furthermore, if r is bijective, by Example 3.1.1, we obtain that $M + a = a + M$, for all $a \in M$. We prove (4.2) by induction on n. Let $(a, b) \in \nu_0$ and $y \in M$. Then, there exists $c \in M$ such that $c \circ a = c \circ b$, and there exists $z \in M$ such that $z + c = c + y$. By (4.1),

$$\lambda_z^{-1}(c \circ a) = \lambda_z^{-1}(c) \circ \lambda_{\lambda_c^{-1}(y)}^{-1}(a).$$

Since $c \circ a = c \circ b$, it follows that

$$\lambda_z^{-1}(c) \circ \lambda^{-1}_{\lambda_c^{-1}(y)}(a) = \lambda_z^{-1}(c) \circ \lambda^{-1}_{\lambda_c^{-1}(y)}(b),$$

and thus

$$(\lambda^{-1}_{\lambda_c^{-1}(y)}(a), \lambda^{-1}_{\lambda_c^{-1}(y)}(b)) \in \nu_0,$$

for all $y \in M$. Hence,

$$\nu_0 \supseteq \{(\lambda_z^{-1}(a), \lambda_z^{-1}(b)) \mid (a,b) \in \nu_0\},$$

for all $z \in M$. Let n be a positive integer and suppose that

$$\nu_{n-1} \supseteq \{(\lambda_z^{-1}(a), \lambda_z^{-1}(b)) \mid (a,b) \in \nu_{n-1}\},$$

for all $z \in M$. Let $(a,b) \in \nu_n$. If n is odd, then there exist $(a,c_1),(c_1,c_2),\dots,(c_k,b) \in \nu_{n-1}$, and by the induction hypothesis,

$$(\lambda_z^{-1}(a), \lambda_z^{-1}(c_1)), (\lambda_z^{-1}(c_1), \lambda_z^{-1}(c_2)), \dots, (\lambda_z^{-1}(c_k), \lambda_z^{-1}(b)) \in \nu_{n-1}.$$

Hence $(\lambda_z^{-1}(a), \lambda_z^{-1}(b)) \in \nu_n$, in this case. If n is even, then either $(a,b) = (c \circ a', c \circ b')$, for some $c \in M$ and $(a',b') \in \nu_{n-1}$, or there exists $c \in M$ such that $(c \circ a, c \circ b) \in \nu_{n-1}$. Assume the former case and let $y \in M$. Since $M + c = c + M$, there exists $z \in M$ such that $z + c = c + y$. By (4.1),

$$\lambda_z^{-1}(a) = \lambda_z^{-1}(c) \circ \lambda^{-1}_{\lambda_c^{-1}(y)}(a'),$$

and

$$\lambda_z^{-1}(b) = \lambda_z^{-1}(c) \circ \lambda^{-1}_{\lambda_c^{-1}(y)}(b').$$

Thus, by the induction hypothesis, $(\lambda_z^{-1}(a), \lambda_z^{-1}(b)) \in \nu_n$, in this case. In the second case, again let $y \in M$, and take $z \in M$ such that $z + c = c + y$. By the induction hypothesis,

$$(\lambda_z^{-1}(c \circ a), \lambda_z^{-1}(c \circ b)) \in \nu_{n-1}.$$

Using (4.1), $\lambda_z^{-1}(c \circ a) = \lambda_z^{-1}(c) \circ \lambda^{-1}_{\lambda_c^{-1}(y)}(a)$, and we get that

$$(\lambda^{-1}_{\lambda_c^{-1}(y)}(a), \lambda^{-1}_{\lambda_c^{-1}(y)}(b)) \in \nu_n,$$

for all $y \in M$. We conclude that

$$\nu_n \supseteq \{(\lambda_z^{-1}(a), \lambda_z^{-1}(b)) \mid (a,b) \in \nu_n\},$$

for all $z \in M$. By induction, it follows that

$$\nu \supseteq \{(\lambda_z^{-1}(a), \lambda_z^{-1}(b)) \mid (a,b) \in \nu\},$$

for all $z \in M$.

Finally, let $(a,b) \in \nu$ and $c \in M$. By (4.2), and as ν is a congruence on $(M,\circ)$, we have that

$$(c + a, c + b) = (c \circ \lambda_c^{-1}(a), c \circ \lambda_c^{-1}(b)) \in \nu.$$

Since $\lambda_a = \lambda_b$, and ν is a congruence on $(M,\circ)$, it follows that

$$(a + c, b + c) = (a \circ \lambda_a^{-1}(c), b \circ \lambda_b^{-1}(c)) = (a \circ \lambda_a^{-1}(c), b \circ \lambda_a^{-1}(c)) \in \nu.$$

Hence, ν is a congruence on $(M,+)$. □

Proposition 4.1.3. *Let (X, r) be a bijective non-degenerate set-theoretic solution of the Yang-Baxter equation, and put $M = M(X, r)$. Let ν be the least left cancellative congruence on $(M, \circ)$, and let η be the least left cancellative congruence on $(M, +)$. Then, $\eta = \nu$, and thus, for every $z \in M$,*

$$\nu = \{(\lambda_z(a), \lambda_z(b)) \mid (a, b) \in \nu\} = \{(\lambda_z^{-1}(a), \lambda_z^{-1}(b)) \mid (a, b) \in \nu\}.$$

Furthermore, $\lambda_a = \lambda_b$, for all $(a, b) \in \eta$.

Proof. From the proof of Lemma 4.1.2, we know that for any non-negative integer n, and any $z \in M$,

$$\nu_n \supseteq \{(\lambda_z^{-1}(a), \lambda_z^{-1}(b)) \mid (a, b) \in \nu_n\}, \tag{4.3}$$

and ν is also a congruence on $(M, +)$. We show by induction on n that

$$\nu_n = \{(\lambda_z(a), \lambda_z(b)) \mid (a, b) \in \nu_n\} = \{(\lambda_z^{-1}(a), \lambda_z^{-1}(b)) \mid (a, b) \in \nu_n\}, \tag{4.4}$$

for all $z \in M$ and all non-negative integers n.

Let $(a, b) \in \nu_0$. Then, there exists $c \in M$ such that $c \circ a = c \circ b$. By (2.6), we have that

$$\lambda_y(c \circ a) = \lambda_y(c) \circ \lambda_{\rho_c(y)}(a),$$

and thus

$$\lambda_y(c) \circ \lambda_{\rho_c(y)}(a) = \lambda_y(c) \circ \lambda_{\rho_c(y)}(b),$$

for all $y \in M$. Hence, $(\lambda_{\rho_c(y)}(a), \lambda_{\rho_c(y)}(b)) \in \nu_0$, for all $y \in M$. Since (X, r) is right non-degenerate, ρ_c is bijective, and it follows that $(\lambda_z(a), \lambda_z(b)) \in \nu_0$, for all $z \in M$. By (4.3), also $(\lambda_z^{-1}(a), \lambda_z^{-1}(b)) \in \nu_0$, for all $z \in M$, and thus

$$\nu_0 = \{(\lambda_z(a), \lambda_z(b)) \mid (a, b) \in \nu_0\} = \{(\lambda_z^{-1}(a), \lambda_z^{-1}(b)) \mid (a, b) \in \nu_0\},$$

for all $z \in M$.

Suppose that $n > 0$ and (4.4) is true for $n - 1$. Let $(a, b) \in \nu_n$ and $z \in M$. If n is odd, then there exist $(a, c_1), (c_1, c_2), \dots, (c_k, b) \in \nu_{n-1}$. Hence,

$$(\lambda_z(a), \lambda_z(c_1)), (\lambda_z(c_1), \lambda_z(c_2)), \dots, (\lambda_z(c_k), \lambda_z(b)) \in \nu_{n-1},$$

and thus $(\lambda_z(a), \lambda_z(b)) \in \nu_n$, in this case. If n is even, then either $(a, b) = (c \circ a', c \circ b')$, for some $c \in M$ and $(a', b') \in \nu_{n-1}$, or there exists $c \in M$ such that $(c \circ a, c \circ b) \in \nu_{n-1}$. In the first case, by (2.6), we get

$$(\lambda_z(a), \lambda_z(b)) = (\lambda_z(c \circ a'), \lambda_z(c \circ b')) = (\lambda_z(c) \circ \lambda_{\rho_c(z)}(a'), \lambda_z(c) \circ \lambda_{\rho_c(z)}(b')).$$

By the induction hypothesis, (4.4) holds for $n - 1$, and since $(a', b') \in \nu_{n-1}$, also

$$(\lambda_{\rho_c(z)}(a'), \lambda_{\rho_c(z)}(b')) \in \nu_{n-1},$$

but then, as n is even,

$$(\lambda_z(a), \lambda_z(b)) = (\lambda_z(c) \circ \lambda_{\rho_c(z)}(a'), \lambda_z(c) \circ \lambda_{\rho_c(z)}(b')) \in \nu_n.$$

In the second case, by the induction hypothesis,

$$(\lambda_y(c\circ a),\lambda_y(c\circ b))\in\nu_{n-1},$$

for all $y\in M$. Hence, by (2.6),

$$(\lambda_{\rho_c(y)}(a),\lambda_{\rho_c(y)}(b))\in\nu_n,$$

for all $y\in M$. As (X,r) is right non-degenerate, it follows that

$$(\lambda_z(a),\lambda_z(b))\in\nu_n,$$

for all $z\in M$. Furthermore, by (4.3),

$$\nu_n=\{(\lambda_z(a),\lambda_z(b))\mid(a,b)\in\nu_n\}=\{(\lambda_z^{-1}(a),\lambda_z^{-1}(b))\mid(a,b)\in\nu_n\},$$

for all $z\in M$. Hence, by induction,

$$\nu=\{(\lambda_z(a),\lambda_z(b))\mid(a,b)\in\nu\}=\{(\lambda_z^{-1}(a),\lambda_z^{-1}(b))\mid(a,b)\in\nu\},$$

for all $z\in M$.

Let $a,b,c,d\in M$ with $(c,d),(c+a,d+b)\in\nu$. Since ν is a congruence on $(M,+)$, $(d+b,c+b)\in\nu$. Thus, using transitivity, $(c+a,c+b)\in\nu$. Then, $(c\circ\lambda_c^{-1}(a),c\circ\lambda_c^{-1}(b))=(c+a,c+b)\in\nu$. Hence, $(\lambda_c^{-1}(a),\lambda_c^{-1}(b))\in\nu$, and by the first part, $(a,b)\in\nu$. Therefore, $(M,+)/\nu$ is left cancellative, and hence $\eta\subseteq\nu$.

By Lemma 4.1.2, $\lambda_a=\lambda_b$, for all $(a,b)\in\eta\subseteq\nu$. Let $(a,b)\in\eta$ and let $c\in M$. By Lemma 3.1.22, we have that $(c\circ a,c\circ b)=(c+\lambda_c(a),c+\lambda_c(b))\in\eta$, and since $\lambda_a=\lambda_b$, it follows that $(a\circ c,b\circ c)=(a+\lambda_a(c),b+\lambda_b(c))=(a+\lambda_a(c),b+\lambda_a(c))\in\eta$. So, η is a congruence on $(M,\circ)$. Let $a,b,c,d\in M$, with $(c,d),(c\circ a,d\circ b)\in\eta$. Then, $(c+\lambda_c(a),d+\lambda_d(b))=(c\circ a,d\circ b)\in\eta$. Since $\lambda_c=\lambda_d$, and η is a congruence on $(M,+)$, we have that

$$(c+\lambda_c(a),d+\lambda_c(b)),(d+\lambda_c(b),c+\lambda_c(b))\in\eta.$$

So, $(c+\lambda_c(a),c+\lambda_c(b))\in\eta$, and thus $(\lambda_c(a),\lambda_c(b))\in\eta$. By Lemma 3.1.22, $(a,b)\in\eta$. Therefore, $(M,\circ)/\eta$ is left cancellative and $\nu\subseteq\eta$. So, $\eta=\nu$ and the result follows. □

Remark 4.1.4. *For finite bijective non-degenerate solutions (X,r), with $M=M(X,r)$ and $A=A(X,r)$, Jespers, Kubat, and Van Antwerpen [97, Proposition 2.9] proved that there exists $t\geq1$ and a central element $(z,\mathrm{id}_M)\in M$, with $z\in Z(A)$ and $g(z)=z$, for all $g\in\mathrm{Im}(\lambda)$, such that the least cancellative congruence on $(A,+)$ is*

$$\begin{aligned}\eta_A&=\{(a,b)\in A\times A\mid a+\underbrace{z+\cdots+z}_{i\ \textit{times}}=b+\underbrace{z+\cdots+z}_{i\ \textit{times}},\ \textit{for all } i\geq t\}\\&=\{(a,b)\in A\times A\mid c+a=c+b\ \textit{for some } c\in A\}\\&=\eta_0.\end{aligned}$$

Note that $(a,b) \in \eta_A$ implies that $\lambda_a = \lambda_b$. Hence, it follows from [97, Proposition 4.2] that the (least) cancellative congruence on $(M,\circ)$ is

$$\eta_M = \{((a,\lambda_a),(b,\lambda_b)) \mid (a,b) \in \eta_A\}.$$

Furthermore, the natural map

$$M/\eta_M \longrightarrow (A/\eta_A) \rtimes \mathrm{Im}(\lambda) : \overline{(a,\lambda_a)} \mapsto (\overline{a},\lambda_a),$$

is an injective monoid homomorphism, and M/η_M is a regular submonoid of $(A/\eta_A) \rtimes$ $\mathrm{Im}(\lambda)$. So, we obtain a bijective 1-cocycle $(M/\eta_M,\circ) \longrightarrow (A/\eta_A,+)$, with respect to $\overline{\lambda}$, that extends the mapping $\overline{(a,\lambda_a)} \mapsto \overline{a}$. Since r is bijective we know (see Example 3.1.1) that $(A,+)$ consists of normal elements, so $(A/\eta_A,+)$ is a left and right Ore monoid and also $(M/\eta_M,\circ)$ is a left and right Ore monoid. Therefore, they both have a group of fractions, denoted $\mathrm{gr}(A/\eta_A)$ and $\mathrm{gr}(M/\eta_M)$ respectively. Furthermore, $\mathrm{gr}(M/\eta_M) = G(X,r)$, the structure group of (X,r), $\mathrm{gr}(A/\eta_A) = A_{\mathrm{gr}}(X,r) = G(X,s)$, the structure group of the left derived solution (X,s) (see Section 2.2), $\mathrm{gr}(M/\eta_M) \subseteq \mathrm{gr}(A/\eta_A) \rtimes \mathrm{Im}(\lambda)$, where by abuse of notation $\lambda : \mathrm{gr}(M/\eta_M) \to \mathrm{Aut}(\mathrm{gr}(A/\eta_A))$ is the natural extension of the mapping $\overline{\lambda}$, and also $\mathrm{gr}(M/\eta_M)$ is a regular subgroup of $\mathrm{gr}(A/\eta_A) \rtimes \mathrm{Im}(\lambda)$. The latter is proven by Lebed and Vendramin in [125, Theorem 3.4.].

4.1.2 Permutation groups

Let (X,r) be a bijective non-degenerate set-theoretic solution of the Yang-Baxter equation. From Remark 2.2.11, we know that $M = M(X,r)$ and $A = A(X,r)$ can be identified, such that $a \circ b = a + \lambda_a(b)$, and $\lambda_a = \lambda'_a$, for all $a,b \in M$. Since X generates M, the map $\lambda_x \in \mathrm{Sym}(X)$ determines $\lambda_x \in \mathrm{Sym}(M)$, and $\lambda_x \in \mathrm{Aut}(M,+)$. The map

$$\{\lambda_x \in \mathrm{Sym}(X) \mid x \in X\} \to \{\lambda_x \in \mathrm{Sym}(M) \mid x \in X\},$$

defined by $\lambda_x \mapsto \lambda_x$, induces an isomorphism of groups

$$\mathrm{gr}(\lambda_x \mid x \in X) \to \mathrm{gr}(\lambda_a \mid a \in M). \tag{4.5}$$

Similarly one can see that the group $\mathrm{gr}(\rho_x \mid x \in X) \subseteq \mathrm{Sym}(X)$ is isomorphic to the group $\mathrm{gr}(\rho_a \mid a \in M) = \mathrm{gr}(\rho_x \mid x \in X) \subseteq \mathrm{Sym}(M)$.

For a bijective non-degenerate set-theoretic solution (X,r), using the notation (1.16) and (1.20), we define various types of permutation groups associated to (X,r),

$$\begin{aligned}
\mathcal{G}_{\mathrm{gen}}(X,r) &= \mathrm{gr}((\lambda_x,\rho_x^{-1},\hat{\lambda}_x,\hat{\rho}_x^{-1}) \mid x \in X) \subseteq \mathrm{Sym}(X)^4,\\
\mathcal{G}_{\lambda,\rho}(X,r) &= \mathrm{gr}((\lambda_x,\rho_x^{-1}) \mid x \in X) \subseteq \mathrm{Sym}(X)^2,\\
\mathcal{G}_{\lambda,\hat{\lambda}}(X,r) &= \mathrm{gr}((\lambda_x,\hat{\lambda}_x) \mid x \in X) \subseteq \mathrm{Sym}(X)^2,\\
\mathcal{G}_{\lambda}(X,r) &= \mathrm{gr}(\lambda_x \mid x \in X) \subseteq \mathrm{Sym}(X),\\
\mathcal{G}_{\rho}(X,r) &= \mathrm{gr}(\rho_x \mid x \in X) \subseteq \mathrm{Sym}(X).
\end{aligned}$$

Lemma 4.1.5. *Let (X,r) be a bijective non-degenerate set-theoretic solution of the Yang-Baxter equation. Then,*

$$\lambda_a^{-1}(x) = \hat{\rho}_{\hat{\lambda}_x^{-1}(a)}(x), \quad \hat{\lambda}_a^{-1}(x) = \rho_{\lambda_x^{-1}(a)}(x),$$
$$\rho_a^{-1}(x) = \hat{\lambda}_{\hat{\rho}_x^{-1}(a)}(x), \quad \hat{\rho}_a^{-1}(x) = \lambda_{\rho_x^{-1}(a)}(x),$$

for all $a \in G(X,r)$ and $x \in X$.

Proof. We will first prove that $\hat{\lambda}_y^{-1}(x) = \rho_{\lambda_x^{-1}(y)}(x)$, for all $x, y \in X$. Indeed, since for any $x, y \in X$, $r^{-1}r(y,x) = (y,x)$, we get that $\hat{\lambda}_{\lambda_y(x)}(\rho_x(y)) = y$. Therefore, $\hat{\lambda}_z(\rho_{\lambda_y^{-1}(z)}(y)) = y$, and thus $\hat{\lambda}_z^{-1}(y) = \rho_{\lambda_y^{-1}(z)}(y)$, for all $y, z \in X$. Similarly, one proves that $\hat{\rho}_y^{-1}(x) = \lambda_{\rho_x^{-1}(y)}(x)$ holds for all $x, y \in X$.

By [6, Lemma 2.1.12], the map $g : G(X,r) \to \mathrm{Sym}(X)$, defined by $g(a) = g_a$ with $g_a(x) = \rho_{\lambda_x^{-1}(a)}(x)$, for all $a \in G(X,r)$ and $x \in X$, is an anti-homomorphism of groups. Similarly, one verifies that the map $f : G(X,r) \to \mathrm{Sym}(X) : a \mapsto f_a$, where $f_a(x) = \lambda_{\rho_x^{-1}(a)}(x)$, for all $a \in G(X,r)$ and $x \in X$, is a homomorphism of groups. Similar to [135, Theorem 1], the map $\hat{\lambda}^{-1} : G(X,r) \to \mathrm{Sym}(X) : a \mapsto \hat{\lambda}_a^{-1}$ is an anti-homomorphism of groups and the map $\hat{\rho}^{-1} : G(X,r) \to \mathrm{Sym}(X) : a \mapsto \hat{\rho}_a^{-1}$ is a homomorphism of groups. Since

$$\hat{\lambda}_x^{-1}(y) = \rho_{\lambda_y^{-1}(x)}(y) = g_x(y), \text{ and } \hat{\rho}_y^{-1}(x) = \lambda_{\rho_x^{-1}(y)}(x) = f_y(x),$$

for all $x, y \in X$, we thus have that

$$\hat{\lambda}_a^{-1}(x) = g_a(x) = \rho_{\lambda_x^{-1}(a)}(x), \text{ and } \hat{\rho}_a^{-1}(x) = f_a(x) = \lambda_{\rho_x^{-1}(a)}(x),$$

for all $a \in G(X,r)$ and $x \in X$. This proves two of the equalities in the statement of the result. The other two equalities are proven similarly. □

In [8, Definition 3.10] (or [6, Definition 2.1.13]), Bachiller defined the permutation group

$$\mathrm{gr}((\lambda_x, g_x^{-1}) \mid x \in X) = \{(\lambda_a, g_a^{-1}) \mid a \in G(X,r)\} \subseteq \mathrm{Sym}(X)^2,$$

with $g_a(x) = \rho_{\lambda_x^{-1}(a)}(x)$, for all $a \in G(X,r)$ and $x \in X$. So, by the previous result, the permutation group in the sense of Bachiller is in our notation the group $\mathcal{G}_{\lambda,\hat{\lambda}}(X,r)$.

Lemma 4.1.6. *Let (X,r) be a bijective non-degenerate set-theoretic solution of the Yang-Baxter equation. Then, the groups $\mathcal{G}_{\mathrm{gen}}(X,r)$, $\mathcal{G}_{\lambda,\rho}(X,r)$, and $\mathcal{G}_{\lambda,\hat{\lambda}}(X,r)$ are isomorphic.*

Proof. Define the maps

$$\begin{aligned} &h_{\mathrm{gen}} : G(X,r) \to \mathcal{G}_{\mathrm{gen}}(X,r) : a \mapsto (\lambda_a, \rho_a^{-1}, \hat{\lambda}_a, \hat{\rho}_a^{-1}), \\ &h_{\lambda,\rho} : G(X,r) \to \mathcal{G}_{\lambda,\rho}(X,r) : a \mapsto (\lambda_a, \rho_a^{-1}), \\ &h_{\lambda,\hat{\lambda}} : G(X,r) \to \mathcal{G}_{\lambda,\hat{\lambda}}(X,r) : a \mapsto (\lambda_a, \hat{\lambda}_a), \end{aligned} \tag{4.6}$$

and note that they are all epimorphisms of groups.

First, we will prove that $\rho_x(\operatorname{Ker}(\lambda)) = \operatorname{Ker}(\lambda)$, for all $x \in X$. Let $a \in \operatorname{Ker}(\lambda)$ and $x \in X$. Denote the inverse of x in $G(X,r)$ by $\overline{x}$ and note that $\lambda_{\overline{x}} = \lambda_x^{-1}$ and $\rho_{\overline{x}} = \rho_x^{-1}$. Then, $\lambda_a = \mathrm{id}_X$, and we have by (1.17),

$$\lambda_x = \lambda_a\lambda_x = \lambda_{\lambda_a(x)}\lambda_{\rho_x(a)} = \lambda_x\lambda_{\rho_x(a)},$$

and

$$\lambda_{\overline{x}} = \lambda_a\lambda_{\overline{x}} = \lambda_{\lambda_a(\overline{x})}\lambda_{\rho_{\overline{x}}(a)} = \lambda_{\overline{x}}\lambda_{\rho_{\overline{x}}(a)}.$$

Hence $\lambda_{\rho_x(a)} = \mathrm{id}_X$ and $\lambda_{\rho_x^{-1}(a)} = \mathrm{id}_X$, and thus $\rho_x(\operatorname{Ker}(\lambda)) = \operatorname{Ker}(\lambda)$. Similarly, one proves that

$$\lambda_x(\operatorname{Ker}(\rho)) = \operatorname{Ker}(\rho), \quad \hat{\rho}_x(\operatorname{Ker}(\hat{\lambda})) = \operatorname{Ker}(\hat{\lambda}), \quad \hat{\lambda}_x(\operatorname{Ker}(\hat{\rho})) = \operatorname{Ker}(\hat{\rho}),$$

for all $x \in X$.

Next, we show that

$$\operatorname{Ker}(\lambda) \cap \operatorname{Ker}(\hat{\lambda}) = \operatorname{Ker}(\lambda) \cap \operatorname{Ker}(\rho) = \operatorname{Ker}(\rho) \cap \operatorname{Ker}(\hat{\rho}),$$

and thus $\operatorname{Ker}(h_{\lambda,\hat{\lambda}}) = \operatorname{Ker}(h_{\lambda,\rho}) = \operatorname{Ker}(h_{\mathrm{gen}})$. Let $a \in \operatorname{Ker}(\lambda) \cap \operatorname{Ker}(\hat{\lambda})$ and $x \in X$. Then, by the first part, $\hat{\lambda}_{\hat{\rho}_x^{-1}(a)} = \mathrm{id}_X$ and $\lambda_{\rho_x^{-1}(a)} = \mathrm{id}_X$. Using Lemma 4.1.5, we obtain

$$\rho_a^{-1}(x) = \hat{\lambda}_{\hat{\rho}_x^{-1}(a)}(x) = x, \text{ and } \hat{\rho}_a^{-1}(x) = \lambda_{\rho_x^{-1}(a)}(x) = x.$$

This shows that $\operatorname{Ker}(\lambda) \cap \operatorname{Ker}(\hat{\lambda}) \subseteq \operatorname{Ker}(\rho) \cap \operatorname{Ker}(\hat{\rho})$. The other inclusion follows by a symmetric argument. We also showed that $\operatorname{Ker}(\lambda) \cap \operatorname{Ker}(\hat{\lambda}) \subseteq \operatorname{Ker}(\rho) \cap \operatorname{Ker}(\lambda)$. Let $b \in \operatorname{Ker}(\rho) \cap \operatorname{Ker}(\lambda)$. As $\operatorname{Ker}(\rho)$ is λ_x-invariant by the first part of this proof, for any $x \in X$, we have that $\rho_{\lambda_x^{-1}(b)} = \mathrm{id}_X$. Therefore, $\hat{\lambda}_b^{-1}(x) = \rho_{\lambda_x^{-1}(b)}(x) = x$, for all $x \in X$. This shows that $\operatorname{Ker}(\rho) \cap \operatorname{Ker}(\lambda) \subseteq \operatorname{Ker}(\lambda) \cap \operatorname{Ker}(\hat{\lambda})$, and thus $\operatorname{Ker}(\lambda) \cap \operatorname{Ker}(\hat{\lambda}) = \operatorname{Ker}(\rho) \cap \operatorname{Ker}(\lambda)$. Thus, we indeed have shown that $\operatorname{Ker}(h_{\lambda,\hat{\lambda}}) = \operatorname{Ker}(h_{\lambda,\rho}) = \operatorname{Ker}(h_{\mathrm{gen}})$. Therefore,

$$\mathcal{G}_{\lambda,\rho}(X,r) \cong G(X,r)/\operatorname{Ker}(h_{\lambda,\rho}) = G(X,r)/\operatorname{Ker}(h_{\mathrm{gen}}) \cong \mathcal{G}_{\mathrm{gen}}(X,r),$$

and

$$\mathcal{G}_{\lambda,\hat{\lambda}}(X,r) \cong G(X,r)/\operatorname{Ker}(h_{\lambda,\hat{\lambda}}) = G(X,r)/\operatorname{Ker}(h_{\mathrm{gen}}) \cong \mathcal{G}_{\mathrm{gen}}(X,r),$$

as desired. □

In the proof of Lemma 4.1.6, we also showed that $\operatorname{Ker}(\lambda) \cap \operatorname{Ker}(\hat{\lambda}) = \operatorname{Ker}(\lambda) \cap \operatorname{Ker}(\rho) = \operatorname{Ker}(\rho) \cap \operatorname{Ker}(\hat{\rho})$. This yields $\operatorname{Ker}(\lambda) \cap \operatorname{Ker}(\rho) = \operatorname{Ker}(\lambda) \cap \operatorname{Ker}(\rho) \cap \operatorname{Ker}(\hat{\lambda}) \cap \operatorname{Ker}(\hat{\rho})$, and by symmetry between (X,r) and (X,r^{-1}) we obtain

$$\operatorname{Ker}(\lambda) \cap \operatorname{Ker}(\rho) = \operatorname{Ker}(\hat{\lambda}) \cap \operatorname{Ker}(\hat{\rho}). \tag{4.7}$$

Definition 4.1.7. *Let (X,r) be a bijective non-degenerate set-theoretic solution of the Yang-Baxter equation. We define the permutation group $\mathcal{G}(X,r)$ of (X,r) as*

$$\mathcal{G}(X,r) = \mathcal{G}_{\lambda,\rho}(X,r).$$

In case the bijective non-degenerate solution (X,r) is involutive, we have $\rho_y(x) = \lambda^{-1}_{\lambda_x(y)}(x)$ and $\lambda_x(y) = \rho^{-1}_{\rho_y(x)}(y)$, for all $x,y \in X$, and $\mathcal{G}(X,r) = \mathcal{G}_{\lambda,\rho}(X,r) = \mathcal{G}_{\lambda}(X,r) = \mathcal{G}_{\rho}(X,r)$.

Remark 4.1.8. *Let (X,r) be a bijective non-degenerate set-theoretic solution of the Yang-Baxter equation, and put $G = G(X,r)$. Then, $(G,+,\circ)$ is a skew left brace (see after Example 3.1.26), and the socle of G is defined as, see Subsection 1.3.1,*

$$\operatorname{Soc}(G) = \{a \in G \mid \lambda_a = \mathrm{id}_G \text{ and } \rho_a = \mathrm{id}_G\}.$$

Note that both λ_a and ρ_a are maps in $\operatorname{Sym}(G)$. If (X,r) is an injective solution (see Section 2.1), then $\lambda_a = \mathrm{id}_G$ if and only if $\lambda_a|_X = \mathrm{id}_X$. In this case $\operatorname{Soc}(G) = \operatorname{Ker}(h_{\lambda,\rho})$, with $h_{\lambda,\rho}$ defined by (4.6), so $G/\operatorname{Soc}(G) \cong \mathcal{G}_{\lambda,\rho}(X,r)$. However, in general, we know that for $a \in G$, $\lambda_a|_X = \mathrm{id}_X$ implies $\lambda_a = \mathrm{id}_G$, and similarly for the ρ-maps. Hence,

$$\operatorname{Ker}(h_{\lambda,\rho}) \subseteq \operatorname{Soc}(G),$$

and thus $G/\operatorname{Soc}(G)$ is an epimorphic image of

$$G/\operatorname{Ker}(h_{\lambda,\rho}) \cong \mathcal{G}_{\lambda,\rho}(X,r).$$

In [8, Example 3.12] (or [6, Example 2.1.15]), Bachiller gives an example of a solution (X,r) where $\mathcal{G}_{\lambda,\hat{\lambda}}(X,r)$ and $G/\operatorname{Soc}(G)$ are not isomorphic. In fact, in this example

$$G/\operatorname{Soc}(G) \cong \mathbb{Z}/2\mathbb{Z} \quad \text{and} \quad \mathcal{G}(X,r) \cong \mathcal{G}_{\lambda,\hat{\lambda}}(X,r) \cong \mathcal{G}_{\lambda,\rho}(X,r) \cong \mathbb{Z}.$$

We provide another example, with the same idea. Let $X = \mathbb{Z}/n\mathbb{Z}$ for a positive integer n. Let $r : X \times X \to X \times X$ be the bijective non-degenerate solution defined by $r(x,y) = (f(y), f(x))$, with $f(x) = x+1$, for all $x,y \in X$. This is a solution of Lyubashenko type. For any $x \in X$, $x \circ (x-1) = x \circ (x+1)$ holds in $G = G(X,r)$, and thus $\iota(x-1) = \iota(x+1)$, where $\iota : X \to G$ is the natural map. If n is odd, then G is free abelian of rank 1, and $\operatorname{Soc}(G) = G$. Hence, $G/\operatorname{Soc}(G) = \{1_G\}$, when n is odd. If n is even, then $G \cong \operatorname{gr}(0,1 \mid 0 \circ 0 = 1 \circ 1)$ and $\operatorname{Soc}(G) \cong \operatorname{gr}(0 \circ 0, 1 \circ 0, 0 \circ 1)$. Hence, $G/\operatorname{Soc}(G) \cong \mathbb{Z}/2\mathbb{Z}$ if n is even. In both cases, $\mathcal{G}(X,r) \cong \mathbb{Z}/n\mathbb{Z}$.

As $\operatorname{Ker}(h_{\lambda,\rho})$ is a normal subgroup of $G(X,r)$, it is easy to see that $\operatorname{Ker}(h_{\lambda,\rho})$ is an ideal of the skew left brace $G(X,r)$. This allows to define an addition on $\mathcal{G}(X,r)$ by $(\lambda_a, \rho_a^{-1}) + (\lambda_b, \rho_b^{-1}) = (\lambda_{a+b}, \rho^{-1}_{a+b})$, for all $a,b \in G(X,r)$. Then, $(\mathcal{G}(X,r),+,\circ)$ is a skew left brace (see [8, Theorem 3.11] or [6, Theorem 2.1.14]).

4.2 Malcev nilpotency of $A(X,r)$ and $A'(X,r)$

Malcev proved that nilpotency of groups can be defined via some specific identities, the so-called Malcev identities, leading to the definition of a Malcev nilpotent semigroup [136]. Let F be the free semigroup on $\{x,y,z_n \mid n \geq 1\}$. For any non-negative integer n, the Malcev words

$$x_n = x_n(x,y;z_1,\dots,z_n) \in F, \quad \text{and} \quad y_n = y_n(x,y;z_1,\dots,z_n) \in F,$$

are defined recursively as

$$\begin{aligned} x_0 &= x, & y_0 &= y, \\ x_{n+1} &= x_n z_{n+1} y_n, & y_{n+1} &= y_n z_{n+1} x_n. \end{aligned}$$

A semigroup S is called *Malcev nilpotent* of nilpotency class n (or, simply, nilpotent of class n) if n is the smallest non-negative integer such that, in S,

$$x_n(s,t;u_1,\dots,u_n) = y_n(s,t;u_1,\dots,u_n),$$

for all $s,t \in S$ and $u_1,\dots,u_n \in S^1$. A group H is Malcev nilpotent of class n if and only if H is nilpotent (in ordinary sense) of class n (see for example [104, 145]).

Let (X,r) be a bijective non-degenerate set-theoretic solution of the Yang-Baxter equation. If $M = M(X,r)$ is Malcev nilpotent of class n then, as an epimorphic image, the subgroups $\operatorname{gr}(\lambda_a \mid a \in M)$ (resp. $\operatorname{gr}(\rho_a \mid a \in M)$) of $\operatorname{Sym}(M)$ is nilpotent, and thus, by (4.5), so is the subgroup $\operatorname{gr}(\lambda_x \mid x \in X)$ (resp. $\operatorname{gr}(\rho_x \mid x \in X)$) of $\operatorname{Sym}(X)$.

In this section we determine when the left and right derived structure monoid $A(X,r)$ and $A'(X,r)$ respectively of a bijective non-degenerate set-theoretic solution (X,r) are Malcev nilpotent. More precisely, we will show that if the permutation group of the right derived solution (X,s') associated to (X,r) is nilpotent of class n, then the structure monoid $M(X,s') = A'(X,r)$ is Malcev nilpotent of class not exceeding $n+2$. Next, we extend a result of Lebed and Mortier [122, Theorem 3.2], and show that the structure group of a finite abelian rack is a finite conjugacy group with torsion subgroup equal to the commutator subgroup. Finally, together with a combinatorial description in terms of r-tuples of lower-triangular matrices with non-negative entries given in [122, Proposition 2.1], it is possible to give a full description of all finite abelian racks, generalizing the result for finite abelian quandles given in [122, Theorem 2.3].

Let (X,r) be a bijective non-degenerate set-theoretic solution of the Yang-Baxter equation. In what follows, we focus on the right derived solution (X,s'), and the right derived structure monoid $A'(X,r)$. To highlight this, we will denote the solution by $(X,r_\lhd)$, and consider the associated rack $(X,\lhd)$, with $\lambda_x(y) = y \lhd x$ (see Subsection 1.3.3 and Section 2.2). So, $r_\lhd(x,y) = (\lambda_x(y),x)$, for all $x,y \in X$. The other situation, i.e. where $(X,r_\lhd) = (X,s)$, can be handled in the same way. We denote $\mathcal{G}(X,r_\lhd)$, $M(X,r_\lhd)$ and $G(X,r_\lhd)$ by $\mathcal{G}(X,\lhd)$, $M(X,\lhd)$ and $G(X,\lhd)$, respectively. Note that $\mathcal{G}(X,\lhd) \cong \mathcal{G}_\lambda(X,r_\lhd)$. To ease notation, identify these groups for this class of solutions, i.e. $\mathcal{G}(X,\lhd) = \operatorname{gr}(\lambda_x \mid x \in X)$.

Proposition 4.2.1. *Let $(X,\lhd)$ be a rack, with permutation group $\mathcal{G}(X,\lhd)$ being nilpotent of class n. Then, the structure monoid $M(X,\lhd)$ of $(X,r_\lhd)$ is Malcev nilpotent of class at most $n+2$, and the structure group $G(X,\lhd)$ of $(X,r_\lhd)$ is nilpotent of class at most $n+2$.*

Proof. Let $(X,\lhd)$ be a rack, and assume that the group $\mathcal{G}(X,\lhd)$ is nilpotent of class n. Put $M = M(X,\lhd)$. Let $a,b,a_1,\dots,a_{n+2} \in M$, and consider, for $1 \le i \le n+2$, Malcev words

$$\begin{aligned} x_i &= x_i(a,b;a_1,\dots,a_i) \in M,\\ y_i &= y_i(a,b;a_1,\dots,a_i) \in M. \end{aligned}$$

Then, it follows that $\lambda_{x_n} = \lambda_{y_n}$, as $\mathcal{G}(X,\triangleleft)$ is Malcev nilpotent of class n. Furthermore, since $(X, r_\triangleleft)$ is a set-theoretic solution of the Yang-Baxter equation, we get by (1.17),

$$\lambda_{y_n}\lambda_{x_n} = \lambda_{x_n}\lambda_{y_n} = \lambda_{\lambda_{x_n}(y_n)}\lambda_{x_n}.$$

Hence, by bijectivity of λ_{x_n}, we conclude that $\lambda_{\lambda_{x_n}(y_n)} = \lambda_{y_n}$. Moreover, using again (1.17), $\lambda_{y_n}\lambda_{y_n} = \lambda_{\lambda_{y_n}(y_n)}\lambda_{y_n}$, so $\lambda_{\lambda_{y_n}(y_n)} = \lambda_{y_n}$. Put $z = \lambda_{y_n}(y_n) \in M$. Then, as $\lambda_z = \lambda_{y_n} = \lambda_{x_n}$, we get $\lambda_z\lambda_{x_n} = \lambda_{x_n}\lambda_z = \lambda_{\lambda_{x_n}(z)}\lambda_{x_n}$ and, in consequence, $\lambda_{\lambda_{x_n}(z)} = \lambda_z$. Thus, in M, we have

$$x_n \circ z = \lambda_{x_n}(z) \circ x_n = \lambda_{\lambda_{x_n}(z)}(x_n) \circ \lambda_{x_n}(z) = \lambda_z(x_n) \circ \lambda_{x_n}(z),$$

implying that

$$\begin{aligned} y_n \circ x_n \circ x_n \circ y_n &= \lambda_{y_n}(x_n) \circ y_n \circ \lambda_{x_n}(y_n) \circ x_n\\ &= \lambda_{y_n}(x_n) \circ \lambda_{y_n}(\lambda_{x_n}(y_n)) \circ y_n \circ x_n\\ &= \lambda_z(x_n) \circ \lambda_{x_n}(z) \circ y_n \circ x_n\\ &= x_n \circ z \circ y_n \circ x_n\\ &= x_n \circ \lambda_{y_n}(y_n) \circ y_n \circ x_n\\ &= x_n \circ y_n \circ y_n \circ x_n. \end{aligned}$$

Using the previous equality, it follows that

$$\begin{aligned} y_n \circ x_n \circ a \circ x_n \circ y_n &= y_n \circ \lambda_{x_n}(a) \circ x_n \circ x_n \circ y_n\\ &= \lambda_{y_n}(\lambda_{x_n}(a)) \circ y_n \circ x_n \circ x_n \circ y_n\\ &= \lambda_{x_n}(\lambda_{y_n}(a)) \circ x_n \circ y_n \circ y_n \circ x_n\\ &= x_n \circ \lambda_{y_n}(a) \circ y_n \circ y_n \circ x_n\\ &= x_n \circ y_n \circ a \circ y_n \circ x_n, \end{aligned}$$

for all $a \in M$. Finally, the last equality leads to

$$\begin{aligned} y_{n+2} &= y_n \circ (a_{n+1} \circ x_n) \circ a_{n+2} \circ (x_n \circ a_{n+1}) \circ y_n\\ &= y_n \circ x_n \circ \lambda^{-1}_{x_n}(a_{n+1}) \circ a_{n+2} \circ \lambda_{x_n}(a_{n+1}) \circ x_n \circ y_n\\ &= (x_n \circ y_n) \circ \lambda^{-1}_{x_n}(a_{n+1}) \circ a_{n+2} \circ \lambda_{x_n}(a_{n+1}) \circ (y_n \circ x_n)\\ &= x_n \circ \lambda_{y_n}(\lambda^{-1}_{x_n}(a_{n+1})) \circ y_n \circ a_{n+2} \circ y_n \circ \lambda^{-1}_{y_n}(\lambda_{x_n}(a_{n+1})) \circ x_n\\ &= x_n \circ a_{n+1} \circ y_n \circ a_{n+2} \circ y_n \circ a_{n+1} \circ x_n\\ &= x_{n+2}. \end{aligned}$$

Hence, M is Malcev nilpotent of class at most $n+2$. Similarly, one proves that $G(X,\triangleleft)$ is Malcev nilpotent of class at most $n+2$, and thus it is nilpotent of class at most $n+2$. □

In [122], Lebed and Mortier describe all finite quandles $(X, \triangleleft)$ with abelian structure group $G(X, r_{\triangleleft})$, where $r_{\triangleleft}(x,y) = (y \triangleleft x, x)$, for all $x, y \in X$. In particular, they prove that these quandles are abelian, i.e. $(a \triangleleft b) \triangleleft c = (a \triangleleft c) \triangleleft b$, for all $a, b, c \in X$. With a similar proof, racks $(X, \triangleleft)$ with abelian structure group $G(X, \triangleleft)$ are abelian. Equivalently, since $\lambda_x(y) = y \triangleleft x$, the associated permutation group $\mathcal{G}(X, \triangleleft) = \operatorname{gr}(\lambda_x \mid x \in X)$ is abelian. Furthermore, in the same paper, it is shown that the structure group $G(X, r_{\triangleleft})$ of a finite abelian quandle $(X, \triangleleft)$ is a central extension of a free abelian group by an explicit finite abelian group isomorphic to the commutator subgroup of $G(X, r_{\triangleleft})$. The latter can also be proven for $G = G(X, \triangleleft)$ in case $(X, \triangleleft)$ is a finite abelian rack (see Corollary 4.2.5). To do so, first note that in G we have $\lambda_x(y) = x \circ y \circ \overline{x}$ for all $x, y \in X$, where $\overline{x}$ denotes the inverse of x in G. The map $\lambda : X \to \operatorname{Sym}(X) : x \mapsto \lambda_x$ induces a unique homomorphism

$$\lambda : G \to \mathcal{G}(X, \triangleleft) : g \mapsto \lambda_g.$$

Furthermore, for $x_1, \dots, x_n \in X$ and $x_i^{\varepsilon_i} \in \{x_i, \overline{x_i}\}$, we have that $x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n} \in \operatorname{Ker}(\lambda)$ if and only if $\lambda_{x_1^{\varepsilon_1}} \cdots \lambda_{x_n^{\varepsilon_n}} = \mathrm{id}_X$, where $\lambda_{\overline{x}} = \lambda_x^{-1}$. Since

$$x_1^{\varepsilon_1} \circ \cdots \circ x_n^{\varepsilon_n} \circ y = \lambda_{x_1^{\varepsilon_1}} \cdots \lambda_{x_n^{\varepsilon_n}}(y) \circ x_1^{\varepsilon_1} \circ \cdots \circ x_n^{\varepsilon_n},$$

for all $y \in X$, it follows that $\operatorname{Ker}(\lambda) \subseteq Z(G)$. Hence, the group $G/Z(G)$ is a homomorphic image of the group $G/\operatorname{Ker}(\lambda) \cong \mathcal{G}(X, \triangleleft)$, which shows the following result (compare with Proposition 4.2.1). However, it may happen that $\operatorname{Ker}(\lambda) \neq Z(G)$ (compare with Remark 4.1.8). To provide an explicit example of this phenomenon consider $X = \{1, 2\}$ and define $x \triangleleft y = f(x)$ for $x, y \in X$, where f is the unique non-trivial permutation of X. Then,

$$G = G(X, \triangleleft) = \operatorname{gr}(1, 2 \mid 1 \circ 1 = 2 \circ 1 = 2 \circ 2 = 1 \circ 2) \cong \mathbb{Z}.$$

So, $G = Z(G)$, but $G/\operatorname{Ker}(\lambda) \cong \mathcal{G}(X, \triangleleft) \cong \mathbb{Z}/2\mathbb{Z}$. Thus, $\operatorname{Ker}(\lambda) \neq Z(G)$.

Corollary 4.2.2. *Let $(X, \triangleleft)$ be a rack and put $G = G(X, \triangleleft)$. Then, the group $G/Z(G)$ is a homomorphic image of the permutation group $\mathcal{G} = \mathcal{G}(X, \triangleleft)$. In particular, G is nilpotent if and only if $\mathcal{G}$ is nilpotent, and the nilpotency class of G is equal to or exceeds by one the nilpotency class of $\mathcal{G}$. Furthermore, G is solvable if and only if $\mathcal{G}$ is solvable, and the derived length of G is equal to or exceeds by one the derived length of $\mathcal{G}$.*

The following lemma contains a known result on the structure of nilpotent structure groups. For more background, see for example [158]. The second part of the lemma is due to Cedó, Gateva-Ivanova, and Smoktunowicz [44] and Lebed and Vendramin [125].

For a group G, we denote

$$T(G) = \{g \in G \mid g^n = 1, \text{ for some positive integer } n\},$$

the set consisting of the elements of finite order (also called the torsion elements), called the *torsion subgroup of* G. Furthermore, the *commutator subgroup of* G is

$$[G, G] = \{[g, h] = ghg^{-1}h^{-1} \mid g, h \in G\},$$

where g^{-1} denotes the inverse of g in the group G.

Lemma 4.2.3 (Cedó, Gateva-Ivanova, and Smoktunowicz [44], and Lebed and Vendramin [125])**.** *Let (X,r) be a finite bijective non-degenerate solution of the Yang-Baxter equation, and put $G = G(X,r)$.*

(1) If the group G is nilpotent, then G is finite-by-(free abelian). Moreover, G is a finite conjugacy group (i.e. G has finite commutator subgroup).

(2) If G is torsion-free, then G is nilpotent if and only if G is abelian, or equivalently the injectivization $\operatorname{Inj}(X,r)$ *of (X,r) is the trivial solution. Hence, if (X,r) is a finite non-degenerate involutive solution, then G is nilpotent if and only if G is abelian.*

Proof. (1) Recall from Chapter 2 that the group G is abelian-by-finite and finitely generated. Assume G is also nilpotent. Then, $T = T(G)$ is a finite characteristic subgroup of G and G/T is torsion-free and nilpotent (see for example [158, 5.2.7]). Furthermore, since G is abelian-by-finite, also G/T is abelian-by-finite. It follows that G/T is a nilpotent Bieberbach group. As a corollary of [77, Theorem 3], we get that G/T is finitely generated and abelian, so by the fundamental theorem for finitely generated abelian groups it is a direct sum of finitely many cyclic groups of infinite or prime-power orders. Hence, as it is also torsion-free, G/T is a free abelian group. So, G itself is indeed finite-by-(free abelian). Furthermore, since G/T is abelian, we get that the commutator subgroup $[G,G] \subseteq T$, and it is finite as T is finite. By a result of Neumann [144, Theorem 5.4] (or see [158, 14.5.11]), G is a finite conjugacy group, meaning that every conjugacy class of G is finite.

(2) Recall from Section 2.1 that $G \cong G(\operatorname{Inj}(X,r))$, and thus it is sufficient to prove the first part for injective solutions (X,r). It was shown in [100, Theorem 6.5] that G is torsion-free if and only if $\operatorname{Inj}(X,r)$ is involutive. The result now follows from the involutive case, which was shown in [44, before Corollary 4]. □

Finally, in order to prove Corollary 4.2.5, we need the following result on the torsion elements of the right derived structure monoid of a finite bijective non-degenerate set-theoretic solution of the Yang-Baxter equation. Recall from Section 2.2 that $A'_{\mathrm{gr}}(X,r)$ is the structure group of the right derived solution (X,s') of (X,r), where $s'(x,y) = (\tau_x(y),x)$ and $\tau_x(y) = \rho_x\lambda_{\rho_y^{-1}(x)}(y)$, for all $x,y \in X$.

Proposition 4.2.4. *Let (X,r) be a finite bijective non-degenerate solution and put $A'_{\mathrm{gr}} = A'_{\mathrm{gr}}(X,r)$. Then $T(A'_{\mathrm{gr}})$, the set of torsion elements of A'_{gr}, coincides with the finite group $[A'_{\mathrm{gr}},A'_{\mathrm{gr}}]$. Also, $T(A_{\mathrm{gr}}(X,r)) = [A_{\mathrm{gr}}(X,r),A_{\mathrm{gr}}(X,r)]$.*

Proof. We only prove $T(A'_{\mathrm{gr}}(X,r)) = [A'_{\mathrm{gr}}(X,r),A'_{\mathrm{gr}}(X,r)]$. The proof of the second part is similar. Put $A'_{\mathrm{gr}} = A'_{\mathrm{gr}}(X,r)$.

For any $x,y \in X$, $x \oplus y \ominus x = \tau_x(y)$ in A'_{gr}, with $\ominus x$ the inverse of x in A'_{gr}. So, the conjugates of x in A'_{gr} are $\{\tau_a(x) \mid a \in A'_{\mathrm{gr}}\} \subseteq X$. Since X is finite, each generator $x \in A'_{\mathrm{gr}}$ has finitely many conjugates in A'_{gr}, and A'_{gr} is a finitely generated finite conjugacy group. Furthermore, by a result of Neumann [144, Theorem 5.1], the commutator subgroup $[A'_{\mathrm{gr}},A'_{\mathrm{gr}}]$ of A'_{gr} is a finite group contained in $T(A'_{\mathrm{gr}})$.

Let $\tau : A'_{\text{gr}} \to \text{Sym}(X) : a \mapsto \tau_a$ be the unique homomorphism such that $\tau_{\iota(x)} = \tau_x$, for all $x \in X$, where $\iota : X \to A'_{\text{gr}}$ is the natural map. Consider the equivalence relation $\approx$ on X, where $x \approx y$, for $x, y \in X$, if there exists $a \in A'_{\text{gr}}$ such that $\tau_a(x) = y$. Write $[x] \in \overline{X} = X/\approx$ for the $\approx$-class of $x \in X$. Consider the free abelian group $F = \text{Fa}(\overline{X})$ on $\overline{X}$. Note that F is the structure group of the solution $(\overline{X}, \overline{s}')$ of the Yang-Baxter equation, where $\overline{s}'([x],[y]) = ([\tau_x(y)],[x]) = ([y],[x])$, for all $x, y \in X$. Because the map $(X, s') \to (\overline{X}, \overline{s}')$, defined as $x \mapsto [x]$, for all $x \in X$, is an epimorphism of solutions, there is a unique morphism of groups $\varphi : A'_{\text{gr}} \to F$ such that $\varphi(x) = [x]$, for all $x \in X$. Clearly, φ factors uniquely through a homomorphism $\overline{\varphi} : A'_{\text{gr}}/[A'_{\text{gr}}, A'_{\text{gr}}] \to F$. On the other hand, $x \oplus y = \tau_x(y) \oplus x$ in A'_{gr} and thus $\tau_x(y) \ominus y \in [A'_{\text{gr}}, A'_{\text{gr}}]$, for all $x, y \in X$. Hence, the map $\overline{X} \to A'_{\text{gr}}/[A'_{\text{gr}}, A'_{\text{gr}}]$, defined by $[x] \mapsto x \oplus [A'_{\text{gr}}, A'_{\text{gr}}]$, for all $x \in X$, is well-defined. So, there exists a unique homomorphism $\psi : F \to A'_{\text{gr}}/[A'_{\text{gr}}, A'_{\text{gr}}]$ such that $\psi([x]) = x \oplus [A'_{\text{gr}}, A'_{\text{gr}}]$, for all $x \in X$. Clearly, ψ is the inverse of $\overline{\varphi}$. So, $F \cong A'_{\text{gr}}/[A'_{\text{gr}}, A'_{\text{gr}}]$, which implies that $T(A'_{\text{gr}}) \subseteq [A'_{\text{gr}}, A'_{\text{gr}}]$. Therefore, $T(A'_{\text{gr}}) = [A'_{\text{gr}}, A'_{\text{gr}}]$, as desired. □

The previous results prove an extended result of Lebed and Mortier. That the left derived structure group $A_{\text{gr}}(X, r)$ of a finite bijective non-degenerate solution (X, r) is a finite conjugacy group, was already shown in [97, Proposition 3.2].

Corollary 4.2.5 (Lebed and Mortier [122, Theorem 3.2])**.** *Let $(X, \triangleleft)$ be a finite abelian rack and put $G = G(X, \triangleleft)$. Then, G is a finite conjugacy group with periodic subgroup $T(G) = [G, G]$, and $G/[G, G]$ is a free abelian group of rank at most $|\iota(X)|$.*

Let $(X, \triangleleft)$ be an abelian rack, and consider the natural action of the permutation group $\mathcal{G}(X, \triangleleft)$ on the set X. Let $X = X_1 \sqcup \cdots \sqcup X_r$ be a decomposition of X into orbits with respect to the action of $\mathcal{G}(X, \triangleleft)$ on X. So, for $1 \le i \le r$, we have $x, y \in X_i$ if and only if there exists $g \in \mathcal{G}(X, \triangleleft)$ such that $g(x) = y$.

Lemma 4.2.6. *Let $(X, \triangleleft)$ be an abelian rack. If $x, y \in X$ belong to the same $\mathcal{G}(X, \triangleleft)$-orbit, then $\lambda_x = \lambda_y$.*

Proof. Let $x, y \in X$. Since the rack $(X, \triangleleft)$ is abelian, the permutation group $\mathcal{G}(X, \triangleleft)$ is abelian (see after Proposition 4.2.1), and by (1.17), we get

$$\lambda_y \lambda_x = \lambda_x \lambda_y = \lambda_{\lambda_x(y)} \lambda_x.$$

As λ_x is bijective, we get $\lambda_y = \lambda_{\lambda_x(y)}$, for all $x, y \in X$, and the result follows. □

Lemma 4.2.7. *Let $(X, \triangleleft)$ be a finite abelian rack with $\mathcal{G}(X, \triangleleft)$-orbits $X_1, \ldots, X_r$. For $1 \le i, j \le r$ and $x_i \in X_i$, the map $\lambda_{x_i}|_{X_j}$ is a permutation of X_j consisting of disjoint cycles all of the same length.*

Proof. Let $f = \lambda_{x_i}|_{X_j} = f_1 \cdots f_s$ be the decomposition of the permutation f of X_j as a product of disjoint cycles. We may assume that f_1 has minimal length, say n. This implies that $f^n = f_1^n \cdots f_s^n$ has a fixed point, say $x_j \in X_j$. We claim that f^n is the identity map. Indeed, let $x \in X_j$. As x is in the same orbit as x_j, there exists $g \in \mathcal{G}(X, \triangleleft)$ such that $g(x_j) = x$. Because $\mathcal{G}(X, \triangleleft)$ is abelian, this implies $f^n(x) = f^n(g(x_j)) = g(f^n(x_j)) = g(x_j) = x$. Thus, all the disjoint cycles of f must have length n. □

With the assumptions as in Lemma 4.2.7, define the following subgroups of $G = G(X, \triangleleft)$,

$$G_i = \mathrm{gr}(X_i \mid x \circ y = \lambda_x(y) \circ x, \text{ for all } x, y \in X_i) \subseteq G.$$

We claim that G_i is an abelian group.

Lemma 4.2.8. *Let $(X, \triangleleft)$ be a finite abelian rack with $\mathcal{G}(X, \triangleleft)$-orbits $X_1, \dots, X_r$. Then, the groups $G_1, \dots, G_r$ are abelian.*

Proof. Fix $1 \leq i \leq r$. To prove that G_i is abelian, it is sufficient to prove that all generators of G_i commute. Note that $x \circ x = \lambda_x(x) \circ x$ in $G = G(X, \triangleleft)$, for all $x \in X$. Therefore, $x = \lambda_x(x)$ in G. So, let $x, y \in X_i$. By Lemma 4.2.6, we get $x \circ y = \lambda_x(y) \circ x = \lambda_y(y) \circ x = y \circ x$, as desired. □

For a finite abelian rack $(X, \triangleleft)$ with $\mathcal{G}(X, \triangleleft)$-orbits $X_1, \dots, X_r$, fix $1 \leq i, j \leq r$. For any $x \in X_i$ and $y \in X_j$, define the commutator

$$g_{x,y} = [x, y] = x \circ y \circ \overline{x} \circ \overline{y} \in G(X, \triangleleft),$$

where $\overline{x}$ denotes the inverse of x in the structure group $(G(X, \triangleleft), \circ)$. Since $g_{x,y} = \lambda_x(y) \circ \overline{y} \in G_j$ and $g_{x,y} = x \circ \overline{\lambda_y(x)} \in G_i$, it follows that $g_{x,y} \in G_i \cap G_j$. Furthermore, by Lemma 4.2.8, both groups G_i and G_j are abelian, and thus $g_{x,y}$ is central in both G_i and G_j. We will prove that $g_{x,y}$ is also central in $G(X, \triangleleft)$.

Lemma 4.2.9. *Let $(X, \triangleleft)$ be a finite abelian rack. Using the above notation, for any $x, x' \in X_i$ and $y, y' \in X_j$, we have $g_{x,y} = g_{x',y'}$. Furthermore, $g_{x,y}$ is central in $G = G(X, \triangleleft)$.*

Proof. Let $1 \leq i, j \leq r$, $x, x' \in X_i$ and $y, y' \in X_j$. As

$$g_{x,y} = x \circ y \circ \overline{x} \circ \overline{y} = \lambda_x(y) \circ \overline{y} = x \circ \overline{\lambda_y(x)},$$

and, by Lemma 4.2.6, $\lambda_x = \lambda_{x'}$, we obtain that $g_{x,y} = \lambda_x(y) \circ \overline{y} = \lambda_{x'}(y) \circ \overline{y} = g_{x',y}$. Similarly, $g_{x',y} = x' \circ \overline{\lambda_y(x')} = x' \circ \overline{\lambda_{y'}(x')} = g_{x',y'}$. Thus, $g_{x,y} = g_{x',y'}$.

To prove that $g_{x,y}$ is central in G, it is sufficient to prove that $g_{x,y}$ commutes with each generator $z \in X$. By the first part, we have that $g_{\lambda_z(x), \lambda_z(y)} = g_{x,y}$. Therefore,

$$\begin{aligned} z \circ g_{x,y} &= z \circ [x, y] \circ \overline{z} \circ z = [z \circ x \circ \overline{z}, z \circ y \circ \overline{z}] \circ z \\ &= [\lambda_z(x), \lambda_z(y)] \circ z = g_{\lambda_z(x), \lambda_z(y)} \circ z = g_{x,y} \circ z, \end{aligned}$$

as desired. □

For $1 \leq i, j \leq r$, $x \in X_i$ and $y \in X_j$, we simply denote $g_{x,y}$ as g_{ij}. By Corollary 4.2.5, we obtain the following result.

Corollary 4.2.10 (Lebed and Vendramin [125, Theorem 8.15])**.** *Let $(X,\triangleleft)$ be a finite abelian rack. If $G = G(X,\triangleleft)$, then*

$$[G,G] = \operatorname{gr}(g_{ij} \mid 1 \leq i,j \leq r) = T(G) \subseteq Z(G).$$

In particular, G is abelian if and only if G is free abelian, or equivalently, G is a torsion-free group.

The last part of Corollary 4.2.10 has been proven more general by Jespers, Kubat, and Van Antwerpen, in [97, 98]. More precisely, for arbitrary finite bijective non-degenerate solutions (X,r), they show that the structure monoid $M(X,r)$ is free abelian if and only if the structure algebra $KM(X,r)$ over an arbitrary field K is a domain, and this is equivalent with $M(X,r)$ being cancellative. In this case, we also get that $KG(X,r)$ is a domain. So, from the positive solution of the zero divisor problem for polycyclic-by-finite groups (see for example [160, Theorem 8.2.35]), it follows that the latter is equivalent with $G(X,r)$ being a torsion-free group.

The following result generalizes a result of Lebed and Mortier, in [122], for finite abelian quandles to finite abelian racks.

Proposition 4.2.11. *Finite abelian racks on a set X are in one-to-one correspondence with partitions $X = X_1 \sqcup \cdots \sqcup X_r$ of X and families of permutations $f_{ij} \in \operatorname{Sym}(X_i)$, for $1 \leq i,j \leq r$, such that*

(1) $f_{ij}f_{ik} = f_{ik}f_{ij}$, for all $1 \leq i,j,k \leq r$,

(2) if $\mathcal{G}_i = \operatorname{gr}(f_{ij} \mid 1 \leq j \leq r)$, then the orbit of x_i with respect to the action of $\mathcal{G}_i$ on X_i, denoted by $\mathcal{G}_i x_i$, is equal to X_i, for all $1 \leq i \leq r$ and $x_i \in X_i$,

(3) if $g \in \mathcal{G}_i$ has a fixed point, for some $1 \leq i \leq r$, then $g = \operatorname{id}_{X_i}$.

If in addition $f_{ii} = \operatorname{id}_{X_i}$, for all $1 \leq i \leq r$, then the decomposition and permutations above correspond to a finite abelian quandle.

Proof. Let $(X,\triangleleft)$ be an abelian rack, and $X = X_1 \sqcup \cdots \sqcup X_r$ the decomposition of X into orbits with respect to the action of $\mathcal{G}(X,\triangleleft)$ on X. In particular, for any $x \in X$, λ_x preserves the components of this decomposition, meaning that $\lambda_x(X_i) = X_i$, for all $1 \leq i \leq r$. Fix $1 \leq i,j,k \leq r$. Choosing $x_j \in X_j$, we define $f_{ij} \in \operatorname{Sym}(X_i)$ as $f_{ij} = \lambda_{x_j}|_{X_i}$, which is well-defined, and does not depend on the representative x_j of the orbit X_j, by Lemma 4.2.6. Since $\mathcal{G}(X,\triangleleft)$ is abelian, $\lambda_{x_j}\lambda_{x_k} = \lambda_{x_k}\lambda_{x_j}$, for all $x_j \in X_j$ and $x_k \in X_k$, and we get that $f_{ij}f_{ik} = f_{ik}f_{ij}$. Furthermore, if $x_i \in X_i$, then

$$X_i = \mathcal{G}(X,\triangleleft)x_i = \{(g|_{X_i})(x_i) \mid g \in \mathcal{G}(X,\triangleleft)\} = \mathcal{G}_i x_i.$$

Moreover, assume that $g \in \mathcal{G}_i$ has a fixed point, say $x_i \in X_i$, and let $x \in X_i$. Then, there exists $f \in \mathcal{G}_i$ with $x = f(x_i)$, and we have

$$g(x) = g(f(x_i)) = f(g(x_i)) = f(x_i) = x,$$

as desired. Finally, if $(X, \triangleleft)$ is a quandle, then $\lambda_x(x) = x$ for $x \in X_i$ yields $f_{ii}(x_i) = x_i$ and thus, by the previous, $f_{ii}(x) = x$ for each $x \in X_i$, that is $f_{ii} = \mathrm{id}_{X_i}$.

Conversely, let $X = X_1 \sqcup \cdots \sqcup X_r$ of X be a partition of X, and $f_{ij} \in \mathrm{Sym}(X_i)$, for $1 \leq i, j \leq r$, a family of permutations satisfying conditions (1)-(3). We define an abelian rack structure on X by $x \triangleleft y = f_{ij}(x)$, for all $x, y \in X$ with $x \in X_i$ and $y \in X_j$. Indeed, if $x \in X_i$, $y \in X_j$ and $z \in X_k$ for some $1 \leq i, j, k \leq r$, then

$$\begin{aligned}(x \triangleleft y) \triangleleft z &= f_{ij}(x) \triangleleft z = f_{ik}(f_{ij}(x)) = f_{ij}(f_{ik}(x)) \\ &= f_{ik}(x) \triangleleft f_{jk}(y) = (x \triangleleft z) \triangleleft (y \triangleleft z).\end{aligned}$$

Moreover, if $y \in X_j$, then the map $f : X \to X$, defined by $f(x) = x \triangleleft y$, is bijective because $f(x) = f_{ij}(x)$, for all $x \in X_i$. So, $f|_{X_i} = f_{ij} \in \mathrm{Sym}(X_i)$. Finally, if $f_{ii} = \mathrm{id}_{X_i}$, for all $1 \leq i \leq r$, then $x \triangleleft x = f_{ii}(x) = x$, for all $x \in X_i$, and $(X, \triangleleft)$ is a quandle.

It is also easy to check that the correspondence between abelian rack structures on X and decompositions of X together with families of maps f_{ij} satisfying all conditions stated in proposition is in fact a one-to-one correspondence. □

In [122, Theorem 2.3], Lebed and Mortier obtain a combinatorial description of families of permutations satisfying the requirements in Proposition 4.2.11. So, they obtain a full description of all finite abelian quandles. This combinatorial description is in terms of r-tuples of lower-triangular matrices with non-negative entries. Quandles corresponding to such r-tuples are called in [122] the filtered-permutation quandles.

Problem 4.2.12. *Describe all finite quandles $(X, \triangleleft)$ with nilpotent permutation group $\mathcal{G}(X, \triangleleft)$ of class 2, or more general, a metabelian permutation group.*

A natural problem is to investigate arbitrary finite solutions (X, r) of the Yang-Baxter equation with $\mathcal{G}(X, r)$ an abelian group.

4.3 Malcev nilpotency of $M(X, r)$

Let (X, r) be a finite bijective non-degenerate set-theoretic solution of the Yang-Baxter equation. From Corollary 3.4.4, we know that $K[(M(X, r), \circ)]$ is a representable algebra. So, $M(X, r)$ is a submonoid of the multiplicative monoid of a matrix ring over a field, i.e. $M(X, r)$ is a linear monoid. Okniński [147], and Jespers and Riley [104], found a criterion for a finitely generated linear semigroup S to be Malcev nilpotent. This criterion is based on information of ideal chains of S with factors that are either power nilpotent or uniform subsemigroups of completely (θ)-simple inverse semigroups. In order to describe when the structure monoid $M(X, r)$ is Malcev nilpotent, we provide a very concrete description of such an ideal chain. It hence will also give an independent proof of the previous for the structure monoids $M(X, r)$ of finite bijective non-degenerate solutions. This is what we first deal with in this section. Afterwards, we discuss in more detail when the structure monoid of a finite bijective non-degenerate Lyubashenko solution is Malcev nilpotent. To end this section, we consider several examples of finite bijective non-degenerate solutions and study whether their structure monoids are Malcev nilpotent.

Let (X,r) be a finite bijective non-degenerate solution, and put $X = \{x_1,\dots,x_n\}$ and $M = M(X,r)$. To avoid confusion later in this section, we denote the generators of $A = A(X,r)$ by $a_1,\dots,a_n$. So,

$$M = \langle x_1,\dots,x_n \mid x_i \circ x_j = \lambda_{x_i}(x_j) \circ \rho_{x_j}(x_i), \text{ for all } 1 \le i,j \le n\rangle^1,$$

and

$$A = \langle a_1,\dots,a_n \mid a_i + \lambda_{a_i}(a_j) = \lambda_{a_i}(a_j) + \lambda_{\lambda_{a_i}(a_j)}(\rho_{a_j}(a_i)), \text{ for all } 1 \le i,j \le n\rangle^1,$$

Actually, $a_i = \pi(x_i)$, for $1 \le i \le n$, where π denotes the bijective 1-cocycle from M to A (see Section 2.2). Furthermore, we have a monoid embedding $f : M(X,r) \to A(X,r) \rtimes \mathrm{Im}(\lambda') : m \mapsto (\pi(m),\lambda'_m)$. By Remark 2.2.11, we can put $\lambda_m = \lambda'_m$, for all $m \in M$, and by abuse of notation, in this section, we will identify m with $f(m)$, and write λ_a instead of $\lambda_{\pi^{-1}(a)}$, for all $a \in A$. So, we can simply write

$$M = \{(a,\lambda_a) \mid a \in A\} = \langle x_i = (a_i,\lambda_{a_i}) \mid 1 \le i \le n\rangle^1,$$

and we denote $(a,\lambda_a)\circ(b,\lambda_b)$ simply by $(a,\lambda_a)(b,\lambda_b)$. Thus, with this notation, we have a mapping

$$\lambda : A \to \mathrm{Aut}(A,+) : a \mapsto \lambda_a,$$

and, for any $a,b \in A$,

$$\lambda_{a+\lambda_a(b)} = \lambda_a\lambda_b. \tag{4.8}$$

Using the notation of [97], we denote $B^e = \{(b,\lambda_b) \mid b \in B\}$, for a subset B of A. Note that $A^e = M$.

The construction of the ideal chain in M that we will provide, is based on earlier works on monoids of I-type, and on monoids of skew and quadratic type (see for example [84, 102, 103, 106]) The construction is based on divisibility of elements of M by elements of X. The same idea was used in [97, 98] to determine the prime ideals of M and KM.

Recall from Subsection 3.4.1 that an element s in a monoid S is *left divisible* by $t \in S$ if $s = tt'$ for some $t' \in S$, and it is *right divisible* by $t \in S$ if $s = t't$ for some $t' \in S$. If all elements of S are normalizing, i.e. $Ss = sS$ for all $s \in S$, then left and right divisibility are the same. This happens, for example, in A (see Example 3.1.1). In this case, we simply say that s is *divisible* by t, or t divides s and write $t \mid s$. If t does not divide s, we write $t \nmid s$. Now, note that in M, an element (a,λ_a) is left divisible by a generator $x_i = (a_i,\lambda_{a_i})$ if and only if a is divisible by a_i. So, left divisibility in M by elements of X can be transferred to divisibility in A by elements of $\{a_1,\dots,a_n\}$, the generators of A. Note, however, that $a \in A$ being divisible by a_i in A does not mean that (a,λ_a) is right divisible by x_i. It only means that $a = a_i + b = c + a_i$ for some $b,c \in A$, or equivalently

$$\begin{aligned}(a,\lambda_a) &= (a_i,\lambda_{a_i})(\lambda_{a_i}^{-1}(b),\lambda_{a_i}^{-1}\lambda_a)\\ &= x_i(\lambda_{a_i}^{-1}(b),\lambda_{a_i}^{-1}\lambda_a)\\ &= (c,\lambda_c)(\lambda_c^{-1}(a_i),\lambda_c^{-1}\lambda_{a_i}),\end{aligned}$$

i.e. (a, λ_a) is left divisible by x_i. For $1 \le i \le n$, put

$$M_i = \{(a, \lambda_a) \in M \mid (a, \lambda_a) \text{ is left divisible by at least } i \text{ different}$$
$$\text{generators among } x_1, \dots, x_n\},$$

and

$$A_i = \{a \in A \mid a \text{ is divisible by at least } i \text{ different}$$
$$\text{generators among } a_1, \dots, a_n\},$$

so that $M_i = A_i^e = \{(a, \lambda_a) \mid a \in A_i\}$. Note that if $a \in A_i$, then also $\lambda_b(a) \in A_i$, for all $b \in A$, as λ_b is bijective.

As stated in [97], each M_i is a two-sided ideal of M. Indeed, for any $(a, \lambda_a) \in M_i$ and $(b, \lambda_b) \in M$, we get $(a, \lambda_a)(b, \lambda_b) = (a + \lambda_a(b), \lambda_a\lambda_b)$ and $(b, \lambda_b)(a, \lambda_a) = (b + \lambda_b(a), \lambda_b\lambda_a)$, and both $a + \lambda_a(b)$ and $b + \lambda_b(a)$ are divisible by at least i different generators of A. Hence, we obtain the following ideal chain in M,

$$\emptyset = M_{n+1} \subseteq M_n \subseteq M_{n-1} \subseteq \dots \subseteq M_1 \subseteq M_0 = M. \tag{4.9}$$

We will refine the above chain (4.9), and work towards Proposition 4.3.6. More precisely, we show that there exist ideals B_i, U_i of M satisfying

$$M_{i+1} \subseteq B_i \subseteq U_i \subseteq M_i,$$

and such that

(i) B_i/M_{i+1} and M_i/U_i are power nilpotent semigroups (if M_i/M_{i+1} is power nilpotent, then we take $B_i = U_i = M_i$).

(ii) If M_i/M_{i+1} is not power nilpotent, then $U_i \setminus B_i$ is a (θ)-disjoint union of sets $U_{i1}, \dots, U_{ik}$ such that $U_{ij}U_{il} \subseteq M_{i+1}$ for $j \neq l$.

(iii) Each $(U_{ij} \cup M_{i+1})/M_{i+1}$ is a uniform subsemigroup of a completely (θ)-simple inverse semigroup.

In fact, we will show that B_i/M_{i+1} and M_i/U_i are nil semigroups, which implies that they are power nilpotent semigroups (see for example [103, Theorem 2.4.10.]). Recall that a semigroup S is called *power nilpotent* if $S^n = \{\theta\}$, with θ the zero element. A left, right or two-sided ideal or a semigroup is called *nil* if all its elements are nilpotent. An ideal I of a semigroup S is said to be in the nil radical of S if I is a nil ideal of S, and the largest nil ideal of a semigroup is called the *nil radical*. Furthermore, see for example [58, Theorem 3.9], a *completely (θ)-simple inverse semigroup* is a semigroup of the form $\mathcal{M}^0(C, r, r, I)$, where C is a group and I is the $r \times r$ identity matrix (see Subsection 3.4.2). A subsemigroup S of $\mathcal{M}^0(C, r, r, I)$ is said to be *uniform* if S intersects each nonzero $\mathcal{H}$-class, i.e. all sets $\{(c, i, j) \mid c \in C\}$, of a completely (θ)-simple subsemigroup $\mathcal{M}^0(C, r', r', I')$, where $r' \le r$ and I' the $r' \times r'$ identity matrix. More details about uniform semigroups can be found in, for example, [103, Section 2.2] and [148, Section 3.1]. We make the agreement that some ideals in the chain can be empty.

Fix i with $1 \leq i \leq n$. Define

$$\mathcal{L} = \{Y \subseteq \{a_1, \dots, a_n\} \mid |Y| = i\},$$

and for $Y, Z \in \mathcal{L}$, put

$$M_{YZ} = A^e_{YZ} = \{(a, \lambda_a) \mid a \in A_{YZ}\},$$

with

$$A_{YZ} = \{a \in A \smallsetminus A_{i+1} \mid a \text{ is divisible by } y, \text{ for all } y \in Y, \text{ and } \lambda_a(Z) = Y\}.$$

So, if $a \in A_{YZ}$ then $a \in A_i \cap \langle Y \rangle$, and $z \nmid a$ for $z \in \{a_1, \dots, a_n\} \smallsetminus Y$. Note that some elements of $A_i \cap \langle Y \rangle$ might belong to A_{i+1}. For $Y \in \mathcal{L}$, define

$$M_{Y*} = \bigcup_{Z \in \mathcal{L}} M_{YZ}, \quad \text{and} \quad M_{*Y} = \bigcup_{Z \in \mathcal{L}} M_{ZY}. \tag{4.10}$$

Lemma 4.3.1. *With the above notation, the following properties hold for $Y \in \mathcal{L}$.*

(1) $M_{YY} \cup M_{i+1}$ is a subsemigroup of M.

(2) $M_{Y*} \cup M_{i+1}$ is a right ideal of M.

(3) $M_{*Y} \cup M_{i+1}$ is a left ideal of M.

Proof. Let $(a, \lambda_a), (b, \lambda_b) \in M_{YY} \cup M_{i+1}$, with $(a, \lambda_a)(b, \lambda_b) = (a + \lambda_a(b), \lambda_a\lambda_b) \notin M_{i+1}$. Note that this must mean that both $(a, \lambda_a) \in M_{YY}$ and $(b, \lambda_b) \in M_{YY}$. Since a is divisible by exactly the elements of Y, we get that $a + \lambda_a(b)$ must be divisible by exactly the elements of Y. As both $\lambda_a(Y) = Y$ and $\lambda_b(Y) = Y$, we get that $\lambda_a\lambda_b(Y) = Y$, and thus $(a, \lambda_a)(b, \lambda_b) \in M_{YY}$.

Let $Z \in \mathcal{L}$. Since M_{i+1} is a two-sided ideal of M, for the second and third part it is enough to prove that $M_{YZ}M \subseteq M_{Y*} \cup M_{i+1}$ and $MM_{ZY} \subseteq M_{*Y} \cup M_{i+1}$. We will start with the former.

Let $(a, \lambda_a) \in M_{YZ}$, and $(b, \lambda_b) \in M$. Then, we have $(a, \lambda_a)(b, \lambda_b) = (a + \lambda_a(b), \lambda_a\lambda_b)$. Assume first that $a + \lambda_a(b)$ is divisible by some $z \in \{a_1, \dots, a_n\} \smallsetminus Y$. Then, $a + \lambda_a(b) \in A_{i+1}$, and thus $(a, \lambda_a)(b, \lambda_b) \in M_{i+1}$. Otherwise, $a + \lambda_a(b) \in \langle Y \rangle \cap (A_i \smallsetminus A_{i+1})$. Furthermore, by (4.8),

$$\lambda^{-1}_{a+\lambda_a(b)}(Y) = (\lambda_a\lambda_b)^{-1}(Y) = \lambda_b^{-1}\lambda_a^{-1}(Y) = \lambda_b^{-1}(Z).$$

Thus, $(a, \lambda_a)(b, \lambda_b) \in M_{Y\lambda_b^{-1}(Z)} \subseteq M_{Y*}$.

Finally, let $(a, \lambda_a) \in M_{ZY}$, and $(b, \lambda_b) \in M$. Then, $(b, \lambda_b)(a, \lambda_a) = (b + \lambda_b(a), \lambda_b\lambda_a)$. If $b + \lambda_b(a) \in A_{i+1}$ then $(b, \lambda_b)(a, \lambda_a) \in M_{i+1}$. So, assume that $b + \lambda_b(a) \in A \smallsetminus A_{i+1}$ Clearly, $\lambda_b(a)$ is divisible by all elements of $\lambda_b(Z)$, and thus also $b + \lambda_b(a)$ is divisible by all elements of $\lambda_b(Z)$. Moreover, $(\lambda_b\lambda_a)^{-1}(\lambda_b(Z)) = \lambda_a^{-1}\lambda_b^{-1}(\lambda_b(Z)) = \lambda_a^{-1}(Z) = Y$. Thus, we have $(b, \lambda_b)(a, \lambda_a) \in M_{\lambda_b(Z)Y} \subseteq M_{*Y}$, and the result follows. □

Let $m = (a, \lambda_a) \in M$. Since $m^n = m \circ \cdots \circ m = (a + \lambda_a(a) + \cdots + \lambda_a^{n-1}(a), \lambda_a^n)$, and X is finite, there exists a positive integer n such that $\lambda_a^n|_X = \mathrm{id}_X$, and thus $\lambda_a^n = \mathrm{id}_A$, for all $a \in A$. So, $m^n = (a + \lambda_a(a) + \cdots + \lambda_a^{n-1}(a), \mathrm{id}_A)$. Put $a' = a + \lambda_a(a) + \cdots + \lambda_a^{n-1}(a)$, so $\lambda_{a'} = \mathrm{id}_A$. By [97, Lemma 2.5], there exists a positive integer, say d, such that $da' \in Z(A)$, where $da' = a' + \cdots + a'$, with a' appearing d times. Hence, for any $m = (a, \lambda_a)$, we can assume that there exists a positive integer $q = nd$ such that $m^q = (a', \mathrm{id}_A)^d = (da', \mathrm{id}_A)$, with $da' \in Z(A)$, for all $m \in M$. Actually, there is more. Since X is finite, there exists a positive integer p such that $\mathfrak{q}^{2p} = \mathfrak{q}^p$, where $\mathfrak{q} : X \to X : x \mapsto \lambda_x^{-1}(x)$ is the diagonal map defined in Section 3.2. In [98, Lemma 2], it is shown that $(pq)x \in Z(A)$ and $\lambda_{(pq)x} = \mathrm{id}_A$, for all $x \in X$. So, to summarize, there exists a positive integer, say d, such that $dx \in Z(A)$ and $\lambda_{dx} = \mathrm{id}_A$, for all $x \in X$.

Let $Y \in \mathcal{L}$, and let d be a positive integer (we choose $d \geq 2$) such that $dy \in Z(A)$ and $\lambda_{dy} = \mathrm{id}_A$, for all $y \in Y \subseteq X$. Define

$$a_Y = \sum_{y \in Y} dy \in A, \quad \text{and} \quad m_Y = (a_Y, \lambda_{a_Y}) = (a_Y, \mathrm{id}_A) \in M. \tag{4.11}$$

Note that a_Y is divisible by all elements of Y. However, it could be divisible by more than i generators, meaning that a_Y could belong to A_{i+1}, or equivalently $m_Y \in M_{i+1}$. In particular, $a_X \in Z(A)$, and $m_X \in Z(M)$. Also,

$$ka_Y = \sum_{y \in Y} kdy, \quad \text{and} \quad m_Y^k = (ka_Y, \mathrm{id}_A), \tag{4.12}$$

for any positive integer k.

Lemma 4.3.2. *Let $Y \in \mathcal{L}$. If $a_Y \in A_{i+1}$, then following properties hold.*

(1) $(M_{YY} \cup M_{i+1})/M_{i+1}$ is a nil subsemigroup of M/M_{i+1}.

(2) $(M_{*Y} \cup M_{i+1})/M_{i+1}$ is a nil left ideal of M/M_{i+1}.

(3) $(M_{Y*} \cup M_{i+1})/M_{i+1}$ is a nil right ideal of M/M_{i+1}.

Hence, in this case, $B_i := M_{i+1} \cup \bigcup_{Y : a_Y \in A_{i+1}} (M_{*Y} \cup M_{Y*})$ is an ideal of M, and B_i/M_{i+1} is in the nil radical of M/M_{i+1}.

Proof. (1) Let $(a, \lambda_a) \in M_{YY}$. Then, for any positive integer k,

$$(a, \lambda_a)^k = (a + \lambda_a(a) + \cdots + \lambda_a^{k-1}(a), \lambda_a^k).$$

Since $\lambda_a(Y) = Y$, it follows that $(a, \lambda_a)^k \in M_{YY} \cup M_{i+1}$. As each $\lambda_a^l(a)$ is divisible by all elements of Y, and because each element of A is normalizing, we obtain that $a + \lambda_a(a) + \cdots + \lambda_a^{k-1}(a)$ is divisible by a_Y for k large enough. It then follows that $(a, \lambda_a)^k \in m_Y M \subseteq M_{i+1}$. Hence, $(M_{YY} \cup M_{i+1})/M_{i+1}$ is nil. The first part then follows from Lemma 4.3.1(1).

(2) Let $Z \in \mathcal{L}$ and $(a, \lambda_a) \in M_{ZY}$. By the first part, we can assume that $Z \neq Y$. Since $\lambda_a(Y) = Z$ and $Z \neq Y$, we obtain that $\lambda_a(Z) \neq Z$. Therefore, $(a, \lambda_a)(a, \lambda_a) =$

$(a+\lambda_a(a), \lambda_a^2)$, and $a+\lambda_a(a)$ is divisible by all elements in $Z\cup\lambda_a(Z)$. As Z is properly contained in $Z\cup\lambda_a(Z)$, this yields $(a,\lambda_a)^2\in M_{i+1}$. By the first part and Lemma 4.3.1, we conclude that $(M_{*Y}\cup M_{i+1})/M_{i+1}$ is a nil left ideal of M/M_{i+1}.

(3) This is shown similar as (2).

Finally, we show that B_i is an ideal of M. By the previous parts, it is enough to prove that, for any $Y,Z\in\mathcal{L}$, with $a_Y\in A_{i+1}$, we get, for any $(a,\lambda_a)\in M_{ZY}$, $(b,\lambda_b)\in M_{YZ}$ and $(c,\lambda_c)\in M$, that both $(a,\lambda_a)(c,\lambda_c), (c,\lambda_c)(b,\lambda_b)\in B_i$. Consider first $(a,\lambda_a)(c,\lambda_c) = (a+\lambda_a(c), \lambda_a\lambda_c)$. Then, either $a+\lambda_a(c)$ is divisible exactly by the elements of Z or it is an element of A_{i+1}. Since $\lambda_a(Y)=Z$, the former means that c is only divisible by elements of Y (if not $\lambda_a(c)$ would be divisible by elements not in Z). Furthermore, there exists $U\in\mathcal{L}$, with $\lambda_c^{-1}\lambda_a^{-1}(Z)=\lambda_c^{-1}(Y)=U$. If $a_Y\in A_{i+1}$, then also $a_U=\lambda_c^{-1}(a_Y)\in A_{i+1}$. Hence, $(a,\lambda_a)(c,\lambda_c)\in M_{i+1}\cup M_{ZU}\subseteq B_i$. Next, consider $(c,\lambda_c)(b,\lambda_b)=(c+\lambda_c(b),\lambda_c\lambda_b)$. Then, either $c+\lambda_c(b)\in A_{i+1}$ or $c+\lambda_c(b)$ is divisible by exactly the elements $\lambda_c(Y)$. The latter means that $(c,\lambda_c)(b,\lambda_b)\in M_{\lambda_c(Y)Z}$, and since $a_Y\in A_{i+1}$, also $a_{\lambda_c(Y)}\in A_{i+1}$. We conclude that $(c,\lambda_c)(b,\lambda_b)\in B_i$. □

The previous result deals with M_{YY}, M_{*Y} and M_{Y*}, for $y\in\mathcal{L}$, in case $a_Y\in A_{i+1}$. The following lemma handles the case where $a_Y\notin A_{i+1}$, so when the generators of A dividing a_Y are precisely those that belong to Y.

Recall from Remark 1.3.2 and Section 2.2, that the left derived solution (X,s) of a bijective non-degenerate solution (X,r) is also bijective and non-degenerate, and is defined by $s(x,y)=(y,\lambda_y\rho_{\lambda_x^{-1}(y)}(x))=(y,\sigma_y(x))$, for all $x,y\in X$. Note that in $A=A(X,r)$, we get that $x+y=y+\sigma_y(x)$, for all $x,y\in X$.

Lemma 4.3.3. *Let $Y\in\mathcal{L}$, and assume that $a_Y\notin A_{i+1}$. Then, the following properties hold.*

(1) The derived solution $s:\{a_1,\dots,a_n\}^2\to\{a_1,\dots,a_n\}^2$ restricts to a finite bijective non-degenerate solution $s_Y:Y^2\to Y^2$.

(2) M_{YY} is a subsemigroup of M.

(3) There exists a positive integer t, so that for all $k\geq t$, $m_Y^kM_{YY}$ is a cancellative subsemigroup of M, and it is an ideal of M_{YY}. We call it a cancellative component of M.

(4) $M_{XX}=M_n$, and $G(X,r)$ is the group of fractions of $m_X^kM_{XX}$.

In particular, by (4.12), replacing if necessary d by a multiple, we may assume that m_YM_{YY} is cancellative, for all $Y\in\mathcal{L}$ with $a_Y\notin A_{i+1}$, and $G(X,r)$ is the group of fractions of m_XM_{XX}.

Proof. (1) Let $x,y\in Y$. To prove that s_Y is well-defined, we need to prove that $(y,\sigma_y(x))\in Y\times Y$, where $\sigma_y(x)=\lambda_y\rho_{\lambda_x^{-1}(y)}(x)$. Assume first that $x\neq y$. Then, $a_Y=dx+dy+b$ with $b=\sum_{x,y\neq z\in Y}dz$. Since $x+y=y+\sigma_y(x)$ in $A=A(X,r)$, for all $x,y\in X$, it follows that

$$a_Y=(d-1)x+x+y+(d-1)y+b=(d-1)x+y+\sigma_y(x)+(d-1)y+b,$$

and thus a_Y is divisible by $\sigma_y(x)$. On the other hand, if $x = y$, then $a_Y = dx + c$ with $c = \sum_{x \neq z \in Y} dz$. So, since by assumption $d \geq 2$, we can write

$$a_Y = (d-2)x + x + x + c = (d-2)x + x + \sigma_x(x) + c,$$

and thus a_Y is divisible by $\sigma_x(x) = \sigma_y(x)$ as well. The assumption $a_Y \notin A_{i+1}$ then yields that $y, \sigma_y(x) \in Y$. This proves the first part.

(2) By its definition, M_{YY} does not contain elements of M_{i+1} (as A_{YY} does not contain elements of A_{i+1}). From part (1) it follows that M_{YY} is multiplicatively closed. Indeed, take $(a, \lambda_a), (b, \lambda_b) \in M_{YY}$. Then, $(a, \lambda_a)(b, \lambda_b) = (a + \lambda_a(b), \lambda_a\lambda_b)$, and since $\lambda_a\lambda_b(Y) = Y$, we only need to prove that $a + \lambda_a(b) \in \langle Y \rangle \cap (A_i \smallsetminus A_{i+1})$. Since $\lambda_a(Y) = Y$, the element $\lambda_a(b)$ is the sum of elements in Y. Furthermore, by the first part, rewriting any two generators $x, y \in Y$ (in the sense of $x + y = y + \sigma_y(x)$) always gives two generators of Y, and never an element $z \in X \smallsetminus Y$. So, rewriting $a + \lambda_a(b)$ will always give a sum of elements in Y, and thus it is not divisible by an element $z \in X \smallsetminus Y$. As a is divisible by all elements of Y, we get indeed that $a + \lambda_a(b) \in \langle Y \rangle \cap (A_i \smallsetminus A_{i+1})$, as desired.

(3) By [97, Proposition 4.2], for any finite bijective non-degenerate solution (X, r) of the Yang-Baxter equation, there exists $t \geq 1$ such that, for any $k \geq t$, $m_X^k M$ is a cancellative ideal of M. By (1), we know that (Y, s_Y) is a finite bijective non-degenerate solution of the Yang-Baxter equation. Hence, the structure monoid of (Y, s_Y) has a cancellative ideal $ka_Y + A(Y, s_Y) = A(Y, s_Y) + ka_Y$ of $A(Y, s_Y)$, for some $t \geq 1$ and all $k \geq t$. This is equivalent with $m_Y^k M_{YY} = M_{YY} m_Y^k$ being a cancellative ideal of M. Indeed, both $m_Y^k(a, \lambda_a)$ and $(a, \lambda_a)m_Y^k$ are equal to $(ka_Y + a, \lambda_a)$, and thus $m_Y^k(a, \lambda_a) = m_Y^k(b, \lambda_b)$, as well as $(a, \lambda_a)m_Y^k = (b, \lambda_b)m_Y^k$, implies that $(a, \lambda_a) = (b, \lambda_b)$. As M_{YY} is a subsemigroup of M by (2), we get that $m_Y^k M_{YY} = M_{YY} m_Y^k$ is a cancellative semigroup of M and an ideal of M_{YY}, as desired.

(4) It is clear that $M_{XX} = M_n$. By part (3), there exists a positive integer t such that $S = m_X^k M_{XX}$, with $k \geq t$, is a cancellative subsemigroup of M. Recall that there exists a positive integer q such that $m^q = (a, \lambda_a)^q = (b, \mathrm{id}_A)$, for all $m \in M$, and $b \in Z(A)$ (see before Lemma 4.3.2). Hence, for any $a, b \in A$, the elements of the type $(a, \lambda_a)^q$ and $(b, \lambda_b)^q$ commute. Using that the solution (X, r) is finite, bijective, and non-degenerate, and that m_X is central in M, one can show that S satisfies the left and right Ore condition. So we can consider the group of quotients $G_{XX} = SS^{-1}$ of S. Since $m_X^k \in M_{XX}$ and $(a_X + a_j, \lambda_{a_j}) \in M_{XX}$ for each generator a_j of A, we get $m_X^{(k+1)} \in S$ and $m_X^{(k+1)} x_j = m_X^k(a_X + a_j, \lambda_{a_j}) \in S$. Hence, each element $(m_X^{(k+1)} x_j)(m_X^{(k+1)})^{-1}$ is in G_{XX}. Next, observe that the natural morphism $S \to G(X, r)$ is injective. Indeed, if $a, b \in S$ are equal in $G(X, r)$ then, by Remark 4.1.4, there exists $l \geq k+1$ such that $m_X^l a = m_X^l b$ in S. Since S is cancellative and $m_X^l \in S$, we get $a = b$. The embedding $S \to G(X, r)$ induces an embedding $G_{XX} \to G(X, r)$. If $\varphi : X \to G(X, r)$ is the natural map, then, because of the above, $\varphi(x_j)$ is in the image of the embedding $G_{XX} \to G(X, r)$, for all $x_j \in X$. As $G(X, r)$ is generated by all $\varphi(x_j)$, we conclude that $G_{XX} = G(X, r)$. □

Lemma 4.3.4. *Let $Y, Z, U, V \in \mathcal{L}$. If $Z \neq U$, then $M_{YZ} M_{UV} \subseteq M_{i+1}$.*

Proof. Let $Y, Z, U, V \in \mathcal{L}$, with $Z \neq U$. For any $(a, \lambda_a) \in M_{YZ}$ and $(b, \lambda_b) \in M_{UV}$, $(a, \lambda_a)(b, \lambda_b) = (a+\lambda_a(b), \lambda_a\lambda_b)$, and $a+\lambda_a(b)$ is divisible by all the elements of $Y \cup \lambda_a(U)$. Since $Z \neq U$ and $\lambda_a(Z) = Y$, it follows that $\lambda_a(U) \neq Y$. So, $a + \lambda_a(b)$ is divisible by at least $i + 1$ elements, and thus $(a, \lambda_a)(b, \lambda_b) \in M_{i+1}$. □

Define
$$\mathcal{L}_u = \{Y \in \mathcal{L} \mid a_Y \notin A_{i+1}\}.$$
By Lemma 4.3.3 and the proof of Lemma 4.3.2,
$$\mathcal{L}_u = \{Y \in \mathcal{L} \mid M_{YY} \text{ is a subsemigroup of } M\}.$$
We define a relation $\sim$ on $\mathcal{L}_u$ as follows. For $Y, Z \in \mathcal{L}_u$, put
$$Y \sim Z \text{ if and only if } M_{YZ} \neq \emptyset \text{ or } M_{ZY} \neq \emptyset.$$

Lemma 4.3.5. *With the above notations, let $Y, Z \in \mathcal{L}_u$. Then, $Y \sim Z$ if and only if both $M_{YZ} \neq \emptyset$ and $M_{ZY} \neq \emptyset$. Moreover, $\sim$ is an equivalence relation on $\mathcal{L}_u$.*

Proof. Let $Y, Z \in \mathcal{L}_u$ such that $Y \sim Z$. Assume that $M_{YZ} \neq \emptyset$, and take $(a, \lambda_a) \in M_{YZ}$. Since $a_Y \notin A_{i+1}$, there exists $b \in A_i \setminus A_{i+1}$ such that $(a + \lambda_a(b), \lambda_a\lambda_b) = (a, \lambda_a)(b, \lambda_b) = (ka_Y, \mathrm{id}_A)$, for some positive integer k. This yields $\lambda_b = \lambda_a^{-1}$, and thus $\lambda_b(Y) = Z$. Also, since $a_Y \notin A_{i+1}$, we get that $a_Y \in A_{YY}$. By Lemma 4.3.3, $(ka_Y, \mathrm{id}_A) \in M_{YY}$, so the generators that divide $\lambda_a(b)$ can only be elements of Y. Moreover, we can always choose b such that the generators of A that divide $\lambda_a(b)$ are precisely the elements of Y, by taking for example $b + \lambda_a^{-1}(a_Y)$ instead of b. Hence, the generators of A that divide b are precisely the elements of $\lambda_a^{-1}(Y) = Z$. It follows that $(b, \lambda_b) = (b, \lambda_a^{-1}) \in M_{ZY}$. Hence $M_{ZY} \neq \emptyset$. Completely analogous, one shows that for $Y, Z \in \mathcal{L}_u$ with $Y \sim Z$ and $M_{ZY} \neq \emptyset$, we have that $M_{YZ} \neq \emptyset$.

Moreover, it is easy to see that $\sim$ is reflexive as $(a_Y, \mathrm{id}_A) \in M_{YY}$ if $a_Y \notin A_{i+1}$. By the first part, it is also clear that $\sim$ is symmetric. To show that it is transitive, let $Y, Z, U \in \mathcal{L}_u$ with $Y \sim Z$ and $Z \sim U$. So, the sets $M_{YZ}, M_{ZY}, M_{ZU}, M_{UZ}$ are all non-empty. We claim that $M_{YZ}M_{ZU} \subseteq M_{YU}$, so that M_{YU} is non-empty. Let $(a, \lambda_a) \in M_{YZ}$ and $(b, \lambda_b) \in M_{ZU}$, and consider $(a, \lambda_a)(b, \lambda_b) = (a + \lambda_a(b), \lambda_a\lambda_b)$. As b is divisible by exactly the elements of Z, and λ_a is bijective mapping Z to Y, by Lemma 4.3.3, it follows that the generators of A that divide $a + \lambda_a(b)$ are precisely the elements of Y. Furthermore, $\lambda_a\lambda_b(U) = \lambda_a(Z) = Y$. Hence, $(a, \lambda_a)(b, \lambda_b) \in M_{YU}$, as desired. □

Using the previous results, we are able to create an ideal chain between M_{i+1} and M_i such that each Rees factor is either a power nilpotent semigroup or a uniform subsemigroup of a completely (θ)-simple inverse semigroup which has as maximal subgroups the groups of fractions of cancellative subsemigroups of M.

Proposition 4.3.6. *Denote by $\mathcal{L}_1, \ldots, \mathcal{L}_k$ the equivalence classes of $\sim$ on $\mathcal{L}_u$. For each $1 \leq j \leq k$, denote*
$$\mathcal{U}_{ij} = \bigcup_{Y,Z \in \mathcal{L}_j} M_{YZ}, \quad U_{ij} = \bigcup_{Y,Z \in \mathcal{L}_j} m_Y M_{YZ}, \quad U_i = \bigcup_{j=1}^{k} U_{ij}.$$

Then, the following properties hold.

(1) $(\mathcal{U}_{ij} \cup M_{i+1})/M_{i+1}$ *is a subsemigroup of* M_i/M_{i+1} *with* $M_{YZ}M_{ZV} \subseteq M_{YV}$ *and* $M_{YZ}M_{UV} \subseteq M_{i+1}$, *for all* $Y, Z, U, V \in \mathcal{L}_j$ *with* $U \neq Z$.

(2) $(U_{ij} \cup M_{i+1})/M_{i+1}$ *is an ideal of* M/M_{i+1} *contained in* $(\mathcal{U}_{ij} \cup M_{i+1})/M_{i+1}$, *and it is a uniform subsemigroup of a completely (0)-simple inverse semigroup with maximal subgroups isomorphic to the group of fractions of* $m_Y M_{YY}$, *for* $Y \in \mathcal{L}_j$. *For simplicity we denote the former as* U_{ij}^0 *and we call it a uniform component of* M *of degree* $|\mathcal{L}_j|$.

(3) $(\mathcal{U}_{ij} \cup M_{i+1})/M_{i+1}$ *does not contain a nil ideal.*

(4) $M_i/B_i = \bigcup_{j=1}^{k} (\mathcal{U}_{ij} \cup B_i)/B_i$, *a (0)-disjoint union, and* $U_i = \bigcup_{j=1}^{k} U_{ij}$ *is a (0)-disjoint union.*

(5) $B_i/M_{i+1} = \left(M_{i+1} \cup \bigcup_{Y : a_Y \in A_{i+1}} (M_{*Y} \cup M_{Y*}) \right) / M_{i+1}$ *is the nil radical of* M_i/M_{i+1}. *Furthermore, if* $a_Y \in A_{i+1}$ *and* $Z \in \mathcal{L}$ *with* $a_Z \notin A_{i+1}$, *then* $M_{YZ} = \varnothing$ *or* $M_{ZY} = \varnothing$.

(6) $M_i/(U_i \cup B_i)$ *is a nil semigroup.*

Hence, we have an ideal chain

$$M_{i+1} \subseteq B_i \subseteq U_{i1} \cup B_i \subseteq U_{i1} \cup U_{i2} \cup B_i \subseteq \cdots \subseteq U_{i1} \cup U_{i2} \cup \cdots \cup U_{ik} \cup B_i = U_i \cup B_i \subseteq M_i,$$

where the first and last Rees factor are (nil, and thus) power nilpotent semigroups, and all other Rees factors are uniform subsemigroups of a completely (0)-simple inverse semigroup with maximal subgroups the groups of fractions of cancellative subsemigroups of M.

Proof. (1) This follows from Lemma 4.3.4 and the proof of Lemma 4.3.5.

(2) To prove that $U_{ij}^0 = (U_{ij} \cup M_{i+1})/M_{i+1}$ is an ideal of M/M_{i+1}, take $m_Y(a, \lambda_a) = (a_Y + a, \lambda_a) \in m_Y M_{YZ}$, and $(b, \lambda_b) \in M$, for some $Y, Z \in \mathcal{L}_j$. Assume that $(a_Y + a, \lambda_a)(b, \lambda_b) = (a_Y + a + \lambda_a(b), \lambda_a\lambda_b)$ is not an element of M_{i+1}. Then, $\lambda_a(b)$ can only be divisible by elements of Y, and as $\lambda_a(Z) = Y$, it follows that b can only be divisible by elements of Z. Hence, $(a_Y + a, \lambda_a)(b, \lambda_b) \in m_Y M_{Y\lambda_b^{-1}(Z)} \subseteq U_{ij}$. On the other hand, if $(b, \lambda_b)(a_Y + a, \lambda_a) = (b + \lambda_b(a_Y) + \lambda_b(a), \lambda_b\lambda_a)$ is not an element of M_{i+1}, then $b + \lambda_b(a_Y) + \lambda_b(a) = b + a_{\lambda_b(Y)} + \lambda_b(a) = a_{\lambda_b(Y)} + b + \lambda_b(a)$ can only be divisible by elements of $\lambda_b(Y)$. Hence, $(b, \lambda_b)(a_Y + a, \lambda_a) \in m_{\lambda_b(Y)} M_{\lambda_b(Y)Z} \subseteq U_{ij}$. This proves that U_{ij}^0 is an ideal of M/M_{i+1} contained in $(\mathcal{U}_{ij} \cup M_{i+1})/M_{i+1}$. By Lemma 4.3.3, we know that its diagonal components, i.e. the subsemigroups $m_Y M_{YY}$ of M are cancellative, with $Y \in \mathcal{L}_j$.

Applying part (4) of Lemma 4.3.3 on each (Y, s_Y), $Y \in \mathcal{L}_j$, it follows that each diagonal component $m_Y M_{YY}$ has a group of fractions, denoted G_{YY}. For any $Y, Z \in \mathcal{L}_j$, we get that $G_{YY} \cong G_{ZZ}$. It is then readily verified that U_{ij}^0 is uniform in the completely (θ)-simple inverse semigroup $\mathcal{M}^0(G_{YY}, d_j, d_j, I_j)$, where $d_j = |\mathcal{L}_j|$ and I_j is the identity matrix of degree d_j. We can present this idea as follows. The sets M_{YZ}, for $Y, Z \in \mathcal{L}_j$ represent the $\mathcal{H}$-classes in the completely (θ)-simple inverse semigroup $\mathcal{M}^0(G_{YY}, d_j, d_j, I_j)$ as follows. If $\mathcal{L}_j = \{Y_1, \dots, Y_{d_j}\}$, then we get

$$\begin{array}{|c|c|c|c|}
\hline
M_{Y_1Y_1} & M_{Y_1Y_2} & \dots & M_{Y_1Y_{d_j}} \\
\hline
M_{Y_2Y_1} & M_{Y_2Y_2} & \dots & M_{Y_2Y_{d_j}} \\
\hline
\vdots & \vdots & \ddots & \vdots \\
\hline
M_{Y_{d_j}Y_1} & M_{Y_{d_j}Y_2} & \dots & M_{Y_{d_j}Y_{d_j}} \\
\hline
\end{array},$$

where the multiplication of elements in M_{YZ} and M_{UV} is given by the multiplication in the semigroup $\mathcal{M}^0(G_{YY}, d_j, d_j, I_j)$. If the multiplication in the latter is equal to the zero element θ, it means that it is an element of M_{i+1}.

(3) By Lemma 4.3.3, each M_{YY} is a subsemigroup of M. In particular, it does not contain a nil ideal, nor does it contain nilpotent elements. Assume that I is a nil ideal of $(\mathcal{U}_{ij} \cup M_{i+1})/M_{i+1}$, and $\theta \neq a \in M_{YZ}$ is in I, for some $Y, Z \in \mathcal{L}_j$. By Lemma 4.3.5, $M_{ZY} \neq \varnothing$, so $\theta \neq ab \in I$, for some $b \in M_{ZY}$. Hence, $0 \neq ab \in M_{YY}$ is nilpotent, a contradiction.

(4) That $M_i/B_i = \bigcup\limits_{j=1}^{k} (\mathcal{U}_{ij} \cup B_i)/B_i$ is clear since any nonzero element $m = (a, \lambda_a) \in M_i/B_i$ is an element of M_{YZ}, for some $Y \subseteq X$ with $|Y| = i$ and $Z = \lambda_a^{-1}(Y)$. As $m \notin B_i$, it follows that $a_Y \notin A_{i+1}$, and thus $Y \in \mathcal{L}_j$, for some $1 \leq j \leq k$ and $m \in \mathcal{U}_{ij}$. That the union is (θ)-disjoint follows because $\mathcal{L}_1, \dots, \mathcal{L}_k$ are the equivalence classes of $\sim$ on $\mathcal{L}_u$. By part (2), it follows that $U_i = \bigcup_{j=1}^{k} U_{ij}$ is a (θ)-disjoint union.

(5) By Lemma 4.3.2, B_i/M_{i+1} is in the nil radical of M/M_{i+1} (and thus also of M_i/M_{i+1}). Moreover, parts (2) and (3) yield that the nil radical of M_i/M_{i+1} does not intersect with any of the uniform components U_{ij}^0. Hence, by part (4), B_i/M_{i+1} is the nil radical of M_i/M_{i+1}. To prove the second statement of (5), let $Z, Y \in \mathcal{L}$ with $a_Y \in A_{i+1}$ and $a_Z \notin A_{i+1}$. Suppose that $M_{YZ} \neq \varnothing$ and $M_{ZY} \neq \varnothing$. Then, $M_{ZY}M_{YZ} \subseteq M_{ZZ}$. So, $M_{ZZ} \neq \varnothing$. By definition of B_i (see Lemma 4.3.2 and (4.10)), $M_{YZ} \subseteq B_i$, and because B_i is an ideal, it follows that $\varnothing \neq M_{ZY}M_{YZ} \subseteq B_i$. So there exists $m \in M_{ZZ}$ that is an element of B_i, a contradiction.

(6) Let $m = (a, \lambda_a) \in M_i \smallsetminus (U_i \cup B_i)$. So, there exists $Y \in \mathcal{L}$ such that a is divisible by (at least) all elements of Y. However, $M_{i+1} \subseteq B_i$, so a is only divisible by the elements of Y. Furthermore, if $\lambda_a^{-1}(Y) \neq Y$, then $m^2 \in M_{i+1} \subseteq B_i$. So, we can assume that $a \in A_{YY}$. If $a_Y \in A_{i+1}$, then by definition of B_i, $m \in B_i$, a contradiction. If not, i.e. $a_Y \notin A_{i+1}$, then there exists a positive integer k, such that $m^k \in m_Y M_{YY} \subseteq U_i$. Hence, the result follows. □

The previous construction of the ideal chain $M_{i+1} \subseteq B_i \subseteq U_i \subseteq M_i$ allows us to determine when $M = M(X, r)$ is Malcev nilpotent. In [104], given an ideal chain $S_1 \subseteq S_2 \subseteq \dots \subseteq S_n = S$ of a semigroup S, with all Rees factors either a union of power nilpotent ideals of bounded nilpotency exponent or uniform with linear cancellative components, an exact characterization of Malcev nilpotency of S is given by properties of the uniform components.

Theorem 4.3.7. *Let (X,r) be a finite bijective non-degenerate set-theoretic solution of the Yang-Baxter equation, and put $n = |X|$. Then, the structure monoid $M = M(X,r)$ is Malcev nilpotent if and only if all cancellative subsemigroups of M (actually it is sufficient that all cancellative components $m_Y M_{YY}$ with $m_Y \notin M_{|Y|+1}$) are Malcev nilpotent and the following condition, called the nilpotency condition, is not satisfied:*

$$\begin{array}{c}\text{there exist subsets } Y \neq Z \text{ of } \{a_1,\dots,a_n\}, \text{ the generators of } A(X,r),\\ \text{with } a_Y \text{ and } a_Z \text{ only divisible by elements of } Y, \text{ respectively } Z, \text{ and}\\ a,b \in \langle Y \cap Z\rangle \text{ such that } \lambda_b(\lambda_a^{-1}(Y)) = Z \text{ and } \lambda_b(\lambda_a^{-1}(Z)) = Y.\end{array} \tag{NC}$$

Proof. By [104, Theorem 11] and the constructed ideal chain of M in Proposition 4.3.6, M is Malcev nilpotent if and only if all cancellative components $m_Y M_{YY}$ of M are Malcev nilpotent and two-by-two orthogonal, and if, furthermore, there does not exist a subset $F = \{f_1, f_1', f_2, f_2'\}$ in a uniform component of M_i/M_{i+1}, say U_{ij}^0, satisfying that every element of F belongs to a cancellative component $m_Y M_{YY}$ with $Y \in \mathcal{L}_j$, f_k and f_k' do not belong to the same cancellative component for $k = 1,2$, and finally, there exist elements $u_1, u_2 \in M$ such that the elements $f_2u_1f_1$, $f_2'u_2f_1$, $f_2'u_1f_1'$, and $f_2u_2f_1'$ are all nonzero in U_{ij}^0. Note that by Lemma 4.3.3, all cancellative subsemigroups of M are Malcev nilpotent if all $m_Y M_{YY}$ with $m_Y \notin M_{|Y|+1}$ are Malcev nilpotent. Furthermore, by Lemma 4.3.4, all cancellative components are orthogonal.

So, to prove the result, it is sufficient to prove that condition (NC) can be translated into the existence of such a subset $F = \{f_1, f_1', f_2, f_2'\}$ described above. By Lemma 4.3.3, M_{YY} is a subsemigroup of M, so for any $m_Y(a,\lambda_a) \in m_Y M_{YY}$, and some positive integer t, we have that $m_Y(a,\lambda_a)^t = m_Y(a', \mathrm{id}_A) \in m_Y M_{YY}$. Thus, without loss of generality, we may assume that each f_1, f_1', f_2, f_2' has the permutation coordinate equal to the identity. Indeed, the replaced element of F remains in the same cancellative component, and if, for $f \in F, u \in M$, $fum_Y(a,\lambda_a)^t$ (resp. $m_Y(a,\lambda_a)^t uf$) is nonzero, then also $fum_Y(a,\lambda_a)$ (resp. $m_Y(a,\lambda_a)uf$) is nonzero. With the assumption that f_k and f_k' do not belong to the same cancellative component, for $k = 1,2$, there exist distinct subsets of $\{a_1,\dots,a_n\}$, say $Y, Z \in \mathcal{L}_j$, with $f_2 \in m_Y M_{YY}$ and $f_2' \in m_Z M_{ZZ}$. Similarly, $f_1 \in m_V M_{VV}$ and $f_1' \in m_W M_{WW}$, for some distinct elements $V, W \in \mathcal{L}_j$. So, $m_Y, m_Z, m_V, m_W \notin M_{i+1}$.

Assume there exist elements $u_1 = (a,\lambda_a)$ and $u_2 = (b,\lambda_b)$ in M with $f_2u_1f_1$, $f_2'u_2f_1$, $f_2'u_1f_1'$, and $f_2u_2f_1'$ all nonzero in U_{ij}^0. As $f_2u_1f_1 \notin M_{i+1}$ and $f_2u_1f_1 \in M_{YV}$, we get that a can only be divisible by elements of Y and $\lambda_a(V) = Y$. Similarly, since $f_2'u_1f_1' \notin M_{i+1}$ and $f_2'u_1f_1' \in M_{ZW}$, we also get that a can only be divisible by elements of Z and $\lambda_a(W) = Z$. Hence, a can only be divisible by elements of $Y \cap Z$ and $a \in \langle Y \cap Z\rangle$. In the same way, conditions $f_2'u_2f_1 \notin M_{i+1}$ and $f_2u_2f_1' \notin M_{i+1}$ imply that $b \in \langle Y \cap Z\rangle$, $\lambda_b(V) = Z$ and $\lambda_b(W) = Y$. Thus, condition (NC) follows.

By Lemma 4.3.3 and Proposition 4.3.6, it easily is verified that condition (NC) implies the existence of F satisfying the required conditions. Indeed, assume, $Y, Z \in \mathcal{L}_j$ and $a, b \in \langle Y \cap Z\rangle$ satisfy the assumptions of (NC). Define $u_1 = (a,\lambda_a), u_2 = (b,\lambda_b) \in M$, and take $f_2 \in m_Y M_{YY}$ and $f_2' \in m_Z M_{ZZ}$. Put $V = \lambda_a^{-1}(Y)$ and $W = \lambda_a^{-1}(Z)$. Then, $(a_Y + a, \lambda_a) \in M_{YV}, (a_Z + a, \lambda_a) \in M_{ZW}$, and thus $Y \sim V, Z \sim W$, and $V, W \in \mathcal{L}_j$. By taking $f_1 \in m_V M_{VV}$ and $f_1' \in m_W M_{WW}$, the subset $F = \{f_1, f_1', f_2, f_2'\}$ satisfies the conditions from above. □

We provide a first example of a solution that satisfies condition (NC). Let $A = (\mathbb{Z}/2\mathbb{Z})^4$ and $C = (\mathbb{Z}/2\mathbb{Z})^2$ be trivial left braces, and $\alpha : C \to \operatorname{Aut}(A)$ a group homomorphism satisfying

$$\alpha(1,0)(a_1,a_2,a_3,a_4) = (a_2,a_1,a_3,a_4),$$
$$\alpha(0,1)(a_1,a_2,a_3,a_4) = (a_1,a_2,a_4,a_3),$$

for all $a_1,a_2,a_3,a_4 \in \mathbb{Z}/2\mathbb{Z}$. Let $B = A \rtimes_\alpha C$ be the semidirect product of the trivial braces A and C via α (see [165]). Then, B is a left brace with addition defined componentwise and multiplication defined using α, i.e.

$$(a,c) + (a',c') = (a+a', c+c'),$$
$$(a,c) \circ (a',c') = (a + \alpha(c)(a'), c+c'),$$

for all $a, a' \in A$ and $c, c' \in C$. Let e_1, e_2, e_3, e_4 be the standard basis of A as a $(\mathbb{Z}/2\mathbb{Z})$-vector space. Consider the finite non-degenerate involutive solution (B, r_B) associated to the left brace B (see Subsection 1.3.1), and the following subsets of the left derived structure monoid $A(B, r_B)$,

$$Y = \{(e_1,(0,0)),(e_3,(0,0)),(0,(1,0)),(0,(0,1))\}$$

and

$$Z = \{(e_2,(0,0)),(e_4,(0,0)),(0,(1,0)),(0,(0,1))\}.$$

Since $A(B, r_B)$ is the free abelian monoid with basis B, it is clear that the elements a_Y and a_Z are only divisible by elements of Y, respectively Z. Let $a = (0,(1,0))$ and $b = (0,(0,1))$ be two elements of $Y \cap Z$. Note that

$$\lambda_b(\lambda_a^{-1}(Y)) = Z \quad \text{and} \quad \lambda_b(\lambda_a^{-1}(Z)) = Y.$$

Hence, condition (NC) is satisfied.

Corollary 4.3.8. *Let (X, r) be a finite bijective non-degenerate set-theoretic solution of the Yang-Baxter equation. If the group $\mathcal{G}_\lambda(X,r) = \operatorname{gr}(\lambda_x \mid x \in X)$ is of odd order or if the uniform components of $M = M(X,r)$ have degree one, then the structure monoid M is Malcev nilpotent if and only if all cancellative subsemigroups of M (actually it is sufficient that all cancellative components $m_Y M_{YY}$ with $m_Y \notin M_{|Y|+1}$) are Malcev nilpotent.*

Proof. If all uniform components are of degree one, then each equivalence class $\mathcal{L}_j$ contains only one element. So, condition (NC) is not satisfied, as no distinct Y and Z exist.

If $\mathcal{G}_\lambda(X,r)$ is of odd order, with notations as in condition (NC), put $f = \lambda_b\lambda_a^{-1}$. Then, $f(Y) = Z$ and $f(Z) = Y$. So, $f^2(Y) = Y$. Since, by assumption, f has odd order, we get that $f(Y) = Y$. Hence, $Y = Z$, and condition (NC) is trivially not satisfied.

The result now follows from Theorem 4.3.7. □

In case the group $\mathrm{gr}(\lambda_x \mid x \in X)$ has even order, the result of Corollary 4.3.8 does not hold in general. We provide an example of a structure monoid that is not Malcev nilpotent, but has abelian cancellative components.

Example 4.3.9. *Let $X = \{1,2,3,4\}$. Define $\lambda_1 = \lambda_2 = \rho_1 = (3,4)$, $\lambda_3 = (2,4), \lambda_4 = (2,3)$ and $\rho_2 = \rho_3 = \rho_4 = \mathrm{id}_X$. Then, (X,r), with r defined by $r(x,y) = (\lambda_x(y), \rho_y(x))$, for all $x,y \in X$, is a finite bijective non-degenerate solution of the Yang-Baxter equation. Furthermore, the associated structure monoid*

$$\begin{aligned} M = M(X,r) = \langle X \mid\, & 1\circ 2 = 2\circ 1,\ 1\circ 3 = 4\circ 1,\ 1\circ 4 = 3\circ 1, \\ & 2\circ 3 = 4\circ 2 = 2\circ 4 = 3\circ 2 = 4\circ 3 = 3\circ 4\rangle^1, \end{aligned}$$

is not abelian. However, the structure group

$$G(X,r) \cong \mathrm{gr}(1,2 \mid 1\circ 2 = 2\circ 1),$$

is abelian. The derived structure monoid is

$$\begin{aligned} A = A(X,r) = \langle X \mid\, & 1+2 = 2+1,\ 1+3 = 3+1,\ 1+4 = 4+1, \\ & 2+4 = 4+2 = 2+3 = 3+4 = 4+3 = 3+2\rangle^1. \end{aligned}$$

Since A is abelian, we may put $d = 2$ in (4.11). Put $Y = \{1,3\}$ and $Z = \{1,4\}$. Then,

$$\begin{aligned} a_Y &= 1+1+3+3 \in A_2 \setminus A_3, & m_Y &= 1\circ 1\circ 3\circ 3 \in M_2 \setminus M_3, \\ a_Z &= 1+1+4+4 \in A_2 \setminus A_3, & m_Z &= 1\circ 1\circ 4\circ 4 \in M_2 \setminus M_3. \end{aligned}$$

We obtain the following non-empty components

$$\begin{aligned} M_{YY} &= \{(a,\lambda_a) \mid a \in 1+1+3+\langle 1+1,3\rangle^1\}, \\ M_{YZ} &= \{(a,\lambda_a) \mid a \in 1+3+\langle 1+1,3\rangle^1\}, \\ M_{ZY} &= \{(a,\lambda_a) \mid a \in 1+4+\langle 1+1,4\rangle^1\}, \\ M_{ZZ} &= \{(a,\lambda_a) \mid a \in 1+1+4+\langle 1+1,4\rangle^1\}. \end{aligned}$$

Let $a = 1 \in \langle Y \cap Z\rangle$ and $b = 1+1 \in \langle Y \cap Z\rangle$. Then, $\lambda_{1+1}\lambda_1^{-1}(Y) = \lambda_1(Y) = Z$ and $\lambda_{1+1}\lambda_1^{-1}(Z) = \lambda_1(Z) = Y$. Hence, condition (NC) is satisfied. Note that M_{YY} and M_{ZZ} are abelian. Let us consider all other non-empty subsemigroups M_{TT} with $|T| < 4$. If $|T| = 1$, then these are $\langle a\rangle^e$, with $a \in X = \{1,2,3,4\}$, and clearly M_{TT} is abelian. If $|T| = 2$, then the only remaining case is $T = \{1,2\}$ and $M_{TT} = \langle 1,2\rangle^e$, an abelian semigroup. In case $|T| = 3$, there is only one such set with $M_{TT} \neq \varnothing$, namely $T = \{2,3,4\}$. Clearly $(T, r|_{T^2})$ is a subsolution of (X,r). Hence, M_{TT} has an ideal that is cancellative and *that has the structure group $G(T, r|_{T^2})$ as its group of fractions. It readily is verified that this group is free abelian of rank* 1*. Hence, all cancellative components of M are abelian (and thus Malcev nilpotent) and condition* (NC) *is satisfied. By Theorem 4.3.7, M is not Malcev nilpotent.*

Theorem 4.3.7 easily can be applied on examples. We illustrate this via the following example of a Malcev nilpotent structure monoid with all cancellative components contained in an abelian group.

Example 4.3.10 (Smoktunowicz and Vendramin [173, Example 4.4])**.** *Consider $X = \{1,2,3,4\}$, $f = (1,2)$ and $g = (3,4)$. Then, (X,r), with $r(x,y) = (f(y), g(x))$, for all $x, y \in X$, is a finite bijective non-degenerate solution of the Yang-Baxter equation of order* 4*. In its structure group we have $1 \circ 2 = 1 \circ 1$ and $3 \circ 4 = 4 \circ 4$. So $G(X,r) = \operatorname{gr}(1,3)$ and the only relation is $1 \circ 3 = 3 \circ 1$. Hence, $G(X,r)$ is the free abelian group of rank* 2*, and is thus nilpotent. Therefore, $m_X M_{XX}$ has a free abelian group of rank two as group of fractions. Now,*

$$\begin{aligned} A(X,r) &= \langle X \mid x + y = y + f(g(x)), \text{ for all } x,y \in X\rangle^1 \\ &= \langle X \mid 1 + x = x + 2,\ 2 + x = x + 1, \\ &\qquad 3 + x = x + 4,\ 4 + x = x + 3, \text{ for all } x \in X\rangle^1. \end{aligned}$$

It is easy to see that

$$A(X,r) = \langle 1,2 \mid 1+1 = 1+2 = 2+2 = 2+1\rangle^1 + \langle 3,4 \mid 3+3 = 3+4 = 4+4 = 4+3\rangle^1,$$

and we have the extra relations

$$1+3 = 3+2 = 2+4 = 4+1 \quad \text{and} \quad 1+4 = 4+2 = 2+3 = 3+1.$$

Notice that all the latter words are in A_4. Let $Y = \{1,2\}$ and $Z = \{3,4\}$. Then,

$$\begin{aligned} A_{YY} &= (A_2 \setminus A_3) \cap \langle 1,2\rangle^1 = 1 + 1 + \langle 1\rangle^1, \\ A_{ZZ} &= (A_2 \setminus A_3) \cap \langle 3,4\rangle^1 = 3 + 3 + \langle 3\rangle^1, \end{aligned}$$

both semigroups are cancellative and commutative. Furthermore, for d large enough in (4.12)*, $m_Y M_{YY} = (a_Y + A_{YY})^e = \{(a, \lambda_a) \mid a \in a_Y + A_{YY}\}$ is abelian and cancellative since both $\lambda_a = \mathrm{id}_A$ and $\lambda_a = f = (1,2)$ act as the identity map on a_Y and A_{YY}. Similarly, $m_Z M_{ZZ}$ is abelian and cancellative. Note that both M_{YZ} and M_{ZY} are empty. Also $A_2 \setminus A_3 = (1+1+\langle 1\rangle^1) \cup (3+3+\langle 3\rangle^1)$, is a disjoint union of abelian cancellative semigroups that are orthogonal modulo A_3. Moreover, $A_1 \setminus A_2 = X$ (and thus $M_1^2 \subseteq M_2$), $A_3 = A_4$ and, as said above, $m_X M_{XX}$ is abelian and cancellative. Hence, all uniform components are of degree* 1 *and all cancellative components are abelian. It follows from Corollary 4.3.8 that $M(X,r)$ is Malvec nilpotent.*

Note that the previous example is a solution of Lyubashenko type (see Section 1.3). We will now handle all finite bijective non-degenerate solutions of Lyubashenko type. We check when the necessary and sufficient conditions of Theorem 4.3.7 are satisfied, and determine when exactly its structure monoid is Malcev nilpotent.

Proposition 4.3.11. *Let (X,r) be a finite bijective non-degenerate Lyubashenko solution defined by $r(x,y)=(f(y),g(x))$, for all $x,y\in X$, and some commuting permutations f and g on X. Then, the structure monoid $M(X,r)$ is Malcev nilpotent if and only if $f=c_1^{k_1}\cdots c_t^{k_t}$ and $g=c_1^{1-k_1}\cdots c_t^{1-k_t}$, where $c_1,\dots,c_t$ are disjoint cycles. In this case, all cancellative components are abelian and their group of fractions is of rank $1\le j\le t$, and all such numbers j can be reached. Furthermore, all uniform components have degree one.*

Proof. For convenience we denote the solution r by $r(x,y)=(f(y),f^{-1}\gamma(x))$, where $\gamma=fg\in \operatorname{Sym}(X)$. Note that $s(x,y)=(y,\gamma(x))$, for all $x,y\in X$. Denote the disjoint cycle decomposition of γ by $\gamma=c_1\cdots c_t$, and the content of the cycle c_i will be denoted by X_i, a subset of X. So $X=X_1\cup\cdots\cup X_t$ is a disjoint union of non-empty sets. Note that X_i is a singleton if $c_i=(x)$, for some $x\in X$.

First, we determine the cancellative components of $M=M(X,r)$. We start with m_XM_{XX}. By Lemma 4.3.3, its group of fractions is the structure group $G=G(X,r)$. Moreover, G is the structure group of the injectivization of (X,r) (see Section 2.1), i.e. $G=G(\iota(X),r_{\iota(X)})$, where $\iota:X\to G$ is the natural mapping and $r_{\iota(X)}=r_G|_{\iota(X)^2}$. Clearly, $r(x,f^{-1}(x))=(x,f^{-1}\gamma(x))$. Hence, we have $f^{-1}\gamma(x)=f^{-1}(x)$ in G, for all $x\in X$, and thus, in G, γ is the identity on $\iota(X)$. Therefore, in G, all elements in the content of c_i, i.e. all elements of X_i, for all $1\le i\le t$, are identified in G. So, $x\circ y=f(y)\circ f^{-1}(x)$. Also, $(\iota(X),r_{\iota(X)})$ is an involutive solution of the Yang-Baxter equation. Indeed, $r_{\iota(X)}(x,y)=(f(y),f^{-1}(x))$ is a Lyubashenko solution with $ff^{-1}=\mathrm{id}_X$, so it is involutive (see Section 2.1). Moreover, the associated monoid $A(\iota(X),r_{\iota(X)})$ is the free abelian monoid on t generators (the number of cycles of γ). Assume now that M is Malcev nilpotent, and thus also m_XM_{XX} is Malcev nilpotent and G is nilpotent. Lemma 4.2.3 yields that G (and thus also m_XM_{XX}) is abelian. If G is abelian, we need that f is the identity when acting on $\iota(X)$. Therefore, on X, f permutes the contents of each c_i, i.e. $f(X_i)=X_i$. Now, since (X,r) is a solution, f and γ commute. Thus, if $c_1=(x_1,\dots,x_k)$ and $X_1=\{x_1,\dots,x_k\}$, then

$$\gamma=f\gamma f^{-1}=(f(x_1),\dots,f(x_k))(fc_2f^{-1})\cdots(fc_tf^{-1}),$$

because $fc_1f^{-1}(f(x_1))=fc_1(x_1)=f(x_2)$ etc., and thus $(f(x_1),\dots,f(x_k))=c_1$. By doing the same for the other cycles, we obtain non-negative integers $k_1,\dots,k_s$ such that $f=c_1^{k_1}\cdots c_t^{k_t}$. Since $\gamma=c_1\cdots c_t$, it follows that $g=c_1^{1-k_1}\cdots c_t^{1-k_t}$. Conversely, if f,g, and thus also γ are of this type, then both γ and f act as the identity map on $\iota(X)$, and the relations in G become $x\circ y=f(y)\circ f^{-1}(x)=y\circ x$, for all $x,y\in\iota(X)$. So, G (and thus also m_XM_{XX}) is abelian.

Now, consider other possible cancellative components, using the description of the mapping f and g. By Lemma 4.3.3 and Lemma 4.3.4, such a component is determined by a subset Y of X, say of cardinality i, with $m_Y\in M_i\setminus M_{i+1}$. In particular, s_Y is a subsolution of s, with $s(x,y)=(y,\gamma(x))$, for all $x,y\in X$. It follows that Y is the union of the contents of some cycles of γ, i.e. the union of some X_j, say $Y=X_{i_1}\cup\cdots\cup X_{i_l}$. Because of the description of $f=c_1^{k_1}\cdots c_t^{k_t}$ and $\gamma=c_1\cdots c_t$ this means that r_Y is a subsolution of r.

Hence, as for the previous case on the entire set X, $m_Y M_{YY}$ has a group of fractions $G(Y, r_Y)$ and this (and thus also $m_Y M_{YY}$) must be abelian as both f and γ act as the identity map on $\iota(Y)$. Conversely, if M is Malcev nilpotent, and thus also $m_Y M_{YY}$ is Malcev nilpotent, then $G(Y, r_Y)$ is nilpotent and abelian, by Lemma 4.2.3, and we get that f, g and γ can be described in this way.

Hence, we have proven that if M is Malcev nilpotent then both $\gamma = c_1 \cdots c_t$ and $f = c_1^{k_1} \cdots c_t^{k_t}$, and thus $g = c_1^{1-k_1} \cdots c_t^{1-k_t}$. Conversely, for such permutations we have that all cancellative components are abelian.

It remains to verify that condition (NC) does not hold. Let Y be a subset of X as above. Then, for any $m = (a, \lambda_a) \in M$, we have $\lambda_a(Y) = f^{\text{length}(a)}(Y) = Y$. Hence, Y is invariant with respect to the action of the group $\operatorname{gr}(\lambda_x \mid x \in X) = \operatorname{gr}(f)$. So, if $a \in \langle Y \rangle \cap (A_i \setminus A_{i+1})$, then $m = (a, \lambda_a) \in M_{YY}$. In particular, if $Y \sim Z$, then M_{YZ} is non-empty by Lemma 4.3.5, and thus $Y = Z$. Hence, all uniform components have degree 1 and the result follows from Corollary 4.3.8. □

We end this section providing some examples. The first example is a solution (X, r), with abelian structure group $G(X, r)$. However, the left derived structure group $A_{\text{gr}}(X, r)$ is not nilpotent. The structure monoid $M(X, r)$ is not abelian, but it is Malcev nilpotent and it has a uniform component of degree two.

Example 4.3.12. *Let $X = \mathbb{Z}/3\mathbb{Z}$. Then, (X, r), defined by $r(x, y) = (-y, x - y)$, for all $x, y \in X$, is a finite bijective non-degenerate set-theoretic solution of the Yang-Baxter equation, with $\lambda_0 = \lambda_1 = \lambda_2 = (1, 2)$, $\rho_0 = \mathrm{id}_X$, $\rho_1 = (0, 2, 1)$ and $\rho_2 = (0, 1, 2)$. Its structure group*

$$G = G(X, r) = \operatorname{gr}(0, 1, 2 \mid 0 \circ 1 = 2 \circ 2 = 1 \circ 0, 0 \circ 2 = 1 \circ 1 = 2 \circ 0),$$

is an abelian group. Indeed, $0 \circ 1 = 2 \circ 2$ implies $2 \circ 0 \circ 1 = 2 \circ 2 \circ 2$, and thus $1 \circ 2 \circ 0 = 1 \circ 1 \circ 1 = 2 \circ 0 \circ 1 = 2 \circ 2 \circ 2 = 2 \circ 1 \circ 0$, so that $1 \circ 2 = 2 \circ 1$. The associated left derived solution is defined by $s(x, y) = (y, -x - y)$, for all $x, y \in X$, and the left derived structure group is

$$\begin{aligned} A_{\text{gr}} = A_{\text{gr}}(X, r) &= \operatorname{gr}(0, 1, 2 \mid 0 + 2 = 2 + 1 = 1 + 0,\ 0 + 1 = 1 + 2 = 2 + 0) \\ &\cong \operatorname{gr}(a, b \mid a + b + a = b + a + b,\ a + b - a = b + a - b,\ 2a + b = b + 2a). \end{aligned}$$

Clearly, $A_{\text{gr}} / \operatorname{gr}(2a, 2b) \cong \operatorname{gr}(a, b \mid 2a = 2b = 3(a + b) = 0) \cong S_3$, and thus A_{gr} is not nilpotent. We can take $d = 2$ in (4.11). We get that

$$\begin{aligned} &A_1 \setminus A_2 = (0 + \langle 0 \rangle^1) \cup (1 + \langle 1 \rangle^1) \cup (2 + \langle 2 \rangle^1), \\ &A_2 \setminus A_3 = \varnothing. \end{aligned}$$

So, we only look at $\mathcal{L} = \{Y \subseteq \{0, 1, 2\} \mid |Y| = i\}$, with $i = 1$. Indeed, for $i = 2$, all M_{YY} with $Y \in \mathcal{L}$ are empty. For $i = 3$, $m_X M_{XX}$ is an abelian cancellative component since G is abelian. Put $i = 1$. Then, $\mathcal{L} = \mathcal{L}_1 \cup \mathcal{L}_2$, where $\mathcal{L}_1 = \{\{0\}\}$ and $\mathcal{L}_2 = \{\{1\}, \{2\}\}$. So, we obtain a uniform component of degree one, and a uniform component of degree two.

Indeed, let $Y = \{1\}$ and $Z = \{2\}$. Then,

$$\begin{aligned}
&a_Y = 1+1, \quad m_Y = (1,\lambda_1)(2,\lambda_2),\\
&a_Z = 2+2, \quad m_Z = (2,\lambda_2)(1,\lambda_1),\\
&M_{YY} = \{(a,\lambda_a) \mid a \in 1+1+\langle 1+1\rangle^1\},\\
&M_{ZZ} = \{(a,\lambda_a) \mid a \in 2+2+\langle 2+2\rangle^1\},\\
&M_{YZ} = \{(a,\lambda_a) \mid a \in 1+\langle 1+1\rangle^1\},\\
&M_{ZY} = \{(a,\lambda_a) \mid a \in 2+\langle 2+2\rangle^1\},
\end{aligned}$$

and the cancellative components $m_Y M_{YY}$ and $m_Z M_{ZZ}$ are abelian, and thus Malcev nilpotent. Since $Y \cap Z$ is empty, and $A_2 \setminus A_3 = \varnothing$, we conclude that condition (NC) is not satisfied. By Theorem 4.3.7, $M(X,r)$ is Malcev nilpotent.

The following example is a finite bijective non-degenerate solution (X,r) with a structure group that is not nilpotent, as it has S_3 as an epimorphic image. Therefore, the cancellative component $m_X M_{XX}$ is not Malcev nilpotent. Hence, the structure monoid itself is not Malcev nilpotent.

Example 4.3.13. *Let $X = S_3$. Then, (X,r), defined by $r(x,y) = (xy^{-1}x^{-1}, xy^2)$, for all $x,y \in X$, is a finite bijective non-degenerate solution of the Yang-Baxter equation. Its structure group $G(X,r)$ has $X = S_3$ as an epimorphic image, and hence it is not nilpotent. By Theorem 4.3.7, $M(X,r)$ is not Malcev nilpotent.*

The final example is a bijective non-degenerate solution (X,r) with abelian structure group. Its structure monoid looks very similar to the one of Example 4.3.9. In contrast to Example 4.3.9, we show that not all cancellative components of $M(X,r)$ are Malcev nilpotent semigroups. Furthermore, condition (NC) holds.

Example 4.3.14. *Let $X = \{1,2,3,4\}$. Define $\lambda_1 = \lambda_2 = \rho_1 = (3,4)$ and $\lambda_3 = \lambda_4 = \rho_2 = \rho_3 = \rho_4 = \mathrm{id}_X$. Then, (X,r), defined by $r(x,y) = (\lambda_x(y), \rho_y(x))$, for all $x,y \in X$, is a finite bijective non-degenerate solution of the Yang-Baxter equation. Furthermore, the associated structure monoid*

$$\begin{aligned}
M = M(X,r) = \langle X \mid\ & 1\circ 2 = 2\circ 1,\ 1\circ 3 = 4\circ 1,\ 1\circ 4 = 3\circ 1,\\
& 2\circ 3 = 4\circ 2 = 2\circ 4 = 3\circ 2,\ 3\circ 4 = 4\circ 3\rangle^1,
\end{aligned}$$

is not abelian. In the structure group, $3 = 4$ and we get an abelian group,

$$G(X,r) = \mathrm{gr}(1,2,3 \mid 1\circ 2 = 2\circ 1,\ 1\circ 3 = 3\circ 1,\ 2\circ 3 = 3\circ 2).$$

The derived structure monoid is equal to

$$\begin{aligned}
A = A(X,r) = \langle X \mid\ & 1+2 = 2+1,\ 1+3 = 3+1,\ 1+4 = 4+1,\\
& 2+4 = 4+2 = 2+3 = 3+2,\ 3+4 = 4+3\rangle^1.
\end{aligned}$$

Since $A(X,r)$ is abelian, we may take $d = 2$ in (4.11). Let $Y = \{1,3\}$ and $Z = \{1,4\}$. Then,

$$\begin{aligned} a_Y &= 1+1+3+3 \in A_2 \setminus A_3, & m_Y &= 1\circ 1\circ 3\circ 3 \in M_2 \setminus M_3, \\ a_Z &= 1+1+4+4 \in A_2 \setminus A_3, & m_Z &= 1\circ 1\circ 4\circ 4 \in M_2 \setminus M_3. \end{aligned}$$

Similar as in Example 4.3.9, we obtain the following non-empty components

$$\begin{aligned} M_{YY} &= \{(a,\lambda_a) \mid a \in 1+1+3+\langle 1+1,3\rangle^1\}, \\ M_{YZ} &= \{(a,\lambda_a) \mid a \in 1+3+\langle 1+1,3\rangle^1\}, \\ M_{ZY} &= \{(a,\lambda_a) \mid a \in 1+4+\langle 1+1,4\rangle^1\}, \\ M_{ZZ} &= \{(a,\lambda_a) \mid a \in 1+1+4+\langle 1+1,4\rangle^1\}. \end{aligned}$$

Take $a = 1 \in \langle Y \cap Z\rangle$ and $b = 1+1 \in \langle Y \cap Z\rangle$. Then, $\lambda_{1+1}\lambda_1^{-1}(Y) = \lambda_1(Y) = Z$ and $\lambda_{1+1}\lambda_1^{-1}(Z) = \lambda_1(Z) = Y$. Hence, condition (NC) is satisfied. Moreover, not all cancellative components are Malcev nilpotent. To see this, take $U = \{1,3,4\}$. Then, $M_{UU} = \{(a,\lambda_a) \mid a \in 1+3+4+\langle 1,3,4\rangle^1\}$. If we restrict r to $U\times U$ we obtain a subsolution r_U with structure group

$$\begin{aligned} G(U,r_U) &= \mathrm{gr}(U \mid 1\circ 3 = 4\circ 1,\ 1\circ 4 = 3\circ 1,\ 3\circ 4 = 4\circ 3) \\ &\cong \mathrm{gr}(3,4 \mid 3\circ 4 = 4\circ 3) \rtimes \mathrm{gr}(1), \end{aligned}$$

where the action of 1 interchanges 3 and 4. Since $G(U,r_U)$ contains the infinite dihedral group, it is not nilpotent. Therefore, $m_U M_{UU}$ is not Malcev nilpotent. To conclude, (X,r) is a solution with abelian structure group, it satisfies condition (NC), and not all cancellative components are Malcev nilpotent. By Theorem 4.3.7, the structure monoid $M(X,r)$ is not Malcev nilpotent.

4.4 Multipermutation solutions

It appears that bijective non-degenerate solutions of Lyubashenko type are better understood than general bijective non-degenerate solutions of the Yang-Baxter equation. In the previous section, we were able to describe exactly when the structure monoid of a finite bijective non-degenerate solution of Lyubashenko type is Malcev nilpotent (see Proposition 4.3.11), which was much more complicated in the general case for arbitrary finite bijective non-degenerate solutions (see Theorem 4.3.7). As a result, the idea of connecting or reducing general solutions to Lyubashenko solutions has been explored. Reducing a solution has been done via the definition of a retract, and it launched the study of multipermutation solutions, see for example [1, 10, 13, 33, 45, 48, 49, 75, 80, 83, 85, 87, 94, 95, 96, 125, 172].

In Section 3.3, the retract relation for non-degenerate set-theoretic solutions was defined, extending the definitions of Etingof, Schedler, and Soloviev [75], and Lebed and Vendramin [125]. In this section, we focus on the retract of arbitrary bijective non-degenerate set-theoretic solutions of the Yang-Baxter equation, and study bijective non-degenerate multipermutation solutions. Starting from a bijective non-degenerate multipermutation solution, we will study its structure group and structure monoid, and their extended solutions (see Section 2.1). In doing so, we will generalize some results of Gateva-Ivanova and Cameron in [83], and Bachiller, Cedó, and Vendramin [13]. We finish this section by proving a result similar to Proposition 4.2.4. Namely, if (X, r) is a finite multipermutation solution and $G = G(X, r)$ is nilpotent, then we show that the torsion subgroup $T(G)$ of G is finite and equal to the additive commutator subgroup $[G, G]_+$ of the group $(G, +)$, the additive group of the skew left brace G.

In [125, Lemma 8.4], it is shown that, for a finite bijective non-degenerate solution (X, r), r induces a finite bijective non-degenerate solution $(\overline{X}, \overline{r})$ on $\overline{X} = X/{\sim}$, with $\sim$ the retract relation on X. In the following lemma, we show that [125, Lemma 8.4] holds for bijective non-degenerate solutions of the Yang-Baxter equation of arbitrary size $|X|$. To avoid confusion, we will denote the inverse of x in $G(X, r)$ as x^{-1} (instead of $\overline{x}$ as we did earlier).

Lemma 4.4.1. *Let (X, r) be a bijective non-degenerate set-theoretic solution of the Yang-Baxter equation. Define an equivalence relation $\sim$ on X by*

$$x \sim y \quad \textit{if and only if} \quad \lambda_x = \lambda_y \textit{ and } \rho_x = \rho_y.$$

Sometimes, this relation will be denoted by $\sim_X$ to emphasize the set X. Then, $(\overline{X}, \overline{r})$ is a bijective non-degenerate solution with $\overline{X} = X/{\sim}$, and $\overline{r}$ is defined by

$$\overline{r}(\overline{x}, \overline{y}) = (\overline{\lambda_x(y)}, \overline{\rho_y(x)}),$$

for all $x, y \in X$. We denote $\operatorname{Ret}(X, r) = (\overline{X}, \overline{r})$ *and it is called the* retract solution *of (X, r). The solution (X, r) is said to be* retractable *if $\sim$ is not the trivial relation, i.e. if $\overline{X} \neq X$. Otherwise, the solution is called* irretractable. *The relation $\sim$ is called the* retract relation.

Proof. By Proposition 3.3.3 and Theorem 3.3.5, $(\overline{X}, \overline{r})$ is a non-degenerate set-theoretic solution of the Yang-Baxter equation. It remains to prove that $\overline{r}$ is bijective. Let $x, y, z \in X$ with $x \sim y$. First, note that

$$\begin{aligned}
\lambda_{\lambda_x(z)}\lambda_{\rho_z(x)} &= \lambda_x\lambda_z = \lambda_y\lambda_z = \lambda_{\lambda_y(z)}\lambda_{\rho_z(y)} = \lambda_{\lambda_x(z)}\lambda_{\rho_z(y)},\\
\rho_{\rho_x(z)}\rho_{\lambda_z(x)} &= \rho_x\rho_z = \rho_y\rho_z = \rho_{\rho_y(z)}\rho_{\lambda_z(y)} = \rho_{\rho_x(z)}\rho_{\lambda_z(y)},\\
\lambda_{\lambda_z(x)}\lambda_{\rho_x(z)} &= \lambda_z\lambda_x = \lambda_z\lambda_y z = \lambda_{\lambda_z(y)}\lambda_{\rho_y(z)} = \lambda_{\lambda_z(y)}\lambda_{\rho_x(z)},\\
\rho_{\rho_z(x)}\rho_{\lambda_x(z)} &= \rho_z\rho_x = \rho_z\rho_y = \rho_{\rho_z(y)}\rho_{\lambda_y(z)} = \rho_{\rho_z(y)}\rho_{\lambda_x(z)}.
\end{aligned}$$

Hence, $\lambda_z(x) \sim \lambda_z(y)$ and $\rho_z(x) \sim \rho_z(y)$, and $\overline{r}$ is well-defined.

From Section 1.3, we know that (X, r^{-1}) is also a bijective non-degenerate solution of the Yang-Baxter equation. Similar as in Subsection 4.1.2 (see (1.20)), write

$$r^{-1}(x, y) = (\hat{\lambda}_x(y), \hat{\rho}_y(x)).$$

By (4.7), $\mathrm{Ker}(\lambda) \cap \mathrm{Ker}(\rho) = \mathrm{Ker}(\hat{\lambda}) \cap \mathrm{Ker}(\hat{\rho})$. So, $x \sim y$ if and only if $x \circ y^{-1} \in \mathrm{Ker}(\lambda) \cap \mathrm{Ker}(\rho)$, which is equivalent with $x \circ y^{-1} \in \mathrm{Ker}(\hat{\lambda}) \cap \mathrm{Ker}(\hat{\rho})$. Similar computations as the proof of Lemma 3.3.4 part (1), (2), and (4), applied on the solution (X, r^{-1}), give us

$$\begin{aligned}\hat{\lambda}_{\hat{\rho}_z(x)} &= \hat{\lambda}_{\hat{\rho}_z(y)},\\ \hat{\rho}_{\hat{\lambda}_z(x)} &= \hat{\rho}_{\hat{\lambda}_z(y)},\\ \hat{\lambda}_{\hat{\lambda}_z(x)} &= \hat{\lambda}_{\hat{\lambda}_z(y)},\\ \hat{\rho}_{\hat{\rho}_z(x)} &= \hat{\rho}_{\hat{\rho}_z(y)}.\end{aligned}$$

So, $\hat{\lambda}_z(x) \circ \hat{\lambda}_z(y)^{-1}, \hat{\rho}_z(x) \circ \hat{\rho}_z(y)^{-1} \in \mathrm{Ker}(\hat{\lambda}) \cap \mathrm{Ker}(\hat{\rho})$. It follows by (4.7) that $\hat{\lambda}_z(x) \sim \hat{\lambda}_z(y)$ and $\hat{\rho}_z(x) \sim \hat{\rho}_z(y)$. The map

$$\overline{r^{-1}} : \overline{X}^2 \to \overline{X}^2 : (\overline{x}, \overline{y}) \mapsto (\overline{\hat{\lambda}_x(y)}, \overline{\hat{\rho}_y(x)}),$$

is thus well-defined. Clearly this is the inverse of $\overline{r}$. So, $\overline{r}$ is a bijective set-theoretic solution of the Yang-Baxter equation. □

This equivalence relation $\sim$ allows us, as before in [75, 125], to define bijective non-degenerate multipermutation solutions.

Definition 4.4.2. *Let (X, r) be a bijective non-degenerate set-theoretic solution of the Yang-Baxter equation. Put, for $n \geq 1$,*

$$(X_0, r_0) = (X, r) \quad \textit{and} \quad (X_n, r_n) = \mathrm{Ret}(X_{n-1}, r_{n-1}).$$

Then, (X, r) is called a multipermutation solution of level m, *if m is the minimal non-negative integer such that $|X_m| = 1$. In this case, we write* $\mathrm{mpl}(X, r) = m$. *In what follows, we denote (X_n, r_n) by $\mathrm{Ret}^n(X, r)$, for all non-negative integers n.*

In the upcoming result, we use the notation of Section 2.2 for the left and right derived solution (X, s) and (X, s') of a bijective non-degenerate solution (X, r).

Corollary 4.4.3. *Let (X, r) be a bijective non-degenerate set-theoretic solution of the Yang-Baxter equation. If (X, r) is retractable, then its left and right derived solutions (X, s) and (X, s') are retractable. In particular, if (X, r) is a multipermutation solution of finite level, then so are (X, s) and (X, s').*

Proof. Let $x, y \in X$ be two distinct elements such that $x \sim y$. As $\lambda_x = \lambda_y$ and $\rho_x = \rho_y$, by (4.7), it follows that $\hat{\lambda}_x = \hat{\lambda}_y$ and $\hat{\rho}_x = \hat{\rho}_y$. Since $\hat{\lambda}_{\lambda_x(y)}(\rho_y(x)) = x$ and $\hat{\rho}_{\rho_y(x)}(\lambda_x(y)) = y$, we get that $\hat{\lambda}_x^{-1}(y) = \rho_{\lambda_y^{-1}(x)}(y)$ and $\hat{\rho}_x^{-1}(y) = \lambda_{\rho_y^{-1}(x)}(y)$. Therefore,

$$\sigma_x = \lambda_x \hat{\lambda}_x^{-1} = \lambda_y \hat{\lambda}_y^{-1} = \sigma_y \quad \text{and} \quad \tau_x = \rho_x \hat{\rho}_x^{-1} = \rho_y \hat{\rho}_y^{-1} = \tau_y,$$

which shows that the left derived solution (X, s) and the right derived solution (X, s') are retractable. □

Clearly, the reverse implication does not hold. Take (X, r) any irretractable non-degenerate involutive solution of the Yang-Baxter equation. Its derived solution (X, s) is trivial, hence it is a multipermutation solution of level 1.

Remark 4.4.4. *In [55], the socle series of a skew brace $(B, +, \circ)$ is defined as follows. Put $\operatorname{Soc}_0(B) = \{0\}$ and, for $n \geq 0$, let $\operatorname{Soc}_{n+1}(B)$ denote the unique ideal of B containing $\operatorname{Soc}_n(B)$ such that $\operatorname{Soc}_{n+1}(B)/\operatorname{Soc}_n(B) = \operatorname{Soc}(B/\operatorname{Soc}_n(B))$. So, $\operatorname{Soc}_1(B) = \operatorname{Soc}(B)$. If there exists a non-negative integer n such that $\operatorname{Soc}_n(B) = B$ then B is said to have a* socle series *and the smallest such n is called the* socle length *of B.*

Cedó, Smoktunowicz and Vendramin, in [55], define a skew left brace of finite multipermutation level using its socle series. Namely, a skew left brace $(B, +, \circ)$ has finite multipermutation level *n if and only if $S_n = \{0\}$, with S_i recursively defined as $S_1 = B$ and $S_i = S_{i-1}/\operatorname{Soc}(S_{i-1})$ for $i > 1$. They show that this is equivalent with B having a socle series of length n. Note furthermore that $\operatorname{Ret}_n(B, r_B) = (B/\operatorname{Soc}_n(B), r_{B/\operatorname{Soc}_n(B)})$. Hence, (B, r_B) is a multipermutation solution of level n if and only if B has socle series of length n.*

For a skew left brace $(B, +, \circ)$, $(\operatorname{Soc}(B), \circ)$ is an abelian group and $(\operatorname{Soc}(B), +, \circ)$ is a trivial skew brace (see for example [6, Proposition 1.1.12]). Hence, $(\operatorname{Soc}(B), r_{\operatorname{Soc}(B)})$ is a multipermutation solution of level 1. If, furthermore, $(B, +, \circ)$ has a socle series of length n, then we obtain an ideal chain

$$\{0\} = \operatorname{Soc}_0(B) \subseteq \operatorname{Soc}_1(B) \subseteq \cdots \subseteq \operatorname{Soc}_n(B) = B,$$

with each factor $\operatorname{Soc}_{i+1}(B)/\operatorname{Soc}_i(B) = \operatorname{Soc}(B/\operatorname{Soc}_i(B))$ abelian, for $0 \leq i < n$. Indeed, since $B/\operatorname{Soc}_i(B)$ is also a skew brace, we get that $(\operatorname{Soc}_{i+1}(B)/\operatorname{Soc}_i(B), \circ) = (\operatorname{Soc}(B/\operatorname{Soc}_i(B)), \circ)$ is abelian.

The following lemma provides a connection between the injectivization (see Section 2.1) and the retract solution of a bijective non-degenerate solution.

Lemma 4.4.5. *Let (X, r) be a bijective non-degenerate set-theoretic solution of the Yang-Baxter equation, and let $\iota : X \to G(X, r)$ and $\overline{\iota} : \overline{X} \to G(\operatorname{Ret}(X, r))$ denote the canonical maps. Then, the rule $\varphi(\iota(x)) = \overline{\iota}(\overline{x})$, where $\overline{x}$ denotes the equivalence class of $x \in X$ in $\overline{X}$, induces a surjective morphism of solutions $\varphi : \operatorname{Inj}(X, r) \to \operatorname{Ret}(X, r)$. Moreover, φ induces a surjective morphism of groups $\varphi' : G(X, r) \to G(\operatorname{Ret}(X, r))$.*

Proof. To prove the result, it is enough to show that φ is well-defined. As it was shown in [97, Proposition 4.2], for all elements $x, y \in X$ satisfying $\iota(x) = \iota(y)$, it holds that $\lambda_x = \lambda_y$. By left-right symmetry, this also shows that $\rho_x = \rho_y$. Hence, $\overline{x} = \overline{y}$, which yields $\overline{\iota}(\overline{x}) = \overline{\iota}(\overline{y})$. By the assumption that $\varphi(\iota(x)) = \overline{\iota}(\overline{x})$, we get that $\varphi : \operatorname{Inj}(X, r) \to \operatorname{Ret}(X, r)$ is a surjective morphism of solutions. As the canonical map $\iota' : \iota(X) \to G(\operatorname{Inj}(X, r)) \cong G(X, r)$ is injective, φ induces a surjective morphism of groups $\varphi' : G(X, r) \to G(\operatorname{Ret}(X, r))$. □

Let $(B, +, \circ)$ be a finite skew left brace of size at least two with associated solution (B, r_B). Smoktunowicz and Vendramin, in [173, Theorem 4.13], proved that the order of r_B is even, and it equals two times the exponent of the group $(B,+)/Z(B,+)$. The following proposition shows that this phenomenon partly appears for multipermutation solutions.

Proposition 4.4.6. *Let (X,r) be a bijective non-degenerate set-theoretic solution of the Yang-Baxter equation with $|X| > 1$. If (X,r) is of finite multipermutation level and r is of finite order, then r is of even order.*

Proof. Let (X,r) be a bijective non-degenerate solution of multipermutation level n. Then, $\operatorname{Ret}^{n-1}(X,r)$ is a multipermutation solution of level 1, and there exists a canonical surjective morphism of solutions $\varphi : (X,r) \to \operatorname{Ret}^{n-1}(X,r)$. This implies that if k is the order of r, the order of the solution $\operatorname{Ret}^{n-1}(X,r)$ is a divisor of k. In particular, if the latter is even, then so is the order of r.

So, we can assume that (X,r) is a multipermutation solution of level 1. Then, there exist commuting permutations f and g of X such that $\lambda_x = f$ and $\rho_x = g$, for all $x \in X$. Suppose that the order $k = 2l + 1$ of r is odd. Then, $(x,y) = r^k(x,y) = (f^{l+1}g^l(y), f^l g^{l+1}(x))$. In particular, we obtain that $f^{l+1}g^l(y) = x$, for all $x,y \in X$. Thus, $f^{l+1}g^l(x) = f^{l+1}g^l(y)$, for all $x,y \in X$. Since $f^{l+1}g^l$ is a bijection, it follows that $x = y$ for all $x,y \in X$, in contradiction with $|X| > 1$. □

Proposition 4.4.6 raises the question whether non-involutive, bijective non-degenerate solutions that are injective and of finite multipermutation level exist. The following example illustrates this.

Example 4.4.7. *Consider the bijective non-degenerate solution (X,r) on the set $X = \{1,2,3,4\}$, defined by $r(x,y) = (\tau_x(y), x)$, for all $x,y \in X$, with $\tau_1 = \tau_2 = (3,4)$ and $\tau_3 = \tau_4 = (1,2)$. It is clear that this solution has multipermutation level 2, and the retract is a trivial solution on a set consisting of two elements. Furthermore,*

$$\begin{aligned} G(X,r) = \operatorname{gr}(1,2,3,4\,|1 \circ 2 = 2 \circ 1,\ 3 \circ 4 = 4 \circ 3,& \\ 1 \circ 3 = 4 \circ 1 = 2 \circ 4 = 3 \circ 2,\ 3 \circ 1 = 2 \circ 3 = 4 \circ 2 = 1 \circ 4).& \end{aligned}$$

From the presentation of $G(X,r)$, it follows that $2 = 3 \circ 1 \circ 3^{-1}$ and $4 = 1 \circ 3 \circ 1^{-1}$ in $G(X,r)$, and we obtain

$$G(X,r) \cong \operatorname{gr}(1,3 \mid 3 \circ 1 \circ 1 = 1 \circ 1 \circ 3,\ 3 \circ 3 \circ 1 = 1 \circ 3 \circ 3,\ 3 \circ 1 \circ 3 \circ 1 = 1 \circ 3 \circ 1 \circ 3).$$

Indeed, we get that

$$\begin{aligned} 3 \circ 1 \circ 1 &= 1 \circ 4 \circ 1 = 1 \circ 1 \circ 3 \circ 1^{-1} \circ 1 = 1 \circ 1 \circ 3, \\ 1 \circ 3 \circ 3 &= 3 \circ 2 \circ 3 = 3 \circ 3 \circ 1 \circ 3^{-1} \circ 3 = 3 \circ 3 \circ 1, \\ 3 \circ 1 \circ 3 \circ 1 &= 1 \circ 4 \circ 3 \circ 1 = 1 \circ 3 \circ 4 \circ 1 = 1 \circ 3 \circ 1 \circ 3. \end{aligned}$$

In particular, $1 \circ 1$ and $3 \circ 3$ are central elements of $G(X,r)$, and the quotient

$$G(X,r)/\operatorname{gr}(1 \circ 1, 3 \circ 3) \cong \operatorname{gr}(a,b \mid a^2 = b^2 = (ab)^4 = 1) \cong D_8,$$

is a non-abelian group, and thus also $G(X,r)$ is a non-abelian group. We will now prove that (X,r) is injective. First, note that the group $G(X,r)$ admits a morphism onto the free abelian group on $\{x,y\}$ by mapping both $1,2$ to x and both $3,4$ to y. This yields that $1 \neq 3$, $1 \neq 4$, $2 \neq 3$, and $2 \neq 4$ in $G(X,r)$. Now suppose, on the contrary, that $1 = 2$ in $G(X,r)$. Then, $3 = 4$ in $G(X,r)$, and thus $G(X,r) \cong \mathrm{gr}(1,3 \mid 1 \circ 3 = 3 \circ 1)$ would be an abelian group, a contradiction. Similarly, on shows that $3 \neq 4$ in $G(X,r)$. Therefore, X embeds into $G(X,r)$, and (X,r) is an injective solution, as claimed. It is also worth to mention that despite $1 \neq 2$ in $G(X,r)$, we have

$$\begin{aligned} 1 \circ 1 \circ 3 \circ 3 &= 1 \circ (1 \circ 3) \circ 3 = 1 \circ (2 \circ 4) \circ 3 = (1 \circ 2) \circ 4 \circ 3 \\ &= (2 \circ 1) \circ 4 \circ 3 = 2 \circ (1 \circ 4) \circ 3 = 2 \circ (2 \circ 3) \circ 3 = 2 \circ 2 \circ 3 \circ 3, \end{aligned}$$

which guarantees that $1 \circ 1 = 2 \circ 2$ in $G(X,r)$.

The following result tells us something about the interplay between the retract solutions of epimorphic bijective non-degenerate solutions of the Yang-Baxter equation. For involutive solutions, the result was already proven by Cedó, Jespers, and Okniński in [49, Lemma 4]. As a consequence, being a multipermutation solution is inherited by epimorphic images.

Proposition 4.4.8. *Let (X,r) and (Y,r') be bijective non-degenerate solutions of the Yang-Baxter equation. Then, any surjective morphism of solutions $\varphi : (X,r) \to (Y,r')$ induces a surjective morphism $\overline{\varphi} : \mathrm{Ret}(X,r) \to \mathrm{Ret}(Y,r')$ of their retract solutions. In particular, if (X,r) is a multipermutation solution of finite level m, then any epimorphic image of (X,r) (for example the injectivization $\mathrm{Inj}(X,r)$) is a multipermutation solution of finite level bounded by m.*

Proof. Let $x,y \in X$ with $x \sim y$, i.e. $\lambda_x = \lambda_y$ and $\rho_x = \rho_y$. Denote the map r' by $r'(u,v) = (\lambda'_u(v), \rho'_v(u))$, for all $u,v \in Y$. Then, for any $z \in X$, it follows that

$$\lambda'_{\varphi(x)}(\varphi(z)) = \varphi(\lambda_x(z)) = \varphi(\lambda_y(z)) = \lambda'_{\varphi(y)}(\varphi(z)).$$

As φ is surjective, this implies that $\lambda'_{\varphi(x)} = \lambda'_{\varphi(y)}$. Similarly, one proves that $\rho'_{\varphi(x)} = \rho'_{\varphi(y)}$, and thus we obtain that $\varphi(x) \sim_Y \varphi(y)$. Therefore, the composition $\pi \circ \varphi : (X,r) \to \mathrm{Ret}(Y,r')$, where $\pi : (Y,r') \to \mathrm{Ret}(Y,r')$ is the canonical epimorphism, induces a surjective morphism of solutions $\overline{\varphi} : \mathrm{Ret}(X,r) \to \mathrm{Ret}(Y,r')$. □

Also subsolutions (see Section 1.3) inherit the property of being multipermutation, which was known already in the involutive case by a result of Cedó, Jespers, and Okniński [49, Lemma 5].

Lemma 4.4.9. *Let (X,r) be a bijective non-degenerate solution of the Yang-Baxter equation and (Y,r') a subsolution of (X,r). If (X,r) is of finite multipermutation level m, then (Y,r') is of finite multipermutation level bounded by m.*

Proof. We will show by induction on n that the map $\mathrm{id}_Y : Y \to Y$ induces a surjective morphism of solutions $\varphi_n : (\overline{Y}_n, r_n|_{(\overline{Y}_n)^2}) \to \mathrm{Ret}^n(Y, r')$, where $\overline{Y}_n = \{\overline{y} \in X_n \mid y \in Y\}$ with $(X_n, r_n) = \mathrm{Ret}^n(X, r)$. For $n = 1$, $\overline{Y}_1 = Y/{\sim_X}$. It is clear that $x \sim_X y$ for some $x, y \in Y$ implies $x \sim_Y y$. In particular, $\mathrm{id}_Y : Y \to Y$ induces an epimorphism of solutions

$$\varphi_1 : (\overline{Y}_1, r_1|_{(\overline{Y}_1)^2}) \to \mathrm{Ret}(Y, r'),$$

where $(\overline{Y}_1, r_1|_{(\overline{Y}_1)^2})$ is a subsolution of $\mathrm{Ret}(X, r)$. Suppose we have shown that the map $\mathrm{id}_Y : Y \to Y$ induces a surjective morphism of solutions $\varphi_n : (\overline{Y}_n, r_n|_{(\overline{Y}_n)^2}) \to \mathrm{Ret}^n(Y, r')$. Let $\overline{x}, \overline{y} \in \overline{Y}_n$ be such that $\overline{x} \sim_{X_n} \overline{y}$. As φ_n is a surjective morphism of solutions, it follows that $\varphi_n(\overline{x}) \sim_{Y_n} \varphi_n(\overline{y})$ in Y_n, where $(Y_n, r'_n) = \mathrm{Ret}^n(Y, r')$. In particular, φ_n induces a surjective map $\varphi_{n+1} : (\overline{Y}_{n+1}, r_{n+1}|_{(\overline{Y}_{n+1})^2}) \to \mathrm{Ret}^{n+1}(Y, r')$, which is by construction a morphism of solutions.

Hence, by induction, it follows that if (X, r) is of multipermutation level m, then (Y, r') is of multipermutation level at most m, as desired. □

Recall from Section 2.1 that a solution of Lyubashenko type, defined by $r(x, y) = (f(y), g(x))$ is injective if and only if it is involutive, which is equivalent to fg being the identity map on X. Since a multipermutation solutions of level 1 is of Lyubashenko type, its injectivization turns out to be always involutive. We include a proof for completeness' sake.

Proposition 4.4.10. *Let (X, r) be a bijective non-degenerate solution of the Yang-Baxter equation of multipermutation level 1. Then, the injectivization $\mathrm{Inj}(X, r)$ of (X, r) is an involutive solution of the Yang-Baxter equation.*

Proof. The injectivization $\mathrm{Inj}(X, r)$ remains a multipermutation solution of level at most 1. If $\mathrm{Inj}(X, r)$ is of multipermutation level 0, then the result follows. Hence, we replace r by its injectivization. Write $r(x, y) = (f(y), g(x))$, for all $x, y \in X$, and some commuting permutations f and g on X. Then, $r(x, f^{-1}(x)) = (x, g(x))$, for all $x \in X$. Since the solution (X, r) is injective, it follows that $g = f^{-1}$, as desired. □

A final intermediate step into proving that a bijective non-degenerate solution (X, r) of the Yang-Baxter equation is a multipermutation solution if and only if so is (M, r_M), where $M = M(X, r)$, and equivalently so is (G, r_G), with $G = G(X, r)$, is to link the retract relations $\sim_X$, $\sim_M$ and $\sim_G$, introduced in Lemma 4.4.1.

Lemma 4.4.11. *Assume that (X, r) is a bijective non-degenerate set-theoretic solution of the Yang-Baxter equation. Let $M = M(X, r)$ and $G = G(X, r)$. If for $x, y \in X$ we have $x \sim_X y$, then $x \sim_M y$ and $x \sim_G y$.*

Proof. From (4.5), we have that $\lambda_x \in \mathrm{Sym}(X)$ induces the map $\lambda_x \in \mathrm{Sym}(M)$ and similarly, ρ_x induces the map $\rho_x \in \mathrm{Sym}(M)$. So, $x \sim_X y$ yields that $x \sim_M y$. Completely analogous, the map $\lambda_x \in \mathrm{Sym}(X)$ induces the map $\lambda_x \in \mathrm{Sym}(G)$ and ρ_x induces the map $\rho_x \in \mathrm{Sym}(G)$. Hence, $x \sim_X y$ implies that $x \sim_G y$, as desired. □

Corollary 4.4.12. *Let (X,r) be a bijective non-degenerate set-theoretic solution of the Yang-Baxter equation of finite multipermutation level m. Then, the solutions associated to $M = M(X,r)$ and $G = G(X,r)$ are of finite multipermutation level, bounded by $m+1$.*

Proof. By Proposition 4.4.8, we may assume that (X,r) is an injective solution. Let

$$M'_n = M(\operatorname{Ret}^n(X,r)) \quad \text{and} \quad G'_n = G(\operatorname{Ret}^n(X,r)),$$

for all $n \geq 0$, with associated solution $(M'_n, r_{M'_n})$ and $(G'_n, r_{G'_n})$ respectively. In particular, $M = M'_0$ and $G = G'_0$. We claim that there exist surjective morphisms of solutions

$$\psi_n : (M'_n, r_{M'_n}) \to \operatorname{Ret}^n(M, r_M) \quad \text{and} \quad \varphi_n : (G'_n, r_{G'_n}) \to \operatorname{Ret}^n(G, r_G).$$

The claim will be proven by induction on n. For $n = 1$, Lemma 4.4.11 yields that $x, y \in X$ with $x \sim_X y$ also satisfy $x \sim_M y$ and $x \sim_G y$. So, there exist surjective morphisms of solutions $\psi_1 : (M'_1, r_{M'_1}) \to \operatorname{Ret}(M, r_M)$ and $\varphi_1 : (G'_1, r_{G'_1}) \to \operatorname{Ret}(G, r_G)$, where the latter is well-defined by Lemma 4.4.5. Indeed, using the same notation as in Lemma 4.4.5, we get that if $\bar{\iota}(\bar{x}) = \bar{\iota}(\bar{y})$ in $G(\operatorname{Ret}(X,r))$, then $\varphi(\iota(x)) = \varphi(\iota(y))$ in $\operatorname{Ret}(X,r)$ (and thus also in $\operatorname{Ret}(G, r_G)$). Now, assume that we have surjective morphisms of solutions ψ_n and φ_n, for some $n \geq 1$. Consider $x, y \in X_n$, with $(X_n, r_{X_n}) = \operatorname{Ret}^n(X,r)$, such that $x \sim_{X_n} y$. Then, $\psi_n(x) \sim_{M_n} \psi_n(y)$ and $\varphi_n(x) \sim_{G_n} \varphi_n(y)$, with $(M_n, r_{M_n}) = \operatorname{Ret}^n(M, r_M)$ and $(G_n, r_{G_n}) = \operatorname{Ret}^n(G, r_G)$, which implies (again by Lemma 4.4.5) that there exists a surjective morphism of solutions $\psi_{n+1} : (M'_{n+1}, r_{M'_{n+1}}) \to \operatorname{Ret}^{n+1}(M, r_M)$ and $\varphi_{n+1} : (G'_{n+1}, r_{G'_{n+1}}) \to \operatorname{Ret}^{n+1}(G, r_G)$. So, the proof of our claim is complete.

As $|X_m| = 1$, we obtain that $M'_m = M(\operatorname{Ret}^m(X,r)) = M(X_m, r_{X_m}) \cong \mathbb{N}$ and $G'_m = G(X_m, r_{X_m}) \cong \mathbb{Z}$. Under this identification, $\psi_m : \mathbb{N} \to \operatorname{Ret}^m(M, r_M)$ and $\varphi_m : \mathbb{Z} \to \operatorname{Ret}^m(G, r_G)$ are surjective morphisms of solutions, where $\mathbb{N}$ and $\mathbb{Z}$ are considered as trivial solutions. In particular, $|\operatorname{Ret}^{m+1}(M, r_M)| = 1$ and $|\operatorname{Ret}^{m+1}(G, r_G)| = 1$, as desired. □

From [174, Theorem 2.6] (see also [6, Theorem 2.1.14]), the permutation group $\mathcal{G} = \mathcal{G}(X,r) = \operatorname{gr}((\lambda_x, \rho_x^{-1}) \mid x \in X)$ of (X,r), defined in Definition 4.1.7, has a skew brace structure (similar as for left braces, see Subsection 1.3.1), and thus also an associated bijective non-degenerate solution of the Yang-Baxter equation. We will denote this solution by $(\mathcal{G}, r_{\mathcal{G}})$.

We are finally in a position to prove one of the main results of this section.

Theorem 4.4.13. *Let (X,r) be a bijective non-degenerate set-theoretic solution of the Yang-Baxter equation. The following properties are equivalent.*

(1) The solution (X,r) is of finite multipermutation level.

(2) The associated solution on $M = M(X,r)$ is of finite multipermutation level.

(3) The associated solution on $G = G(X,r)$ is of finite multipermutation level.

Proof. If (X,r) is a bijective non-degenerate solution of finite multipermutation level then, by Corollary 4.4.12, both solutions (M,r_M) and (G,r_G) are of finite multipermutation level.

Since (X,r) is a subsolution of (M,r_M), it follows by Lemma 4.4.9 that if (M,r_M) is of finite multipermutation level, then (X,r) is of finite multipermutation level.

Finally, suppose that (G,r_G) is of finite multipermutation level. The natural map $G \to \mathcal{G}$ from the structure group to the permutation group of (X,r) is a surjective homomorphism of solutions from (G,r_G) to $(\mathcal{G},r_{\mathcal{G}})$. By Proposition 4.4.8, $(\mathcal{G},r_{\mathcal{G}})$ is of finite multipermutation level. Consider the map $\psi : X \to \mathcal{G} : x \mapsto (\lambda_x, \rho_x^{-1})$. Then, ψ is a morphism of solutions from (X,r) to $(\mathcal{G},r_{\mathcal{G}})$. Clearly, ψ induces an injective morphism of solutions $\overline{\psi} : \mathrm{Ret}(X,r) \to (\mathcal{G},r_{\mathcal{G}})$, so $\mathrm{Ret}(X,r)$ is a subsolution of $(\mathcal{G},r_{\mathcal{G}})$. By Lemma 4.4.9, $\mathrm{Ret}(X,r)$ is of finite multipermutation level, and thus so is (X,r). □

Note that in the proof of Theorem 4.4.13, the retraction of a solution (X,r) was shown to be a subsolution of the solution associated to its permutation group (as a skew left brace). In particular, this leads to the following corollary. Note that the result also immediately follows from the surjective morphism of solutions $\varphi : \mathrm{Inj}(X,r) \to \mathrm{Ret}(X,r)$ of Lemma 4.4.5.

Corollary 4.4.14. *Let (X,r) be a bijective non-degenerate set-theoretic solution of the Yang-Baxter equation. If (X,r) is irretractable, then (X,r) is an injective solution.*

The following result provides a connection between multipermutation solutions and solvability and (Malcev) nilpotency of their structure monoids and groups.

Theorem 4.4.15. *Let (X,r) be a bijective non-degenerate multipermutation solution of level m. Then, the group $G = G(X,r)$ is solvable of derived length bounded by $m+1$. Moreover, the monoid $A(X,r)$ is Malcev nilpotent of class at most $m+3$, and the group $A_{\mathrm{gr}}(X,r)$ is nilpotent of class at most $m+1$.*

Proof. By Corollary 4.4.12, the solution (G,r_G) associated to the structure group $G = G(X,r)$ is of multipermutation level at most $m+1$. Then, by Remark 4.4.4, G has a finite socle series of length at most $m+1$. As this series is also a subnormal series with abelian factors, the first part of the result follows. Moreover, the same series can be considered as a refinement of the upper central series of $A_{\mathrm{gr}}(X,r)$, since $A_{\mathrm{gr}}(X,r)$ can be seen as the additive part of the skew brace $(G,+,\circ)$. Thus, the group $A_{\mathrm{gr}}(X,r)$ is nilpotent of class not exceeding $m+1$.

As before (see Section 2.2), let (X,s) be the left derived solution of (X,r), that is

$$s(x,y) = (y, \lambda_y(\rho_{\lambda_x^{-1}(y)}(x))) = (y, \sigma_y(x)),$$

for all $x,y \in X$. We know that $\mathcal{G}(X,s) = \mathrm{gr}(\sigma_x \mid x \in X)$ is an epimorphic image of $A_{\mathrm{gr}}(X,r)$. Hence, $\mathcal{G}(X,s)$ is a nilpotent group of class at most $m+1$. Proposition 4.2.1 yields that $A(X,r)$ is Malcev nilpotent of class at most $m+3$. □

If (X, r) is a square-free non-degenerate involutive set-theoretic solution of the Yang-Baxter equation and it is a multipermutation solution of level m, then Gateva-Ivanova and Cameron proved, in [83, Theorem 6.10], that the structure group $G(X, r)$ is solvable of derived length bounded by m. The following corollary generalizes this result. Moreover, for square-free solutions it improves the bounds obtained in Theorem 4.4.15.

Corollary 4.4.16. *Let (X, r) be a square-free bijective non-degenerate set-theoretic solution of the Yang-Baxter equation. If (X, r) is a multipermutation solution of level m, then the associated solution (G, r_G) on $G = G(X, r)$ satisfies $m - 1 \le \operatorname{mpl}(G, r_G) \le m$. If, furthermore, (X, r) is an injective solution, then $\operatorname{mpl}(G, r_G) = m$.*

Moreover, the additive group of the skew left brace G is nilpotent of class bounded by m, and the structure group G is solvable of derived length bounded by m.

Proof. The proof is by induction on m. Let $m = 1$. Then, (X, r) is a solution of Lyubashenko type, i.e. $r(x, y) = (f(y), g(x))$, for some commuting permutations $f, g \in \operatorname{Sym}(X)$. Since (X, r) is square-free, $f(x) = x = g(x)$, for all $x \in X$. Hence, (X, r) is the trivial solution. In this case, the extended solution (G, r_G) is also trivial, and thus the result follows for $m = 1$.

Now, let $m > 1$, and assume that the result holds for square-free bijective non-degenerate solutions of multipermutation level at most $m-1$. Let $\mathcal{G} = \mathcal{G}(X, r)$. The map $\operatorname{Ret}(X, r) \to (\mathcal{G}, r_{\mathcal{G}}) : \overline{x} \mapsto (\lambda_x, \rho_x^{-1})$ is an injective morphism of solutions, so there is a morphism of skew left braces $\varphi : G(\operatorname{Ret}(X, r)) \to \mathcal{G}$ such that $\varphi(\overline{x}) = (\lambda_x, \rho_x^{-1})$, for all $x \in X$. As $\operatorname{Ret}(X, r)$ is a square-free bijective non-degenerate solution of multipermutation level $m - 1$, it follows by the induction hypothesis that $(G(\operatorname{Ret}(X, r)), r_{G(\operatorname{Ret}(X,r))})$ has multipermutation level $m - 1$. Since φ is clearly surjective, by Proposition 4.4.8, $(\mathcal{G}, r_{\mathcal{G}})$ is of multipermutation level $\le m - 1$. As $\operatorname{Ret}(X, r)$ is of multipermutation level $m - 1$, by Lemma 4.4.9, we have that $(\mathcal{G}, r_{\mathcal{G}})$ is of multipermutation level exactly $m - 1$. Moreover, there are epimorphisms of skew left braces $G \to \mathcal{G} : a \mapsto (\lambda_a, \rho_a^{-1})$ and $\mathcal{G} \to G/\operatorname{Soc}(G) : (\lambda_a, \rho_a^{-1}) \mapsto \overline{a}$, and thus also epimorphism between their associated solutions. Since the solution on $\operatorname{Soc}(G)$ (considered as a trivial skew brace) is of finite multipermutation level 1 (see Remark 4.4.4), we thus get, by Proposition 4.4.8, $m - 1 \le \operatorname{mpl}(G, r_G) \le m$. If, furthermore, (X, r) is injective, then (X, r) is a subsolution of (G, r_G), and by Lemma 4.4.9, (G, r_G) is of multipermutation level m. Thus, the first part of the result follows by induction.

By Remark 4.4.4, the second part of the result follows in a similar fashion to the proof of Theorem 4.4.15. □

Actually, one can see that nilpotency gives severe restrictions on the structure of $G(X, r)$. In Lemma 4.2.3, we proved that for a finite bijective non-degenerate solution (X, r) with nilpotent structure group $G = G(X, r)$, the torsion subgroup $T = T(G)$ of $(G, \circ)$ is finite and G is finite-by-(free abelian). Furthermore, the torsion subgroup $T(A_{\mathrm{gr}}(X, r))$ of $(G, +) = A_{\mathrm{gr}}(X, r)$ is equal to the additive commutator subgroup $[G, G]_+$ of $(G, +)$. If, moreover, the solution is a multipermutation solution, we will show that the latter is also true for $T(G)$.

Proposition 4.4.17. *Let (X, r) be a finite bijective non-degenerate multipermutation solution of the Yang-Baxter equation. If the structure group $G = G(X, r)$ is nilpotent, then the torsion subgroup $T = T(G)$ of $(G, \circ)$ is finite. Furthermore, the additive commutator subgroup $[G, G]_+$ of the additive group $(G, +) = A_{\mathrm{gr}}(X, r)$ of the skew left brace $(G, +, \circ)$ is a subgroup of $(G, \circ)$, and equal to T.*

Proof. By Lemma 4.2.3, T is a finite characteristic subgroup of $(G, \circ)$. That $[G, G]_+ \subseteq T$ is true, is shown in [100, Theorem 6.5] for any finite bijective non-degenerate solution. We repeat the argument for completeness' sake. In [97, Theorem 2.7], it was shown that $A_{\mathrm{gr}} = A_{\mathrm{gr}}(X, r)$ is central-by-finite, and thus, by Schur's theorem (see for example [158, 10.1.4]), $[G, G]_+ = [A_{\mathrm{gr}}, A_{\mathrm{gr}}]$ is finite. Furthermore, $[G, G]_+$ is a multiplicative subgroup of $(G, \circ)$ as it is invariant under all maps $\lambda_a \in \mathrm{Aut}(G, +)$, with $a \in G$, and for any $a, b \in [G, G]_+$, $a \circ b = a + \lambda_a(b) \in [G, G]_+$. Hence, it is a torsion subgroup of $(G, \circ)$, which shows that $[G, G]_+ \subseteq T$.

Suppose that (X, r) is a multipermutation solution of level m. We prove that $T = [G, G]_+$ by induction on m. If $m = 1$, then, by Proposition 4.4.10, the solution $\mathrm{Inj}(X, r)$ is finite, non-degenerate, and involutive, and thus $G \cong G(\mathrm{Inj}(X, r))$ is a torsion-free group (by a result of [88, Theorem 1.6]), and $(G, +) = A_{\mathrm{gr}}$ is a free abelian group. So, the result holds in this case. Assume now that $m > 1$ and the result is true for finite bijective non-degenerate solutions of multipermutation level at most m. Consider the natural surjective morphism $\varphi : G \to G(\mathrm{Ret}(X, r))$ of groups defined in Lemma 4.4.5. Let N denote its kernel. If $a \in N$, then $\lambda_a = \mathrm{id}_G = \rho_a$, which implies that $a \in \mathrm{Soc}(G)$. So, $N \subseteq \mathrm{Soc}(G)$ and $G/N \cong G(\mathrm{Ret}(X, r))$. For $a, b \in N$, since $\lambda_a = \mathrm{id}_G$, we get that $a + b = a \circ \lambda_a^{-1}(b) = a \circ b \in N$. Thus, N is also an additive subgroup of G, i.e. it is a subgroup of A_{gr}. Since $\mathrm{Ret}(X, r)$ has multipermutation level $m - 1$, the induction hypothesis shows that $T(G/N) = [G/N, G/N]_+$, and thus $T \subseteq N \circ [G, G]_+ = N + [G, G]_+$. Let $g \in T$. There exist $a \in N$ and $b \in [G, G]_+$ such that $g = a + b$. Since $[G, G]_+ \subseteq T$, and T is a characteristic subgroup of $(G, \circ)$, we obtain $a = g \circ \overline{\lambda_a^{-1}(b)} \in T \cap N$. Because $N \subseteq \mathrm{Soc}(G)$, we have $a^n = na$, for all integers n. Thus, as $a \in T$, $\mathrm{gr}(a) = \mathrm{gr}(a)_+$ is a finite subgroup of A_{gr}, and $(\mathrm{gr}(a) + [G, G]_+)/[G, G]_+$ is a finite subgroup of $A_{\mathrm{gr}}/[G, G]_+$. By Proposition 4.2.4, $A_{\mathrm{gr}}/[G, G]_+$ is a torsion-free group. So, $a \in [G, G]_+$. Therefore, $g = a + b \in [G, G]_+$ and, as a consequence, $T \subseteq [G, G]_+$. Thus $T = [G, G]_+$, and the result follows by induction. □

Corollary 4.4.18. *Let (X, r) be a finite bijective non-degenerate multipermutation solution. If the structure group $G = G(X, r)$ is nilpotent, then $\overline{G} = G/[G, G]_+$ is a trivial left brace. In particular, the image $(\overline{X}, \overline{r})$ of (X, r) in $(\overline{G}, r_{\overline{G}})$ is a trivial solution.*

Proof. By Lemma 4.2.3 and Proposition 4.4.17, it follows that $T(G, \circ) = [G, G]_+$ is a characteristic subgroup of G. As $[G, G]_+$ is also a characteristic subgroup of the additive structure, it follows that $[G, G]_+$ is an ideal of the skew left brace G. Therefore, $\overline{G} = G/[G, G]_+$ has a natural skew left brace structure. Moreover, by construction, the additive structure is abelian, thus $(\overline{G}, +, \circ)$ is a left brace. Since $\overline{G}$ is a left brace, the solution $(\overline{G}, r_{\overline{G}})$ is involutive. Clearly, there exists a natural epimorphism $\varphi : G(\overline{X}, \overline{r}) \to$

$(\overline{G},\circ)$. Furthermore, there exists a natural epimorphism $\psi : G(X,r) \to G(\overline{X},\overline{r})$, induced by the morphism of solutions $(X,r) \to (\overline{X},\overline{r})$. Recall that the relations in $(G,+)$ are defined by the left derived solution, $s(x,y) = (y,\sigma_y(x))$, for all $x,y \in X$. Therefore, $[G,G]_+ = \mathrm{gr}(x+y-x-y \mid x,y \in X) = \mathrm{gr}(x-\sigma_y(x) \mid x,y \in X)$. Hence, $\psi(x) = \psi(\sigma_y(x))$ in $\overline{G}$ and thus also in $G(\overline{X},\overline{r})$, for all $x,y \in X$. Thus, ψ can be factored through an epimorphism $\psi_2 : (\overline{G},\circ) \to G(\overline{X},\overline{r})$. As both $\varphi\circ\psi_2$ and $\psi_2\circ\varphi$ correspond to the identity mapping on the generators of the corresponding groups, it follows that both maps are isomorphisms. In particular, $(\overline{G},\circ)$ can be treated as the structure group of $(\overline{X},\overline{r})$. As $(G,\circ)$ is nilpotent, it follows that $(\overline{G},\circ)$ is nilpotent. By [44, Theorem 2], it follows that $(\overline{G},+,\circ)$ is a trivial left brace. In particular, this implies that the solution $(\overline{X},\overline{r})$ is trivial. □

Let (X,r) be a finite bijective non-degenerate solution, and put $G = G(X,r)$. By Proposition 4.4.17, $[G,G]_+$ is a subgroup of $(G,\circ)$. A natural question is whether $[G,G]_+ = T(G,\circ)$ in general. However, this is not true which is shown in the following example. Crucial is to construct an example of a skew left brace B such that its left ideal $[B,B]_+$ is not an ideal, i.e. as a multiplicative group it is not a normal subgroup of $(B,\circ)$. Note that $[B,B]_+$ is a normal subgroup of $(B,+)$, and thus it is a strong left ideal of the skew left brace B, as introduced in [99].

Example 4.4.19. *Consider the trivial left brace $A = (\mathbb{Z}/2\mathbb{Z})^2$. Then, the automorphism group $\mathrm{Aut}(A)$ of A is isomorphic to the symmetric group of degree 3. Then, $(\mathrm{Aut}(A),+,\circ)$ is a skew left brace, with $f+g = f\circ g$, for all $f,g \in \mathrm{Aut}(A)$. Consider the semidirect product $B = \mathrm{Hol}(A) = A \rtimes \mathrm{Aut}(A)$ of skew left braces. This means that*

$$((a,b),f) + ((c,d),g) = ((a+c,b+d), f\circ g),$$
$$((a,b),f) \circ ((c,d),g) = ((a,b) + f(c,d), f\circ g),$$

for all $(a,b),(c,d) \in A$ and $f,g \in \mathrm{Aut}(A)$. Then, $(B,+,\circ)$ is a skew left brace. Note that $[B,B]_+ = \{((0,0),\mathrm{id}_A),((0,0),f),((0,0),f^2)\}$, where $f \in \mathrm{Aut}(A)$ is defined as $f(a,b) = (b,a+b)$, for all $(a,b) \in A$. Since

$$\begin{aligned}((1,0),\mathrm{id}_A)^{-1}\circ((0,0),f)\circ((1,0),\mathrm{id}_A) &= ((1,0),\mathrm{id}_A)\circ((0,1),f)\\ &= ((1,1),f) \notin [B,B]_+,\end{aligned}$$

we have that $[B,B]_+$, as a multiplicative group, is not a normal subgroup of $(B,\circ)$, and thus it is not an ideal of the skew left brace $(B,+,\circ)$. By [8, Proposition 3.18] (or [6, Corollary 2.3.5]), there exists a finite bijective non-degenerate solution (X,r) such that $\mathcal{G} = \mathcal{G}_{\lambda,\rho}(X,r) \cong B$ as skew left braces. Let $G = G(X,r)$ and let $\alpha : G \to \mathcal{G}$ be the map defined by $\alpha(a) = (\lambda_a, \rho_a^{-1})$, for all $a \in G$. We know by Lemma 4.1.6 and Remark 4.1.8 that α is an epimorphism of skew left braces, and $\mathrm{Ker}(\alpha)$ is an ideal of the skew left brace G contained in its socle. Note that $\alpha^{-1}([\mathcal{G},\mathcal{G}]_+) = [G,G]_+ + \mathrm{Ker}(\alpha)$. Since $[\mathcal{G},\mathcal{G}]_+ \cong [B,B]_+$ is not an ideal of the skew left brace $\mathcal{G}$, we have that $[G,G]_+ + \mathrm{Ker}(\alpha)$ is not an ideal of the skew left brace G.

Note that if $[G,G]_+ = T(G,\circ)$*, then* $[G,G]_+$ *is an ideal of the skew left brace* G*. This yields that* $[G,G]_+ + \mathrm{Ker}(\alpha)$ *is also an ideal of* G*, a contradiction. So,* $[G,G]_+$ *is not equal to* $T(G,\circ)$*.*

Chapter 5

Idempotent and cubic solutions and skew lattices

Let's build bridges, not walls.

Martin Luther King Jr.

Many structures from Section 1.3, as well as YB-semitrusses from Chapter 3, cover involutive and bijective solutions. Another important class of solutions is the class of idempotent or cubic solutions. Recall from Section 1.3 that a set-theoretic solution of the Yang-Baxter equation (X, r) is called idempotent if $r^2 = r$, and cubic if $r^3 = r$. In [161], a bijective correspondence is given between left non-degenerate involutive set-theoretic solutions of the Yang-Baxter equation and cycle sets (see Subsection 1.3.2). In [176], this correspondence is generalized to left non-degenerate idempotent solutions and twisted Ward left quasigroups. Idempotent solutions have interesting applications, extensively explained in [120]. For example, a connection is given between the (co)homology of an idempotent solution and the Hochschild (co)homology of its structure monoid. Furthermore, different algebraic structures, like factorizable monoids, Young tableaux, and distributive lattices, are studied using so-called σ-normal words and normal forms of words in the structure monoid of idempotent solutions. Up to isomorphism, all 16 idempotent set-theoretic solutions on a two-element set are provided in [120].

Distributive lattices are meaningful as they provide idempotent set-theoretic solutions of the Yang-Baxter equation (see for example [146] for the same solution on Boolean algebras). In this section, the idea of using distributive lattices to obtain solutions is generalized. More precisely, following [69] (Cvetko-Vah and Verwimp), we use skew lattices, a non-commutative lattice that first appeared in [111], and later intensively studied in, for example, [64, 65, 66, 68, 116, 126, 127, 128, 129, 175]. We first recall the necessary information on skew lattices and several varieties. Given a family of pairwise disjoint sets or skew lattices, we include several ways to construct skew lattices, and see which properties remain true for the constructed skew lattice. Thereupon, we focus on set-theoretic solutions defined using the algebraic structure of a skew lattice, sometimes in need of extra properties. These solutions will be either idempotent or cubic, and in most cases, the solutions will be degenerate, i.e. not left non-degenerate nor right non-degenerate. At this point, finding a structure that corresponds to all degenerate solutions seems to be a far-off goal. Nevertheless, a humble first step towards this problem is given here, using skew lattices.

5.1 Preliminaries

Although skew lattices first appeared in [111], their modern definition was first given in [126], where today's study of skew lattices was launched. A *skew lattice* is a set S equipped with a pair of idempotent and associative operations $\wedge$ (meet) and $\vee$ (join) that satisfy the absorption laws

$$x \wedge (x \vee y) = x = x \vee (x \wedge y) \text{ and } (x \wedge y) \vee y = y = (x \vee y) \wedge y, \tag{5.1}$$

for all $x, y \in S$, and is denoted by $(S, \wedge, \vee)$.

Easy examples of skew lattices are lattices, i.e. a skew lattice $(S, \wedge, \vee)$ where both operations $\wedge$ and $\vee$ are commutative, meaning that $x \wedge y = y \wedge x$ and $x \vee y = y \vee x$, for all $x, y \in S$. The following example presents a skew lattice that is not a lattice.

Example 5.1.1. *Let $S = \{0, 1, 2\}$, and define the meet and join operation by*

$\wedge$	0	1	2
0	0	0	0
1	0	1	1
2	0	2	2

,

$\vee$	0	1	2
0	0	1	2
1	1	1	2
2	2	1	2

.

Then, $1 \wedge 2 = 1$, but $2 \wedge 1 = 2$. So, $(S, \wedge, \vee)$ is not a lattice. However, one can check that $(S, \wedge, \vee)$ is a skew lattice.

A skew lattice is called *rectangular* if it satisfies the identities $x \wedge y \wedge z = x \wedge z$ and $x \vee y = y \wedge x$. For lattices, the absorption laws yield an absorption duality between the meet and join operation, i.e. $a \wedge b = a$ if and only if $a \vee b = b$. In a similar manner, the following pair of dualities hold in any skew lattice [126], for any $x, y \in S$,

$$\begin{aligned} x \wedge y = x &\quad \text{if and only if} \quad x \vee y = y, \\ x \wedge y = y &\quad \text{if and only if} \quad x \vee y = x. \end{aligned}$$

Recall from [93] (see also Section 1.3) that a *band* is a semigroup of idempotents. A band $(S, \cdot)$ is called *regular* if $xyxzx = xyzx$, for all $x, y, z \in S$. A complete list of varieties of bands can be found in [151]. Given a skew lattice $(S, \wedge, \vee)$, both semigroups $(S, \wedge)$ and $(S, \vee)$ are regular bands [126, Theorem 1.15], i.e. the identities

$$x \wedge y \wedge x \wedge z \wedge x = x \wedge y \wedge z \wedge x, \tag{5.2}$$
$$x \vee y \vee x \vee z \vee x = x \vee y \vee z \vee x, \tag{5.3}$$

are satisfied.

5.1.1 Green's equivalence relations and Leech's Decomposition Theorems for skew lattices

In semigroup theory, *Green's equivalence relations* $\mathcal{L}, \mathcal{R}, \mathcal{D}, \mathcal{H}$, and $\mathcal{J}$ are fundamental tools to study a semigroup. Given a semigroup $(S, \cdot)$, relation $\mathcal{L}$ is a right congruence, i.e. $a \mathcal{L} b$ implies $ac \mathcal{L} bc$, for all $c \in S$, while relation $\mathcal{R}$ is a left congruence, i.e. $a \mathcal{R} b$ implies $ca \mathcal{R} cb$, for all $c \in S$, see [93, Proposition 2.1.2]. Moreover, each $\mathcal{D}$-class is a union of $\mathcal{L}$-classes and likewise a union of $\mathcal{R}$-classes. The intersection of an $\mathcal{L}$-class and an $\mathcal{R}$-class is either empty or an $\mathcal{H}$-class. Because of this, a $\mathcal{D}$-class is sometimes visualized as an "eggbox", with rows corresponding to $\mathcal{R}$-classes, columns corresponding to $\mathcal{L}$-classes, and intersections of rows and columns corresponding to $\mathcal{H}$-classes. A *left-zero semigroup* is a semigroup $(S, \wedge)$ satisfying the identity $x \wedge y = x$, while a *right-zero semigroup* is a semigroup $(S, \wedge)$ satisfying the identity $x \wedge y = y$. For more information on the topic, we refer to [93].

For bands, $\mathcal{D} = \mathcal{J}$, and $\mathcal{H}$ is the diagonal relation (the $\mathcal{H}$-classes are singletons), making only the first three relations relevant. They are given by, see [152, Lemma I.7.1],

$$\begin{aligned} x\mathcal{L}y &\text{ if and only if } xy = x,\ yx = y,\\ x\mathcal{R}y &\text{ if and only if } xy = y,\ yx = x,\\ x\mathcal{D}y &\text{ if and only if } xyx = x,\ yxy = y. \end{aligned}$$

In general, Green's relation $\mathcal{D}$ on a semigroup is not necessarily a congruence. However, by Clifford-McLean Theorem ([57, Theorem3] and [141, Theorem 1]), $\mathcal{D}$ is a congruence on any band, and any band factorizes as a commutative band (also called a semilattice) of rectangular bands.

Given a skew lattice $(S, \wedge, \vee)$, we denote the corresponding Green's relations by $\mathcal{L}_\wedge$, $\mathcal{R}_\wedge$, $\mathcal{D}_\wedge$, and $\mathcal{L}_\vee$, $\mathcal{R}_\vee$, $\mathcal{D}_\vee$. By Leech's First Decomposition Theorem [126, Theorem 1.7], Green's relations $\mathcal{D}_\wedge$ and $\mathcal{D}_\vee$ coincide on any skew lattice $(S, \wedge, \vee)$. This relation, simply denoted by $\mathcal{D}$, is a congruence, $S/\mathcal{D}$ is the maximal lattice image of S, and each $\mathcal{D}$-class is a rectangular skew lattice. Moreover, on a skew lattice S we obtain $\mathcal{R}_\vee = \mathcal{L}_\wedge$, simply denoted by $\mathcal{L}$, and $\mathcal{R}_\wedge = \mathcal{L}_\vee$, simply denoted by $\mathcal{R}$. A skew lattice is called *left-handed* if $\mathcal{L} = \mathcal{D}$, and it is called *right-handed* if $\mathcal{R} = \mathcal{D}$. In other words, a skew lattice $(S, \wedge, \vee)$ is left-handed if and only if, for any $x, y, z \in S$,

$$x \wedge y \wedge x = x \wedge y, \text{ or equivalently, } x \vee y \vee x = y \vee x. \tag{5.4}$$

It is right-handed if and only if

$$x \wedge y \wedge x = y \wedge x, \text{ or equivalently, } x \vee y \vee x = x \vee y, \tag{5.5}$$

for all $x, y, z \in S$. Leech's Second Decomposition Theorem for skew lattices [126, Theorem 1.15], a skew lattice version of Kimura's result for regular bands [115, Theorem 4], states that Green's relations $\mathcal{L}$ and $\mathcal{R}$ are congruences on any skew lattice $(S, \wedge, \vee)$. Furthermore, S factors as a fiber product of a left-handed skew lattice $S/\mathcal{R}$, called the left factor of S, by a right-handed skew lattice $S/\mathcal{L}$, called the right factor of S, over their common maximal lattice image. In particular, if $(S, \wedge, \vee)$ is a rectangular skew lattice (which is equivalent to S having exactly one $\mathcal{D}$-class), then S factors as a direct product $S \cong L \times R$ of a left-zero semigroup L, by a right-zero semigroup R.

On a skew lattice $(S, \wedge, \vee)$, we can define a *natural preorder* $\preceq$, by

$$x \preceq y \quad \text{if and only if} \quad x \wedge y \wedge x = x,$$

or equivalently, if and only if $y \vee x \vee y = y$. Note that $x \preceq y$ and $y \preceq x$ if and only if $x \, \mathcal{D} \, y$. Furthermore, $x \preceq y$ in S is equivalent with $\mathcal{D}_x \leq \mathcal{D}_y$ in the lattice $S/\mathcal{D}$, where $\mathcal{D}_z = \{t \in S \mid z \, \mathcal{D} \, t\}$ is the $\mathcal{D}$-class of $z \in S$. The *natural partial order*, denoted by $\leq$, is given by

$$x \leq y \quad \text{if and only if} \quad x \wedge y = x = y \wedge x, \tag{5.6}$$

or equivalently, if and only if $x \vee y = y = y \vee x$. Note that, for any $x, y \in S$, $x \leq y$ implies $x \preceq y$.

The natural partial order allows us to draw diagrams representing visual images of skew lattices. This diagram is called a *Hasse diagram.* Full down edges indicate elements related by the natural partial order, with $a \leq b$ if a is below b, and horizontal dash edges indicate that two elements are $\mathcal{D}$-related. For lattices, the Hasse diagram uniquely defines both operations of the lattice. This, however, is no longer true for skew lattices. This can be seen by the skew lattices $(\{a, b\}, \wedge_1, \vee_1)$ and $(\{a, b\}, \wedge_2, \vee_2)$ with operations defined by

$$\begin{array}{c|cc} \wedge_1 & \mathrm{a} & \mathrm{b} \\ \hline \mathrm{a} & \mathrm{a} & \mathrm{a} \\ \mathrm{b} & \mathrm{b} & \mathrm{b} \end{array}\;, \qquad \begin{array}{c|cc} \vee_1 & \mathrm{a} & \mathrm{b} \\ \hline \mathrm{a} & \mathrm{a} & \mathrm{b} \\ \mathrm{b} & \mathrm{a} & \mathrm{b} \end{array}\;,$$

and $x \wedge_2 y = x \vee_1 y$, $x \vee_2 y = x \wedge_1 y$, for all $x, y \in \{a, b\}$. Both skew lattices can be represented by the Hasse diagram below.

$$a \text{ - - - - - } b$$

The following significant result has contributed to fruitful progress in the theory of skew lattices.

Theorem 5.1.2 (Cvetko-Vah [64, Corollary 3])**.** *A skew lattice satisfies an identity or an equational implication if and only if both its left and right factor satisfy this identity or equational implication.*

Thus, to prove a result for a skew lattice $(S, \wedge, \vee)$, it is enough to prove it first assuming that S is left-handed (satisfying (5.4)), and next assuming that S is right-handed (satisfying (5.5)). We will use this fact frequently in what follows.

5.1.2 Varieties of skew lattices

A class of algebras is called a *variety* if it is closed under homomorphic images, substructures, and direct products. By Birkhoff's Theorem [29, Theorem 11.9] a class of algebras is a variety if and only if it is equationally defined, i.e. if it is defined by a set of identities.

Throughout this chapter several varieties are defined. A fundamental one among them is symmetry [126, Subsection 2.3]. A skew lattice $(S, \wedge, \vee)$ is said to be *symmetric* if

$$x \wedge y = y \wedge x \quad \text{if and only if} \quad x \vee y = y \vee x, \tag{5.7}$$

for all $x, y \in S$. A skew lattice $(S, \wedge, \vee)$ is called *normal* (resp. *conormal*) if

$$x \wedge y \wedge z \wedge x = x \wedge z \wedge y \wedge x, \quad (\text{resp. } x \vee y \vee z \vee x = x \vee z \vee y \vee x), \tag{5.8}$$

for all $x, y, z \in S$. A *binormal* skew lattice is a skew lattice that is both normal and conormal. Binormal skew lattices factor as a direct product of a lattice with a rectangular algebra [171].

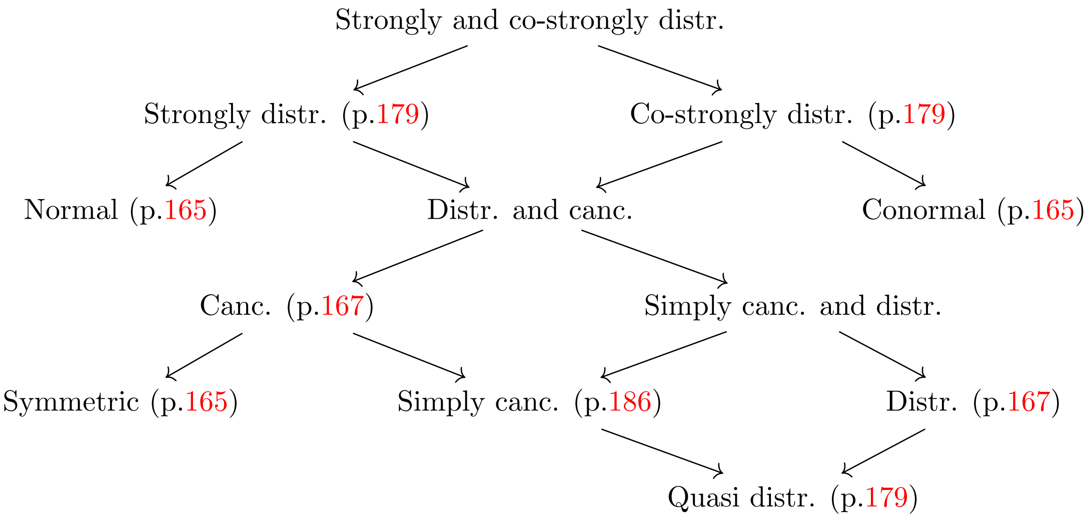
Remark 5.1.3. *Note that the condition of normality (resp. conormality) is in fact equivalent to*

$$x \wedge y \wedge z \wedge w = x \wedge z \wedge y \wedge w, \quad (\textit{resp. } x \vee y \vee z \vee w = x \vee z \vee y \vee w). \tag{5.9}$$

Indeed, using normality, and associativity and idempotency of $\wedge$, we obtain

$$\begin{aligned}
x \wedge y \wedge z \wedge w &= (x \wedge y \wedge z \wedge w) \wedge (x \wedge y \wedge z \wedge w) \\
&= x \wedge y \wedge (z \wedge w \wedge x \wedge y \wedge z) \wedge w \\
&= (x \wedge y \wedge z \wedge x) \wedge y \wedge w \wedge z \wedge w \\
&= x \wedge (z \wedge y \wedge x \wedge y \wedge w \wedge z) \wedge w \\
&= x \wedge z \wedge y \wedge (w \wedge y \wedge x \wedge z \wedge w) \\
&= (x \wedge z \wedge y \wedge w) \wedge (x \wedge z \wedge y \wedge w) \\
&= x \wedge z \wedge y \wedge w.
\end{aligned}$$

The equality $x \vee y \vee z \vee w = x \vee z \vee y \vee w$ can be proven similarly using conormality.



The diagram above presents an overview of the varieties used in this chapter. The reader might find this diagram useful when thinking about the partial order between different varieties of skew lattices. There can be other varieties of skew lattices that are not shown in the diagram and lie in between the varieties that are shown. The diagram, therefore, provides the information regarding the partial order on the set of listed varieties, but it does not imply, for instance, that quasi-distributive skew lattices form the join of simply cancellative skew lattices and distributive skew lattices.

5.1.3 Skew lattices in rings

Let $(R,+,\cdot)$ be a ring and $E.(R) = \{e \in R \mid e^2 = e\}$ the set of idempotents in $(R,\cdot)$. Given $x,y \in E.(R)$, xy is not necessarily idempotent. We say that a subset S of $E.(R)$ is a *multiplicative band* in R if for any $x,y \in S$, we have $xy \in S$. Given a multiplicative band S in a ring R, defining the meet operation as the multiplication, there are two natural ways to define the join operation on S,

(i) The *quadratic join*: $x \circ y = x + y - xy$, for all $x,y \in S$.

(ii) The *cubic join*: $x \nabla y = (x \circ y)^2 = x + y + yx - xyx - yxy$, for all $x,y \in S$.

In general, given $x,y \in E.(R)$, $x \circ y$ is not necessarily in $E.(R)$. If $x \circ y \in E.(R)$, then $x \nabla y = x \circ y$. When $E.(R)$ is a multiplicative band in R, we obtain $x \nabla y \in E.(R)$, for all $x,y \in E.(R)$. However, ∇ is not necessarily associative. So, in general, $(S,\cdot,\circ)$ and $(S,\cdot,\nabla)$ are not necessarily skew lattices for a multiplicative band S in R. In some cases, we do obtain skew lattices. The following results are proven in [126], for any ring $(R,+,\cdot)$,

(i) If $(S,\cdot)$ is a multiplicative band in R that is closed under the quadratic join $\circ$, then $(S,\cdot,\circ)$ is a skew lattice, called a *quadratic skew lattice*.

(ii) If $(S,\cdot)$ is a multiplicative band in R that is also closed under ∇, with ∇ being associative on S, then $(S,\cdot,\nabla)$ is a skew lattice, called a *cubic skew lattice*.

A band $(S,\cdot)$ is called *right regular* (resp. *left regular*) if for any $x,y \in S$, $xyx = yx$ (resp. $xyx = xy$). It is called *normal* if $xyzx = xzyx$, or equivalently $xyzt = xzyt$, for all $x,y,z,t \in S$. The following results are proven in [126] and [127].

(i) Any maximal left or right regular band in a ring forms a quadratic skew lattice. Any left or right regular band in a ring generates a quadratic skew lattice.

(ii) Any maximal normal band in a ring forms a normal cubic skew lattice. Any normal band in a ring generates a normal cubic skew lattice.

5.2 Constructions of skew lattices

It will become clear that skew lattices are a fundamental algebraic structure to produce set-theoretic solutions of the Yang-Baxter equation, that are either idempotent or cubic.

Consequently, finding ways to construct skew lattices out of sets or other skew lattices is worth its attention. In this part, we present multiple constructions and discuss whether certain properties are inherited.

To start, we construct a skew lattice on an arbitrary family of pairwise disjoint sets, following [69, Section 2] (Cvetko-Vah and Verwimp). The constructed skew lattice is both distributive and cancellative. A skew lattice is said to be *(fully) cancellative* if the following pair of implications hold,

$$x \vee y = x \vee z,\, x \wedge y = x \wedge z \quad \text{implies} \quad y = z, \tag{5.10}$$

$$x \vee z = y \vee z,\, x \wedge z = y \wedge z \quad \text{implies} \quad x = y. \tag{5.11}$$

A skew lattice satisfying (5.10) (resp. (5.11)) is called *left* (resp. *right*) *cancellative*. Cancellative skew lattices were introduced in [126], and intensively studied in [65], where it was shown that they form a variety. A skew lattice is called *distributive* [126] if the following pair of identities are satisfied,

$$x \wedge (y \vee z) \wedge x = (x \wedge y \wedge x) \vee (x \wedge z \wedge x), \tag{5.12}$$

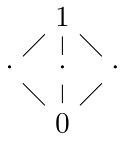
$$x \vee (y \wedge z) \vee x = (x \vee y \vee x) \wedge (x \vee z \vee x). \tag{5.13}$$

For lattices, the identities (5.12) and (5.13) agree. By [175, Theorem 2.3], both identities also agree for symmetric skew lattices. However, for arbitrary skew lattices they are not necessarily equivalent. A counterexample to this is provided in [175]. There exists a different notion for distributivity of lattices. A lattice $(L, \wedge, \vee)$ is called *distributive* if, for any $x, y, z \in L$,

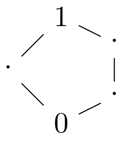
$$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z), \text{ and } x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z). \tag{5.14}$$

Later, we will see that there are several ways to generalize the notion of distributivity to the non-commutative setting. A thorough study of distributivity in skew lattices can be found in [116]. For lattices, all these definitions are equal to the definition of distributivity of a lattice given above. Moreover, while for skew lattices cancellation and distributivity are two different concepts, they agree for lattices. So a lattice is cancellative if and only if it is distributive [130, Theorem 1.1.3]. Another third characterization is that the lattices M_3 nor N_5, with Hasse diagrams given below, can be embedded in the given lattice [130].

M_3:



N_5:



Alongside a construction of a skew lattice on a family of pairwise disjoint sets, we provide several constructions of skew lattices $(S, \wedge, \vee)$ given a family of pairwise disjoint skew lattices $\{(S_i, \wedge_i, \vee_i) \mid i \in I\}$, such that $S = \bigcup_{i \in I} S_i$. We also study if properties (like cancellativity and distributivity) on the skew lattices S_i, $i \in I$, are inherited by the skew lattice S.

5.2.1 Construction on a family of pairwise disjoint sets

Let $(I,\leq)$ be a totally ordered set and $S = \dot{\bigcup}_{i\in I} A_i$ the disjoint union of a family of pairwise disjoint sets A_i, $i \in I$. For any $x, y \in S$ with $i, j \in I$ such that $x \in A_i$, $y \in A_j$, we define the meet and join operation on S as

$$x \wedge y = \begin{cases} x & \text{if } i < j \\ y & \text{if } j \leq i \end{cases}, \qquad x \vee y = \begin{cases} y & \text{if } i < j \\ x & \text{if } j \leq i \end{cases}.$$

Proposition 5.2.1. *Let $(I,\leq)$ be a totally ordered set and $S = \dot{\bigcup}_{i\in I} A_i$ a disjoint union of a family of pairwise disjoint sets. Then, $(S,\wedge,\vee)$ is a distributive and cancellative skew lattice, where $\wedge$ and $\vee$ are defined as above.*

Proof. Both $x \wedge (y \wedge z)$ and $(x \wedge y) \wedge z$ reduce to the minimal element of $\{x,y,z\}$ that appears most right in the expression $x \wedge y \wedge z$. Similarly, $x \vee (y \vee z)$ and $(x \vee y) \vee z$ both reduce to the maximal element of $\{x,y,z\}$ that appears most left in the expression $x \vee y \vee z$. Hence, both $\wedge$ and $\vee$ are associative operations. It is also clear that both operations are idempotent.

To prove the absorption laws (5.1), let $x \in A_i$, $y \in A_j$. Assume first that $i < j$. Then, $x \wedge (x \vee y) = x \wedge y = x$. On the other hand, if $j \leq i$ then $x \wedge (x \vee y) = x \wedge x = x$. The other absorption laws are proven similarly.

Given $x \in A_i$ and $y \in A_j$, the expression $x\,\mathcal{D}\,y$ is equivalent to $i = j$. Moreover, $x \in A_i$ commutes with $y \in A_j$ for either of the operations $\wedge$, $\vee$, if and only if $i \neq j$. By construction, S is a skew chain, meaning that its maximal lattice image $S/\mathcal{D}$ is totally ordered (in our case, isomorphic to I). By [63, Proposition 5], skew chains are always cancellative.

It remains to prove that $(S,\wedge,\vee)$ is distributive. Take any $x,y,z \in S$ with $i,j,k \in I$ such that $x \in A_i$, $y \in A_j$, and $z \in A_k$, and consider the elements $\alpha = x \wedge (y \vee z) \wedge x$ and $\beta = (x \wedge y \wedge x) \vee (x \wedge z \wedge x)$. To prove that (5.12) holds, we need to show that $\alpha = \beta$. If $j = k$, then $y\,\mathcal{D}\,z$, and thus $(x \wedge y \wedge x)\,\mathcal{D}\,(x \wedge z \wedge x)$. This means that there exists $l \in I$ such that $x \wedge y \wedge x$ and $x \wedge z \wedge x$ both lie in A_l. It follows that $\alpha = x \wedge y \wedge x$ and, likewise, $\beta = x \wedge y \wedge x$. If $j \neq k$, then y and z commute for both operations $\wedge$, $\vee$, with either $y \wedge z = z \wedge y = y$ and $y \vee z = z \vee y = z$, or $y \wedge z = z \wedge y = z$ and $y \vee z = z \vee y = y$. Thus, by the definition of the natural partial order (5.6), we have either $y < z$ or $z < y$, as $y \neq z$. If $y < z$ then, by regularity (5.2), $x \wedge y \wedge x \wedge x \wedge z \wedge x = x \wedge y \wedge z \wedge x = x \wedge y \wedge x$, and thus $x \wedge y \wedge x \leq x \wedge z \wedge x$. It follows that $\alpha = x \wedge z \wedge x = \beta$. Similarly, if $z < y$, then $\alpha = x \wedge y \wedge x = \beta$, as desired. The proof of (5.13) is similar, hence the result. □

5.2.2 Constructions on a family of pairwise disjoint skew lattices

Given a set I and a family of pairwise disjoint skew lattices $\{(S_i,\wedge_i,\vee_i) \mid i \in I\}$, we present several constructions of skew lattices $(S,\wedge,\vee)$ such that $S = \bigcup_{i\in I} S_i$. We also study if properties, like cancellativity and distributivity, on the skew lattices S_i, $i \in I$, are inherited by the skew lattice S. The results of Subsection 5.2.2 are personal, new, and unpublished.

A simple construction technique is given by considering the direct product of skew lattices and defining the operations componentwise. If all given skew lattices are distributive (resp. left/right/fully cancellative), then, of course, their direct product is also distributive (resp. left/right/fully cancellative). Another construction that we will establish can visually be seen as putting the given skew lattices in one vertical line. The meet of two elements of different skew lattices is equal to the element of the skew lattice with the lowest position, while their join is equal to the element of the skew lattice with the highest position.

Proposition 5.2.2. *Let $(I, \leq)$ be a finite or countable totally ordered set, and $(S_i, \wedge_i, \vee_i)$, $i \in I$, a family of pairwise disjoint skew lattices. Then, $(S = \bigcup_{i \in I} S_i, \wedge, \vee)$ is a skew lattice, where for any $s_i \in S_i, s'_j \in S_j$,*

$$s_i \wedge s'_j = \begin{cases} s_i \wedge_i s'_j & \textit{if } i = j \\ s_i & \textit{if } i < j \\ s'_j & \textit{if } j < i \end{cases},$$

and

$$s_i \vee s'_j = \begin{cases} s_i \vee_i s'_j & \textit{if } i = j \\ s'_j & \textit{if } i < j \\ s_i & \textit{if } j < i \end{cases}.$$

If all skew lattices S_i, $i \in I$, are distributive (resp. left/right/fully cancellative), then S is distributive (resp. left/right/fully cancellative).

Proof. It is easy to see that both $\wedge$ and $\vee$ are idempotent binary operations. Let $x, y, z \in X$. Then $(x \wedge y) \wedge z$, but also $x \wedge (y \wedge z)$, is equal to (the meet of) the element(s) of the skew lattice with the lowest index. Hence, the operation $\wedge$, and similarly $\vee$, is associative.

To show that $(S, \wedge, \vee)$ is a skew lattice, we are left to prove that (5.1) is satisfied. Let $s_i \in S_i, s'_j \in S_j$, with $i \neq j$. First, we prove that $s_i \wedge (s_i \vee s'_j) = s_i$. Indeed, if $i < j$, then $s_i \wedge (s_i \vee s'_j) = s_i \wedge s'_j = s_i$. While, if $j < i$, then $s_i \wedge (s_i \vee s'_j) = s_i \wedge s_i = s_i$. Next, we prove that $s_i \vee (s_i \wedge s'_j) = s_i$. If $j < i$, then $s_i \vee (s_i \wedge s'_j) = s_i \vee s'_j = s_i$. Next, if $i < j$, then $s_i \vee (s_i \wedge s'_j) = s_i \vee s_i = s_i$. Similarly, one can prove that $(s'_j \vee s_i) \wedge s_i = s_i$ and $(s'_j \wedge s_i) \vee s_i = s_i$.

Assume that all skew lattices S_i, $i \in I$, are distributive, i.e. satisfying (5.12) and (5.13). We need to prove that, for any $x, y, z \in S$, $x \wedge (y \vee z) \wedge x = (x \wedge y \wedge x) \vee (x \wedge z \wedge x)$ and $x \vee (y \wedge z) \vee x = (x \vee y \vee x) \wedge (x \vee z \vee x)$ hold. If x, y, z are elements of the same skew lattice S_i, the result is clear. Assume that $x, y \in S_i$ and $z \in S_j$, for some $i \neq j \in I$. Then,

$$x \wedge (y \vee z) \wedge x = (x \wedge y \wedge x) \vee (x \wedge z \wedge x) = \begin{cases} x & \text{if } i < j \\ x \wedge y \wedge x & \text{if } j < i \end{cases},$$

similarly $x \wedge (z \vee y) \wedge x = (x \wedge z \wedge x) \vee (x \wedge y \wedge x)$, and

$$z \wedge (x \vee y) \wedge z = (z \wedge x \wedge z) \vee (z \wedge y \wedge z) = \begin{cases} x \vee y & \text{if } i < j \\ z & \text{if } j < i \end{cases}.$$

If $x \in S_i, y \in S_j$ and $z \in S_k$ for different elements $i, j, k \in I$, then

$$x \wedge (y \vee z) \wedge x = (x \wedge y \wedge x) \vee (x \wedge z \wedge x) = \begin{cases} x & \text{if } i < \max\{j, k\} \\ y & \text{if } k < j < i \\ z & \text{if } j < k < i \end{cases}.$$

Similarly, $x \vee (y \wedge z) \vee x = (x \vee y \vee x) \wedge (x \vee z \vee x)$ holds, for all $x, y, z \in S$.

Assume that all skew lattices S_i, $i \in I$, are left cancellative, i.e. satisfying (5.10). We need to prove that (5.10) holds, for all $x, y, z \in S$. If $x, y, z \in S_i$ for some $i \in I$, then (5.10) follows from left cancellation of S_i. Let $x \in S_i, y, z \in S_j$ for some $i \neq j$, and assume that $x \wedge y = x \wedge z$ and $x \vee y = x \vee z$. Then,

$$y = (x \wedge y) \vee y = (x \wedge z) \vee y = \begin{cases} y & \text{if } i < j \\ z \vee y & \text{if } j < i \end{cases},$$

$$y = (x \vee y) \wedge y = (x \vee z) \wedge y = \begin{cases} z \wedge y & \text{if } i < j \\ y & \text{if } j < i \end{cases}.$$

So, if $i < j$, then $y = z \wedge y$, and if $j < i$, then $y = z \vee y$. Similarly, one can prove that if $i < j$, then $z = y \wedge z$, and if $j < i$, then $z = y \vee z$. Hence, if $i < j$, then

$$y = y \vee (y \wedge z) = y \vee z \geq z,$$
$$z = z \vee (z \wedge y) = z \vee y \geq y.$$

Furthermore, if $j < i$,

$$y = y \wedge (y \vee z) = y \wedge z \leq z,$$
$$z = z \wedge (z \vee y) = z \wedge y \leq y.$$

We conclude that $y = z$.

Assume now that $x \wedge y = x \wedge z$ and $x \vee y = x \vee z$, for some $x, y \in S_i, z \in S_j$ and $i \neq j$. As $x \wedge z = x \wedge y \in S_i$, we need that $i < j$. Similarly, because $x \vee z = x \vee y \in S_i$, we need that $j < i$, which is a contradiction.

Let $x \in S_i, y \in S_j, z \in S_k$, for different i, j, and k in I, and assume that $x \wedge y = x \wedge z$ and $x \vee y = x \vee z$. However, note that this only holds if $\min\{i, j\} = \min\{i, k\}$ and $\max\{i, j\} = \max\{i, k\}$. For simplicity denote $i \wedge j = \min\{i, j\}$ and $i \vee j = \max\{i, j\}$, for all $i, j \in I$. Note that $(I, \wedge, \vee)$ is a distributive lattice. Then,

$$j = (i \wedge j) \vee j = (i \wedge k) \vee j = (i \vee j) \wedge (k \vee j) = (i \vee k) \wedge (k \vee j) \geq k,$$
$$k = (i \wedge k) \vee k = (i \wedge j) \vee k = (i \vee k) \wedge (j \vee k) = (i \vee j) \wedge (j \vee k) \geq j.$$

This contradicts the assumption $j \neq k$.

Starting from right cancellative skew lattices, i.e. satisfying (5.11), the right cancellativity of S is proven similarly. Hence, the result follows. □

The assumption in Proposition 5.2.2 that I is a totally ordered set is rather strong. In the upcoming construction, we only assume that I is a lattice. However, in this case, some extra conditions on the given skew lattices are needed. More precisely, every skew lattice $(S_i, \wedge_i, \vee_i)$ needs a top element 1_i and a bottom element 0_i, satisfying $0_i \wedge_i s_i = 0_i = s_i \wedge_i 0_i$, $0_i \vee_i s_i = s_i = s_i \vee_i 0_i$, $1_i \wedge_i s_i = s_i = s_i \wedge_i 1_i$, $1_i \vee_i s_i = 1_i = s_i \vee_i 1_i$, for all $s_i \in S_i$, and $0_i \wedge_i 1_i = 0_i = 1_i \wedge_i 0_i$, $0_i \vee_i 1_i = 1_i = 1_i \vee_i 0_i$.

Proposition 5.2.3. *Let $(I, \wedge, \vee)$ be a finite or countable lattice and let $(S_i, \wedge_i, \vee_i)$, $i \in I$, be a family of pairwise disjoint skew lattices such that S_i contains a top and bottom element 0_i and 1_i respectively, for all $i \in I$. Then, $(S = \dot\bigcup_{i \in I} S_i, \wedge, \vee)$ is a skew lattice defined by, for any $s_i \in S_i, s'_j \in S_j$,*

$$s_i \wedge s'_j = \begin{cases} s_i \wedge_i s'_j & \text{if } i = j \\ s_i & \text{if } i < j \\ s'_j & \text{if } j < i \\ 1_k & \text{if } i \wedge j = k, k \neq i, k \neq j \end{cases},$$

and

$$s_i \vee s'_j = \begin{cases} s_i \vee_i s'_j & \text{if } i = j \\ s_i & \text{if } j < i \\ s'_j & \text{if } i < j \\ 0_k & \text{if } i \vee j = k, k \neq i, k \neq j \end{cases}.$$

Proof. It is easy to see that both $\wedge$ and $\vee$ are idempotent binary operations. To prove associativity for $\wedge$, let $s_i \in S_i, s'_j \in S_j, s''_k \in S_k$. If $i = j = k$, then the associativity follows from the associativity of $\wedge_i$. Next, assume that $i = j \neq k$. Then, it is clear that $(s_i \wedge s'_i) \wedge s''_k = s_i \wedge (s'_i \wedge s''_k)$ and $s''_k \wedge (s_i \wedge s'_i) = (s''_k \wedge s_i) \wedge s'_i$. Furthermore,

$$s_i \wedge (s''_k \wedge s'_i) = \begin{cases} s_i \wedge s'_i & \text{if } i < k \\ s''_k & \text{if } k < i \\ 1_l & \text{if } k \wedge i = l, l \neq i, l \neq k \end{cases},$$

and

$$(s_i \wedge s''_k) \wedge s'_i = \begin{cases} s_i \wedge s'_i & \text{if } i < k \\ s''_k & \text{if } k < i \\ 1_l & \text{if } i \wedge k = l, l \neq i, l \neq k \end{cases}.$$

As $(I, \wedge, \vee)$ is a lattice, $i \wedge k = k \wedge i$, so $s_i \wedge (s''_k \wedge s'_i) = (s_i \wedge s''_k) \wedge s'_i$. Finally, assume that $i \neq j \neq k$. Then,

$$s_i \wedge (s'_j \wedge s''_k) = \begin{cases} s_i & \text{if } i < j \text{ and } i < k \\ s'_j & \text{if } j < i \text{ and } j < k \\ s''_k & \text{if } k < i \text{ and } k < j \\ 1_l & \text{if } i \wedge (j \wedge k) = l, l \neq i, l \neq j, l \neq k \end{cases},$$

and

$$(s_i \wedge s'_j) \wedge s''_k = \begin{cases} s_i & \text{if } i < j \text{ and } i < k \\ s'_j & \text{if } j < i \text{ and } j < k \\ s''_k & \text{if } k < i \text{ and } k < j \\ 1_l & \text{if } (i \wedge j) \wedge k = l, l \neq i, l \neq j, l \neq k \end{cases}.$$

Hence, $s_i \wedge (s'_j \wedge s''_k) = (s_i \wedge s'_j) \wedge s''_k$ and $\wedge$ is an associative operation. Similarly, one shows that $\vee$ is an associative operation.

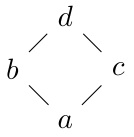
We are left to prove that $\wedge$ and $\vee$ satisfy the absorption laws (5.1). Let $s_i \in S_i, s'_j \in S_j$ with $i \neq j$. First, we prove that $s_i \wedge (s_i \vee s'_j) = s_i$. Indeed, if $i \vee j = k$, for $i \neq k, j \neq k$, then $i \wedge k = i$ because of the absorption laws in the lattice I. Hence, in this case, $s_i \wedge (s_i \vee s'_j) = s_i \wedge 0_k = s_i$. If $i < j$, then $s_i \wedge (s_i \vee s'_j) = s_i \wedge s_j = s_i$, and if $j < i$, then $s_i \wedge (s_i \vee s'_j) = s_i \wedge s_i = s_i$. Similarly, one can prove that $s_i \vee (s_i \wedge s'_j) = s_i$, $(s'_j \vee s_i) \wedge s_i = s_i$, and $(s'_j \wedge s_i) \vee s_i = s_i$. □

If some skew lattices do not contain a top and bottom element, one can simply add these elements to the skew lattice. Hence, the previous proposition is still applicable.

Corollary 5.2.4. *Let $(I, \wedge, \vee)$ be a finite or countable lattice and let $(S_i, \wedge_i, \vee_i)$, $i \in I$, be a family of pairwise disjoint skew lattices. Add to each skew lattice S_i, that does not contain a bottom (resp. top) element, the element 0_i (resp. 1_i) such that $0_i \wedge_i s_i = 0_i = s_i \wedge_i 0_i$ and $0_i \vee_i s_i = s_i = s_i \vee_i 0_i$ (resp. $1_i \wedge_i s_i = s_i = s_i \wedge_i 1_i$ and $1_i \vee_i s_i = 1_i = s_i \vee_i 1_i$), for all $s_i \in S_i$, and such that $0_i \wedge 1_i = 0_i = 1_i \wedge 0_i$ and $0_i \vee 1_i = 1_i = 1_i \vee 0_i$, if both elements are added. Then, $(S = \biguplus_{i \in I} S_i, \wedge, \vee)$ is a skew lattice, where the operations $\wedge$ and $\vee$ are defined as in Proposition 5.2.3.*

For the constructions of Proposition 5.2.3 and Corollary 5.2.4, properties like distributivity and cancellativity will not necessarily be inherited. This makes sense since the used lattice $(I, \wedge, \vee)$ does not have to be distributive. However, even in the distributive case there are counterexamples.

Example 5.2.5. *Let $(I, \wedge, \vee)$, with $I = \{a, b, c, d\}$, be the distributive lattice defined by the Hasse diagram below.*



Let $S_i, i \in I$ be a family of pairwise disjoint distributive skew lattices and assume that there exist $x, y \in S_b$ such that $y < x$ (take for example $0_b < 1_b$, if $|S_b| \geq 2$). For $z \in S_c$, we get

$$x \wedge (y \vee z) \wedge x = x \wedge 0_d \wedge x = x,$$

while

$$(x \wedge y \wedge x) \vee (x \wedge z \wedge x) = y \vee 1_a = y.$$

If all skew lattices $S_i, i \in I$ are left/right/fully cancellative, the above constructed skew lattice is not necessarily left/right/fully cancellative. For example, if $|S_c| \geq 2$, take $x \in S_b$ and

$$x \wedge 0_c = 1_a = x \wedge 1_c \text{ and } x \vee 0_c = 0_d = x \vee 1_c,$$

and similarly

$$0_c \wedge x = 1_a = 1_c \wedge x \text{ and } 0_c \vee x = 0_d = 1_c \vee x,$$

but $0_c \neq 1_c$ if $|S_c| \geq 2$.

To end this part, we show that the constructed skew lattices from Proposition 5.2.2, Proposition 5.2.3, and Corollary 5.2.4 do not necessarily inherit normality and conormality. For example, consider $I = \{0, 1\}$ the lattice with two elements on top of each other (1 above 0). Let $(S_0, \wedge_0, \vee_0)$ and $(S_1, \wedge_1, \vee_1)$ be two normal skew lattices, such that there exists $x, y \in S_0$ with $x \wedge_0 y \neq y \wedge_0 x$. Then, for $z \in S_1$, we get $z \wedge x \wedge y \wedge z = x \wedge y$, while $z \wedge y \wedge x \wedge z = y \wedge x$. A counterexample for conormal skew lattices is given in the same manner.

5.3 Solutions obtained from general skew lattices

In Section 1.3, the importance of several algebraic structures became clear by connecting them to set-theoretic solutions of the Yang-Baxter equation. In this section, we follow [69, Section 3] (Cvetko-Vah and Verwimp), focus on arbitrary skew lattices, and study how they provide set-theoretic solutions of the Yang-Baxter equation. Using only one of the binary operations of a skew lattice $(S, \wedge, \vee)$, we already obtain many solutions as both $(S, \wedge)$ and $(S, \vee)$ are bands. Hence, we get solutions by, for example, putting $r(x, y) = (x \wedge y, y)$ or $r(x, y) = (x, x \vee y)$, see also Section 1.3. In this section, however, we determine non-trivial solutions where the map r of the solution is defined using both binary operations of an arbitrary skew lattice. It turns out that the found solutions are of idempotent type, and thus of importance as shown in [120].

Before we dive into this result, we need to define the lower update of two elements of a skew lattice [68]. Let $(S, \wedge, \vee)$ be a skew lattice and $x, y \in S$. The *lower update* of x by y is defined as

$$x\lfloor y \rfloor = (y \wedge x \wedge y) \vee x \vee (y \wedge x \wedge y).$$

The *upper update* of x by y is defined similarly, i.e. $x\lceil y \rceil = (y \vee x \vee y) \wedge x \wedge (y \vee x \vee y)$. It turns out that there is no unique definition for an update operation of a skew lattice.

One can find several definitions in [68]. We now only focus on the lower update. Note however that similar results can be obtained for the upper update.

Let $(S, \wedge, \vee)$ be a skew lattice and $x, y \in S$. Then, $x\lfloor y \rfloor \in \mathcal{D}_x$. Indeed, by the absorption laws (5.1), we obtain

$$\begin{aligned} x \vee x\lfloor y \rfloor \vee x &= x \vee (y \wedge x \wedge y) \vee x \vee (y \wedge x \wedge y) \vee x \\ &= x \vee (y \wedge x \wedge y) \vee x \\ &= (y \wedge x) \vee x \vee (y \wedge x \wedge y) \vee x \\ &= (y \wedge x) \vee (y \wedge x \wedge y) \vee x \vee (y \wedge x \wedge y) \vee x \\ &= (y \wedge x) \vee (y \wedge x \wedge y) \vee x \\ &= (y \wedge x) \vee x \\ &= x, \end{aligned}$$

and it is clear that $x\lfloor y \rfloor \vee x \vee x\lfloor y \rfloor = x\lfloor y \rfloor$. If a skew lattice is left-handed, satisfying (5.4) (resp. right-handed, satisfying (5.5)), then the lower update can be simplified to $x\lfloor y \rfloor = x \vee (y \wedge x)$ (resp. $x\lfloor y \rfloor = (x \wedge y) \vee x$).

To prove Lemma 5.3.3 below, we need to recall some further facts and definitions from skew lattice theory in the following remark, which is based on results of [128] where the geometric structure of a skew lattice is studied. Given a skew lattice $(S, \wedge, \vee)$ with comparable $\mathcal{D}$-classes A, B such that $A > B$ holds in the lattice $S/\mathcal{D}$, a *coset of A in B* is a subset $A \wedge b \wedge A = \{a \wedge b \wedge a' \mid a, a' \in A\} \subseteq B$, with $b \in B$. Likewise, a *coset of B in A* is a subset $B \vee a \vee B = \{b \vee a \vee b' \mid b, b' \in B\} \subseteq A$, where $a \in A$. Cosets of skew lattices are studied in, for example, [66, 67, 128, 153, 154, 155].

Remark 5.3.1. *Let $(S, \wedge, \vee)$ be a skew lattice with $\mathcal{D}$-classes A, B such that $A > B$ holds in $S/\mathcal{D}$. By [128], the cosets of A in B form a partition of B, and similarly, the cosets of B in A form a partition of A. By [67, Proposition 7], elements a, a' of A lie in a common coset of B in A if and only if $b \vee a \vee b = b \vee a' \vee b$, for all $b \in B$, which is further equivalent to $b \vee a \vee b = b \vee a' \vee b$, for some $b \in B$. A dual similarity holds for elements $b, b' \in B$ that lie in a common coset of A in B. Moreover, given any coset B_j of A in B and any coset A_i of B in A, there exists a bijection $\varphi_{ji} : A_i \to B_j$ which maps an element $x \in A_i$ to the unique element $y \in B_j$ with the property $y \leq x$, with respect to the natural partial order* (5.6)*.*

In order to prove that a pair of elements of A are equal, it thus suffices to show that they lie in the same coset of B in A and that they are both above the same element of B with respect to the natural partial order (5.6)*. Likewise, a pair of elements of B are equal if and only if they lie in the same coset of A in B and are both below the same element of A with respect to the natural partial order* (5.6)*.*

In [68, Theorem 4.3], other properties of the update operation are proven. We mention those that are needed in this section.

Theorem 5.3.2 (Cvetko-Vah and Pita Costa [68, Theorem 4.3])**.** *Let $(S, \wedge, \vee)$ be a skew lattice, and $x, y \in S$. Put $M = \mathcal{D}_x \wedge \mathcal{D}_y = \{a \wedge b \mid a \in \mathcal{D}_x, b \in \mathcal{D}_y\}$, then*

(1) $x\lfloor y\rfloor$ *is the unique element of the coset* $M\vee x\vee M$ *in* $\mathcal{D}_x$ *such that* $y\wedge x\wedge y\leq x\lfloor y\rfloor$*,*

(2) $x\lfloor y\rfloor\wedge y=y\wedge x\wedge y=y\wedge x\lfloor y\rfloor$*.*

The technique from Remark 5.3.1 is applied in the proof of Lemma 5.3.3 below.

Lemma 5.3.3. *Let* $(S,\wedge,\vee)$ *be a skew lattice and* $x,y,z\in S$*. Then,*

$$(x\lfloor y\rfloor)\lfloor y\lfloor z\rfloor\rfloor=x\lfloor y\lfloor z\rfloor\rfloor. \tag{5.15}$$

Proof. Denote $M=\mathcal{D}_x\wedge\mathcal{D}_y=\{a\wedge b\mid a\in\mathcal{D}_x,b\in\mathcal{D}_y\}$. The element $(x\lfloor y\rfloor)\lfloor y\lfloor z\rfloor\rfloor$, being an (multiple) update of x, lies in $\mathcal{D}_x$. In fact, it is the unique element of the coset $M\vee x\vee M$ in $\mathcal{D}_x$ that is above $y\lfloor z\rfloor\wedge x\lfloor y\rfloor\wedge y\lfloor z\rfloor$ with respect to the natural partial order (5.6), see Theorem 5.3.2. Likewise, $x\lfloor y\lfloor z\rfloor\rfloor$ also lies in $\mathcal{D}_x$, and it is the unique element of $M\vee x\vee M$ that is above $y\lfloor z\rfloor\wedge x\wedge y\lfloor z\rfloor$. In order to prove (5.15) it suffices to show that $u=v$, where $u=y\lfloor z\rfloor\wedge x\lfloor y\rfloor\wedge y\lfloor z\rfloor$ and $v=y\lfloor z\rfloor\wedge x\wedge y\lfloor z\rfloor$.

As $(x\lfloor y\rfloor)\lfloor y\lfloor z\rfloor\rfloor\in\mathcal{D}_{x\lfloor y\rfloor}=\mathcal{D}_x$ and $y\lfloor z\rfloor\in\mathcal{D}_y$, by Theorem 5.3.2(2), we get that $u=(x\lfloor y\rfloor)\lfloor y\lfloor z\rfloor\rfloor\wedge y\lfloor z\rfloor\in\mathcal{D}_x\wedge\mathcal{D}_y=M$. Similarly, $v=x\lfloor y\lfloor z\rfloor\rfloor\wedge y\lfloor z\rfloor\in\mathcal{D}_x\wedge\mathcal{D}_y=M$. We claim that u and v lie in a common coset of $\mathcal{D}_y$ in M, i.e. that $\mathcal{D}_y\wedge u\wedge\mathcal{D}_y=\mathcal{D}_y\wedge v\wedge\mathcal{D}_y$ holds. The coset $\mathcal{D}_y\wedge u\wedge\mathcal{D}_y$ contains the element $y\wedge u\wedge y=y\wedge y\lfloor z\rfloor\wedge x\lfloor y\rfloor\wedge y\lfloor z\rfloor\wedge y$. Using regularity (5.2), the latter is equal to $y\wedge y\lfloor z\rfloor\wedge y\wedge x\lfloor y\rfloor\wedge y\wedge y\lfloor z\rfloor\wedge y$. Using Theorem 5.3.2(2), the above equals $y\wedge y\lfloor z\rfloor\wedge y\wedge x\wedge y\wedge y\lfloor z\rfloor\wedge y$, which by regularity (5.2) simplifies to $y\wedge y\lfloor z\rfloor\wedge x\wedge y\lfloor z\rfloor\wedge y=y\wedge v\wedge y$, which is an element of the coset $\mathcal{D}_y\wedge v\wedge\mathcal{D}_y$. It follows that the cosets $\mathcal{D}_y\wedge u\wedge\mathcal{D}_y$ and $\mathcal{D}_y\wedge v\wedge\mathcal{D}_y$ intersect, and are thus equal.

Finally, observe that u and v both lie below $y\lfloor z\rfloor$, i.e. $y\lfloor z\rfloor\wedge u=u=u\wedge y\lfloor z\rfloor$ and $y\lfloor z\rfloor\wedge v=v=v\wedge y\lfloor z\rfloor$. By Remark 5.3.1, it follows that $u=v$. □

This leads to the first main result. It gives a formulation of an idempotent set-theoretic solution of the Yang-Baxter equation by using arbitrary skew lattices. As a consequence, finding and constructing (new) skew lattices becomes a highly motivated research topic. In particular, all skew lattices constructed in Subsection 5.2.1 induce set-theoretic solutions of the Yang-Baxter equation.

Theorem 5.3.4. *Let* $(S,\wedge,\vee)$ *be a skew lattice. Then,* (S,r) *with*

$$r:S\times S\to S\times S:(x,y)\mapsto((x\wedge y)\vee x,y),$$

is an idempotent set-theoretic solution of the Yang-Baxter equation.

Proof. Let $x,y,z\in S$. Then,

$$\begin{aligned}
r_{12}r_{23}r_{12}(x,y,z)&=r_{12}r_{23}((x\wedge y)\vee x,y,z)\\
&=r_{12}((x\wedge y)\vee x,(y\wedge z)\vee y,z)\\
&=((((x\wedge y)\vee x)\wedge((y\wedge z)\vee y))\vee((x\wedge y)\vee x),(y\wedge z)\vee y,z),
\end{aligned}$$

and

$$\begin{aligned} r_{23}r_{12}r_{23}(x,y,z) &= r_{23}r_{12}(x,(y\wedge z)\vee y,z) \\ &= r_{23}((x\wedge((y\wedge z)\vee y))\vee x,(y\wedge z)\vee y,z) \\ &= ((x\wedge((y\wedge z)\vee y))\vee x,(((y\wedge z)\vee y)\wedge z)\vee((y\wedge z)\vee y),z). \end{aligned}$$

To prove that (S,r) is a solution, we use Theorem 5.1.2 to show, for any $x,y,z\in S$,

$$(((x\wedge y)\vee x)\wedge((y\wedge z)\vee y))\vee((x\wedge y)\vee x)=(x\wedge((y\wedge z)\vee y))\vee x, \tag{5.16}$$

and

$$(y\wedge z)\vee y=(((y\wedge z)\vee y)\wedge z)\vee((y\wedge z)\vee y). \tag{5.17}$$

First, assume that S is left-handed, i.e. satisfying (5.4). Then, using absorption (5.1),

$$(x\wedge y)\vee x=(x\wedge y\wedge x)\vee x=x, \tag{5.18}$$

for all $x,y\in S$. Hence, (5.16) simplifies to $(x\wedge y)\vee x=(x\wedge y)\vee x$ (and even to $x=x$). Similarly, (5.17) is equivalent to $y=y$.

If S is right-handed, i.e. satisfying (5.5), then

$$(x\wedge y)\vee x=(y\wedge x\wedge y)\vee x=(y\wedge x\wedge y)\vee x\vee(y\wedge x\wedge y)=x\lfloor y\rfloor, \tag{5.19}$$

for all $x,y\in S$. Hence, (5.16) simplifies to (5.15), which holds by Lemma 5.3.3. Furthermore, (5.17) is equivalent to $y\lfloor z\rfloor=(y\lfloor z\rfloor\wedge z)\vee((y\wedge z)\vee y)$, where the right hand side is equal to $(z\wedge y\wedge z)\vee((y\wedge z)\vee y)$, by Theorem 5.3.2(2). Using right-handedness, the latter further simplifies to $(y\wedge z)\vee((y\wedge z)\vee y)=(y\wedge z)\vee y=y\lfloor z\rfloor$.

It remains to prove that the solution is idempotent. Again, by Theorem 5.1.2, it is enough to prove this separately for left-handed and right-handed skew lattices. Assume first that S is left-handed. Then, (5.18) holds, and thus, $r(x,y)=(x,y)=r^2(x,y)$. If S is right-handed, then by (5.19), $r(x,y)=(x\lfloor y\rfloor,y)$ and $r^2(x,y)=((x\lfloor y\rfloor)\lfloor y\rfloor,y)$. However, using right-handedness, $(x\lfloor y\rfloor)\lfloor y\rfloor=(x\lfloor y\rfloor\wedge y)\vee(x\lfloor y\rfloor)=(x\lfloor y\rfloor\wedge y)\vee((x\wedge y)\vee x)$, which, shown in the previous part, is equal to $x\lfloor y\rfloor$. □

For lattices, the previously found solution just becomes the solution defined by $r(x,y)=(x,y)$. This solution is degenerate if the given set has two or more elements. It is clear that the solution from Theorem 5.3.4 is not right non-degenerate. Examples give a hint that the solution from Theorem 5.3.4 will be degenerate in most cases, however no proof of this is known. Some specific examples of skew lattices do, however, yield left non-degenerate solutions.

Example 5.3.5. *Let $(S,\wedge,\vee)$ be a skew lattice such that, for any $x,y\in S$, $x\wedge y=y$ and $x\vee y=x$. Then, the solution of Theorem 5.3.4 becomes (S,r), with r defined by $r(x,y)=(y,y)$, for all $x,y\in S$, which is left non-degenerate.*

Note that, there is another way to prove that $x\lfloor y\rfloor = (x\lfloor y\rfloor)\lfloor y\rfloor$, for all $x, y \in S$. By Theorem 5.3.2, $x\lfloor y\rfloor$ is the unique element of the coset $M \vee x \vee M$ in $\mathcal{D}_x$, where $M = \mathcal{D}_x \wedge \mathcal{D}_y$, such that $y \wedge x \wedge y \leq x\lfloor y\rfloor$. On the other hand, $(x\lfloor y\rfloor)\lfloor y\rfloor$ is the unique element of the coset $N \vee x\lfloor y\rfloor \vee N$ in $\mathcal{D}_{x\lfloor y\rfloor}$, where $N = \mathcal{D}_{x\lfloor y\rfloor} \wedge \mathcal{D}_y$, such that $y \wedge x\lfloor y\rfloor \wedge y \leq (x\lfloor y\rfloor)\lfloor y\rfloor$. Moreover, $\mathcal{D}_x = \mathcal{D}_{x\lfloor y\rfloor}$ yields $N = M$, and $(x\lfloor y\rfloor)\lfloor y\rfloor \in N \vee x\lfloor y\rfloor \vee N \subseteq N \vee M \vee x \vee M \vee N = M \vee x \vee M$. Finally, since $y \wedge x \wedge y = y \wedge (y \wedge x \wedge y) \wedge y \leq y \wedge x\lfloor y\rfloor \wedge y \leq (x\lfloor y\rfloor)\lfloor y\rfloor$, we conclude that $(x\lfloor y\rfloor)\lfloor y\rfloor$ is also an element of the coset $M \vee x \vee M$ that lies above $y \wedge x \wedge y$ with respect to the natural partial order (5.6). Hence, $x\lfloor y\rfloor = (x\lfloor y\rfloor)\lfloor y\rfloor$.

Corollary 5.3.6. *Let $(S, \wedge, \vee)$ be a skew lattice. The map $r(x, y) = (x\lfloor y\rfloor, y)$ defines an idempotent set-theoretic solution of the Yang-Baxter equation.*

Proof. Let $x, y, z \in S$. Then,

$$r_{12}r_{23}r_{12}(x, y, z) = ((x\lfloor y\rfloor)\lfloor y\lfloor z\rfloor\rfloor, y\lfloor z\rfloor, z),$$

and

$$r_{23}r_{12}r_{23}(x, y, z) = (x\lfloor y\lfloor z\rfloor\rfloor, (y\lfloor z\rfloor)\lfloor z\rfloor, z).$$

The equality of the first components follows by Lemma 5.3.3. The equality of the second components holds, because $y\lfloor z\rfloor$ and $(y\lfloor z\rfloor)\lfloor z\rfloor$ are both elements of the coset $M \vee y \vee M$, where $M = \mathcal{D}_y \wedge \mathcal{D}_z$, that lie above $z \wedge y \wedge z$. Since such elements are unique (see Theorem 5.3.2(1)), it follows that $y\lfloor z\rfloor = (y\lfloor z\rfloor)\lfloor z\rfloor$. □

5.4 Strong distributive solutions of the Yang-Baxter equation

In Section 5.3, an idempotent set-theoretic solution of the Yang-Baxter equation is achieved, using an arbitrary skew lattice. In the case of lattices, the solution becomes the identity map, and thus less significant.

In this section, we study another map r, defined by $r(x, y) = (x \wedge y, x \vee y)$, for all elements x, y of a given skew lattice $(S, \wedge, \vee)$. The inspiration for the definition of this map r comes from the following well-known result, see for example [120, 146]. To each lattice $(L, \wedge, \vee)$, one may associate an idempotent map $r : L \times L \to L \times L$ defined as

$$r(x, y) = (x \wedge y, x \vee y). \tag{5.20}$$

Moreover, (L, r) is a solution of the Yang-Baxter equation if and only if L is a distributive lattice, i.e. satisfying (5.14). Indeed, for any $x, y, z \in L$,

$$\begin{aligned} r_{12}r_{23}r_{12}(x, y, z) &= r_{12}r_{23}(x \wedge y, x \vee y, z) \\ &= r_{12}(x \wedge y, (x \vee y) \wedge z, (x \vee y) \vee z) \\ &= ((x \wedge y) \wedge ((x \vee y) \wedge z), (x \wedge y) \vee ((x \vee y) \wedge z), (x \vee y) \vee z), \end{aligned}$$

while

$$\begin{aligned} r_{23}r_{12}r_{23}(x,y,z) &= r_{23}r_{12}(x, y\wedge z, y\vee z)\\ &= r_{23}(x\wedge(y\wedge z), x\vee(y\wedge z), y\vee z)\\ &= (x\wedge(y\wedge z), (x\vee(y\wedge z))\wedge(y\vee z), (x\vee(y\wedge z))\vee(y\vee z)). \end{aligned}$$

By commutativity and absorption of the lattice, the first and last components of both computations agree. Thus, we obtain a solution if and only if the second components are equal, i.e. $(x\wedge y)\vee((x\vee y)\wedge z) = (x\vee(y\wedge z))\wedge(y\vee z)$. Using distributivity and absorption of the lattice, we obtain $(x\wedge y)\vee((x\vee y)\wedge z) = (x\vee y)\wedge(x\vee z)\wedge(y\vee z) = (x\vee(y\wedge z))\wedge(y\vee z)$. Conversely, assume that $(L,\wedge,\vee)$ is a lattice satisfying $(x\wedge y)\vee((x\vee y)\wedge z) = (x\vee(y\wedge z))\wedge(y\vee z)$. For any $x,y,z\in L$, using the latter in the second and second last equation and absorption in the other equations below,

$$\begin{aligned} x\wedge(y\vee z) &= (x\wedge(y\vee z))\wedge((z\wedge y)\vee(x\wedge(y\vee z)))\\ &= (x\wedge(y\vee z))\wedge(z\vee(y\wedge x))\wedge(x\vee y)\\ &= x\wedge(y\vee z)\wedge(z\vee(y\wedge x))\\ &= x\wedge(z\vee(y\wedge x)\vee y)\wedge(z\vee(y\wedge x))\\ &= x\wedge(z\vee(y\wedge x))\\ &= (x\vee((x\wedge y)\wedge z))\wedge(z\vee(x\wedge y))\\ &= (x\wedge(x\wedge y))\vee((x\vee(x\wedge y))\wedge z)\\ &= (x\wedge y)\vee(x\wedge z). \end{aligned}$$

By swapping $\wedge$ and $\vee$, we also get $x\vee(y\wedge z) = (x\vee y)\wedge(x\vee z)$, for all $x,y,z\in L$, as desired.

We say that a skew lattice $(S,\wedge,\vee)$ is a *strong distributive solution* if the map $r : S\times S\to S\times S$ defined by (5.20), i.e.

$$r(x,y) = (x\wedge y, x\vee y),$$

is a set-theoretic solution of the Yang-Baxter equation. It turns out that strong distributive solutions form a variety, since they are defined by a set of identities.

Theorem 5.4.1. *The class of skew lattices that form strong distributive solutions is a variety, defined by the following identities*

$$x\wedge y\wedge(x\vee y)\wedge z = x\wedge y\wedge z, \tag{5.21}$$

$$(x\wedge y)\vee((x\vee y)\wedge z) = (x\vee(y\wedge z))\wedge(y\vee z), \tag{5.22}$$

$$x\vee y\vee z = x\vee(y\wedge z)\vee y\vee z. \tag{5.23}$$

Proof. Let $(S,\wedge,\vee)$ be a skew lattice and define $r : S\times S\to S\times S$ by (5.20). For any $x,y,z\in S$,

$$\begin{aligned} r_{12}r_{23}r_{12}(x,y,z) &= r_{12}r_{23}(x\wedge y, x\vee y, z)\\ &= r_{12}(x\wedge y, (x\vee y)\wedge z, (x\vee y)\vee z)\\ &= ((x\wedge y)\wedge((x\vee y)\wedge z), (x\wedge y)\vee((x\vee y)\wedge z), (x\vee y)\vee z), \end{aligned}$$

and

$$\begin{aligned}r_{23}r_{12}r_{23}(x,y,z) &= r_{23}r_{12}(x,y\wedge z,y\vee z)\\ &= r_{23}(x\wedge(y\wedge z),x\vee(y\wedge z),y\vee z)\\ &= (x\wedge(y\wedge z),(x\vee(y\wedge z))\wedge(y\vee z),(x\vee(y\wedge z))\vee(y\vee z)).\end{aligned}$$

Hence, a skew lattice S is a strong distributive solution if and only if it satisfies (5.21), (5.22), and (5.23). □

As mentioned in Section 5.2, there are several ways to generalize the concept of distributivity for lattices. The weakest of them is the notion of *quasi-distributivity*, which is defined as having a distributive maximal lattice image [65]. In particular, it means that its maximal lattice image $S/\mathcal{D}$ is a distributive lattice [126]. In [65], it was proven that quasi-distributive skew lattices form a variety, characterized by the identity

$$(x\wedge(y\vee z))\wedge((x\wedge y)\vee(x\wedge z))\wedge(x\wedge(y\vee z)) = x\wedge(y\vee z),$$

i.e. by $x\wedge(y\vee z)\leq(x\wedge y)\vee(x\wedge z)$. Distributive skew lattices, but also (left/right/fully) cancellative skew lattices, are always quasi-distributive [65, Corollary 3.3]. It turns out that strong distributive solutions are also quasi-distributive.

Corollary 5.4.2. *Let $(S,\wedge,\vee)$ be a strong distributive solution.*

(1) The maximal lattice image $S/\mathcal{D}$ is a strong distributive solution.

(2) The skew lattice S is quasi-distributive.

Proof. (1) By Theorem 5.4.1, strong distributive solutions form a variety, so all homomorphic images of strong distributive solutions are again strong distributive solutions. The maximal lattice image $S/\mathcal{D}$ is the homomorphic image of the strong distributive solution $(S,\wedge,\vee)$ under the natural projection $\pi : S\to S/\mathcal{D}$ which maps each element to its $\mathcal{D}$-class.

(2) By definition, S is quasi-distributive if and only if $S/\mathcal{D}$ is distributive. By (1), the lattice $S/\mathcal{D}$ is a strong distributive solution. However, a lattice is a strong distributive solution if and only if it is distributive. So, $S/\mathcal{D}$ must be a distributive lattice and S is quasi-distributive. □

In order to state and prove the following theorem, we need the notion of strongly and co-strongly distributive skew lattices.

A skew lattice is said to be *strongly distributive* if it satisfies the identities

$$(x\vee y)\wedge z=(x\wedge z)\vee(y\wedge z)\text{ and }x\wedge(y\vee z)=(x\wedge y)\vee(x\wedge z).\tag{5.24}$$

It is called *co-strongly distributive* if it satisfies the identities

$$(x\wedge y)\vee z=(x\vee z)\wedge(y\vee z)\text{ and }x\vee(y\wedge z)=(x\vee y)\wedge(x\vee z).\tag{5.25}$$

The interplay between normal and distributive skew lattices has been studied in [127]. An essential result is that a skew lattice is strongly distributive if and only if it is symmetric, quasi-distributive and normal. Dually, a skew lattice is co-strongly distributive if and only if it is symmetric, quasi-distributive and conormal. Another conclusion in [127] is that a skew lattice that is either strongly distributive or co-strongly distributive is distributive. Moreover, by a result in [116], cancellation is implied either by strong distributivity or co-strong distributivity.

Theorem 5.4.3. *Let $(S, \wedge, \vee)$ be a skew lattice which is both strongly and co-strongly distributive. Then, S is a strong distributive solution, i.e. $r : S \times S \to S \times S : (x, y) \mapsto (x \wedge y, x \vee y)$ satisfies the Yang-Baxter equation (1.15). Furthermore, this solution is cubic, i.e. $r^3 = r$.*

Proof. By Theorem 5.4.1, we need to prove that S satisfies the identities (5.21)-(5.23). Let $x, y, z \in S$. Recall that strong distributivity implies normality, and co-strong distributivity implies conormality. Using strong distributivity (5.24) and normality (5.9), we deduce

$$\begin{aligned}(x \wedge y) \wedge ((x \vee y) \wedge z) &= ((x \wedge y \wedge x) \vee (x \wedge y)) \wedge z\\ &= (x \wedge y \wedge x \wedge z) \vee (x \wedge y \wedge z)\\ &= (x \wedge x \wedge y \wedge z) \vee (x \wedge y \wedge z)\\ &= (x \wedge y \wedge z) \vee (x \wedge y \wedge z)\\ &= x \wedge (y \wedge z).\end{aligned}$$

Furthermore, by co-strong distributivity (5.25) and conormality (5.9), we obtain

$$\begin{aligned}(x \vee (y \wedge z)) \vee (y \vee z) &= x \vee ((y \vee z) \wedge (z \vee y \vee z))\\ &= (x \vee y \vee z) \wedge (x \vee z \vee y \vee z)\\ &= (x \vee y \vee z) \wedge (x \vee y \vee z \vee z)\\ &= (x \vee y \vee z) \wedge (x \vee y \vee z)\\ &= (x \vee y) \vee z.\end{aligned}$$

Thus, we are left to prove that

$$(x \wedge y) \vee ((x \vee y) \wedge z) = (x \vee (y \wedge z)) \wedge (y \vee z). \tag{5.26}$$

The left hand side of this equation is equal to

$$(x \wedge y) \vee ((x \vee y) \wedge z) = (x \wedge y) \vee (x \wedge z) \vee (y \wedge z),$$

where we used that the skew lattice is strongly distributive (5.24). Using strong distributivity (5.24), conormality (5.9), and the absorption rules (5.1), the right hand side of equation (5.26) can be rewritten as

$$\begin{aligned}(x \vee (y \wedge z)) \wedge (y \vee z) &= (x \wedge (y \vee z)) \vee ((y \wedge z) \wedge (y \vee z))\\ &= (x \wedge y) \vee (x \wedge z) \vee (y \wedge z \wedge y) \vee (y \wedge z)\\ &= (x \wedge y) \vee (x \wedge z) \vee (y \wedge z \wedge y) \vee (y \wedge z) \vee (y \wedge z)\\ &= (x \wedge y) \vee (x \wedge z) \vee (y \wedge z) \vee (y \wedge z \wedge y) \vee (y \wedge z)\\ &= (x \wedge y) \vee (x \wedge z) \vee (y \wedge z) \vee (y \wedge z)\\ &= (x \wedge y) \vee (x \wedge z) \vee (y \wedge z),\end{aligned}$$

as desired.

Let $x, y \in S$. To prove that the solution is cubic, we compute

$$\begin{aligned}r^3(x,y) &= r^2(x \wedge y, x \vee y)\\ &= r((x \wedge y) \wedge (x \vee y), (x \wedge y) \vee (x \vee y))\\ &= (((x \wedge y) \wedge (x \vee y)) \wedge ((x \wedge y) \vee (x \vee y)),\\ &\quad ((x \wedge y) \wedge (x \vee y)) \vee ((x \wedge y) \vee (x \vee y))).\end{aligned}$$

By normality (5.9) and the absorption rule (5.1), we deduce

$$\begin{aligned}((x \wedge y) \wedge (x \vee y)) \wedge ((x \wedge y) \vee (x \vee y)) &= (x \wedge y) \wedge (x \vee y) \wedge (x \wedge y) \wedge ((x \wedge y) \vee (x \vee y))\\ &= (x \wedge y) \wedge (x \vee y) \wedge (x \wedge y)\\ &= x \wedge y \wedge x \wedge (x \vee y) \wedge x \wedge y\\ &= x \wedge y \wedge x \wedge x \wedge y\\ &= x \wedge y.\end{aligned}$$

Similarly, by conormality (5.9) and the absorption rule (5.1),

$$\begin{aligned}((x \wedge y) \wedge (x \vee y)) \vee ((x \wedge y) \vee (x \vee y)) &= ((x \wedge y) \wedge (x \vee y)) \vee (x \vee y) \vee (x \wedge y) \vee (x \vee y)\\ &= (x \vee y) \vee (x \wedge y) \vee (x \vee y)\\ &= x \vee y \vee x \vee (x \wedge y) \vee x \vee y\\ &= x \vee y \vee x \vee x \vee y\\ &= x \vee y.\end{aligned}$$

Hence, $r^3(x,y) = (x \wedge y, x \vee y) = r(x,y)$. □

In general, we can not omit either strong distributivity or co-strong distributivity from the assumptions of Theorem 5.4.3, as is verified by the following pair of examples.

Example 5.4.4. *Let* $\mathbf{3}^{R,0}$ *be a* 3*-element skew lattice given by the following pair of Cayley tables,*

$\wedge$	0	1	2
0	0	0	0
1	0	1	2
2	0	1	2

,

$\vee$	0	1	2
0	0	1	2
1	1	1	1
2	2	2	2

.

It is easy to check that $\mathbf{3}^{R,0}$ is a right-handed skew lattice with two comparable $\mathcal{D}$-classes $\{1,2\} > \{0\}$, and it is strongly distributive [127, Theorem 3.2], but not co-strongly distributive as $(0 \wedge 1) \vee 2 = 2$, but $(0 \vee 2) \wedge (1 \vee 2) = 1$. We claim that $\mathbf{3}^{R,0}$ is not a strong distributive solution, more specifically, it does not satisfy (5.22). Take $x = 0$, $y = 1$, and $z = 2$. Then, $(x \wedge y) \vee ((x \vee y) \wedge z) = (0 \wedge 1) \vee ((0 \vee 1) \wedge 2) = 0 \vee (1 \wedge 2) = 0 \vee 2 = 2$, while $(x \vee (y \wedge z)) \wedge (y \vee z) = (0 \vee (1 \wedge 2)) \wedge (1 \vee 2) = (0 \vee 2) \wedge 1 = 2 \wedge 1 = 1$.

Example 5.4.5. *Let $\mathbf{3}^{R,1}$ be a 3-element skew lattice given by the following pair of Cayley tables,*

$$\begin{array}{c|ccc} \wedge & 0 & 1 & 2 \\ \hline 0 & 0 & 0 & 2 \\ 1 & 0 & 1 & 2 \\ 2 & 0 & 2 & 2 \end{array}, \qquad \begin{array}{c|ccc} \vee & 0 & 1 & 2 \\ \hline 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 2 & 2 & 1 & 2 \end{array}.$$

Similar argumentation as in Example 5.4.4 shows that $\mathbf{3}^{R,1}$ is a co-strongly distributive (but not strongly distributive) skew lattice, which is not a strong distributive solution.

In case the skew lattice is left-handed, the story is different.

Proposition 5.4.6. *Let $(S, \wedge, \vee)$ be a left-handed skew lattice. Then, S satisfies the identities (5.21) and (5.23). If, in addition to being left-handed, S is either strongly or co-strongly distributive, then (5.22) is also satisfied and S is a strong distributive solution.*

Proof. Let $x, y, z \in S$. Using left-handedness (5.4), we obtain $(x \wedge y) \wedge ((x \vee y) \wedge z) = x \wedge y \wedge x \wedge (x \vee y) \wedge z$, which by (5.1) simplifies to $x \wedge y \wedge x \wedge z$, and then by (5.4) further to $x \wedge y \wedge z$. Furthermore, using left-handedness, $x \vee (y \wedge z) \vee y \vee z = x \vee (y \wedge z) \vee z \vee y \vee z$, and again by absorption and left-handedness, the latter first simplifies to $x \vee z \vee y \vee z$, and then to $x \vee y \vee z$. Hence, both (5.21) and (5.23) are satisfied.

Assume now that S is strongly distributive (5.24) (the case where S is co-strongly distributive (5.25) is handled dually). By the previous part and Theorem 5.4.1, we are left to prove (5.22), for all $x, y, z \in S$. Let $x, y, z \in S$. Then, using strong distributivity, $(x \wedge y) \vee ((x \vee y) \wedge z) = (x \wedge y) \vee (x \wedge z) \vee (y \wedge z)$, and $(x \vee (y \wedge z)) \wedge (y \vee z) = (x \wedge (y \vee z)) \vee (y \wedge z \wedge (y \vee z))$. Again using strong distributivity and left-handedness, the latter expands to $(x \wedge y) \vee (x \wedge z) \vee (y \wedge z \wedge y \wedge (y \vee z))$. By absorption and left-handedness, this simplifies to $(x \wedge y) \vee (x \wedge z) \vee (y \wedge z)$. □

The following example shows that the converse of Theorem 5.4.3 is not true. Hence, we get that the class of strongly and co-strongly distributive skew lattices forms a strict subclass of the class of strong distributive solutions.

Example 5.4.7. *Consider the skew lattice $(S, \wedge, \vee)$ with $S = \{0, 1, 2\}$, and*

$$\begin{array}{c|ccc} \wedge & 0 & 1 & 2 \\ \hline 0 & 0 & 1 & 2 \\ 1 & 1 & 1 & 1 \\ 2 & 2 & 2 & 2 \end{array}, \qquad \begin{array}{c|ccc} \vee & 0 & 1 & 2 \\ \hline 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 2 \\ 2 & 0 & 1 & 2 \end{array}.$$

Then, one can check that $(S, \wedge, \vee)$ is a strong distributive solution, but it is not strongly distributive. The latter can be seen by considering $x = 0$, $y = 1$, and $z = 2$ in the identity $(x \vee y) \wedge z = (x \wedge z) \vee (y \wedge z)$.

The Automated Theorem Prover *Prover9* [139] is able to derive a proof that every strong distributive solution is distributive and cancellative, see Code 1, Code 2, and Code 3 in the appendix. The converse, however, is not true. For example, the program *Mace4* [138, 139] was able to find a 16-element example of a left-handed, distributive and cancellative skew lattice, that is not a strong distributive solution (see Code 4 in the appendix). So the class of strong distributive solutions forms a strict subclass of the distributive and cancellative skew lattices.

For most examples, the set-theoretic solution (5.20) obtained from a strong distributive skew lattice is degenerate. Nevertheless, there are cases where the solution is non-degenerate.

Example 5.4.8. *Let S be a non-empty set and let the skew lattice operations $\wedge$ and $\vee$ on S be defined by $x \wedge y = y$ and $x \vee y = x$, for all $x, y \in S$. Then, $(S, \wedge, \vee)$ is a strongly and co-strongly distributive skew lattice, and thus a strong distributive solution by Theorem 5.4.3. In fact, $x \mathcal{R} y$ holds, for all $x, y \in S$, and $(S, \wedge)$ is a right-zero semigroup, i.e. it satisfies $x \wedge y = y$. So, S is a right-handed skew lattice with one $\mathcal{D}$-class. The associated map (5.20) is the twist map $r(x, y) = (y, x)$. This solution is non-degenerate as both $\lambda_x : X \to X : t \mapsto x \wedge t = t$ and $\rho_y : X \to X : t \mapsto t \vee y = t$ are bijective maps, for all $x, y \in S$.*

In fact, the skew lattices given by Example 5.4.8 above are the only strong distributive solutions that give (left or right) non-degenerate set-theoretic solutions of the Yang-Baxter equation.

Proposition 5.4.9. *Let $(S, \wedge, \vee)$ be a skew lattice that is a strong distributive solution, where the associated solution is left or right non-degenerate. Then, $(S, \wedge, \vee)$ is the skew lattice from Example 5.4.8.*

Proof. Assume first that S is a strong distributive solution and that the obtained solution from the map (5.20) is left non-degenerate, i.e. $\lambda_x : y \mapsto x \wedge y$ is bijective, for all $x \in S$. We claim that $x \wedge y = y$ and $x \vee y = x$, for all $x, y \in S$. Take $x, y \in S$ two arbitrary elements. Since the map λ_x is bijective, there exists an element $t \in S$ such that $\lambda_x(t) = x \wedge t = y$. Thus, $x \wedge y = x \wedge (x \wedge t) = x \wedge t = y$. Furthermore, using absorption (5.1), $x \vee y = x \vee (x \wedge y) = x$. Hence, we obtain a skew lattice as in Example 5.4.8.

The proof for the right non-degenerate case is similar to the left non-degenerate case. □

5.5 More distributive solutions

In this section, we naturally associate other idempotent solutions with skew lattices, inspired by the solution of Section 5.4. For lattices, all the maps provided in this section are equal to the map defined by (5.20).

5.5.1 Left distributive solutions

Let $(S, \wedge, \vee)$ be a skew lattice and $r_L : S \times S \to S \times S$ the map defined by

$$r_L(x, y) = (x \wedge y, y \vee x). \tag{5.27}$$

We say that a skew lattice S is a *left distributive solution*, if (S, r_L) is a set-theoretic solution of the Yang-Baxter equation.

Proposition 5.5.1. *Let $(S, \wedge, \vee)$ be a skew lattice. If S is a left distributive solution, then (S, r_L) is an idempotent solution.*

Proof. For any $x, y \in S$, using the absorption laws (5.1), we obtain

$$\begin{aligned} r_L^2(x, y) &= r_L(x \wedge y, y \vee x) \\ &= ((x \wedge y) \wedge (y \vee x), (y \vee x) \vee (x \wedge y)) \\ &= (x \wedge y, y \vee x) \\ &= r_L(x, y), \end{aligned}$$

as desired. □

Theorem 5.5.2. *The class of left distributive solutions is a variety, defined by the identity*

$$((y \vee x) \wedge z) \vee (x \wedge y) = ((y \wedge z) \vee x) \wedge (z \vee y). \tag{5.28}$$

Proof. A skew lattice $(S, \wedge, \vee)$ is a left distributive solution if and only if it satisfies, for any $x, y, z \in S$,

$$(r_L \times \mathrm{id}_S)(\mathrm{id}_S \times r_L)(r_L \times \mathrm{id}_S)(x, y, z) = (\mathrm{id}_S \times r_L)(r_L \times \mathrm{id}_S)(\mathrm{id}_S \times r_L)(x, y, z). \tag{5.29}$$

Computing the left side of (5.29) yields

$$\begin{aligned} &(r_L \times \mathrm{id}_S)(\mathrm{id}_S \times r_L)(r_L \times \mathrm{id}_S)(x, y, z) \\ &= (r_L \times \mathrm{id}_S)(\mathrm{id}_S \times r_L)(x \wedge y, y \vee x, z) \\ &= (r_L \times \mathrm{id}_S)(x \wedge y, (y \vee x) \wedge z, z \vee y \vee x) \\ &= (x \wedge y \wedge (y \vee x) \wedge z), ((y \vee x) \wedge z) \vee (x \wedge y), z \vee y \vee x). \end{aligned}$$

On the other hand, the right side of (5.29) expands as

$$\begin{aligned} &(\mathrm{id}_S \times r_L)(r_L \times \mathrm{id}_S)(\mathrm{id}_S \times r_L)(x, y, z) \\ &= (\mathrm{id}_S \times r_L)(r_L \times \mathrm{id}_S)(x, y \wedge z, z \vee y) \\ &= (\mathrm{id}_S \times r_L)(x \wedge y \wedge z, (y \wedge z) \vee x, z \vee y) \\ &= (x \wedge y \wedge z, ((y \wedge z) \vee x) \wedge (z \vee y), z \vee y \vee (y \wedge z) \vee x). \end{aligned}$$

By absorption (5.1), $x \wedge y \wedge (y \vee x) \wedge z$ reduces to $x \wedge y \wedge z$. Similarly, $z \vee y \vee (y \wedge z) \vee x$ reduces to $z \vee y \vee x$. Hence, $(S, \wedge, \vee)$ is a left distributive solution if and only it satisfies the identity $((y \vee x) \wedge z) \vee (x \wedge y) = ((y \wedge z) \vee x) \wedge (z \vee y)$, as desired. □

Recall that a skew lattice is called quasi-distributivity if it has a distributive maximal lattice image. Since for a lattice the map defined by (5.27) is equal to the map defined by (5.20), we obtain that a lattice is a left distributive solution if and only if the lattice is distributive. Thus, we get a similar result as Corollary 5.4.2.

Corollary 5.5.3. *Let $(S, \wedge, \vee)$ be a skew lattice. If S is a left distributive solution, then the maximal lattice image $S/\mathcal{D}$ is also a left distributive solution, and thus S is quasi-distributive.*

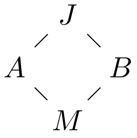
In Section 5.4, we obtained that strongly and co-strongly distributive skew lattices are strong distributive solutions. The following result shows that these skew lattices are also left distributive solutions.

Proposition 5.5.4. *Let $(S, \wedge, \vee)$ be a skew lattice that is strongly distributive or co-strongly distributive. Then, S is a left distributive solution.*

Proof. We give a proof for the case of strongly distributive skew lattices. The case of co-strongly distributive skew lattices is handled in a dual fashion. By Theorem 5.5.2, we need to prove that S satisfies the identity $((y \vee x) \wedge z) \vee (x \wedge y) = ((y \wedge z) \vee x) \wedge (z \vee y)$. Let $x, y, z \in S$. Using strong distributivity (5.24), $((y \vee x) \wedge z) \vee (x \wedge y)$ simplifies to $(y \wedge z) \vee (x \wedge z) \vee (x \wedge y)$. On the other hand, $((y \wedge z) \vee x) \wedge (z \vee y)$ is equal to $(y \wedge z \wedge (z \vee y)) \vee (x \wedge (z \vee y))$, which by absorption (5.1) and strong distributivity (5.24) further simplifies to $(y \wedge z) \vee (x \wedge z) \vee (x \wedge y)$. □

In fact, the result of Proposition 5.5.4 can be strengthened to a more general class of skew lattices (see Proposition 5.5.6).

To prove Lemma 5.5.5 and Proposition 5.5.6 below, we use the technique of Remark 5.3.1. A *skew diamond* $\{J > A, B > M\}$ is a sub-skew lattice of a skew lattice $(S, \wedge, \vee)$ with four $\mathcal{D}$-classes A, B, M, J, such that $M = A \wedge B$ and $J = A \vee B$. This is illustrated in the Hasse diagram below.



Given a skew diamond $\{J > A, B > M\}$, the cosets of A in J are given by $A \vee b \vee A$, where $b \in B$. Likewise, the cosets of A in M are given by $A \wedge b \wedge A$, where $b \in B$. For more information, see [66].

Finally, we define some more varieties of skew lattices used in the following results. The definition of a symmetric skew lattice, i.e. a skew lattice satisfying (5.7), can be generalized in two ways. A skew lattice is called *upper symmetric* if

$$x \wedge y = y \wedge x \quad \text{implies} \quad x \vee y = y \vee x, \tag{5.30}$$

and it is said to be *lower symmetric* if

$$x \vee y = y \vee x \quad \text{implies} \quad x \wedge y = y \wedge x. \tag{5.31}$$

Finally, a skew lattice is called *simply cancellative* if it satisfies

$$x \vee z \vee x = y \vee z \vee y, x \wedge z \wedge x = y \wedge z \wedge y \quad \text{implies} \quad x = y. \tag{5.32}$$

Note that a simply cancellative skew lattice is defined differently (and incorrect) in [69] (Cvetko-Vah and Verwimp), however all results in the paper were obtained using the correct definition given above. In [65, Theorem 5.1], it is shown that a skew lattice is cancellative if and only if it is simply cancellative and symmetric.

Lemma 5.5.5. *Let S be a simply cancellative skew lattice, $\{J > A, B > M\}$ a skew diamond in S and $x_1, x_2 \in A$.*

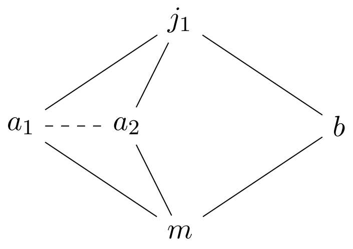
(1) Let S be upper symmetric. If $B \vee x_1 \vee B = B \vee x_2 \vee B$, then $M \vee x_1 \vee M = M \vee x_2 \vee M$.

(2) Let S be lower symmetric. If $B \wedge x_1 \wedge B = B \wedge x_2 \wedge B$, then $J \wedge x_1 \wedge J = J \wedge x_2 \wedge J$.

Proof. (1) Let S be upper symmetric and $x_1, x_2 \in A$ such that $B \vee x_1 \vee B = B \vee x_2 \vee B$ and $M \vee x_1 \vee M \neq M \vee x_2 \vee M$. So, there exists $m \in M$ such that $a_1 \neq a_2$, where $a_1 = m \vee x_1 \vee m$ and $a_2 = m \vee x_2 \vee m$. Note that $a_1, a_2 \in A$, $m < a_1$, $m < a_2$, as $m \wedge a_1 = m = a_1 \wedge m$ and $m \wedge a_2 = m = a_2 \wedge m$. Take $b \in B$ such that $m < b$ (take for example $b = m \vee b' \vee m$, for some $b' \in B$). Since $m < a_1$ and $m < b$, it follows that $a_1 \wedge b = m = b \wedge a_1$, and likewise $a_2 \wedge b = m = b \wedge a_2$. Indeed, assume $a_1 \wedge b = m_1$ and $b \wedge a_1 = m_2$, for some $m_1, m_2 \in M$. Since M is a $\mathcal{D}$-class, we get $m_1 = m_1 \wedge m \wedge m_1 = m_1 \wedge m \wedge (a_1 \wedge b) = m_1 \wedge m = a_1 \wedge b \wedge m = m$. Similarly, $m_2 = m$. In a same way one proves $a_2 \wedge b = m = b \wedge a_2$. By (5.30), we obtain

$$a_1 \vee b = b \vee a_1 \text{ and } a_2 \vee b = b \vee a_2. \tag{5.33}$$

Denote $j_1 = a_1 \vee b$ and $j_2 = a_2 \vee b$. By Remark 5.3.1, the assumption $B \vee x_1 \vee B = B \vee x_2 \vee B$ implies $b \vee a_1 \vee b = b \vee m \vee x_1 \vee m \vee b = b \vee x_1 \vee b = b \vee x_2 \vee b = b \vee a_2 \vee b$. By (5.33), it follows that $j_1 = a_1 \vee b \vee b = b \vee a_1 \vee b = b \vee a_2 \vee b = a_2 \vee b = j_2$, and the set $\{m, a_1, a_2, b, j_1\}$ forms a subalgebra S', given by the diagram below.



The subalgebra S' is isomorphic either to $\mathbf{NC}_5^{\mathcal{R}}$ (a right-handed skew lattice with $a_1 \wedge a_2 = a_2$, $a_2 \wedge a_1 = a_1$, $a_1 \vee a_2 = a_1$, and $a_2 \vee a_1 = a_2$) or to $\mathbf{NC}_5^{\mathcal{L}}$ (a left-handed skew lattice with $a_1 \wedge a_2 = a_1$, $a_2 \wedge a_1 = a_2$, $a_1 \vee a_2 = a_2$, and $a_2 \vee a_1 = a_1$). It was proven in [65, Lemma 3.4] that a skew lattice is simply cancellative if and only if it contains no sub-skew lattice isomorphic to $\mathbf{NC}_5^{\mathcal{R}}$ or $\mathbf{NC}_5^{\mathcal{L}}$. Thus S is not simply cancellative, which is a contradiction.

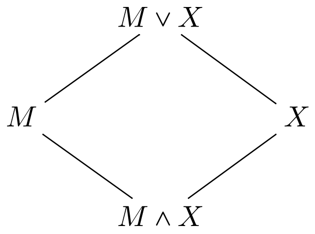
The proof of (2) is similar. □

To prove the following proposition, we use the fact that for a skew diamond $\{J > A, B > M\}$ in a lower symmetric skew lattice, cosets of J in M are exactly intersections of cosets of A in M by cosets of B in M. This result is shown in [128, Theorem 3.5] for symmetric skew lattices. However, the last part of the proof of [128, Theorem 3.5] shows that if more than one coset of J in M lies inside the intersection of a coset of A in M by a coset of B in M, then there are pairs of elements that join commute but that do not meet commute, i.e. the skew lattice is not lower symmetric.

Proposition 5.5.6. *Let S be a left-handed (resp. right-handed), distributive, simply cancellative, and lower (resp. upper) symmetric skew lattice. Then, S is a left distributive solution of the Yang-Baxter equation.*

Proof. Let $(S, \wedge, \vee)$ be a left-handed, distributive, simply cancellative, and lower symmetric skew lattice. Take $x, y, z \in S$ arbitrary and define $\alpha = ((y \vee x) \wedge z) \vee (x \wedge y)$ and $\beta = ((y \wedge z) \vee x) \wedge (z \vee y)$. Denote the corresponding $\mathcal{D}$-classes by $X = \mathcal{D}_x$, $Y = \mathcal{D}_y$, $Z = \mathcal{D}_z$, $M = \mathcal{D}_\alpha$. By Theorem 5.5.2, we need to prove that $\alpha = \beta$. Since S is distributive, it follows that $S/\mathcal{D}$ is a distributive lattice, and thus a left distributive solution as the maps (5.27) and (5.20) coincide for lattices. So, $\alpha = \beta$ in $S/\mathcal{D}$, $\alpha \,\mathcal{D}\, \beta$, and thus $\alpha, \beta \in M$. We divide the proof into several steps.

First, we consider the skew diamond below.



(a) We claim that $X \wedge \alpha \wedge X = X \wedge \beta \wedge X$, i.e. $x \wedge \alpha \wedge x$ and $x \wedge \beta \wedge x$ lie in the same coset of X in $M \wedge X$. Since the cosets of X form a partition of $M \wedge X$, it suffices to prove $x \wedge \alpha \wedge x = x \wedge \beta \wedge x$. Using distributivity (5.12), regularity (5.2), and absorption (5.1), we obtain

$$\begin{aligned} x \wedge \alpha \wedge x &= (x \wedge ((y \vee x) \wedge z) \wedge x) \vee (x \wedge (x \wedge y) \wedge x) \\ &= (x \wedge (y \vee x) \wedge x \wedge z \wedge x) \vee (x \wedge y \wedge x) \\ &= (x \wedge z \wedge x) \vee (x \wedge y \wedge x) \\ &= x \wedge (z \vee y) \wedge x. \end{aligned}$$

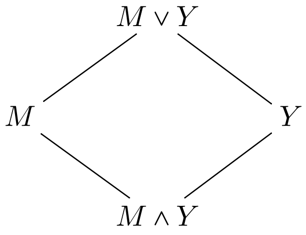
On the other hand, using regularity (5.2) and absorption (5.1), we obtain

$$\begin{aligned} x \wedge \beta \wedge x &= x \wedge ((y \wedge z) \vee x) \wedge x \wedge (z \vee y) \wedge x \\ &= x \wedge (z \vee y) \wedge x, \end{aligned}$$

as desired.

(b) We claim that $(M \vee X) \wedge \alpha \wedge (M \vee X) = (M \vee X) \wedge \beta \wedge (M \vee X)$. By applying Lemma 5.5.5(2) to the skew diamond above, with $\alpha, \beta \in M$, step (a) yields exactly $(M \vee X) \wedge \alpha \wedge (M \vee X) = (M \vee X) \wedge \beta \wedge (M \vee X)$.

(c) We claim that $Y \wedge \alpha \wedge Y = Y \wedge \beta \wedge Y$ and $(M \vee Y) \wedge \alpha \wedge (M \vee Y) = (M \vee Y) \wedge \beta \wedge (M \vee Y)$. Similar as in steps (a) and (b), it is enough to prove that $y \wedge \alpha \wedge y = y \wedge \beta \wedge y$, and then apply Lemma 5.5.5(2) to the skew diamond below.



Using distributivity (5.12) and absorption (5.1), we obtain

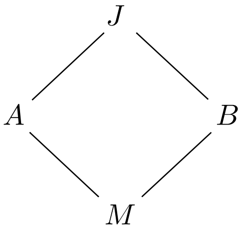
$$\begin{aligned} y \wedge \alpha \wedge y &= (y \wedge ((y \vee x) \wedge z) \wedge y) \vee (y \wedge (x \wedge y) \wedge y) \\ &= (y \wedge z \wedge y) \vee (y \wedge x \wedge y), \end{aligned}$$

while

$$\begin{aligned} y \wedge \beta \wedge y &= y \wedge ((y \wedge z) \vee x) \wedge (z \vee y) \wedge y \\ &= (y \wedge y \wedge z \wedge y) \vee (y \wedge x \wedge y), \end{aligned}$$

and thus they are equal.

Denote further $A = M \vee X$, $B = M \vee Y$ and $J = A \vee B$. Since S is distributive, the D-classes form a distributive lattice, and we obtain $M = (X \wedge Y) \vee (X \wedge Z) \vee (Y \wedge Z)$, $A \wedge B = M$ and $J = X \vee Y$. We consider the skew diamond below.



(d) We claim that $J \wedge \alpha \wedge J = J \wedge \beta \wedge J$. Observe that using our new notation, in steps (b) and (c) we proved that α and β lie in the same coset of A in M and that they lie in the same coset of B in M. By [128, Theorem 3.5], the cosets of J in M are exactly intersections of cosets of A in M by cosets of B in M. It follows that α and β lie in the same coset of J in M.

(e) We have just proven that α and β lie in the same coset of J in M. In order to prove that they are equal, it suffices, by Remark 5.3.1, to show that they both lie below a common element of J. In fact, we claim that $\alpha \leq y \vee x$ and $\beta \leq y \vee x$. By (5.1), we obtain

$y \vee x \vee \alpha = y \vee x \vee ((y \vee x) \wedge z) \vee (x \wedge y) = y \vee x \vee (x \wedge y) = y \vee x$. On the other hand, since S is left-handed (5.4), we obtain $\alpha \vee (y \vee x) = (y \vee x) \vee \alpha \vee (y \vee x) = (y \vee x) \vee (y \vee x) = y \vee x$, and thus $\alpha \leq y \vee x$. Moreover, by (5.4), we obtain $\beta = (x \vee (y \wedge z) \vee x) \wedge (z \vee y)$, which, by distributivity (5.13), expands to $(x \vee y \vee x) \wedge (x \vee z \vee x) \wedge (z \vee y)$, and then, by left-handedness (5.4), to $(y \vee x) \wedge (z \vee x) \wedge (z \vee y)$. It follows that $(y \vee x) \wedge \beta = \beta$, and $\beta \wedge (y \vee x) = \beta \wedge (y \vee x) \wedge \beta = \beta \wedge \beta = \beta$. Thus, $\beta \leq y \vee x$, as desired.

The case where S is a right-handed, distributive, simply cancellative and upper symmetric skew lattice is handled similarly. □

The following result shows that any distributive and left cancellative skew lattice is a left distributive solution.

Theorem 5.5.7. *Let S be a distributive and left cancellative skew lattice. Then, S is a left distributive solution of the Yang-Baxter equation.*

Proof. Let S be any distributive and left cancellative skew lattice. The left factor S_L of S is a left-handed and left cancellative skew lattice, and thus it is simply cancellative and lower symmetric by [65, Theorem 5.1]. Since S_L is also a distributive skew lattice, it follows by Proposition 5.5.6 that it is a left distributive solution. Dually, the right factor S_R of S is a right-handed, distributive and left cancellative skew lattice, and thus it is simply cancellative and upper symmetric by a result of [65, Theorem 5.1]. It follows by Proposition 5.5.6 that S_R is also a left distributive solution. By Theorem 5.1.2, S is a left distributive solution. □

The converse of Theorem 5.5.7 was proven by the Automated Theorem Prover *Prover9* [139], see Code 5 and Code 6 in the appendix, which was able to derive a proof that every left distributive solution is distributive and left cancellative.

Since a strong distributive solution is distributive and cancellative, as a consequence of Theorem 5.5.7, a strong distributive solution is also a left distributive solution.

Like strong distributive solutions, the set-theoretic solution obtained from a left distributive solution will be degenerate in general. Nevertheless, there are examples where the solution is left non-degenerate. Take for instance the skew lattice from Example 5.4.8. This skew lattice S is a left distributive solution and one can see that $r_L(x,y) = (y,y)$, for all $x, y \in S$. Hence, we obtain a left non-degenerate solution.

5.5.2 Right distributive solutions

Let $(S, \wedge, \vee)$ be a skew lattice. Consider the map $r_R : S \times S \to S \times S$ defined by

$$r_R(x,y) = (y \wedge x, x \vee y). \tag{5.34}$$

We say that a skew lattice S is a *right distributive solution* if (S, r_R) is a set-theoretic solution of the Yang-Baxter equation. Note that $r_R = r_L \circ \tau$, where τ is the twist map $\tau(x,y) = (y,x)$.

The following theorem is proven similar to the corresponding results for left distributive solutions. However, the latter uses left cancellative skew lattices. So, for the following theorem, we use right cancellative skew lattices.

Theorem 5.5.8. *(1) The class of right distributive solutions of the Yang-Baxter equation is a variety. Moreover, this variety is defined by the identity*

$$(y \wedge x) \vee (z \wedge (x \vee y)) = (y \vee z) \wedge (x \vee (z \wedge y)). \tag{5.35}$$

(2) Right distributive solutions are always idempotent, i.e. $r_R^2 = r_R$.

(3) Every strong distributive solution is also a right distributive solution.

(4) Every left-handed, distributive, simply cancellative and upper symmetric skew lattice is a right distributive solution.

(5) Every right-handed, distributive, simply cancellative and lower symmetric skew lattice is a right distributive solution.

(6) Every distributive and right cancellative skew lattice is a right distributive solution.

The converse of Theorem 5.5.8(6) was proven by the Automated Theorem Prover *Prover9* [139], see Code 7 and Code 8 in the appendix, which was able to derive a proof that every right distributive solution is distributive and right cancellative.

Similar to strong distributive solutions, the set-theoretic solution obtained from a right distributive solution will be degenerate in general. Nevertheless, there are examples where the solution is right non-degenerate, and thus not degenerate. Take again the skew lattice from Example 5.4.8. This skew lattice S is a right distributive solution and one can see that $r_R(x, y) = (x, x)$, for all $x, y \in S$. Hence, (S, r_R) is a right non-degenerate solution.

5.5.3 Weak distributive solutions

Let $(S, \wedge, \vee)$ be a skew lattice. Consider the map $r_W : S \times S \to S \times S$ defined by

$$r_W(x, y) = (x \wedge y \wedge x, x \vee y \vee x). \tag{5.36}$$

We say that a skew lattice $(S, \wedge, \vee)$ is a *weak distributive solution* if (S, r_W) is a set-theoretic solution of the Yang-Baxter equation.

Theorem 5.5.9. *The class of weak distributive solutions of the Yang-Baxter equation is a variety. Moreover, this variety is defined by the identity*

$$\begin{aligned}&(x \wedge y \wedge x) \vee ((x \vee y \vee x) \wedge z \wedge (x \vee y \vee x)) \vee (x \wedge y \wedge x)\\ &= (x \vee (y \wedge z \wedge y) \vee x) \wedge (y \vee z \vee y) \wedge (x \vee (y \wedge z \wedge y) \vee x).\end{aligned} \tag{5.37}$$

Proof. Let $(S, \wedge, \vee)$ be a skew lattice and $x, y, z \in S$. Then,

$$\begin{aligned}
&(r_W \times \mathrm{id}_S)(\mathrm{id}_S \times r_W)(r_W \times \mathrm{id}_S)(x,y,z) \\
&= (r_W \times \mathrm{id}_S)(\mathrm{id}_S \times r_W)(x \wedge y \wedge x, x \vee y \vee x, z) \\
&= (r_W \times \mathrm{id}_S)(x \wedge y \wedge x, (x \vee y \vee x) \wedge z \wedge (x \vee y \vee x), (x \vee y \vee x) \vee z \vee (x \vee y \vee x)) \\
&= ((x \wedge y \wedge x) \wedge ((x \vee y \vee x) \wedge z \wedge (x \vee y \vee x)) \wedge (x \wedge y \wedge x), \\
&\qquad (x \wedge y \wedge x) \vee ((x \vee y \vee x) \wedge z \wedge (x \vee y \vee x)) \vee (x \wedge y \wedge x), \\
&\qquad (x \vee y \vee x) \vee z \vee (x \vee y \vee x)),
\end{aligned}$$

and

$$\begin{aligned}
&(\mathrm{id}_S \times r_W)(r_W \times \mathrm{id}_S)(\mathrm{id}_S \times r_W)(x,y,z) \\
&= (\mathrm{id}_S \times r_W)(r_W \times \mathrm{id}_S)(x, y \wedge z \wedge y, y \vee z \vee y) \\
&= (\mathrm{id}_S \times r_W)(x \wedge (y \wedge z \wedge y) \wedge x, x \vee (y \wedge z \wedge y) \vee x, y \vee z \vee y) \\
&= (x \wedge (y \wedge z \wedge y) \wedge x, \\
&\qquad (x \vee (y \wedge z \wedge y) \vee x) \wedge (y \vee z \vee y) \wedge (x \vee (y \wedge z \wedge y) \vee x), \\
&\qquad (x \vee (y \wedge z \wedge y) \vee x) \vee (y \vee z \vee y) \vee (x \vee (y \wedge z \wedge y) \vee x)).
\end{aligned}$$

Using absorption (5.1) and regularity (5.2), $(x \wedge y \wedge x) \wedge ((x \vee y \vee x) \wedge z \wedge (x \vee y \vee x)) \wedge (x \wedge y \wedge x)$ simplifies to $x \wedge y \wedge z \wedge y \wedge x$. Likewise, using regularity (5.3), $(x \vee y \vee x) \vee z \vee (x \vee y \vee x)$ reduces to $x \vee y \vee z \vee y \vee x$, and by (5.1) and (5.3), $(x \vee (y \wedge z \wedge y) \vee x) \vee (y \vee z \vee y) \vee (x \vee (y \wedge z \wedge y) \vee x) = x \vee y \vee z \vee y \vee x$. So, the class of weak distributive solutions is defined by (5.37), as desired. □

Direct application of left-handedness (resp. right-handedness) to the defining identities for weak distributive solutions yields defining identities for left (resp. right) distributive solutions. Hence, the following result.

Lemma 5.5.10. *Let S be a skew lattice.*

(1) If S is left-handed, then, for any $x, y \in S$, $r_W(x,y) = r_L(x,y)$.

(2) If S is right-handed, then, for any $x, y \in S$, $r_W(x,y) = r_R(x,y)$.

Using Lemma 5.5.10 and Theorem 5.1.2, we obtain results for weak distributive solutions similar to the results for left and right distributive solutions.

Theorem 5.5.11. *(1) Weak distributive solutions are always idempotent, i.e. $r_W^2 = r_W$.*

(2) Every strong distributive solution is a weak distributive solution.

(3) Every distributive, simply cancellative and lower symmetric skew lattice is a weak distributive solution.

Proof. Denote by S_L and S_R the left and the right factor of S, respectively. By Lemma 5.5.10, $r_W = r_L$ in S_L, and $r_W = r_R$ in S_R.

(1) and (2) hold because they hold for S_L, by Proposition 5.5.1 and Theorem 5.5.7, and for S_R, by Theorem 5.5.8.

(3) Let S be a distributive, simply cancellative and lower symmetric skew lattice. By Theorem 5.1.2, it is enough to prove that both S_L and S_R are weak distributive solutions. Since S_L is left-handed, it follows from Lemma 5.5.10 that S_L is a weak distributive solution if and only if it is a left distributive solution. Similarly, S_R is a weak distributive solution if and only if it is a right distributive solution. By [65, Theorem 5.1], a left-handed skew lattice is left cancellative if and only if it is lower symmetric and simply cancellative. Similarly, a right-handed skew lattice is right cancellative if and only if it is lower symmetric and simply cancellative. Hence, S_L is distributive and left cancellative, and thus a left distributive solution by Theorem 5.5.7. Likewise, S_R is distributive and right cancellative, and thus a right distributive solution by Theorem 5.5.8. □

The Automated Theorem Prover *Prover9* was able to prove the converse of Theorem 5.5.11(3), see Code 9, Code 10, and Code 11 in the appendix, i.e. that any weak distributive solution is distributive, simply cancellative and lower symmetric.

The skew lattice from Example 5.4.8 is a weak distributive solution. The associated map r_W is defined by $r_W(x, y) = (x, x)$, for all $x, y \in S$. Thus, (S, r_W) is a right non-degenerate idempotent solution.

By [65, Theorem 5.1] different kinds of cancellation (left/right/simple/full) coincide in the presence of symmetry. As a consequence, by using the results of the Automated Theorem Prover *Prover9*, we obtain the following corollary.

Corollary 5.5.12. *Let S be a symmetric skew lattice. Using the results of the Automated Theorem Prover* Prover9, *the following properties are equivalent.*

(1) S is a left distributive solution.

(2) S is a right distributive solution.

(3) S is a weak distributive solution.

Proof. If a skew lattice is symmetric, then it is left cancellative if and only if it is right cancellative if and only if it is cancellative if and only if it is simply cancellative, see [65, Theorem 5.1] . By Theorem 5.5.11 and the Automated Theorem Prover *Prover9*, a skew lattice S is a weak distributive solution if and only if it is distributive, lower symmetric, and simply cancellative. By Theorem 5.5.7 and the Automated Theorem Prover *Prover9*, S is a left distributive solution if and only if it is distributive and left cancellative. Finally, by Theorem 5.5.8 and the Automated Theorem Prover *Prover9*, S is a right distributive if and only if it is distributive and right cancellative. It follows that all three notions of distributive solutions are equivalent for the class of symmetric skew lattices. □

One can easily notice that for a lattice, the maps (5.20), r_L, r_R, and r_W coincide. Thus, we have the following proposition.

Proposition 5.5.13. *The following conditions are equivalent for a lattice* $(L, \wedge, \vee)$.

(1) L is a strong distributive solution.

(2) L is a left distributive solution.

(3) L is a right distributive solution.

(4) L is a weak distributive solution.

One, and thus all of the above conditions are satisfied if and only if the lattice L is distributive.

Fig. 5.1 below gives an overview of all solutions discussed in this chapter, where we abbreviate skew lattice by SL and the arrows are inclusions between families of skew lattices.

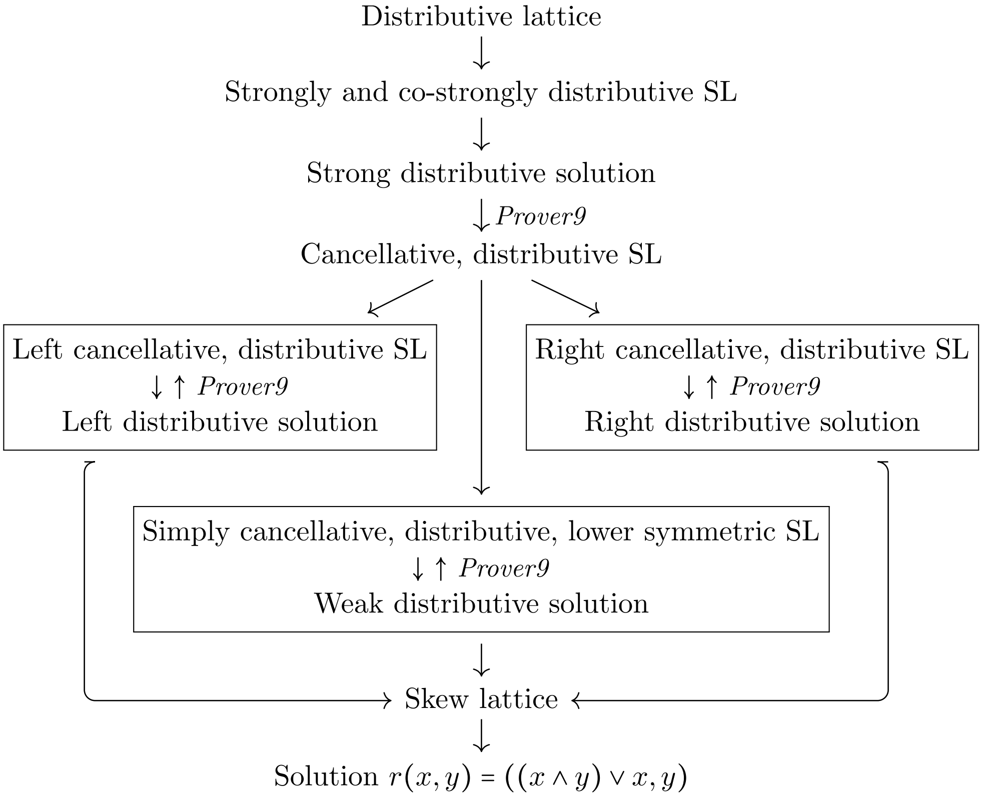

Distributive lattice
Strongly and co-strongly distributive SL
Strong distributive solution
Prover9
Cancellative, distributive SL
Left cancellative, distributive SL
Prover9
Left distributive solution
Right cancellative, distributive SL
Prover9
Right distributive solution
Simply cancellative, distributive, lower symmetric SL
Prover9
Weak distributive solution
Skew lattice
Solution $r(x,y) = ((x \wedge y) \vee x, y)$

Figure 5.1: Overview of all solutions discussed in this chapter.

From Fig. 5.1, the following corollary is clear.

Corollary 5.5.14. *The skew lattice constructed in Proposition 5.2.1 is a left, right, and weak distributive solution. If* $\{S_i \mid i \in I\}$ *is a family of pairwise disjoint distributive and* *cancellative skew lattices, then the skew lattice constructed in Proposition 5.2.2 is a left, right, and weak distributive solution. In case all skew lattices $S_i, i \in I$ are distributive and left (resp. right) cancellative, the constructed skew lattice is a left (resp. right) distributive solution.*

5.5.4 Solutions in rings

Quadratic skew lattices in rings are cancellative and distributive by [126, Theorems 2.6 and 2.8]. Cubic skew lattices in rings are cancellative and distributive by [64, Corollary 5]. The following pair of results are immediate corollaries of Theorem 5.5.7.

Corollary 5.5.15. *Let $(R, +, \cdot)$ be a ring and $S \subseteq E.(R)$ a multiplicative band that is closed under the operation $\circ$ with $x \circ y = x + y - xy$. Then, $(S, \cdot, \circ)$ is a left, right, and weak distributive solution of the Yang-Baxter equation.*

Corollary 5.5.16. *Let $(R, +, \cdot)$ be a ring and $S \subseteq E.(R)$ a multiplicative band such that the operation ∇, with $x \nabla y = (x \circ y)^2 = x + y + yx - xyx - yxy$, is closed and associative on S. Then, $(S, \cdot, \nabla)$ is a left, right, and weak distributive solution of the Yang-Baxter equation.*

Bibliography

[1] E. Acri, R. Lutowski, and L. Vendramin. Retractability of solutions to the Yang-Baxter equation and p-nilpotency of skew braces. *Internat. J. Algebra Comput.*, 30(1):91–115, 2020.

[2] J. Almeida, J.-E. Pin, and P. Weil. Semigroups whose idempotents form a subsemigroup. *Math. Proc. Cambridge Philos. Soc.*, 111(2):241–253, 1992.

[3] A. Z. Anan'in. An intriguing story about representable algebras. In *Ring theory 1989 (Ramat Gan and Jerusalem, 1988/1989)*, volume 1 of *Israel Math. Conf. Proc.*, pages 31–38. Weizmann, Jerusalem, 1989.

[4] N. Andruskiewitsch and M. Graña. From racks to pointed Hopf algebras. *Adv. Math.*, 178(2):177–243, 2003.

[5] E. Artin. Theorie der Zöpfe. *Abh. Math. Sem. Univ. Hamburg*, 4(1):47–72, 1925.

[6] D. Bachiller. *Study of the algebraic structure of left braces and the Yang-Baxter equation.* PhD thesis, Universitat Autònoma de Barcelona, 2016.

[7] D. Bachiller. Extensions, matched products, and simple braces. *J. Pure Appl. Algebra*, 222(7):1670–1691, 2018.

[8] D. Bachiller. Solutions of the Yang-Baxter equation associated to skew left braces, with applications to racks. *J. Knot Theory Ramifications*, 27(8):1850055, 36, 2018.

[9] D. Bachiller, F. Cedó, and E. Jespers. Solutions of the Yang-Baxter equation associated with a left brace. *J. Algebra*, 463:80–102, 2016.

[10] D. Bachiller, F. Cedó, E. Jespers, and J. Okniński. A family of irretractable square-free solutions of the Yang-Baxter equation. *Forum Math.*, 29(6):1291–1306, 2017.

[11] D. Bachiller, F. Cedó, E. Jespers, and J. Okniński. Iterated matched products of finite braces and simplicity; new solutions of the Yang-Baxter equation. *Trans. Amer. Math. Soc.*, 370(7):4881–4907, 2018.

[12] D. Bachiller, F. Cedó, E. Jespers, and J. Okniński. Asymmetric product of left braces and simplicity; new solutions of the Yang-Baxter equation. *Commun. Contemp. Math.*, 21(8):1850042, 30, 2019.

[13] D. Bachiller, F. Cedó, and L. Vendramin. A characterization of finite multipermutation solutions of the Yang-Baxter equation. *Publ. Mat.*, 62(2):641–649, 2018.

[14] V. Bardakov and T. Nasybullov. Embeddings of quandles into groups. *J. Algebra Appl.*, 19(7):2050136, 20, 2020.

[15] K. Bauwens and M. Van den Bergh. Normalizing extensions of the two-Veronese of a three-dimensional Artin-Schelter regular algebra on two generators. *J. Algebra*, 205(2):368–390, 1998.

[16] R. J. Baxter. Colorings of a hexagonal lattice. *J. Mathematical Phys.*, 11:784–789, 1970.

[17] R. J. Baxter. Three-colorings of the square lattice: A hard squares model. *J. Mathematical Phys.*, 11(10):3116–3124, 1970.

[18] R. J. Baxter. Eight-Vertex Model in Lattice Statistics. *Phys. Rev. Lett.*, 26:832–833, 1971.

[19] R. J. Baxter. Partition function of the eight-vertex lattice model. *Ann. Physics*, 70(1):193–228, 1972.

[20] R. J. Baxter. *Exactly solved models in statistical mechanics.* Academic Press, Inc. [Harcourt Brace Jovanovich, Publishers], London, 1982.

[21] F. A. Berezin, G. P. Pohil, and V. M. Finkel′berg. The Schrödinger equation for a system of one-dimensional particles with point interaction. *Vestnik Moskov. Univ. Ser. I Mat. Meh.*, 1964(1):21–28, 1964.

[22] F. A. Berezin and V. N. Sushko. Relativistic two-dimensional model of a self-interacting fermion field with nonvanishing rest mass. *Zh.Eksp.Theor.Fiz.*, 48:1293–1306, [Sov. Phys. JETP 21 (1965), 865–873], 1965.

[23] H. Bethe. Zur theorie der metalle. *Zeitschrift für Physik*, 71(3):205–226, 1931.

[24] M. Bonatto, A. Crans, T. Nasybullov, and G. Whitney. Quandles with orbit series conditions. *J. Algebra*, 567:284–309, 2021.

[25] E. Brézin and J. Zinn-Justin. Un problème à N corps soluble. *C. R. Acad. Sci. Paris Sér. A-B*, 263:B670–B673, 1966.

[26] T. Brzeziński. Towards semi-trusses. *Rev. Roumaine Math. Pures Appl.*, 63(2):75–89, 2018.

[27] T. Brzeziński. Trusses: between braces and rings. *Trans. Amer. Math. Soc.*, 372(6):4149–4176, 2019.

[28] O. Bühler. *A brief introduction to classical, statistical, and quantum mechanics*, volume 13 of *Courant Lecture Notes in Mathematics*. New York University, Courant Institute of Mathematical Sciences, New York; American Mathematical Society, Providence, RI, 2006.

[29] S. Burris and H. P. Sankappanavar. *A course in universal algebra*, volume 78 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1981.

[30] M. Castelli, F. Catino, M. M. Miccoli, and G. Pinto. Dynamical extensions of quasi-linear left cycle sets and the Yang-Baxter equation. *J. Algebra Appl.*, 18(11):1950220, 16, 2019.

[31] M. Castelli, F. Catino, and G. Pinto. A new family of set-theoretic solutions of the Yang-Baxter equation. *Comm. Algebra*, 46(4):1622–1629, 2018.

[32] M. Castelli, F. Catino, and G. Pinto. Indecomposable involutive set-theoretic solutions of the Yang-Baxter equation. *J. Pure Appl. Algebra*, 223(10):4477–4493, 2019.

[33] M. Castelli, F. Catino, and P. Stefanelli. Indecomposable involutive set-theoretic solutions of the Yang-Baxter equation and orthogonal dynamical extensions of cycle sets. *Mediterr. J. Math.*, 18(6):Paper No. 246, 27, 2021.

[34] M. Castelli, F. Catino, and P. Stefanelli. Left non-degenerate set-theoretic solutions of the Yang-Baxter equation and dynamical extensions of q-cycle sets. *Accepted for publication in Journal of Algebra and Its Applications*, 2021. DOI:10.1142/S0219498822501547.

[35] M. Castelli, G. Pinto, and W. Rump. On the indecomposable involutive set-theoretic solutions of the Yang-Baxter equation of prime-power size. *Comm. Algebra*, 48(5):1941–1955, 2020.

[36] F. Catino, I. Colazzo, and P. Stefanelli. Regular subgroups of the affine group and asymmetric product of radical braces. *J. Algebra*, 455:164–182, 2016.

[37] F. Catino, I. Colazzo, and P. Stefanelli. Semi-braces and the Yang-Baxter equation. *J. Algebra*, 483:163–187, 2017.

[38] F. Catino, I. Colazzo, and P. Stefanelli. The matched product of set-theoretical solutions of the Yang-Baxter equation. *J. Pure Appl. Algebra*, 224(3):1173–1194, 2020.

[39] F. Catino, I. Colazzo, and P. Stefanelli. The matched product of the solutions to the Yang-Baxter equation of finite order. *Mediterr. J. Math.*, 17(2):Paper No. 58, 22, 2020.

[40] F. Catino, I. Colazzo, and P. Stefanelli. Set-theoretic solutions to the Yang-Baxter equation and generalized semi-braces. *Forum Math.*, 33(3):757–772, 2021.

[41] F. Catino, M. Mazzotta, M. M. Miccoli, and P. Stefanelli. Set-theoretic solutions of the Yang-Baxter equation associated to skew inverse semi-braces, 2021. arXiv:2105.02537.

[42] F. Catino, M. Mazzotta, and P. Stefanelli. Inverse semi-braces and the Yang-Baxter equation. *J. Algebra*, 573:576–619, 2021.

[43] F. Cedó. Left braces: solutions of the Yang-Baxter equation. *Adv. Group Theory Appl.*, 5:33–90, 2018.

[44] F. Cedó, T. Gateva-Ivanova, and A. Smoktunowicz. On the Yang-Baxter equation and left nilpotent left braces. *J. Pure Appl. Algebra*, 221(4):751–756, 2017.

[45] F. Cedó, T. Gateva-Ivanova, and A. Smoktunowicz. Braces and symmetric groups with special conditions. *J. Pure Appl. Algebra*, 222(12):3877–3890, 2018.

[46] F. Cedó, E. Jespers, and A. del Río. Involutive Yang-Baxter groups. *Trans. Amer. Math. Soc.*, 362(5):2541–2558, 2010.

[47] F. Cedó, E. Jespers, Ł. Kubat, A. Van Antwerpen, and C. Verwimp. On various types of nilpotency of the structure monoid and group of a set-theoretic solution of the Yang-Baxter equation, 2020. arXiv:2011.01724.

[48] F. Cedó, E. Jespers, and J. Okniński. Retractability of set theoretic solutions of the Yang-Baxter equation. *Adv. Math.*, 224(6):2472–2484, 2010.

[49] F. Cedó, E. Jespers, and J. Okniński. Braces and the Yang-Baxter equation. *Commun. Math. Phys.*, 327:101–116, 2014.

[50] F. Cedó, E. Jespers, and J. Okniński. An abundance of simple left braces with abelian multiplicative Sylow subgroups. *Rev. Mat. Iberoam.*, 36(5):1309–1332, 2020.

[51] F. Cedó, E. Jespers, and J. Okniński. Every finite abelian group is a subgroup of the additive group of a finite simple left brace. *J. Pure Appl. Algebra*, 225(1):Paper No. 106476, 10, 2021.

[52] F. Cedó, E. Jespers, and C. Verwimp. Structure monoids of set-theoretic solutions of the Yang-Baxter equation. *Publ. Mat.*, 65:499–528, 2021.

[53] F. Cedó, E. Jespers, and C. Verwimp. Corrigendum and addendum to "Structure monoids of set-theoretic solutions of the Yang-Baxter equation", 2022. arXiv:2202.03174.

[54] F. Cedó and J. Okniński. Gröbner bases for quadratic algebras of skew type. *Proc. Edinb. Math. Soc. (2)*, 55(2):387–401, 2012.

[55] F. Cedó, A. Smoktunowicz, and L. Vendramin. Skew left braces of nilpotent type. *Proc. Lond. Math. Soc. (3)*, 118(6):1367–1392, 2019.

[56] W. E. Clark, M. Elhamdadi, M. Saito, and T. Yeatman. Quandle colorings of knots and applications. *J. Knot Theory Ramifications*, 23(6):1450035, 29, 2014.

[57] A. H. Clifford. Bands of semigroups. *Proc. Amer. Math. Soc.*, 5:499–504, 1954.

[58] A. H. Clifford and G. B. Preston. *The algebraic theory of semigroups. Vol. I.* Mathematical Surveys, No. 7. American Mathematical Society, Providence, R.I., 1961.

[59] I. Colazzo. *Left semi-braces and the Yang-Baxter equation.* PhD thesis, Universitá del Salento, 2017.

[60] I. Colazzo, E. Jespers, A. Van Antwerpen, and C. Verwimp. Left non-degenerate set-theoretic solutions of the Yang-Baxter equation and semitrusses, 2021. arXiv:2109.04978.

[61] I. Colazzo and A. Van Antwerpen. The algebraic structure of left semi-trusses. *J. Pure Appl. Algebra*, 225(2):Paper No. 106467, 15, 2021.

[62] A. S. Crans. *Lie 2-algebras.* PhD thesis, University of California, Riverside, 2004.

[63] K. Cvetko-Vah. A new proof of Spinks' theorem. *Semigroup Forum*, 73(2):267–272, 2006.

[64] K. Cvetko-Vah. Internal decompositions of skew lattices. *Comm. Algebra*, 35(1):243–247, 2007.

[65] K. Cvetko-Vah, M. Kinyon, J. Leech, and M. Spinks. Cancellation in skew lattices. *Order*, 28(1):9–32, 2011.

[66] K. Cvetko-Vah and J. Pita Costa. On the coset laws for skew lattices in rings. *Novi Sad J. Math.*, 40(3):11–25, 2010.

[67] K. Cvetko-Vah and J. Pita Costa. On the coset laws for skew lattices. *Semigroup Forum*, 83(3):395–411, 2011.

[68] K. Cvetko-Vah and J. Pita Costa. On the update operation in skew lattices. *J. Appl. Logics*, 5(8):1765–1774, 2018.

[69] K. Cvetko-Vah and C. Verwimp. Skew lattices and set-theoretic solutions of the Yang-Baxter equation. *J. Algebra*, 542:65–92, 2020.

[70] P. Dehornoy. Set-theoretic solutions of the Yang-Baxter equation, RC-calculus, and Garside germs. *Adv. Math.*, 282:93–127, 2015.

[71] V. G. Drinfeld. Quantum groups. In *Proceedings of the International Congress of Mathematicians, Vol. 1, 2 (Berkeley, Calif., 1986)*, pages 798–820. Amer. Math. Soc., Providence, RI, 1987.

[72] V. G. Drinfeld. On some unsolved problems in quantum group theory. In *Quantum groups (Leningrad, 1990)*, volume 1510 of *Lecture Notes in Math.*, pages 1–8. Springer, Berlin, 1992.

[73] H. A. Dye. Unitary solutions to the Yang-Baxter equation in dimension four. *Quantum Inf. Process.*, 2(1-2):117–151 (2003), 2002.

[74] M. Eisermann. Yang-Baxter deformations and rack cohomology. *Trans. Amer. Math. Soc.*, 366(10):5113–5138, 2014.

[75] P. Etingof, T. Schedler, and A. Soloviev. Set-theoretical solutions to the quantum Yang-Baxter equation. *Duke Math. J.*, 100(2):169–209, 1999.

[76] C. Fan and F. Y. Wu. General lattice model of phase transitions. *Phys. Rev. B*, 2:723–733, Aug 1970.

[77] D. R. Farkas. Miscellany on Bieberbach group algebras. *Pacific J. Math.*, 59(2):427–435, 1975.

[78] R. Fenn and C. Rourke. Racks and links in codimension two. *J. Knot Theory Ramifications*, 1(4):343–406, 1992.

[79] T. Gateva-Ivanova. Quadratic algebras, Yang-Baxter equation, and Artin-Schelter regularity. *Adv. Math.*, 230(4-6):2152–2175, 2012.

[80] T. Gateva-Ivanova. Set-theoretic solutions of the Yang-Baxter equation, braces and symmetric groups. *Adv. Math.*, 338:649–701, 2018.

[81] T. Gateva-Ivanova. The braided group of a square-free solution of the Yang-Baxter equation and its group algebra, 2019. arXiv:1902.00962.

[82] T. Gateva-Ivanova. A combinatorial approach to noninvolutive set-theoretic solutions of the Yang-Baxter equation. *Publ. Mat.*, 65:747–808, 2021.

[83] T. Gateva-Ivanova and P. Cameron. Multipermutation solutions of the Yang-Baxter equation. *Comm. Math. Physics*, 309:583–621, 2012.

[84] T. Gateva-Ivanova, E. Jespers, and J. Okniński. Quadratic algebras of skew type and the underlying monoids. *J. Algebra*, 270(2):635–659, 2003.

[85] T. Gateva-Ivanova and S. Majid. Set-theoretic solutions of the Yang-Baxter equation, graphs and computations. *J. Symbolic Comput.*, 42(11-12):1079–1112, 2007.

[86] T. Gateva-Ivanova and S. Majid. Matched pairs approach to set theoretic solutions of the Yang-Baxter equation. *J. Algebra*, 319(4):1462–1529, 2008.

[87] T. Gateva-Ivanova and S. Majid. Quantum spaces associated to multipermutation solutions of level two. *Algebr. Represent. Theory*, 14(2):341–376, 2011.

[88] T. Gateva-Ivanova and M. Van den Bergh. Semigroups of I-type. *J. Algebra*, 206(1):97–112, 1998.

[89] A. Ghobadi. Drinfeld twists on skew braces, 2021. arXiv:2105.03286v1.

[90] T. Gombor and B. Pozsgay. Superintegrable cellular automata and dual unitary gates from Yang-Baxter maps, 2022. arXiv:2112.01854.

[91] D. J. Griffiths. *Introduction to Quantum Mechanics*. Pearson Prentice Hall, 2nd edition edition, 2004.

[92] L. Guarnieri and L. Vendramin. Skew braces and the Yang-Baxter equation. *Math. Comp.*, 86(307):2519–2534, 2017.

[93] J. M. Howie. *An introduction to semigroup theory*. L. M. S. Monographs, No. 7. Academic Press [Harcourt Brace Jovanovich, Publishers], London-New York, 1976.

[94] P. Jedlička, A. Pilitowska, and A. Zamojska-Dzienio. The retraction relation for biracks. *J. Pure Appl. Algebra*, 223(8):3594–3610, 2019.

[95] P. Jedlička, A. Pilitowska, and A. Zamojska-Dzienio. The construction of multipermutation solutions of the Yang-Baxter equation of level 2. *J. Combin. Theory Ser. A*, 176:105295, 35, 2020.

[96] P. Jedlička, A. Pilitowska, and A. Zamojska-Dzienio. Indecomposable involutive solutions of the Yang-Baxter equation of multipermutational level 2 with abelian permutation group. *Forum Math.*, 33(5):1083–1096, 2021.

[97] E. Jespers, Ł. Kubat, and A. Van Antwerpen. The structure monoid and algebra of a non-degenerate set-theoretic solution of the Yang-Baxter equation. *Trans. Amer. Math. Soc.*, 372(10):7191–7223, 2019.

[98] E. Jespers, Ł. Kubat, and A. Van Antwerpen. Corrigendum and addendum to "The structure monoid and algebra of a non-degenerate set-theoretic solution of the Yang-Baxter equation". *Trans. Amer. Math. Soc.*, 373(6):4517–4521, 2020.

[99] E. Jespers, Ł. Kubat, A. Van Antwerpen, and L. Vendramin. Factorizations of skew braces. *Math. Ann.*, 375(3-4):1649–1663, 2019.

[100] E. Jespers, Ł. Kubat, A. Van Antwerpen, and L. Vendramin. Radical and weight of skew braces and their applications to structure groups of solutions of the Yang-Baxter equation. *Adv. Math.*, 385:Paper No. 107767, 20, 2021.

[101] E. Jespers and J. Okniński. Monoids and groups of I-type. *Algebr. Represent. Theory*, 8(5):709–729, 2005.

[102] E. Jespers and J. Okniński. Quadratic algebras of skew type. In *Algebras, rings and their representations*, pages 93–112. World Sci. Publ., Hackensack, NJ, 2006.

[103] E. Jespers and J. Okniński. *Noetherian semigroup algebras*, volume 7 of *Algebra and Applications*. Springer, Dordrecht, 2007.

[104] E. Jespers and D. Riley. Nilpotent linear semigroups. *Internat. J. Algebra Comput.*, 16(1):141–160, 2006.

[105] E. Jespers and A. Van Antwerpen. Left semi-braces and solutions of the Yang-Baxter equation. *Forum Math.*, 31(1):241–263, 2019.

[106] E. Jespers and M. Van Campenhout. Finitely generated algebras defined by homogeneous quadratic monomial relations and their underlying monoids II. *J. Algebra*, 492:524–546, 2017.

[107] M. Jimbo. A q-difference analogue of $U(\mathfrak{g})$ and the Yang-Baxter equation. *Lett. Math. Phys.*, 10(1):63–69, 1985.

[108] M. Jimbo. A q-analogue of $U(\mathfrak{gl}(N+1))$, Hecke algebra, and the Yang-Baxter equation. *Lett. Math. Phys.*, 11(3):247–252, 1986.

[109] V. F. R. Jones. Hecke algebra representations of braid groups and link polynomials. *Annals of Mathematics*, 126(2):335–388, 1987.

[110] V. F. R. Jones. On knot invariants related to some statistical mechanical models. *Pacific J. Math.*, 137(2):311–334, 1989.

[111] P. Jordan. Über nichtkommutative Verbände. *Arch. Math. (Basel)*, 2:56–59, 1949.

[112] D. Joyce. A classifying invariant of knots, the knot quandle. *J. Pure Appl. Algebra*, 23(1):37–65, 1982.

[113] L. H. Kauffman and S. J. Lomonaco. Quantum computing and quantum topology. In *Mathematics of quantum computation and quantum technology*, Chapman & Hall/CRC Appl. Math. Nonlinear Sci. Ser., pages 409–514. Chapman & Hall/CRC, Boca Raton, FL, 2008.

[114] M. Kępczyk. A ring which is a sum of two PI subrings is always a PI ring. *Israel J. Math.*, 221(1):481–487, 2017.

[115] N. Kimura. The structure of idempotent semigroups. I. *Pacific J. Math.*, 8:257–275, 1958.

[116] M. Kinyon, J. Leech, and J. Pita Costa. Distributivity in skew lattices. *Semigroup Forum*, 91(2):378–400, 2015.

[117] A. Koch and P. J. Truman. Opposite skew left braces and applications. *J. Algebra*, 546:218–235, 2020.

[118] A. Konovalov, A. Smoktunowicz, and L. Vendramin. On skew braces and their ideals. *Exp. Math.*, 30(1):95–104, 2021.

[119] P. P. Kulish, N. Y. Reshetikhin, and E. K. Sklyanin. Yang-Baxter equations and representation theory. I. *Lett. Math. Phys.*, 5(5):393–403, 1981.

[120] V. Lebed. Cohomology of idempotent braidings with applications to factorizable monoids. *Internat. J. Algebra Comput.*, 27(4):421–454, 2017.

[121] V. Lebed. Applications of self-distributivity to Yang-Baxter operators and their cohomology. *J. Knot Theory Ramifications*, 27(11):1843012, 20, 2018.

[122] V. Lebed and A. Mortier. Abelian quandles and quandles with abelian structure group. *J. Pure Appl. Algebra*, 225(1):Paper No. 106474, 22, 2021.

[123] V. Lebed and L. Vendramin. Cohomology and extensions of braces. *Pacific J. Math.*, 284(1):191–212, 2016.

[124] V. Lebed and L. Vendramin. Homology of left non-degenerate set-theoretic solutions to the Yang-Baxter equation. *Adv. Math.*, 304:1219–1261, 2017.

[125] V. Lebed and L. Vendramin. On structure groups of set-theoretic solutions to the Yang-Baxter equation. *Proc. Edinb. Math. Soc. (2)*, 62(3):683–717, 2019.

[126] J. Leech. Skew lattices in rings. *Algebra Universalis*, 26(1):48–72, 1989.

[127] J. Leech. Normal skew lattices. *Semigroup Forum*, 44(1):1–8, 1992.

[128] J. Leech. The geometric structure of skew lattices. *Trans. Amer. Math. Soc.*, 335(2):823–842, 1993.

[129] J. Leech. Recent developments in the theory of skew lattices. *Semigroup forum*, 52(1):7–24, 1996.

[130] J. Leech. *Noncommutative Lattices: Skew Lattices, Skew Boolean Algebras and Beyond.* Famnit Lectures / Famnitova predavanja 4, Koper, 2020.

[131] E. H. Lieb. Exact solution of the f model of an antiferroelectric. *Phys. Rev. Lett.*, 18(24):1046–1048, 1967.

[132] E. H. Lieb. Exact solution of the two-dimensional slater kdp model of a ferroelectric. *Phys. Rev. Lett.*, 19(3):108–110, 1967.

[133] E. H. Lieb. Residual entropy of square ice. *Physical Review*, 162(1):162–172, 1967.

[134] E. H. Lieb and W. Liniger. Exact analysis of an interacting bose gas. i. the general solution and the ground state. *Physical Review (U.S.) Superseded in part by Phys. Rev. A, Phys. Rev. B: Solid State, Phys. Rev. C, and Phys. Rev. D*, 130, 5 1963.

[135] J.-H. Lu, M. Yan, and Y.-C. Zhu. On the set-theoretical Yang-Baxter equation. *Duke Math. J.*, 104(1):1–18, 2000.

[136] A. I. Malcev. Nilpotent semigroups. *Uc. Zap. Ivanovsk. Ped. Inst.*, 4:107–111, 1953.

[137] V. Manturov. *Knot Theory.* Chapman & Hall/CRC, Boca Raton, FL, 2004.

[138] W. McCune. Mace4 reference manual and guide. *CoRR*, cs.SC/0310055, 2003.

[139] W. McCune. Prover9 and mace4. `http://www.cs.unm.edu/~mccune/prover9/`, 2005–2010.

[140] J. B. McGuire. Study of exactly soluble one-dimensional N-body problems. *J. Mathematical Phys.*, 5:622–636, 1964.

[141] D. McLean. Idempotent semigroups. *Amer. Math. Monthly*, 61:110–113, 1954.

[142] M. M. Miccoli. Almost semi-braces and the Yang-Baxter equation. *Note Mat.*, 38(1):83–88, 2018.

[143] S. Montgomery. *Hopf algebras and their actions on rings.* Regional Conference Series on Mathematics 82. AMS, 3 edition, 1999.

[144] B. H. Neumann. Groups with finite classes of conjugate elements. *Proc. London Math. Soc. (3)*, 1:178–187, 1951.

[145] B. H. Neumann and T. Taylor. Subsemigroups of nilpotent groups. *Proc. Roy. Soc. London Ser. A*, 274:1–4, 1963.

[146] F. F. Nichita. On the set-theoretical Yang-Baxter equation. *Acta Universitatis Apulensis*, (5):97–100, 2003.

[147] J. Okniński. Nilpotent semigroups of matrices. *Math. Proc. Cambridge Philos. Soc.*, 120(4):617–630, 1996.

[148] J. Okniński. *Semigroups of matrices*, volume 6 of *Series in Algebra.* World Scientific Publishing Co., Inc., River Edge, NJ, 1998.

[149] L. Onsager. Crystal statistics. I. A two-dimensional model with an order-disorder transition. *Phys. Rev. (2)*, 65:117–149, 1944.

[150] J. H. H. Perk and H. Au-Yang. Yang-Baxter equations. *Encyclopedia of Mathematical Physics*, pages 465–473, 2006.

[151] M. Petrich. A construction and a classification of bands. *Math. Nachr.*, 48:263–274, 1971.

[152] M. Petrich and N. R. Reilly. *Completely regular semigroups*, volume 23 of *Canadian Mathematical Society Series of Monographs and Advanced Texts*. John Wiley & Sons, Inc., New York, 1999. A Wiley-Interscience Publication.

[153] J. Pita Costa. Coset laws for categorical skew lattices. *Algebra Universalis*, 68(1-2):75–89, 2012.

[154] J. Pita Costa. On the coset category of a skew lattice. *Demonstr. Math.*, 47(3):539–554, 2014.

[155] J. Pita Costa and J. Leech. On the coset structure of distributive skew lattices. *Art Discrete Appl. Math.*, 2(2):Paper No. 2.05, 17, 2019.

[156] J. H. Przytycki. 3-coloring and other elementary invariants of knots. In *Knot theory (Warsaw, 1995)*, volume 42 of *Banach Center Publ.*, pages 275–295. Polish Acad. Sci. Inst. Math., Warsaw, 1998.

[157] K. Reidemeister. Elementare Begründung der Knotentheorie. *Abh. Math. Sem. Univ. Hamburg*, 5(1):24–32, 1927.

[158] D. J. S. Robinson. *A course in the theory of groups*, volume 80 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1996.

[159] L. H. Rowen. General polynomial identities. II. *J. Algebra*, 38(2):380–392, 1976.

[160] L. H. Rowen. *Ring theory*. Academic Press, Inc., Boston, MA, student edition, 1991.

[161] W. Rump. A decomposition theorem for square-free unitary solutions of the quantum Yang-Baxter equation. *Adv. Math.*, 193(1):40–55, 2005.

[162] W. Rump. Modules over braces. *Algebra Discrete Math.*, (2):127–137, 2006.

[163] W. Rump. Braces, radical rings, and the quantum Yang-Baxter equation. *J. Algebra*, 307(1):153–170, 2007.

[164] W. Rump. Classification of cyclic braces. *J. Pure Appl. Algebra*, 209(3):671–685, 2007.

[165] W. Rump. Semidirect products in algebraic logic and solutions of the quantum Yang-Baxter equation. *J. Algebra Appl.*, 7(4):471–490, 2008.

[166] W. Rump. A covering theory for non-involutive set-theoretic solutions to the Yang-Baxter equation. *J. Algebra*, 520:136–170, 2019.

[167] W. Rump. Set-theoretic solutions to the Yang-Baxter equation, skew-braces, and related near-rings. *J. Algebra Appl.*, 18(8):1950145, 22, 2019.

[168] W. Rump. Classification of indecomposable involutive set-theoretic solutions to the Yang-Baxter equation. *Forum Math.*, 32(4):891–903, 2020.

[169] W. Rump. Degenerate involutive set-theoretic solutions to the Yang-Baxter equation. *J. Algebra*, 590:293–312, 2022.

[170] L. Šamaj and Z. Bajnok. *Introduction to the statistical physics of integrable many-body systems*. Cambridge University Press, Cambridge, 2013.

[171] B. M. Šaĭn. Pseudo-semilattices and pseudo-lattices. *Izv. Vysš. Učebn. Zaved. Matematika*, 2(117):81–94, 1972.

[172] A. Smoktunowicz. A note on set-theoretic solutions of the Yang-Baxter equation. *J. Algebra*, 500:3–18, 2018.

[173] A. Smoktunowicz and L. Vendramin. On skew braces (with an appendix by N. Byott and L. Vendramin). *J. Comb. Algebra*, 2(1):47–86, 2018.

[174] A. Soloviev. Non-unitary set-theoretical solutions to the quantum Yang-Baxter equation. *Math. Res. Lett.*, 7(5-6):577–596, 2000.

[175] M. Spinks. On middle distributivity for skew lattices. *Semigroup Forum*, 61(3):341–345, 2000.

[176] D. Stanovský and P. Vojtěchovský. Idempotent solutions of the Yang-Baxter equation and twisted group division. *Fund. Math.*, 255(1):51–68, 2021.

[177] B. Sutherland. Two-dimensional hydrogen bonded crystals without the ice rule. *Journal of Mathematical Physics*, 11(11):3183–3186, 1970.

[178] M. Takeuchi. Survey on matched pairs of groups—an elementary approach to the ESS-LYZ theory. In *Noncommutative geometry and quantum groups (Warsaw, 2001)*, volume 61 of *Banach Center Publ.*, pages 305–331. Polish Acad. Sci. Inst. Math., Warsaw, 2003.

[179] V. G. Turaev. The Yang-Baxter equation and invariants of links. *Inventiones mathematicae*, 92(3):527–553, 1988.

[180] L. Vendramin. Problems on skew left braces. *Adv. Group Theory Appl.*, 7:15–37, 2019.

[181] C. Verwimp. Braces and the Yang-Baxter equation. Master's thesis, Vrije Universiteit Brussel, Belgium, 2018.

[182] P. Vojtěchovský and S. Y. Yang. Enumeration of racks and quandles up to isomorphism. *Math. Comp.*, 88(319):2523–2540, 2019.

[183] F. Y. Wu. The Yang-Baxter equation in knot theory. *Internat. J. Modern Phys. B*, 7(20-21):3737–3750, 1993.

[184] C. N. Yang. Some exact results for the many-body problem in one dimension with repulsive delta-function interaction. *Phys. Rev. Lett.*, 19(23):1312–1315, 1967.

[185] C. N. Yang. S-matrix for one-dimensional n-body problem with repulsive or attractive δ- function interaction. *Phys. Rev.*, 168:1920–1923, 1968.

[186] C. N. Yang and M. L. Ge. *Braid Group, Knot Theory and Statistical Mechanics II.* World Scientific, 1994.

[187] A. B. Zamolodchikov. Z_4-symmetric factorized S-matrix in two space-time dimensions. *Comm. Math. Phys.*, 69(2):165–178, 1979.

[188] A. B. Zamolodchikov and A. B. Zamolodchikov. Relativistic factorized S-matrix in two dimensions having $O(N)$ isotopic symmetry. *Nuclear Phys. B*, 133(3):525–535, 1978.

[189] A. B. Zamolodchikov and A. B. Zamolodchikov. Factorized S-matrices in two dimensions as the exact solutions of certain relativistic quantum field theory models. *Ann. Physics*, 120(2):253–291, 1979.

[190] B. Zygelman. *A first Introduction to Quantum Computing and Information.* Springer, 2018.

Appendix

In this appendix, we include the input and output codes of the Automated Theorem Prover *Prover9* and *Mace4*, used in Chapter 5.

Code 1: Any strong distributive solution is distributive.

```
============================== INPUT =================================

formulas(assumptions).
ClearAll.
x ^ x = x.
x v x = x.
x ^ (y ^ z) = (x ^ y) ^ z.
x v (y v z) = (x v y) v z.
x ^ (x v y) = x.
x v (x ^ y) = x.
(x v y) ^ y = y.
(x ^ y) v y = y.
x ^ (y ^ ((x v y) ^ z)) = x ^ (y ^ z).
(x ^ y) v ((x v y) ^ z) = (x v (y ^ z)) ^ (y v z).
x v (y v z) = x v (((y ^ z) v y) v z).
end_of_list.

formulas(goals).
(x ^ (y v z)) ^ x = ((x ^ y) ^ x) v ((x ^ z) ^ x).
(x v (y ^ z)) v x = ((x v y) v x) ^ ((x v z) v x).
end_of_list.

============================== end of input ==========================

============================== PROOF =================================

% Proof 1 at 0.04 (+ 0.01) seconds.
% Length of proof is 30.
% Level of proof is 8.
% Maximum clause weight is 25.000.
% Given clauses 47.

2 (x v (y ^ z)) v x = ((x v y) v x) ^ ((x v z) v x) # label(non_clause) # label(goal).  [goal].
5 x v x = x.  [assumption].
6 x ^ (y ^ z) = (x ^ y) ^ z.  [assumption].
7 (x ^ y) ^ z = x ^ (y ^ z).  [copy(6),flip(a)].
8 x v (y v z) = (x v y) v z.  [assumption].
```

```
9 (x v y) v z = x v (y v z).  [copy(8),flip(a)].
10 x ^ (x v y) = x.  [assumption].
11 x v (x ^ y) = x.  [assumption].
12 (x v y) ^ y = y.  [assumption].
13 (x ^ y) v y = y.  [assumption].
14 x ^ (y ^ ((x v y) ^ z)) = x ^ (y ^ z).  [assumption].
15 (x ^ y) v ((x v y) ^ z) = (x v (y ^ z)) ^ (y v z).  [assumption].
20 (c4 v (c5 ^ c6)) v c4 != ((c4 v c5) v c4) ^ ((c4 v c6) v c4).  [deny(2)].
21 c4 v ((c5 ^ c6) v c4) != (c4 v (c5 v c4)) ^ (c4 v (c6 v c4)).
↪  [copy(20),rewrite([9(7),9(12),9(17)])].
24 x v (y v (x v y)) = x v y.  [para(9(a,1),5(a,1))].
28 (x v y) ^ (x v (y v z)) = x v y.  [para(9(a,1),10(a,1,2))].
32 (x v y) ^ (y ^ z) = y ^ z.  [para(12(a,1),7(a,1,1)),flip(a)].
33 (x v (y v z)) ^ z = z.  [para(9(a,1),12(a,1,1))].
46 ((x v (y ^ z)) ^ (y v z)) v u = (x ^ y) v (((x v y) ^ z) v u).  [para(15(a,1),9(a,1,1))].
54 x v ((y v x) ^ z) = (y v x) ^ (x v z).
↪  [para(12(a,1),15(a,1,1)),rewrite([9(2),5(1),9(6),11(5)])].
55 (x ^ (y v z)) v z = (x v z) ^ (y v z).  [para(12(a,1),15(a,2,1,2)),rewrite([33(5),9(6),5(5)])].
105 x ^ ((y v x) ^ z) = x ^ z.  [para(32(a,1),14(a,1)),rewrite([9(2),5(1),32(6)])].
109 (x v (y v x)) ^ z = (y v x) ^ z.  [para(24(a,1),32(a,1,1)),rewrite([105(5)]),flip(a)].
114 c4 v ((c5 ^ c6) v c4) != (c5 v c4) ^ (c4 v (c6 v c4)).  [back_rewrite(21),rewrite([109(18)])].
157 x v (y v x) = (y v x) ^ (x v y).
↪  [para(5(a,1),28(a,1,2)),rewrite([9(2),109(4),9(5)]),flip(a)].
172 ((c5 ^ c6) v c4) ^ (c4 v (c5 ^ c6)) != (c5 v c4) ^ ((c6 v c4) ^ (c4 v c6)).
↪  [back_rewrite(114),rewrite([157(7),157(19)])].
296 (x ^ y) v z = (x v z) ^ (y v z).
↪  [para(13(a,1),46(a,2,2)),rewrite([55(5),9(3),13(2)]),flip(a)].
417 (c5 v c4) ^ ((c6 v c4) ^ (c4 v (c5 ^ c6))) != (c5 v c4) ^ ((c6 v c4) ^ (c4 v c6)).
↪  [back_rewrite(172),rewrite([296(5),7(13)])].
565 (x v y) ^ ((z v y) ^ (y v (x ^ z))) = (x v y) ^ ((z v y) ^ (y v z)).
↪  [para(296(a,1),157(a,1,2)),rewrite([54(4),157(3),296(7),7(11)]),flip(a)].
566 $F.  [resolve(565,a,417,a)].

============================== end of proof ==========================
```

Code 2: Any strong distributive solution is left cancellative.

```
============================== INPUT =================================

formulas(assumptions).
ClearAll.
x ^ x = x.
x v x = x.
x ^ (y ^ z) = (x ^ y) ^ z.
x v (y v z) = (x v y) v z.
x ^ (x v y) = x.
x v (x ^ y) = x.
(x v y) ^ y = y.
(x ^ y) v y = y.
x ^ (y ^ ((x v y) ^ z)) = x ^ (y ^ z).
(x ^ y) v ((x v y) ^ z) = (x v (y ^ z)) ^ (y v z).
x v (y v z) = x v (((y ^ z) v y) v z).
end_of_list.

formulas(goals).
x ^ y = x ^ z & x v y = x v z -> y = z.
end_of_list.

============================== end of input ==========================
============================== PROOF =================================

% Proof 1 at 0.20 (+ 0.02) seconds.
% Length of proof is 78.
% Level of proof is 18.
% Maximum clause weight is 27.000.
% Given clauses 171.

1 x ^ y = x ^ z & x v y = x v z -> y = z # label(non_clause) # label(goal).  [goal].
3 x ^ x = x.  [assumption].
4 x v x = x.  [assumption].
5 x ^ (y ^ z) = (x ^ y) ^ z.  [assumption].
6 (x ^ y) ^ z = x ^ (y ^ z).  [copy(5),flip(a)].
7 x v (y v z) = (x v y) v z.  [assumption].
8 (x v y) v z = x v (y v z).  [copy(7),flip(a)].
9 x ^ (x v y) = x.  [assumption].
10 x v (x ^ y) = x.  [assumption].
11 (x v y) ^ y = y.  [assumption].
12 (x ^ y) v y = y.  [assumption].
13 x ^ (y ^ ((x v y) ^ z)) = x ^ (y ^ z).  [assumption].
14 (x ^ y) v ((x v y) ^ z) = (x v (y ^ z)) ^ (y v z).  [assumption].
15 x v (y v z) = x v (((y ^ z) v y) v z).  [assumption].
16 x v ((y ^ z) v (y v z)) = x v (y v z).  [copy(15),rewrite([8(5)]),flip(a)].
17 c1 ^ c3 = c1 ^ c2.  [deny(1)].
18 c1 v c3 = c1 v c2.  [deny(1)].
19 c3 != c2.  [deny(1)].
21 x ^ (x ^ y) = x ^ y.  [para(3(a,1),6(a,1,1)),flip(a)].
22 x v (y v (x v y)) = x v y.  [para(8(a,1),4(a,1))].
23 x v (x v y) = x v y.  [para(4(a,1),8(a,1,1)),flip(a)].
24 x ^ ((x v y) ^ z) = x ^ z.  [para(9(a,1),6(a,1,1)),flip(a)].
26 (x v y) ^ (x v (y v z)) = x v y.  [para(8(a,1),9(a,1,2))].
30 (x v y) ^ (y ^ z) = y ^ z.  [para(11(a,1),6(a,1,1)),flip(a)].
31 (x v (y v z)) ^ z = z.  [para(8(a,1),11(a,1,1))].
38 x ^ (y ^ (x ^ z)) = x ^ (y ^ z).
 ↪  [para(10(a,1),13(a,1,2,2,1)),rewrite([6(3),21(4),6(5),21(6)])].
41 (x ^ y) v (x v y) = (x v (y ^ (x v y))) ^ (y v (x v y)).  [para(3(a,1),14(a,1,2))].
44 ((x v (y ^ z)) ^ (y v z)) v u = (x ^ y) v (((x v y) ^ z) v u).  [para(14(a,1),8(a,1,1))].
51 (x v (y ^ z)) ^ ((y v z) ^ ((x v y) ^ z)) = (x v y) ^ z.
 ↪  [para(14(a,1),11(a,1,1)),rewrite([6(7)])].
53 (x ^ (y v z)) v z = (x v z) ^ (y v z).  [para(11(a,1),14(a,2,1,2)),rewrite([31(5),8(6),4(5)])].
59 x v ((y v (z ^ (y v z))) ^ (z v (y v z))) = x v (y v z).  [back_rewrite(16),rewrite([41(3)])].
62 (c1 ^ c2) v c3 = c3.  [para(17(a,1),12(a,1,1))].
63 (c1 v (c3 ^ x)) ^ (c3 v x) = (c1 v (c2 ^ x)) ^ (c2 v x).
 ↪  [para(17(a,1),14(a,1,1)),rewrite([18(6),14(8)]),flip(a)].
64 c1 v (c3 v x) = c1 v (c2 v x).  [para(18(a,1),8(a,1,1)),rewrite([8(4)]),flip(a)].
65 (c1 v c2) ^ c3 = c3.  [para(18(a,1),11(a,1,1))].
71 c1 v (c2 v c3) = c1 v c2.  [para(65(a,1),10(a,1,2)),rewrite([8(5)])].
73 (c1 v (c2 ^ c3)) ^ (c2 v c3) = c3.  [para(65(a,1),14(a,1,2)),rewrite([62(5)]),flip(a)].
101 (c1 v c2) ^ (c2 v c3) = c2 v c3.  [para(71(a,1),11(a,1,1))].
135 x ^ ((y v x) ^ z) = x ^ z.  [para(30(a,1),13(a,1)),rewrite([8(2),4(1),30(6)])].
139 (x v (y v x)) ^ z = (y v x) ^ z.  [para(22(a,1),30(a,1,1)),rewrite([135(5)]),flip(a)].
168 c3 v (c1 v (c2 v c1)) = c3 v c1.  [para(64(a,1),22(a,1,2))].
179 x v (y v x) = (y v x) ^ (x v y).
 ↪  [para(4(a,1),26(a,1,2)),rewrite([8(2),139(4),8(5)]),flip(a)].
181 (x v (y ^ z)) ^ (x v z) = x v (y ^ z).  [para(12(a,1),26(a,1,2,2))].
194 c3 v ((c2 v c1) ^ (c1 v c2)) = c3 v c1.  [back_rewrite(168),rewrite([179(6)])].
196 (x v y) ^ ((y v x) ^ z) = (x v y) ^ z.  [back_rewrite(139),rewrite([179(2),6(4)])].
198 x v ((y v (z ^ (y v z))) ^ ((y v z) ^ (z v y))) = x v (y v z).
 ↪  [back_rewrite(59),rewrite([179(5)])].
200 (x ^ y) v (x v y) = (x v (y ^ (x v y))) ^ ((x v y) ^ (y v x)).
 ↪  [back_rewrite(41),rewrite([179(8)])].
202 c1 v (c2 ^ c3) = c1 v c2.  [para(73(a,1),10(a,1,2)),rewrite([8(7),12(6),18(3)]),flip(a)].
```

```
207 c2 v c3 = c3.  [para(73(a,1),21(a,1,2)),rewrite([202(5),65(5),202(6),101(8)]),flip(a)].
215 c2 ^ (c3 ^ x) = c2 ^ x.  [para(207(a,1),24(a,1,2,1))].
217 (x v c2) ^ (x v c3) = x v c2.  [para(207(a,1),26(a,1,2,2))].
254 (c2 ^ x) v (c3 ^ x) = c3 ^ x.  [para(215(a,1),12(a,1,1))].
377 (c3 v c2) ^ c3 = c3 v c2.  [para(4(a,1),217(a,1,2))].
454 c2 v (c3 ^ c2) = c3 ^ c2.  [para(3(a,1),254(a,1,1))].
466 c1 v (c3 ^ c2) = c1 v c2.  [para(454(a,1),64(a,2,2)),rewrite([10(6),18(3)]),flip(a)].
482 (x ^ y) v z = (x v z) ^ (y v z).
 ↪  [para(12(a,1),44(a,2,2)),rewrite([53(5),8(3),12(2)]),flip(a)].
657 (x v (y ^ (x v y))) ^ ((x v y) ^ (y v x)) = (x v y) ^ (y v x).
 ↪  [back_rewrite(200),rewrite([482(3),23(2),179(3),21(5)]),flip(a)].
701 x v ((y v z) ^ (z v y)) = x v (y v z).  [back_rewrite(198),rewrite([657(7)])].
709 c3 v (c2 v c1) = c3 v c1.  [back_rewrite(194),rewrite([701(9)])].
963 (c1 v c2) ^ (c3 v c2) = c2.  [para(3(a,1),63(a,2,1,2)),rewrite([466(5),4(13),11(12)])].
1015 (x v (c1 v c2)) ^ (c3 v c2) = c2.  [para(963(a,1),51(a,1,1,2)),rewrite([8(9),179(8),207(9),3⌋
 ↪  77(8),64(7),4(6),135(14),963(9),11(4)]),flip(a)].
1059 x ^ (c3 v c2) = x ^ c2.  [para(1015(a,1),24(a,1,2)),flip(a)].
1089 c3 v c2 = c2.  [para(1059(a,1),3(a,1)),rewrite([11(5)]),flip(a)].
1090 c3 v (c2 v x) = c2 v x.  [para(1089(a,1),8(a,1,1)),flip(a)].
1094 c3 v c1 = c2 v c1.  [back_rewrite(709),rewrite([1090(5)]),flip(a)].
1255 c3 v (x v c2) = (x v c2) ^ (c2 v x).  [para(179(a,1),1090(a,1,2)),rewrite([701(7),179(8)])].
2111 (x v (y ^ x)) ^ x = x v (y ^ x).  [para(4(a,1),181(a,1,2))].
2138 (c3 v (x ^ c2)) ^ c2 = c3 v (x ^ c2).  [para(1089(a,1),181(a,1,2))].
2723 (x v y) ^ (z ^ ((y v x) ^ u)) = (x v y) ^ (z ^ u).
 ↪  [para(196(a,1),38(a,1,2,2)),rewrite([38(5)]),flip(a)].
2726 x v (y ^ x) = (x v y) ^ x.  [para(196(a,1),51(a,1,2)),rewrite([11(4),2111(3)])].
2727 (x v y) ^ ((z v y) ^ ((x v z) ^ ((y v x) ^ z))) = (x v y) ^ ((z v y) ^ z).
 ↪  [para(51(a,1),196(a,1,2)),rewrite([482(2),6(6),2723(6),482(6),6(12)]),flip(a)].
2728 (x v (y ^ z)) ^ ((y v x) ^ ((z v x) ^ z)) = (x v y) ^ z.
 ↪  [para(51(a,1),196(a,2)),rewrite([482(4),6(10),2727(10)])].
2755 (x v (y ^ z)) ^ ((y v x) ^ ((z v x) ^ u)) = (x v (y ^ z)) ^ u.
 ↪  [para(482(a,1),196(a,1,2,1)),rewrite([6(6)])].
2799 (x v (y ^ z)) ^ z = (x v y) ^ z.  [back_rewrite(2728),rewrite([2755(7)])].
2805 c3 v (x ^ c2) = (c3 v x) ^ c2.  [back_rewrite(2138),rewrite([2799(6)]),flip(a)].
2848 (c2 v c1) ^ c3 = (c2 v c1) ^ c2.
 ↪  [para(17(a,1),2726(a,1,2)),rewrite([2805(5),1094(3),1094(8)]),flip(a)].
2849 c3 = c2.  [para(65(a,1),2726(a,1,2)),rewrite([4(3),1255(6),6(10),2848(9),196(10),11(6)])].
2850 $F.  [resolve(2849,a,19,a)].

============================== end of proof ==========================
```

Code 3: Any strong distributive solution is right cancellative.

```
============================== INPUT =================================

formulas(assumptions).
ClearAll.
x ^ x = x.
x v x = x.
x ^ (y ^ z) = (x ^ y) ^ z.
x v (y v z) = (x v y) v z.
x ^ (x v y) = x.
x v (x ^ y) = x.
(x v y) ^ y = y.
(x ^ y) v y = y.
x ^ (y ^ ((x v y) ^ z)) = x ^ (y ^ z).
(x ^ y) v ((x v y) ^ z) = (x v (y ^ z)) ^ (y v z).
x v (y v z) = x v (((y ^ z) v y) v z).
end_of_list.
```

```
formulas(goals).
y ^ x = z ^ x & y v x = z v x -> y = z.
end_of_list.

============================== end of input ==========================

============================== PROOF =================================

% Proof 1 at 0.20 (+ 0.02) seconds.
% Length of proof is 66.
% Level of proof is 14.
% Maximum clause weight is 31.000.
% Given clauses 157.

1 y ^ x = z ^ x & y v x = z v x -> y = z # label(non_clause) # label(goal).  [goal].
3 x ^ x = x.  [assumption].
4 x v x = x.  [assumption].
5 x ^ (y ^ z) = (x ^ y) ^ z.  [assumption].
6 (x ^ y) ^ z = x ^ (y ^ z).  [copy(5),flip(a)].
7 x v (y v z) = (x v y) v z.  [assumption].
8 (x v y) v z = x v (y v z).  [copy(7),flip(a)].
9 x ^ (x v y) = x.  [assumption].
10 x v (x ^ y) = x.  [assumption].
11 (x v y) ^ y = y.  [assumption].
12 (x ^ y) v y = y.  [assumption].
13 x ^ (y ^ ((x v y) ^ z)) = x ^ (y ^ z).  [assumption].
14 (x ^ y) v ((x v y) ^ z) = (x v (y ^ z)) ^ (y v z).  [assumption].
17 c3 ^ c2 = c1 ^ c2.  [deny(1)].
18 c3 v c2 = c1 v c2.  [deny(1)].
19 c3 != c1.  [deny(1)].
21 x ^ (x ^ y) = x ^ y.  [para(3(a,1),6(a,1,1)),flip(a)].
22 x v (y v (x v y)) = x v y.  [para(8(a,1),4(a,1))].
23 x v (x v y) = x v y.  [para(4(a,1),8(a,1,1)),flip(a)].
24 x ^ ((x v y) ^ z) = x ^ z.  [para(9(a,1),6(a,1,1)),flip(a)].
26 (x v y) ^ (x v (y v z)) = x v y.  [para(8(a,1),9(a,1,2))].
30 (x v y) ^ (y ^ z) = y ^ z.  [para(11(a,1),6(a,1,1)),flip(a)].
31 (x v (y v z)) ^ z = z.  [para(8(a,1),11(a,1,1))].
38 x ^ (y ^ (x ^ z)) = x ^ (y ^ z).
 ↪  [para(10(a,1),13(a,1,2,2,1)),rewrite([6(3),21(4),6(5),21(6)])].
44 ((x v (y ^ z)) ^ (y v z)) v u = (x ^ y) v (((x v y) ^ z) v u).  [para(14(a,1),8(a,1,1))].
51 (x v (y ^ z)) ^ ((y v z) ^ ((x v y) ^ z)) = (x v y) ^ z.
 ↪  [para(14(a,1),11(a,1,1)),rewrite([6(7)])].
52 x v ((y v x) ^ z) = (y v x) ^ (x v z).
 ↪  [para(11(a,1),14(a,1,1)),rewrite([8(2),4(1),8(6),10(5)])].
53 (x ^ (y v z)) v z = (x v z) ^ (y v z).  [para(11(a,1),14(a,2,1,2)),rewrite([31(5),8(6),4(5)])].
61 c3 ^ (c2 ^ x) = c1 ^ (c2 ^ x).  [para(17(a,1),6(a,1,1)),rewrite([6(4)]),flip(a)].
62 c3 v (c1 ^ c2) = c3.  [para(17(a,1),10(a,1,2))].
64 c3 v (c2 v x) = c1 v (c2 v x).  [para(18(a,1),8(a,1,1)),rewrite([8(4)]),flip(a)].
65 c3 ^ (c1 v c2) = c3.  [para(18(a,1),9(a,1,2))].
72 c3 v (c1 v c2) = c1 v c2.  [para(65(a,1),12(a,1,1))].
128 x ^ ((y v x) ^ z) = x ^ z.  [para(30(a,1),13(a,1)),rewrite([8(2),4(1),30(6)])].
131 (x v (y ^ z)) ^ ((y v z) ^ ((x v y) ^ (z ^ u))) = (x v y) ^ (z ^ u).
 ↪  [para(14(a,1),30(a,1,1)),rewrite([6(7),6(8),6(11)])].
132 (x v (y v x)) ^ z = (y v x) ^ z.  [para(22(a,1),30(a,1,1)),rewrite([128(5)]),flip(a)].
147 x v (y v x) = (y v x) ^ (x v y).
 ↪  [para(4(a,1),26(a,1,2)),rewrite([8(2),132(4),8(5)]),flip(a)].
149 (x v (y ^ z)) ^ (x v z) = x v (y ^ z).  [para(12(a,1),26(a,1,2,2))].
158 (c3 v c1) ^ (c1 v c2) = c3 v c1.  [para(72(a,1),26(a,1,2))].
161 (x v y) ^ ((y v x) ^ z) = (x v y) ^ z.  [back_rewrite(132),rewrite([147(2),6(4)])].
315 x ^ (y ^ ((x v z) ^ u)) = x ^ (y ^ u).  [para(38(a,1),24(a,1,2)),rewrite([24(4)]),flip(a)].
320 c2 ^ (c3 ^ x) = c2 ^ (c1 ^ x).  [para(61(a,1),38(a,1,2)),rewrite([38(6)]),flip(a)].
356 c2 ^ c3 = c2 ^ c1.  [para(65(a,1),320(a,1,2)),rewrite([9(9)])].
```

```
450 (x ^ y) v z = (x v z) ^ (y v z).
 ↪  [para(12(a,1),44(a,2,2)),rewrite([53(5),8(3),12(2)]),flip(a)].
758 (c3 v c1) ^ c2 = c1 ^ c2.  [para(62(a,1),51(a,1,1)),rewrite([315(11),11(6),17(3)]),flip(a)].
912 c3 v c1 = c1.  [para(158(a,1),52(a,2)),rewrite([758(6),10(5)]),flip(a)].
1873 (x v (y ^ x)) ^ x = x v (y ^ x).  [para(4(a,1),149(a,1,2))].
1891 (c3 v (x ^ c1)) ^ c1 = c3 v (x ^ c1).  [para(912(a,1),149(a,1,2))].
1898 (x v (y ^ (z v x))) ^ ((z v x) ^ (x v z)) = x v (y ^ (z v x)).  [para(147(a,1),149(a,1,2))].
2475 (x v y) ^ (z ^ ((y v x) ^ u)) = (x v y) ^ (z ^ u).
 ↪  [para(161(a,1),38(a,1,2,2)),rewrite([38(5)]),flip(a)].
2478 x v (y ^ x) = (x v y) ^ x.  [para(161(a,1),51(a,1,2)),rewrite([11(4),1873(3)])].
2479 (x v y) ^ ((z v y) ^ ((x v z) ^ ((y v x) ^ z))) = (x v y) ^ ((z v y) ^ z).
 ↪  [para(51(a,1),161(a,1,2)),rewrite([450(2),6(6),2475(6),450(6),6(12)]),flip(a)].
2480 (x v (y ^ z)) ^ ((y v x) ^ ((z v x) ^ z)) = (x v y) ^ z.
 ↪  [para(51(a,1),161(a,2)),rewrite([450(4),6(10),2479(10)])].
2500 (x v (y ^ z)) ^ ((y v x) ^ ((z v x) ^ u)) = (x v (y ^ z)) ^ u.
 ↪  [para(450(a,1),161(a,1,2,1)),rewrite([6(6)])].
2503 (x v y) ^ ((z v y) ^ ((x v z) ^ ((y v x) ^ (z ^ u)))) = (x v y) ^ ((z v y) ^ (z ^ u)).
 ↪  [para(131(a,1),161(a,1,2)),rewrite([450(2),6(7),2475(7),450(7),6(14)]),flip(a)].
2504 (x v (y ^ z)) ^ (z ^ u) = (x v y) ^ (z ^ u).
 ↪  [para(131(a,1),161(a,2)),rewrite([450(4),6(11),2503(11),2500(8)])].
2544 (x v (y ^ z)) ^ z = (x v y) ^ z.  [back_rewrite(2480),rewrite([2500(7)])].
2547 x v (y ^ (z v x)) = (x v y) ^ ((z v x) ^ (x v z)).
 ↪  [back_rewrite(1898),rewrite([2504(7)]),flip(a)].
2551 c3 v (x ^ c1) = (c3 v x) ^ c1.  [back_rewrite(1891),rewrite([2544(6)]),flip(a)].
2587 (c2 v c3) ^ c2 = (c2 v c1) ^ c2.  [para(17(a,1),2478(a,1,2)),rewrite([2478(5)]),flip(a)].
2588 (c1 v c2) ^ c3 = (c1 v c2) ^ c1.
 ↪  [para(18(a,1),2478(a,2,1)),rewrite([356(4),2551(5),18(3)]),flip(a)].
2594 c3 v ((c2 v x) ^ c2) = c1 v ((c2 v x) ^ c2).
 ↪  [para(2478(a,1),64(a,1,2)),rewrite([2478(11)])].
2718 c2 v c3 = c2 v c1.
 ↪  [para(2587(a,1),10(a,1,2)),rewrite([8(9),2594(8),52(8),2547(9),23(5),161(11),3(7)]),flip(a)].
2820 (c2 v c1) ^ c3 = c3.  [para(2718(a,1),11(a,1,1))].
2855 c3 = c1.  [para(2820(a,1),161(a,2)),rewrite([2588(8),161(9),11(5)]),flip(a)].
2856 $F.  [resolve(2855,a,19,a)].

============================== end of proof ==========================
```

Code 4: A 16-element example of a left-handed, distributive and cancellative skew lattice, that is not a strong distributive solution. Note that we only search for an example of size 16 that does not satisfy (5.22).

```
============================== INPUT =================================

formulas(sos).
x ^ x = x.
x v x = x.
x ^ (x v y) = x.
x v (x ^ y) = x.
(x ^ y) v y = y.
(x v y) ^ y = y.
(x ^ y) ^ x = x ^ y.
x v (y v x) = y v x.
x ^ (y ^ z) = (x ^ y) ^ z.
x v (y v z) = (x v y) v z.
(x ^ (y v z)) ^ x = ((x ^ y) ^ x) v ((x ^ z) ^ x).
(x v (y ^ z)) v x = ((x v y) v x) ^ ((x v z) v x).
x ^ y = x ^ z & x v y = x v z -> y = z.
y ^ x = z ^ x & y v x = z v x -> y = z.
end_of_list.
```

```
formulas(goals).
(x ^ y) v ((x v y) ^ z) = (x v (y ^ z)) ^ (y v z).
end_of_list.

% From the command line: clear(verbose).
% assign(domain_size, 16) -> assign(start_size, 16).
% assign(domain_size, 16) -> assign(end_size, 16).

% From the command line: assign(domain_size, 16).

============================== end of input ==========================


============================== CLAUSES FOR SEARCH ====================

formulas(mace4_clauses).
x ^ x = x.
x v x = x.
x ^ (x v y) = x.
x v (x ^ y) = x.
(x ^ y) v y = y.
(x v y) ^ y = y.
(x ^ y) ^ x = x ^ y.
x v (y v x) = y v x.
x ^ (y ^ z) = (x ^ y) ^ z.
x v (y v z) = (x v y) v z.
(x ^ (y v z)) ^ x = ((x ^ y) ^ x) v ((x ^ z) ^ x).
(x v (y ^ z)) v x = ((x v y) v x) ^ ((x v z) v x).
x ^ y != x ^ z | x v y != x v z | y = z.
x ^ y != z ^ y | x v y != z v y | x = z.
(c1 ^ c2) v ((c1 v c2) ^ c3) != (c1 v (c2 ^ c3)) ^ (c2 v c3).
end_of_list.

============================== end of clauses for search =============


============================== DOMAIN SIZE 16 ========================

============================== MODEL =================================

interpretation( 16, [number=1, seconds=1], [

function(c1, [ 0 ]),

function(c2, [ 1 ]),

function(c3, [ 2 ]),

function(^(_,_), [
0, 3, 2, 3, 0, 5, 6, 6, 2, 6, 0, 0, 6, 3, 5, 3,
1, 1, 5, 1, 1, 5, 1, 1, 5, 1, 1, 1, 1, 1, 5, 1,
2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2,
3, 3, 5, 3, 3, 5, 3, 3, 5, 3, 3, 3, 3, 3, 5, 3,
4, 1, 8, 1, 4, 5, 9, 9, 8, 9, 4, 4, 9, 1, 5, 1,
5, 5, 5, 5, 5, 5, 5, 5, 5, 5, 5, 5, 5, 5, 5, 5,
6, 6, 2, 6, 6, 2, 6, 6, 2, 6, 6, 6, 6, 6, 2, 6,
7, 7, 2, 7, 7, 2, 7, 7, 2, 7, 7, 7, 7, 7, 2, 7,
8, 8, 8, 8, 8, 8, 8, 8, 8, 8, 8, 8, 8, 8, 8, 8,
9, 9, 8, 9, 9, 8, 9, 9, 8, 9, 9, 9, 9, 9, 8, 9,
10,13, 2,13,10,14, 7, 7, 2, 7,10,10, 7,13,14,13,
11,15, 8,15,11,14,12,12, 8,12,11,11,12,15,14,15,
12,12, 8,12,12, 8,12,12, 8,12,12,12,12,12, 8,12,
13,13,14,13,13,14,13,13,14,13,13,13,13,13,14,13,
14,14,14,14,14,14,14,14,14,14,14,14,14,14,14,14,
15,15,14,15,15,14,15,15,14,15,15,15,15,15,14,15 ]),

function(v(_,_), [
0, 4, 0, 0, 4, 0, 0,10,11, 4,10,11,11,10,11,11,
0, 1, 7, 3, 4, 1, 6, 7, 9, 9,10,11,12,13,13,15,
0, 1, 2, 3, 4, 5, 6, 7, 8, 9,10,11,12,13,14,15,
0, 1, 6, 3, 4, 3, 6, 7,12, 9,10,11,12,13,15,15,
0, 4,10, 0, 4, 4, 0,10, 4, 4,10,11,11,10,10,11,
0, 1, 2, 3, 4, 5, 6, 7, 8, 9,10,11,12,13,14,15,
0, 1, 6, 3, 4, 3, 6, 7,12, 9,10,11,12,13,15,15,
0, 1, 7, 3, 4, 1, 6, 7, 9, 9,10,11,12,13,13,15,
0, 1, 2, 3, 4, 5, 6, 7, 8, 9,10,11,12,13,14,15,
0, 1, 7, 3, 4, 1, 6, 7, 9, 9,10,11,12,13,13,15,
0, 4,10, 0, 4, 4, 0,10, 4, 4,10,11,11,10,10,11,
0, 4, 0, 0, 4, 0, 0,10,11, 4,10,11,11,10,11,11,
0, 1, 6, 3, 4, 3, 6, 7,12, 9,10,11,12,13,15,15,
0, 1, 7, 3, 4, 1, 6, 7, 9, 9,10,11,12,13,13,15,
0, 1, 2, 3, 4, 5, 6, 7, 8, 9,10,11,12,13,14,15,
0, 1, 6, 3, 4, 3, 6, 7,12, 9,10,11,12,13,15,15 ])
]).

============================== end of model ==========================
```

Code 5: Any left distributive solution is distributive. A proof is given, first for the left-handed case, and then for the right-handed case.

```
============================== INPUT =================================

formulas(sos).
x ^ x = x.
x v x = x.
x ^ (y ^ z) = (x ^ y) ^ z.
x v (y v z) = (x v y) v z.
x ^ (x v y) = x.
x v (x ^ y) = x.
(x ^ y) v y = y.
(x v y) ^ y = y.
((y v x) ^ z) v (x ^ y) = ((y ^ z) v x) ^ (z v y).
(x ^ y) ^ x = x ^ y.
(x v y) v x = y v x.
end_of_list.

formulas(goals).
(x ^ (y v z)) ^ x = ((x ^ y) ^ x) v ((x ^ z) ^ x).
(x v (y ^ z)) v x = ((x v y) v x) ^ ((x v z) v x).
end_of_list.

============================== end of input ==========================

============================== PROOF =================================

% -------- Comments from original proof --------
% Proof 1 at 1.03 (+ 0.16) seconds.
% Length of proof is 27.
% Level of proof is 7.
% Maximum clause weight is 19.
% Given clauses 176.
```

```
1 x ^ ((y v z) ^ x) = (x ^ (y ^ x)) v (x ^ (z ^ x)) # label(non_clause) # label(goal).  [goal].
3 x ^ x = x.  [assumption].
5 x ^ (y ^ z) = (x ^ y) ^ z.  [assumption].
6 (x ^ y) ^ z = x ^ (y ^ z).  [copy(5),flip(a)].
7 x v (y v z) = (x v y) v z.  [assumption].
8 (x v y) v z = x v (y v z).  [copy(7),flip(a)].
10 x v (x ^ y) = x.  [assumption].
11 (x v y) ^ y = y.  [assumption].
13 x ^ (y ^ x) = x ^ y.  [assumption].
14 x v (y v x) = y v x.  [assumption].
15 ((x v y) ^ z) v (y ^ x) = ((x ^ z) v y) ^ (z v x).  [assumption].
16 (c1 ^ (c2 ^ c1)) v (c1 ^ (c3 ^ c1)) != c1 ^ ((c2 v c3) ^ c1).  [deny(1)].
17 (c1 ^ c2) v (c1 ^ c3) != c1 ^ (c2 v c3).  [copy(16),rewrite([13(5),13(8),13(14)])].
20 x ^ (x ^ y) = x ^ y.  [para(3(a,1),6(a,1,1)),flip(a)].
26 x v ((x ^ y) v z) = x v z.  [para(10(a,1),8(a,1,1)),flip(a)].
28 (x v y) ^ (y ^ z) = y ^ z.  [para(11(a,1),6(a,1,1)),flip(a)].
35 x ^ (y v x) = x.  [para(11(a,1),13(a,1,2)),rewrite([3(1)]),flip(a)].
39 x v (y v (z v x)) = y v (z v x).  [para(8(a,1),14(a,1,2)),rewrite([8(5)])].
40 (x ^ y) v x = x.  [para(10(a,1),14(a,1,2)),rewrite([10(4)])].
57 (x ^ y) v (x ^ z) = x ^ (y v (x ^ z)).  [para(20(a,1),15(a,1,2)),rewrite([40(2),6(5),40(6)])].
61 c1 ^ (c2 v (c1 ^ c3)) != c1 ^ (c2 v c3).  [back_rewrite(17),rewrite([57(7)])].
62 x ^ ((y v x) ^ z) = x ^ z.  [para(35(a,1),6(a,1,1)),flip(a)].
120 (x ^ y) v (z v x) = z v x.  [para(14(a,1),26(a,2)),rewrite([39(4)])].
145 ((x v y) ^ z) v (y ^ u) = (x v y) ^ (z v (y ^ u)).
↪  [para(28(a,1),15(a,1,2)),rewrite([120(3),6(6),120(8)])].
151 ((x ^ y) v z) ^ (y v x) = (x v z) ^ (y v (z ^ x)).
↪  [back_rewrite(15),rewrite([145(4)]),flip(a)].
8237 x ^ (y v (x ^ z)) = x ^ (y v z).  [para(151(a,1),62(a,1,2)),rewrite([62(5)])].
8238 $F.  [resolve(8237,a,61,a)].

============================== end of proof ==========================

============================== PROOF =================================

% -------- Comments from original proof --------
% Proof 2 at 1.03 (+ 0.17) seconds.
% Length of proof is 27.
% Level of proof is 7.
% Maximum clause weight is 19.
% Given clauses 176.

2 x v ((y ^ z) v x) = (x v (y v x)) ^ (x v (z v x)) # label(non_clause) # label(goal).  [goal].
3 x ^ x = x.  [assumption].
5 x ^ (y ^ z) = (x ^ y) ^ z.  [assumption].
6 (x ^ y) ^ z = x ^ (y ^ z).  [copy(5),flip(a)].
7 x v (y v z) = (x v y) v z.  [assumption].
8 (x v y) v z = x v (y v z).  [copy(7),flip(a)].
10 x v (x ^ y) = x.  [assumption].
11 (x v y) ^ y = y.  [assumption].
13 x ^ (y ^ x) = x ^ y.  [assumption].
14 x v (y v x) = y v x.  [assumption].
15 ((x v y) ^ z) v (y ^ x) = ((x ^ z) v y) ^ (z v x).  [assumption].
18 c4 v ((c5 ^ c6) v c4) != (c4 v (c5 v c4)) ^ (c4 v (c6 v c4)).  [deny(2)].
19 (c5 ^ c6) v c4 != (c5 v c4) ^ (c6 v c4).  [copy(18),rewrite([14(7),14(10),14(13)])].
26 x v ((x ^ y) v z) = x v z.  [para(10(a,1),8(a,1,1)),flip(a)].
28 (x v y) ^ (y ^ z) = y ^ z.  [para(11(a,1),6(a,1,1)),flip(a)].
35 x ^ (y v x) = x.  [para(11(a,1),13(a,1,2)),rewrite([3(1)]),flip(a)].
39 x v (y v (z v x)) = y v (z v x).  [para(8(a,1),14(a,1,2)),rewrite([8(5)])].
40 (x ^ y) v x = x.  [para(10(a,1),14(a,1,2)),rewrite([10(4)])].
50 ((x v y) ^ z) v y = ((y ^ z) v (x v y)) ^ (z v y).  [para(11(a,1),15(a,1,2)),rewrite([14(2)])].
64 x ^ (y v (z v x)) = x.  [para(8(a,1),35(a,1,2))].
```

```
120 (x ^ y) v (z v x) = z v x.  [para(14(a,1),26(a,2)),rewrite([39(4)])].
127 ((x ^ y) v z) ^ (u v (x v z)) = (x ^ y) v z.  [para(26(a,1),64(a,1,2,2))].
130 ((x v y) ^ z) v y = (x v y) ^ (z v y).  [back_rewrite(50),rewrite([120(6)])].
145 ((x v y) ^ z) v (y ^ u) = (x v y) ^ (z v (y ^ u)).
↪  [para(28(a,1),15(a,1,2)),rewrite([120(3),6(6),120(8)])].
151 ((x ^ y) v z) ^ (y v x) = (x v z) ^ (y v (z ^ x)).
↪  [back_rewrite(15),rewrite([145(4)]),flip(a)].
8420 (x ^ y) v z = (x v z) ^ (y v z).
↪  [para(151(a,1),130(a,1,1)),rewrite([130(5),8(4),40(3),8(7),127(8)]),flip(a)].
8421 $F.  [resolve(8420,a,19,a)].

============================== end of proof ==========================


============================== INPUT =================================

formulas(sos).
x ^ x = x.
x v x = x.
x ^ (y ^ z) = (x ^ y) ^ z.
x v (y v z) = (x v y) v z.
x ^ (x v y) = x.
x v (x ^ y) = x.
(x ^ y) v y = y.
(x v y) ^ y = y.
((y v x) ^ z) v (x ^ y) = ((y ^ z) v x) ^ (z v y).
(x ^ y) ^ x = y ^ x.
(x v y) v x = x v y.
end_of_list.

formulas(goals).
(x ^ (y v z)) ^ x = ((x ^ y) ^ x) v ((x ^ z) ^ x).
(x v (y ^ z)) v x = ((x v y) v x) ^ ((x v z) v x).
end_of_list.

============================== end of input ==========================

============================== PROOF =================================

% -------- Comments from original proof --------
% Proof 1 at 0.01 (+ 0.00) seconds.
% Length of proof is 18.
% Level of proof is 5.
% Maximum clause weight is 19.
% Given clauses 32.

2 x v ((y ^ z) v x) = (x v (y v x)) ^ (x v (z v x)) # label(non_clause) # label(goal).  [goal].
4 x v x = x.  [assumption].
7 x v (y v z) = (x v y) v z.  [assumption].
8 (x v y) v z = x v (y v z).  [copy(7),flip(a)].
9 x ^ (x v y) = x.  [assumption].
10 x v (x ^ y) = x.  [assumption].
13 x ^ (y ^ x) = y ^ x.  [assumption].
14 x v (y v x) = x v y.  [assumption].
15 ((x v y) ^ z) v (y ^ x) = ((x ^ z) v y) ^ (z v x).  [assumption].
18 c4 v ((c5 ^ c6) v c4) != (c4 v (c5 v c4)) ^ (c4 v (c6 v c4)).  [deny(2)].
19 c4 v (c5 ^ c6) != (c4 v c5) ^ (c4 v c6).  [copy(18),rewrite([14(7),14(10),14(13)])].
21 x v (x v y) = x v y.  [para(4(a,1),8(a,1,1)),flip(a)].
35 (x v y) ^ x = x.  [para(9(a,1),13(a,1,2)),rewrite([9(4)])].
36 x v (y ^ x) = x.  [para(13(a,1),10(a,1,2))].
61 x v (y ^ (x v z)) = (x v y) ^ (x v z).
↪  [para(35(a,1),15(a,2,1,1)),rewrite([8(2),35(3),21(6)])].
```

```
64 x v ((y ^ x) v z) = x v z.  [para(36(a,1),8(a,1,1)),flip(a)].
195 x v (y ^ z) = (x v y) ^ (x v z).  [para(15(a,1),64(a,1,2)),rewrite([61(5),64(3)]),flip(a)].
196 $F.  [resolve(195,a,19,a)].

============================== end of proof ==========================

============================== PROOF =================================

% -------- Comments from original proof --------
% Proof 2 at 0.14 (+ 0.00) seconds.
% Length of proof is 29.
% Level of proof is 6.
% Maximum clause weight is 25.
% Given clauses 80.

1 x ^ ((y v z) ^ x) = (x ^ (y ^ x)) v (x ^ (z ^ x)) # label(non_clause) # label(goal).  [goal].
3 x ^ x = x.  [assumption].
4 x v x = x.  [assumption].
5 x ^ (y ^ z) = (x ^ y) ^ z.  [assumption].
6 (x ^ y) ^ z = x ^ (y ^ z).  [copy(5),flip(a)].
7 x v (y v z) = (x v y) v z.  [assumption].
8 (x v y) v z = x v (y v z).  [copy(7),flip(a)].
9 x ^ (x v y) = x.  [assumption].
10 x v (x ^ y) = x.  [assumption].
11 (x v y) ^ y = y.  [assumption].
12 (x ^ y) v y = y.  [assumption].
13 x ^ (y ^ x) = y ^ x.  [assumption].
15 ((x v y) ^ z) v (y ^ x) = ((x ^ z) v y) ^ (z v x).  [assumption].
16 (c1 ^ (c2 ^ c1)) v (c1 ^ (c3 ^ c1)) != c1 ^ ((c2 v c3) ^ c1).  [deny(1)].
17 (c2 ^ c1) v (c3 ^ c1) != (c2 v c3) ^ c1.  [copy(16),rewrite([13(5),13(8),13(14)])].
21 x v (x v y) = x v y.  [para(4(a,1),8(a,1,1)),flip(a)].
22 x ^ ((x v y) ^ z) = x ^ z.  [para(9(a,1),6(a,1,1)),flip(a)].
26 x v ((x ^ y) v z) = x v z.  [para(10(a,1),8(a,1,1)),flip(a)].
28 (x v y) ^ (y ^ z) = y ^ z.  [para(11(a,1),6(a,1,1)),flip(a)].
35 (x v y) ^ x = x.  [para(9(a,1),13(a,1,2)),rewrite([9(4)])].
36 x v (y ^ x) = x.  [para(13(a,1),10(a,1,2))].
61 x v (y ^ (x v z)) = (x v y) ^ (x v z).
↪  [para(35(a,1),15(a,2,1,1)),rewrite([8(2),35(3),21(6)])].
64 x v ((y ^ x) v z) = x v z.  [para(36(a,1),8(a,1,1)),flip(a)].
83 (x v y) ^ (z ^ (((x ^ z) v y) ^ ((z v x) ^ u))) = (x v y) ^ (z ^ u).
↪  [para(15(a,1),22(a,1,2,1)),rewrite([6(7),6(8),6(11)])].
143 (x v y) ^ (((x ^ z) v y) ^ u) = ((x ^ z) v y) ^ u.  [para(26(a,1),28(a,1,1))].
195 x v (y ^ z) = (x v y) ^ (x v z).  [para(15(a,1),64(a,1,2)),rewrite([61(5),64(3)]),flip(a)].
234 ((c2 ^ c1) v c3) ^ c1 != (c2 v c3) ^ c1.  [back_rewrite(17),rewrite([195(7),12(10)])].
1176 ((x ^ y) v z) ^ y = (x v z) ^ y.  [para(3(a,1),83(a,2,2)),rewrite([35(5),13(5),143(5)])].
1177 $F.  [resolve(1176,a,234,a)].

============================== end of proof ==========================
```

Code 6: Any left distributive solution is left cancellative.

```
============================== INPUT =================================

formulas(sos).
x ^ x = x.
x v x = x.
x ^ (y ^ z) = (x ^ y) ^ z.
x v (y v z) = (x v y) v z.
x ^ (x v y) = x.
x v (x ^ y) = x.
```

```
(x ^ y) v y = y.
(x v y) ^ y = y.
((y v x) ^ z) v (x ^ y) = ((y ^ z) v x) ^ (z v y).
end_of_list.

formulas(goals).
x ^ y = x ^ z & x v y = x v z -> y = z.
end_of_list.

============================== end of input ==========================

============================== PROOF =================================

% Proof 1 at 0.59 (+ 0.02) seconds.
% Length of proof is 81.
% Level of proof is 16.
% Maximum clause weight is 25.000.
% Given clauses 227.

1 x ^ y = x ^ z & x v y = x v z -> y = z # label(non_clause) # label(goal).  [goal].
2 x ^ x = x.  [assumption].
3 x v x = x.  [assumption].
4 x ^ (y ^ z) = (x ^ y) ^ z.  [assumption].
5 (x ^ y) ^ z = x ^ (y ^ z).  [copy(4),flip(a)].
6 x v (y v z) = (x v y) v z.  [assumption].
7 (x v y) v z = x v (y v z).  [copy(6),flip(a)].
8 x ^ (x v y) = x.  [assumption].
9 x v (x ^ y) = x.  [assumption].
10 (x ^ y) v y = y.  [assumption].
11 (x v y) ^ y = y.  [assumption].
12 ((x v y) ^ z) v (y ^ x) = ((x ^ z) v y) ^ (z v x).  [assumption].
13 c1 ^ c3 = c1 ^ c2.  [deny(1)].
14 c1 v c3 = c1 v c2.  [deny(1)].
15 c3 != c2.  [deny(1)].
16 x ^ (y ^ (x ^ y)) = x ^ y.  [para(5(a,1),2(a,1))].
17 x ^ (x ^ y) = x ^ y.  [para(2(a,1),5(a,1,1)),flip(a)].
20 x ^ ((x v y) ^ z) = x ^ z.  [para(8(a,1),5(a,1,1)),flip(a)].
23 (x ^ y) v (x ^ (y ^ z)) = x ^ y.  [para(5(a,1),9(a,1,2))].
24 x v ((x ^ y) v z) = x v z.  [para(9(a,1),7(a,1,1)),flip(a)].
26 (x ^ (y ^ z)) v z = z.  [para(5(a,1),10(a,1,1))].
28 (x v y) ^ (y ^ z) = y ^ z.  [para(11(a,1),5(a,1,1)),flip(a)].
29 (x v (y v z)) ^ z = z.  [para(7(a,1),11(a,1,1))].
30 ((x ^ y) v x) ^ (y v x) = (x ^ y) v x.  [para(2(a,1),12(a,1,2)),rewrite([3(1)]),flip(a)].
32 (((x ^ y) v z) ^ (y v x)) v u = ((x v z) ^ y) v ((z ^ x) v u).  [para(12(a,1),7(a,1,1))].
34 (x v y) ^ (z ^ (((x ^ z) v y) ^ (z v x))) = (x v y) ^ z.
↪  [para(12(a,1),8(a,1,2)),rewrite([5(7)])].
36 (x ^ y) v (x ^ (z ^ x)) = ((x ^ y) v (x ^ z)) ^ (y v x).
↪  [para(9(a,1),12(a,1,1,1)),rewrite([5(3)])].
37 ((x ^ (y ^ x)) v y) ^ x = y ^ x.  [para(12(a,1),10(a,1)),rewrite([10(5)])].
38 ((x ^ (y ^ z)) v y) ^ (z v (x ^ y)) = ((y ^ z) v (y ^ x)) ^ (z v y).
↪  [para(10(a,1),12(a,1,1,1)),rewrite([36(4),5(7)]),flip(a)].
39 ((x ^ y) v z) ^ ((y v x) ^ (z ^ x)) = z ^ x.  [para(12(a,1),11(a,1,1)),rewrite([5(6)])].
43 c1 ^ (c3 ^ x) = c1 ^ (c2 ^ x).  [para(13(a,1),5(a,1,1)),rewrite([5(4)]),flip(a)].
44 (c1 ^ c2) v c3 = c3.  [para(13(a,1),10(a,1,1))].
46 c1 v (c3 v x) = c1 v (c2 v x).  [para(14(a,1),7(a,1,1)),rewrite([7(4)]),flip(a)].
47 (c1 v c2) ^ c3 = c3.  [para(14(a,1),11(a,1,1))].
51 (x ^ y) v (y ^ (x ^ y)) = y ^ (x ^ y).  [para(16(a,1),10(a,1,1))].
57 c2 v (c3 ^ c1) = c3 ^ (c2 v c1).  [para(44(a,1),12(a,2,1)),rewrite([14(3),11(5)])].
59 c1 v (c2 v c3) = c1 v c2.  [para(47(a,1),9(a,1,2)),rewrite([7(5)])].
60 c3 v (c2 ^ c1) = c2 ^ (c3 v c1).  [para(47(a,1),12(a,1,1)),rewrite([13(8),10(10)])].
92 (c1 v c2) ^ (c2 v c3) = c2 v c3.  [para(59(a,1),11(a,1,1))].
101 x ^ (y ^ ((x v z) ^ y)) = x ^ y.  [para(16(a,1),20(a,1,2)),rewrite([20(3)]),flip(a)].
```

```
143 (c1 v c2) ^ ((c2 v c3) ^ x) = (c2 v c3) ^ x.  [para(59(a,1),28(a,1,1))].
177 c2 ^ (c3 ^ (c2 v c1)) = c2.  [para(57(a,1),8(a,1,2))].
193 c3 ^ (c2 ^ (c3 v c1)) = c3.  [para(60(a,1),8(a,1,2))].
203 c1 v (c2 ^ (c3 v c1)) = c1 v c2.  [para(60(a,1),46(a,1,2)),rewrite([9(13)])].
217 (c2 ^ c3) v c2 = c2 ^ c3.  [para(177(a,1),23(a,1,2))].
220 (c3 ^ c2) v c3 = c3 ^ c2.  [para(193(a,1),23(a,1,2))].
222 c2 ^ (c3 ^ c2) = c2.  [para(217(a,1),11(a,1,1)),rewrite([5(5)])].
225 c2 ^ (c3 ^ (c2 ^ x)) = c2 ^ x.  [para(217(a,1),28(a,1,1)),rewrite([5(6)])].
227 ((c2 ^ x) v (c2 ^ c3)) ^ (x v c2) = (c2 ^ x) v c2.
 ↪  [para(222(a,1),12(a,1,2)),rewrite([10(5),5(8),38(15)]),flip(a)].
231 c3 ^ (c2 ^ c3) = c3.  [para(220(a,1),11(a,1,1)),rewrite([5(5)])].
234 c3 ^ (c2 ^ (c3 ^ x)) = c3 ^ x.  [para(220(a,1),28(a,1,1)),rewrite([5(6)])].
245 c3 v (c2 ^ c3) = c2 ^ c3.  [para(231(a,1),10(a,1,1))].
268 (x ^ y) v (x v (y v x)) = y v x.  [para(30(a,1),10(a,1,1)),rewrite([7(4)])].
383 ((c1 ^ (c2 v c3)) v c2) ^ (c2 v (c3 v c1)) = c2.
 ↪  [para(92(a,1),12(a,1,1)),rewrite([7(7),60(6),9(7),7(13)]),flip(a)].
606 ((c2 ^ c1) v (c2 ^ (c3 v c1))) ^ (c1 v c2) = (c2 ^ c1) v (c2 ^ (c3 v c1)).
 ↪  [para(203(a,1),30(a,1,2)),rewrite([5(7),11(6),5(20),11(19)])].
616 c2 ^ (c3 v c1) = c2 ^ c3.  [para(193(a,1),225(a,1,2)),flip(a)].
626 (c2 ^ c1) v (c2 ^ c3) = (c2 ^ c1) v c2.
 ↪  [back_rewrite(606),rewrite([616(8),227(11),616(13)]),flip(a)].
638 c3 v (c2 ^ c1) = c2 ^ c3.  [back_rewrite(60),rewrite([616(10)])].
709 (c2 v c3) ^ c2 = c2 v c3.  [para(92(a,1),34(a,2)),rewrite([7(18),383(19),143(9)])].
747 c2 v (c3 v c2) = c2.  [para(709(a,1),10(a,1,1)),rewrite([7(5)])].
830 c2 ^ (c3 v c2) = c3 v c2.  [para(747(a,1),11(a,1,1))].
850 c3 v c2 = c2 ^ c3.  [para(830(a,1),225(a,1,2,2)),rewrite([8(6),830(8)]),flip(a)].
933 c3 ^ (c2 v c1) = c3 ^ c2.  [para(177(a,1),234(a,1,2)),flip(a)].
962 c2 v (c3 ^ c1) = c3 ^ c2.  [back_rewrite(57),rewrite([933(10)])].
1130 (x v y) ^ (x ^ (y ^ x)) = y ^ x.  [para(2(a,1),39(a,1,1,1)),rewrite([3(2)])].
1823 x ^ ((y v (x v z)) ^ x) = x.  [para(11(a,1),101(a,2)),rewrite([7(3),28(6)])].
1931 c3 ^ ((x v (c2 ^ c3)) ^ c3) = c3.  [para(245(a,1),1823(a,1,2,1,2))].
2014 c3 ^ ((x v (y v (c2 ^ c3))) ^ c3) = c3.  [para(7(a,1),1931(a,1,2,1))].
2017 c3 ^ (((c3 ^ x) v c2) ^ c3) = c3.  [para(12(a,1),1931(a,1,2,1)),rewrite([5(10),11(9)])].
2086 ((c3 ^ x) v c2) ^ c3 = c2 ^ c3.
 ↪  [para(2017(a,1),37(a,1,1,1)),rewrite([24(6),850(3),5(5),2(4)]),flip(a)].
2106 c3 ^ (x ^ (c2 ^ c3)) = c3 ^ (x ^ c3).  [para(2086(a,1),20(a,1,2)),rewrite([5(6),5(10)])].
2621 ((x v (y ^ (x ^ y))) ^ y) v ((y ^ x) v z) = (y ^ (x ^ y)) v z.
 ↪  [para(51(a,1),32(a,1,1,1)),rewrite([5(4),5(3),8(2),5(10),5(9),16(10)]),flip(a)].
2629 (x v (y ^ (x ^ y))) ^ y = y ^ (x ^ y).
 ↪  [para(51(a,1),34(a,1,2,2,1)),rewrite([5(7),5(6),8(5),17(6),11(6)]),flip(a)].
2646 (x ^ (y ^ x)) v ((x ^ y) v z) = (x ^ (y ^ x)) v z.  [back_rewrite(2621),rewrite([2629(4)])].
3266 c2 ^ c3 = c2.
 ↪  [para(638(a,1),268(a,1,2,2)),rewrite([5(5),13(4),626(12),2646(11),26(7),638(6)]),flip(a)].
3394 c3 ^ (x ^ c3) = c3 ^ (x ^ c2).  [back_rewrite(2106),rewrite([3266(4)]),flip(a)].
3399 c3 ^ c2 = c3.  [back_rewrite(2014),rewrite([3266(4),3394(7),29(6)])].
3636 c2 v (c3 ^ c1) = c3.  [back_rewrite(962),rewrite([3399(8)])].
6474 c3 ^ c1 = c2 ^ c1.  [para(14(a,1),1130(a,1,1)),rewrite([43(8),1130(9)]),flip(a)].
6602 c3 = c2.  [back_rewrite(3636),rewrite([6474(4),9(5)]),flip(a)].
6603 $F.  [resolve(6602,a,15,a)].

============================== end of proof ==========================
```

Code 7: Any right distributive solution is distributive. A proof is given, first for the left-handed case, and then for the right-handed case.

```
============================== INPUT =================================

formulas(sos).
x ^ x = x.
x v x = x.
```

```
x ^ (y ^ z) = (x ^ y) ^ z.
x v (y v z) = (x v y) v z.
x ^ (x v y) = x.
x v (x ^ y) = x.
(x ^ y) v y = y.
(x v y) ^ y = y.
(y ^ x) v (z ^ (x v y)) = (y v z) ^ (x v (z ^ y)).
x ^ (y ^ x) = x ^ y.
x v (y v x) = y v x.
end_of_list.

formulas(goals).
(x ^ (y v z)) ^ x = ((x ^ y) ^ x) v ((x ^ z) ^ x).
(x v (y ^ z)) v x = ((x v y) v x) ^ ((x v z) v x).
end_of_list.

============================== end of input ==========================

============================== PROOF =================================

% Proof 1 at 0.04 (+ 0.01) seconds.
% Length of proof is 19.
% Level of proof is 5.
% Maximum clause weight is 23.000.
% Given clauses 60.

2 (x v (y ^ z)) v x = ((x v y) v x) ^ ((x v z) v x) # label(non_clause) # label(goal).  [goal].
3 x ^ x = x.  [assumption].
4 x v x = x.  [assumption].
7 x v (y v z) = (x v y) v z.  [assumption].
8 (x v y) v z = x v (y v z).  [copy(7),flip(a)].
10 x v (x ^ y) = x.  [assumption].
12 (x v y) ^ y = y.  [assumption].
13 (x ^ y) v (z ^ (y v x)) = (x v z) ^ (y v (z ^ x)).  [assumption].
14 x ^ (y ^ x) = x ^ y.  [assumption].
15 x v (y v x) = y v x.  [assumption].
18 (c4 v (c5 ^ c6)) v c4 != ((c4 v c5) v c4) ^ ((c4 v c6) v c4).  [deny(2)].
19 (c5 ^ c6) v c4 != (c5 v c4) ^ (c6 v c4).
 ↪  [copy(18),rewrite([8(7),15(7),8(10),15(10),8(13),15(13)])].
36 ((x v y) ^ (z v (y ^ x))) v u = (x ^ z) v ((y ^ (z v x)) v u).  [para(13(a,1),8(a,1,1))].
52 x ^ (y v x) = x.  [para(12(a,1),14(a,1,2)),rewrite([3(1)]),flip(a)].
57 (x ^ y) v x = x.  [para(10(a,1),15(a,1,2)),rewrite([10(4)])].
62 x ^ (y v (z v x)) = x.  [para(8(a,1),52(a,1,2))].
64 ((x v y) ^ z) v y = (x v y) ^ (z v y).  [para(52(a,1),13(a,2,2,2)),rewrite([62(5),8(5),4(4)])].
784 (x ^ y) v z = (x v z) ^ (y v z).
 ↪  [para(57(a,1),36(a,2,2)),rewrite([64(5),8(4),57(3)]),flip(a)].
785 $F.  [resolve(784,a,19,a)].

============================== end of proof ==========================

============================== PROOF =================================

% Proof 2 at 0.09 (+ 0.01) seconds.
% Length of proof is 28.
% Level of proof is 6.
% Maximum clause weight is 25.000.
% Given clauses 70.

1 (x ^ (y v z)) ^ x = ((x ^ y) ^ x) v ((x ^ z) ^ x) # label(non_clause) # label(goal).  [goal].
3 x ^ x = x.  [assumption].
5 x ^ (y ^ z) = (x ^ y) ^ z.  [assumption].
6 (x ^ y) ^ z = x ^ (y ^ z).  [copy(5),flip(a)].
```

```
7 x v (y v z) = (x v y) v z.  [assumption].
8 (x v y) v z = x v (y v z).  [copy(7),flip(a)].
9 x ^ (x v y) = x.  [assumption].
10 x v (x ^ y) = x.  [assumption].
11 (x ^ y) v y = y.  [assumption].
12 (x v y) ^ y = y.  [assumption].
13 (x ^ y) v (z ^ (y v x)) = (x v z) ^ (y v (z ^ x)).  [assumption].
14 x ^ (y ^ x) = x ^ y.  [assumption].
16 ((c1 ^ c2) ^ c1) v ((c1 ^ c3) ^ c1) != (c1 ^ (c2 v c3)) ^ c1.  [deny(1)].
17 (c1 ^ c2) v (c1 ^ c3) != c1 ^ (c2 v c3).
↪  [copy(16),rewrite([6(5),14(5),6(8),14(8),6(14),14(14)])].
20 x ^ (x ^ y) = x ^ y.  [para(3(a,1),6(a,1,1)),flip(a)].
24 (x v y) ^ (x v (y v z)) = x v y.  [para(8(a,1),9(a,1,2))].
35 (x ^ y) v (z ^ (u ^ (y v x))) = (x v (z ^ u)) ^ (y v (z ^ (u ^ x))).
↪  [para(6(a,1),13(a,1,2)),rewrite([6(9)])].
44 (x v y) ^ ((z v (y ^ x)) ^ (y ^ (z v x))) = y ^ (z v x).
↪  [para(13(a,1),12(a,1,1)),rewrite([6(7)])].
49 x ^ (y ^ (x ^ z)) = x ^ (y ^ z).  [para(14(a,1),6(a,1,1)),rewrite([6(2),6(4)]),flip(a)].
52 x ^ (y v x) = x.  [para(12(a,1),14(a,1,2)),rewrite([3(1)]),flip(a)].
60 x ^ ((y v x) ^ z) = x ^ z.  [para(52(a,1),6(a,1,1)),flip(a)].
62 x ^ (y v (z v x)) = x.  [para(8(a,1),52(a,1,2))].
94 x ^ (y ^ (z v x)) = x ^ y.  [para(10(a,1),62(a,1,2,2)),rewrite([6(3)])].
151 (x v (y ^ z)) ^ (x v z) = x v (y ^ z).  [para(11(a,1),24(a,1,2,2))].
524 (x ^ y) v (x ^ z) = x ^ (y v (x ^ z)).  [para(10(a,1),35(a,2,1)),rewrite([94(4),14(5)])].
653 c1 ^ (c2 v (c1 ^ c3)) != c1 ^ (c2 v c3).  [back_rewrite(17),rewrite([524(7)])].
1386 x ^ (y v (x ^ z)) = x ^ (y v z).
↪  [para(44(a,1),60(a,1,2)),rewrite([20(3),49(8),151(6)]),flip(a)].
1387 $F.  [resolve(1386,a,653,a)].

============================== end of proof ==========================


============================== INPUT =================================

formulas(sos).
x ^ x = x.
x v x = x.
x ^ (y ^ z) = (x ^ y) ^ z.
x v (y v z) = (x v y) v z.
x ^ (x v y) = x.
x v (x ^ y) = x.
(x ^ y) v y = y.
(x v y) ^ y = y.
(y ^ x) v (z ^ (x v y)) = (y v z) ^ (x v (z ^ y)).
x ^ (y ^ x) = y ^ x.
x v (y v x) = x v y.
end_of_list.

formulas(goals).
(x ^ (y v z)) ^ x = ((x ^ y) ^ x) v ((x ^ z) ^ x).
(x v (y ^ z)) v x = ((x v y) v x) ^ ((x v z) v x).
end_of_list.

============================== end of input ==========================

============================== PROOF =================================

% Proof 1 at 0.03 (+ 0.00) seconds.
% Length of proof is 26.
% Level of proof is 7.
% Maximum clause weight is 19.000.
% Given clauses 54.
```

```
2 (x v (y ^ z)) v x = ((x v y) v x) ^ ((x v z) v x) # label(non_clause) # label(goal).  [goal].
5 x ^ (y ^ z) = (x ^ y) ^ z.  [assumption].
6 (x ^ y) ^ z = x ^ (y ^ z).  [copy(5),flip(a)].
7 x v (y v z) = (x v y) v z.  [assumption].
8 (x v y) v z = x v (y v z).  [copy(7),flip(a)].
9 x ^ (x v y) = x.  [assumption].
10 x v (x ^ y) = x.  [assumption].
11 (x ^ y) v y = y.  [assumption].
13 (x ^ y) v (z ^ (y v x)) = (x v z) ^ (y v (z ^ x)).  [assumption].
14 x ^ (y ^ x) = y ^ x.  [assumption].
15 x v (y v x) = x v y.  [assumption].
18 (c4 v (c5 ^ c6)) v c4 != ((c4 v c5) v c4) ^ ((c4 v c6) v c4).  [deny(2)].
19 c4 v (c5 ^ c6) != (c4 v c5) ^ (c4 v c6).
 ↪  [copy(18),rewrite([8(7),15(7),8(10),15(10),8(13),15(13)])].
29 (x ^ y) v (y v z) = y v z.  [para(11(a,1),8(a,1,1)),flip(a)].
39 x v (y ^ (x v z)) = (x v y) ^ (x v (z v (y ^ x))).
 ↪  [para(9(a,1),13(a,1,1)),rewrite([8(2),15(2),8(7)])].
51 (x v y) ^ x = x.  [para(9(a,1),14(a,1,2)),rewrite([9(4)])].
52 x v (y ^ x) = x.  [para(14(a,1),10(a,1,2))].
59 (x v (y v z)) ^ (x v y) = x v y.  [para(8(a,1),51(a,1,1))].
63 x v (y ^ (z ^ x)) = x.  [para(6(a,1),52(a,1,2))].
64 x v ((y ^ x) v z) = x v z.  [para(52(a,1),8(a,1,1)),flip(a)].
93 x v (y v (z ^ x)) = x v y.  [para(9(a,1),63(a,1,2,2)),rewrite([8(3)])].
98 x v (y ^ (x v z)) = (x v y) ^ (x v z).  [back_rewrite(39),rewrite([93(7)])].
179 (x v (y v z)) ^ (x v (z ^ y)) = (x v z) ^ (x v y).
 ↪  [para(13(a,1),64(a,1,2)),rewrite([98(5),98(8)])].
568 (x v (y v z)) ^ (x v (u ^ y)) = x v (u ^ y).  [para(29(a,1),59(a,1,1,2))].
578 x v (y ^ z) = (x v y) ^ (x v z).  [back_rewrite(179),rewrite([568(5)])].
579 $F.  [resolve(578,a,19,a)].

============================== end of proof ==========================

============================== PROOF =================================

% Proof 2 at 0.03 (+ 0.00) seconds.
% Length of proof is 35.
% Level of proof is 7.
% Maximum clause weight is 25.000.
% Given clauses 54.

1 (x ^ (y v z)) ^ x = ((x ^ y) ^ x) v ((x ^ z) ^ x) # label(non_clause) # label(goal).  [goal].
3 x ^ x = x.  [assumption].
5 x ^ (y ^ z) = (x ^ y) ^ z.  [assumption].
6 (x ^ y) ^ z = x ^ (y ^ z).  [copy(5),flip(a)].
7 x v (y v z) = (x v y) v z.  [assumption].
8 (x v y) v z = x v (y v z).  [copy(7),flip(a)].
9 x ^ (x v y) = x.  [assumption].
10 x v (x ^ y) = x.  [assumption].
11 (x ^ y) v y = y.  [assumption].
12 (x v y) ^ y = y.  [assumption].
13 (x ^ y) v (z ^ (y v x)) = (x v z) ^ (y v (z ^ x)).  [assumption].
14 x ^ (y ^ x) = y ^ x.  [assumption].
15 x v (y v x) = x v y.  [assumption].
16 ((c1 ^ c2) ^ c1) v ((c1 ^ c3) ^ c1) != (c1 ^ (c2 v c3)) ^ c1.  [deny(1)].
17 (c2 ^ c1) v (c3 ^ c1) != (c2 v c3) ^ c1.
 ↪  [copy(16),rewrite([6(5),14(5),6(8),14(8),6(14),14(14)])].
26 x v ((x ^ y) v z) = x v z.  [para(10(a,1),8(a,1,1)),flip(a)].
29 (x ^ y) v (y v z) = y v z.  [para(11(a,1),8(a,1,1)),flip(a)].
35 (x ^ y) v (z ^ (u ^ (y v x))) = (x v (z ^ u)) ^ (y v (z ^ (u ^ x))).
 ↪  [para(6(a,1),13(a,1,2)),rewrite([6(9)])].
```

```
39 x v (y ^ (x v z)) = (x v y) ^ (x v (z v (y ^ x))).
 ↪  [para(9(a,1),13(a,1,1)),rewrite([8(2),15(2),8(7)])].
51 (x v y) ^ x = x.  [para(9(a,1),14(a,1,2)),rewrite([9(4)])].
52 x v (y ^ x) = x.  [para(14(a,1),10(a,1,2))].
59 (x v (y v z)) ^ (x v y) = x v y.  [para(8(a,1),51(a,1,1))].
63 x v (y ^ (z ^ x)) = x.  [para(6(a,1),52(a,1,2))].
64 x v ((y ^ x) v z) = x v z.  [para(52(a,1),8(a,1,1)),flip(a)].
66 (x ^ y) v (z ^ y) = ((x ^ y) v z) ^ y.  [para(52(a,1),13(a,1,2,2)),rewrite([6(2),3(1),63(8)])].
69 ((c2 ^ c1) v c3) ^ c1 != (c2 v c3) ^ c1.  [back_rewrite(17),rewrite([66(7)])].
93 x v (y v (z ^ x)) = x v y.  [para(9(a,1),63(a,1,2,2)),rewrite([8(3)])].
98 x v (y ^ (x v z)) = (x v y) ^ (x v z).  [back_rewrite(39),rewrite([93(7)])].
110 x v (y ^ (x ^ z)) = x.  [para(52(a,1),26(a,1,2)),rewrite([10(2)]),flip(a)].
179 (x v (y v z)) ^ (x v (z ^ y)) = (x v z) ^ (x v y).
 ↪  [para(13(a,1),64(a,1,2)),rewrite([98(5),98(8)])].
432 ((x ^ y) v z) ^ y = (x v (z ^ y)) ^ y.  [para(9(a,1),35(a,1,2,2)),rewrite([66(3),110(8)])].
521 (c2 v (c3 ^ c1)) ^ c1 != (c2 v c3) ^ c1.  [back_rewrite(69),rewrite([432(7)])].
568 (x v (y v z)) ^ (x v (u ^ y)) = x v (u ^ y).  [para(29(a,1),59(a,1,1,2))].
578 x v (y ^ z) = (x v y) ^ (x v z).  [back_rewrite(179),rewrite([568(5)])].
600 $F.  [back_rewrite(521),rewrite([578(5),6(9),12(8)]),xx(a)].

============================== end of proof ==========================
```

Code 8: Any right distributive solution is right cancellative.

```
============================== INPUT =================================

formulas(sos).
x ^ x = x.
x v x = x.
x ^ (y ^ z) = (x ^ y) ^ z.
x v (y v z) = (x v y) v z.
x ^ (x v y) = x.
x v (x ^ y) = x.
(x ^ y) v y = y.
(x v y) ^ y = y.
(y ^ x) v (z ^ (x v y)) = (y v z) ^ (x v (z ^ y)).
end_of_list.

formulas(goals).
y ^ x = z ^ x & y v x = z v x -> y = z.
end_of_list.

============================== end of input ==========================

============================== PROOF =================================

% Proof 1 at 0.64 (+ 0.03) seconds.
% Length of proof is 77.
% Level of proof is 18.
% Maximum clause weight is 21.000.
% Given clauses 229.

1 y ^ x = z ^ x & y v x = z v x -> y = z # label(non_clause) # label(goal).  [goal].
2 x ^ x = x.  [assumption].
3 x v x = x.  [assumption].
4 x ^ (y ^ z) = (x ^ y) ^ z.  [assumption].
5 (x ^ y) ^ z = x ^ (y ^ z).  [copy(4),flip(a)].
6 x v (y v z) = (x v y) v z.  [assumption].
7 (x v y) v z = x v (y v z).  [copy(6),flip(a)].
8 x ^ (x v y) = x.  [assumption].
```

```
9 x v (x ^ y) = x.  [assumption].
10 (x ^ y) v y = y.  [assumption].
11 (x v y) ^ y = y.  [assumption].
12 (x ^ y) v (z ^ (y v x)) = (x v z) ^ (y v (z ^ x)).  [assumption].
13 c3 ^ c2 = c1 ^ c2.  [deny(1)].
14 c3 v c2 = c1 v c2.  [deny(1)].
15 c3 != c1.  [deny(1)].
16 x ^ (y ^ (x ^ y)) = x ^ y.  [para(5(a,1),2(a,1))].
18 x v (y v (x v y)) = x v y.  [para(7(a,1),3(a,1))].
20 x ^ ((x v y) ^ z) = x ^ z.  [para(8(a,1),5(a,1,1)),flip(a)].
23 (x ^ y) v (x ^ (y ^ z)) = x ^ y.  [para(5(a,1),9(a,1,2))].
24 x v ((x ^ y) v z) = x v z.  [para(9(a,1),7(a,1,1)),flip(a)].
26 (x ^ (y ^ z)) v z = z.  [para(5(a,1),10(a,1,1))].
27 (x ^ y) v (y v z) = y v z.  [para(10(a,1),7(a,1,1)),flip(a)].
28 (x v y) ^ (y ^ z) = y ^ z.  [para(11(a,1),5(a,1,1)),flip(a)].
29 (x v (y v z)) ^ z = z.  [para(7(a,1),11(a,1,1))].
30 (x v y) ^ (x v (y ^ x)) = x v (y ^ x).  [para(2(a,1),12(a,1,1)),rewrite([3(1)]),flip(a)].
35 x ^ (y ^ ((x v z) ^ (y v (z ^ x)))) = x ^ y.  [para(12(a,1),8(a,1,2)),rewrite([5(6)])].
36 x v (y ^ (x v (z v x))) = (x v y) ^ (x v (z v (y ^ x))).
↪  [para(8(a,1),12(a,1,1)),rewrite([7(2),7(8)])].
37 x v (y ^ (x v (y v x))) = x v y.  [para(8(a,1),12(a,2)),rewrite([8(2),7(2)])].
46 c3 ^ (c2 ^ x) = c1 ^ (c2 ^ x).  [para(13(a,1),5(a,1,1)),rewrite([5(4)]),flip(a)].
47 c3 v (c1 ^ c2) = c3.  [para(13(a,1),9(a,1,2))].
49 c3 v (c2 v x) = c1 v (c2 v x).  [para(14(a,1),7(a,1,1)),rewrite([7(4)]),flip(a)].
50 c3 ^ (c1 v c2) = c3.  [para(14(a,1),8(a,1,2))].
51 (c2 ^ c3) v (x ^ (c1 v c2)) = (c2 v x) ^ (c3 v (x ^ c2)).  [para(14(a,1),12(a,1,2,2))].
58 c3 ^ (c1 ^ c2) = c1 ^ c2.  [para(47(a,1),11(a,1,1))].
60 (c2 ^ c3) v c1 = (c2 v c1) ^ c3.  [para(47(a,1),12(a,2,2)),rewrite([14(7),8(8)])].
64 (c2 ^ c1) v c3 = (c2 v c3) ^ c1.  [para(50(a,1),12(a,1,2)),rewrite([13(12),9(13)])].
79 (x v (y v z)) ^ (z ^ u) = z ^ u.  [para(29(a,1),5(a,1,1)),flip(a)].
94 x ^ (y ^ ((x v z) ^ y)) = x ^ y.  [para(16(a,1),20(a,1,2)),rewrite([20(3)]),flip(a)].
102 x v (y v ((x ^ z) v y)) = x v y.  [para(18(a,1),24(a,1,2)),rewrite([24(3)]),flip(a)].
130 c2 v (c1 v (c2 v c3)) = c2 v c3.  [para(49(a,1),18(a,1,2))].
156 (c2 v c1) ^ (c3 ^ c1) = c1.  [para(60(a,1),11(a,1,1)),rewrite([5(7)])].
168 c2 ^ (c3 ^ c1) = c2 ^ c1.  [para(156(a,1),20(a,1,2)),flip(a)].
217 (c2 v c3) ^ (c1 ^ c3) = c3.  [para(64(a,1),11(a,1,1)),rewrite([5(7)])].
222 c2 v ((c2 v c3) ^ c1) = c2 v c3.  [para(64(a,1),24(a,1,2))].
227 c3 v (c1 ^ c3) = c1 ^ c3.  [para(217(a,1),10(a,1,1))].
230 c2 ^ (c1 ^ c3) = c2 ^ c3.  [para(217(a,1),20(a,1,2)),flip(a)].
233 c3 ^ (c1 ^ c3) = c3.  [para(227(a,1),8(a,1,2))].
235 c3 ^ (c1 ^ (c3 ^ x)) = c3 ^ x.  [para(227(a,1),20(a,1,2,1)),rewrite([5(5)])].
243 x v (y v (x v (y ^ x))) = x v y.  [para(30(a,1),9(a,1,2)),rewrite([7(4)])].
798 (c3 ^ c1) v (c3 ^ x) = c3 ^ c1.  [para(235(a,1),23(a,1,2))].
806 x ^ (y ^ (x ^ (y v x))) = x ^ y.  [para(2(a,1),35(a,1,2,2,2,2)),rewrite([3(1)])].
1099 c3 ^ (c1 v c3) = c3 ^ c1.  [para(798(a,1),12(a,1)),rewrite([3(6),2(8)]),flip(a)].
1429 x ^ ((y v (x v z)) ^ x) = x.  [para(11(a,1),94(a,2)),rewrite([7(3),28(6)])].
1433 (x ^ (y ^ z)) v (z ^ ((y v u) ^ z)) = z ^ ((y v u) ^ z).  [para(94(a,1),26(a,1,1,2))].
1534 c1 ^ ((c2 v c3) ^ c1) = c1.  [para(130(a,1),1429(a,1,2,1))].
1708 c1 v ((c2 v c3) ^ c1) = (c2 v c3) ^ c1.  [para(1534(a,1),10(a,1,1))].
2022 x v ((y ^ (x ^ z)) v x) = x.  [para(10(a,1),102(a,2)),rewrite([5(3),27(6)])].
2094 c3 v (c1 v c3) = c3.  [para(156(a,1),2022(a,1,2,1))].
2095 c3 v ((c2 v c3) ^ c1) = c3.  [para(168(a,1),2022(a,1,2,1)),rewrite([64(6)])].
2100 c1 v ((c2 v c1) ^ c3) = c1.  [para(230(a,1),2022(a,1,2,1)),rewrite([60(6)])].
2147 c1 v c3 = c3 ^ c1.  [para(2094(a,1),11(a,1,1)),rewrite([1099(5)]),flip(a)].
2151 c3 v c1 = c1 ^ c3.  [para(2094(a,1),37(a,1,2,2)),rewrite([227(5)]),flip(a)].
2376 (c2 v c3) ^ c1 = c3 ^ c1.
↪  [para(2095(a,1),36(a,2,2,2)),rewrite([2151(8),9(9),1708(7),2147(13),79(14)])].
2410 c2 v (c3 ^ c1) = c2 v c3.  [back_rewrite(222),rewrite([2376(6)])].
2438 c3 v ((c2 v c1) ^ c3) = c1 ^ c3.
↪  [para(2100(a,1),36(a,2,2,2)),rewrite([2147(8),9(9),49(12),2151(15),79(16)])].
2500 (c2 v c3) ^ (c1 ^ x) = c3 ^ (c1 ^ x).  [para(2376(a,1),5(a,1,1)),rewrite([5(4)]),flip(a)].
```

```
2530 (c2 ^ c3) v (c3 ^ c1) = c3.
 ↪  [para(2410(a,1),51(a,2,1)),rewrite([5(10),8(9),5(16),58(16),47(15),11(12)])].
2579 c3 ^ ((c2 v c1) ^ c3) = c3.
 ↪  [para(2530(a,1),12(a,2,2)),rewrite([60(11),1433(13),2147(10),5(12),233(12)])].
2598 (c2 v c1) ^ c3 = c1 ^ c3.  [para(2579(a,1),10(a,1,1)),rewrite([2438(7)]),flip(a)].
2640 (c2 ^ c3) v c1 = c1 ^ c3.  [back_rewrite(60),rewrite([2598(10)])].
3595 c2 v c3 = c2 v c1.  [para(13(a,1),243(a,1,2,2,2)),rewrite([49(8),243(9)]),flip(a)].
3715 c3 ^ (c1 ^ x) = c1 ^ x.  [back_rewrite(2500),rewrite([3595(3),28(6)]),flip(a)].
3809 c1 ^ c3 = c3.  [back_rewrite(233),rewrite([3715(5)])].
4047 (c2 ^ c3) v c1 = c3.  [back_rewrite(2640),rewrite([3809(8)])].
7595 c2 ^ c3 = c2 ^ c1.  [para(14(a,1),806(a,1,2,2,2)),rewrite([46(8),806(9)]),flip(a)].
7707 c3 = c1.  [back_rewrite(4047),rewrite([7595(3),10(5)]),flip(a)].
7708 $F.  [resolve(7707,a,15,a)].

============================== end of proof ==========================
```

Code 9: Any weak distributive solution is distributive. A proof is given, first for the left-handed case, and then for the right-handed case.

```
============================== INPUT =================================

formulas(sos).
x ^ x = x.
x v x = x.
x ^ (y ^ z) = (x ^ y) ^ z.
x v (y v z) = (x v y) v z.
x ^ (x v y) = x.
x v (x ^ y) = x.
(x ^ y) v y = y.
(x v y) ^ y = y.
((x ^ y) ^ x) v ((((x v y) v x) ^ (z ^ ((x v y) v x))) v ((x ^ y) ^ x)) = ((x v ((y ^ z) ^ y)) v
 ↪  x) ^ (((y v z) v y) ^ ((x v ((y ^ z) ^ y)) v x)).
x ^ (y ^ x) = x ^ y.
x v (y v x) = y v x.
end_of_list.

formulas(goals).
(x ^ (y v z)) ^ x = ((x ^ y) ^ x) v ((x ^ z) ^ x).
(x v (y ^ z)) v x = ((x v y) v x) ^ ((x v z) v x).
end_of_list.

============================== end of input ==========================

============================== PROOF =================================

% -------- Comments from original proof --------
% Proof 1 at 0.92 (+ 0.17) seconds.
% Length of proof is 28.
% Level of proof is 7.
% Maximum clause weight is 19.
% Given clauses 176.

1 x ^ ((y v z) ^ x) = (x ^ (y ^ x)) v (x ^ (z ^ x)) # label(non_clause) # label(goal).  [goal].
3 x ^ x = x.  [assumption].
5 x ^ (y ^ z) = (x ^ y) ^ z.  [assumption].
6 (x ^ y) ^ z = x ^ (y ^ z).  [copy(5),flip(a)].
7 x v (y v z) = (x v y) v z.  [assumption].
8 (x v y) v z = x v (y v z).  [copy(7),flip(a)].
10 x v (x ^ y) = x.  [assumption].
11 (x v y) ^ y = y.  [assumption].
```

```
13 x ^ (y ^ x) = x ^ y.  [assumption].
14 x v (y v x) = y v x.  [assumption].
15 ((x ^ y) ^ x) v ((((x v y) v x) ^ (z ^ ((x v y) v x))) v ((x ^ y) ^ x)) = ((x v ((y ^ z) ^ y))
↪  v x) ^ (((y v z) v y) ^ ((x v ((y ^ z) ^ y)) v x)).  [assumption].
16 ((x v y) ^ z) v (y ^ x) = ((x ^ z) v y) ^ (z v x).
↪  [copy(15),rewrite([6(2),13(2),8(3),14(3),8(4),14(4),13(5),6(5),13(5),14(6),6(6),13(6),8(7),14⌋
↪  (7),8(8),14(8),6(9),13(9),8(10),14(10),13(11)])].
17 (c1 ^ (c2 ^ c1)) v (c1 ^ (c3 ^ c1)) != c1 ^ ((c2 v c3) ^ c1).  [deny(1)].
18 (c1 ^ c2) v (c1 ^ c3) != c1 ^ (c2 v c3).  [copy(17),rewrite([13(5),13(8),13(14)])].
21 x ^ (x ^ y) = x ^ y.  [para(3(a,1),6(a,1,1)),flip(a)].
27 x v ((x ^ y) v z) = x v z.  [para(10(a,1),8(a,1,1)),flip(a)].
29 (x v y) ^ (y ^ z) = y ^ z.  [para(11(a,1),6(a,1,1)),flip(a)].
36 x ^ (y v x) = x.  [para(11(a,1),13(a,1,2)),rewrite([3(1)]),flip(a)].
40 x v (y v (z v x)) = y v (z v x).  [para(8(a,1),14(a,1,2)),rewrite([8(5)])].
41 (x ^ y) v x = x.  [para(10(a,1),14(a,1,2)),rewrite([10(4)])].
58 (x ^ y) v (x ^ z) = x ^ (y v (x ^ z)).  [para(21(a,1),16(a,1,2)),rewrite([41(2),6(5),41(6)])].
62 c1 ^ (c2 v (c1 ^ c3)) != c1 ^ (c2 v c3).  [back_rewrite(18),rewrite([58(7)])].
63 x ^ ((y v x) ^ z) = x ^ z.  [para(36(a,1),6(a,1,1)),flip(a)].
121 (x ^ y) v (z v x) = z v x.  [para(14(a,1),27(a,2)),rewrite([40(4)])].
146 ((x v y) ^ z) v (y ^ u) = (x v y) ^ (z v (y ^ u)).
↪  [para(29(a,1),16(a,1,2)),rewrite([121(3),6(6),121(8)])].
152 ((x ^ y) v z) ^ (y v x) = (x v z) ^ (y v (z ^ x)).
↪  [back_rewrite(16),rewrite([146(4)]),flip(a)].
8238 x ^ (y v (x ^ z)) = x ^ (y v z).  [para(152(a,1),63(a,1,2)),rewrite([63(5)])].
8239 $F.  [resolve(8238,a,62,a)].

============================== end of proof ==========================

============================== PROOF =================================

% -------- Comments from original proof --------
% Proof 2 at 0.94 (+ 0.17) seconds.
% Length of proof is 28.
% Level of proof is 7.
% Maximum clause weight is 19.
% Given clauses 176.

2 x v ((y ^ z) v x) = (x v (y v x)) ^ (x v (z v x)) # label(non_clause) # label(goal).  [goal].
3 x ^ x = x.  [assumption].
5 x ^ (y ^ z) = (x ^ y) ^ z.  [assumption].
6 (x ^ y) ^ z = x ^ (y ^ z).  [copy(5),flip(a)].
7 x v (y v z) = (x v y) v z.  [assumption].
8 (x v y) v z = x v (y v z).  [copy(7),flip(a)].
10 x v (x ^ y) = x.  [assumption].
11 (x v y) ^ y = y.  [assumption].
13 x ^ (y ^ x) = x ^ y.  [assumption].
14 x v (y v x) = y v x.  [assumption].
15 ((x ^ y) ^ x) v ((((x v y) v x) ^ (z ^ ((x v y) v x))) v ((x ^ y) ^ x)) = ((x v ((y ^ z) ^ y))
↪  v x) ^ (((y v z) v y) ^ ((x v ((y ^ z) ^ y)) v x)).  [assumption].
16 ((x v y) ^ z) v (y ^ x) = ((x ^ z) v y) ^ (z v x).
↪  [copy(15),rewrite([6(2),13(2),8(3),14(3),8(4),14(4),13(5),6(5),13(5),14(6),6(6),13(6),8(7),14⌋
↪  (7),8(8),14(8),6(9),13(9),8(10),14(10),13(11)])].
19 c4 v ((c5 ^ c6) v c4) != (c4 v (c5 v c4)) ^ (c4 v (c6 v c4)).  [deny(2)].
20 (c5 ^ c6) v c4 != (c5 v c4) ^ (c6 v c4).  [copy(19),rewrite([14(7),14(10),14(13)])].
27 x v ((x ^ y) v z) = x v z.  [para(10(a,1),8(a,1,1)),flip(a)].
29 (x v y) ^ (y ^ z) = y ^ z.  [para(11(a,1),6(a,1,1)),flip(a)].
36 x ^ (y v x) = x.  [para(11(a,1),13(a,1,2)),rewrite([3(1)]),flip(a)].
40 x v (y v (z v x)) = y v (z v x).  [para(8(a,1),14(a,1,2)),rewrite([8(5)])].
41 (x ^ y) v x = x.  [para(10(a,1),14(a,1,2)),rewrite([10(4)])].
51 ((x v y) ^ z) v y = ((y ^ z) v (x v y)) ^ (z v y).  [para(11(a,1),16(a,1,2)),rewrite([14(2)])].
65 x ^ (y v (z v x)) = x.  [para(8(a,1),36(a,1,2))].
```

```
121 (x ^ y) v (z v x) = z v x.  [para(14(a,1),27(a,2)),rewrite([40(4)])].
128 ((x ^ y) v z) ^ (u v (x v z)) = (x ^ y) v z.  [para(27(a,1),65(a,1,2,2))].
131 ((x v y) ^ z) v y = (x v y) ^ (z v y).  [back_rewrite(51),rewrite([121(6)])].
146 ((x v y) ^ z) v (y ^ u) = (x v y) ^ (z v (y ^ u)).
 ↪  [para(29(a,1),16(a,1,2)),rewrite([121(3),6(6),121(8)])].
152 ((x ^ y) v z) ^ (y v x) = (x v z) ^ (y v (z ^ x)).
 ↪  [back_rewrite(16),rewrite([146(4)]),flip(a)].
8421 (x ^ y) v z = (x v z) ^ (y v z).
 ↪  [para(152(a,1),131(a,1,1)),rewrite([131(5),8(4),41(3),8(7),128(8)]),flip(a)].
8422 $F.  [resolve(8421,a,20,a)].

============================== end of proof ==========================


============================== INPUT =================================

formulas(sos).
x ^ x = x.
x v x = x.
x ^ (y ^ z) = (x ^ y) ^ z.
x v (y v z) = (x v y) v z.
x ^ (x v y) = x.
x v (x ^ y) = x.
(x ^ y) v y = y.
(x v y) ^ y = y.
((x ^ y) ^ x) v ((((x v y) v x) ^ (z ^ ((x v y) v x))) v ((x ^ y) ^ x)) = ((x v ((y ^ z) ^ y)) v
 ↪  x) ^ (((y v z) v y) ^ ((x v ((y ^ z) ^ y)) v x)).
x ^ (y ^ x) = y ^ x.
x v (y v x) = x v y.
end_of_list.

formulas(goals).
(x ^ (y v z)) ^ x = ((x ^ y) ^ x) v ((x ^ z) ^ x).
(x v (y ^ z)) v x = ((x v y) v x) ^ ((x v z) v x).
end_of_list.

============================== end of input ==========================

============================== PROOF =================================

% -------- Comments from original proof --------
% Proof 1 at 0.05 (+ 0.00) seconds.
% Length of proof is 27.
% Level of proof is 7.
% Maximum clause weight is 19.
% Given clauses 52.

2 x v ((y ^ z) v x) = (x v (y v x)) ^ (x v (z v x)) # label(non_clause) # label(goal).  [goal].
5 x ^ (y ^ z) = (x ^ y) ^ z.  [assumption].
6 (x ^ y) ^ z = x ^ (y ^ z).  [copy(5),flip(a)].
7 x v (y v z) = (x v y) v z.  [assumption].
8 (x v y) v z = x v (y v z).  [copy(7),flip(a)].
9 x ^ (x v y) = x.  [assumption].
10 x v (x ^ y) = x.  [assumption].
12 (x ^ y) v y = y.  [assumption].
13 x ^ (y ^ x) = y ^ x.  [assumption].
14 x v (y v x) = x v y.  [assumption].
15 ((x ^ y) ^ x) v ((((x v y) v x) ^ (z ^ ((x v y) v x))) v ((x ^ y) ^ x)) = ((x v ((y ^ z) ^ y))
 ↪  v x) ^ (((y v z) v y) ^ ((x v ((y ^ z) ^ y)) v x)).  [assumption].
16 (x ^ y) v (z ^ (y v x)) = (x v z) ^ (y v (z ^ x)).
 ↪  [copy(15),rewrite([6(2),13(2),8(3),14(3),8(4),14(4),13(5),6(5),13(5),14(6),6(6),13(6),8(7),14
 ↪  (7),8(8),14(8),6(9),13(9),8(10),14(10),13(11)])].
```

```
19 c4 v ((c5 ^ c6) v c4) != (c4 v (c5 v c4)) ^ (c4 v (c6 v c4)).  [deny(2)].
20 c4 v (c5 ^ c6) != (c4 v c5) ^ (c4 v c6).  [copy(19),rewrite([14(7),14(10),14(13)])].
32 (x ^ y) v (y v z) = y v z.  [para(12(a,1),8(a,1,1)),flip(a)].
36 (x v y) ^ x = x.  [para(9(a,1),13(a,1,2)),rewrite([9(4)])].
37 x v (y ^ x) = x.  [para(13(a,1),10(a,1,2))].
47 x v (y ^ (x v z)) = (x v y) ^ (x v (z v (y ^ x))).
↪  [para(9(a,1),16(a,1,1)),rewrite([8(2),14(2),8(7)])].
60 (x v (y v z)) ^ (x v y) = x v y.  [para(8(a,1),36(a,1,1))].
64 x v (y ^ (z ^ x)) = x.  [para(6(a,1),37(a,1,2))].
65 x v ((y ^ x) v z) = x v z.  [para(37(a,1),8(a,1,1)),flip(a)].
96 x v (y v (z ^ x)) = x v y.  [para(9(a,1),64(a,1,2,2)),rewrite([8(3)])].
101 x v (y ^ (x v z)) = (x v y) ^ (x v z).  [back_rewrite(47),rewrite([96(7)])].
180 (x v (y v z)) ^ (x v (z ^ y)) = (x v z) ^ (x v y).
↪  [para(16(a,1),65(a,1,2)),rewrite([101(5),101(8)])].
427 (x v (y v z)) ^ (x v (u ^ y)) = x v (u ^ y).  [para(32(a,1),60(a,1,1,2))].
431 x v (y ^ z) = (x v y) ^ (x v z).  [back_rewrite(180),rewrite([427(5)])].
432 $F.  [resolve(431,a,20,a)].

============================== end of proof ==========================

============================== PROOF =================================

% -------- Comments from original proof --------
% Proof 2 at 17.73 (+ 1.75) seconds.
% Length of proof is 74.
% Level of proof is 14.
% Maximum clause weight is 31.
% Given clauses 547.

1 x ^ ((y v z) ^ x) = (x ^ (y ^ x)) v (x ^ (z ^ x)) # label(non_clause) # label(goal).  [goal].
3 x ^ x = x.  [assumption].
4 x v x = x.  [assumption].
5 x ^ (y ^ z) = (x ^ y) ^ z.  [assumption].
6 (x ^ y) ^ z = x ^ (y ^ z).  [copy(5),flip(a)].
7 x v (y v z) = (x v y) v z.  [assumption].
8 (x v y) v z = x v (y v z).  [copy(7),flip(a)].
9 x ^ (x v y) = x.  [assumption].
10 x v (x ^ y) = x.  [assumption].
11 (x v y) ^ y = y.  [assumption].
12 (x ^ y) v y = y.  [assumption].
13 x ^ (y ^ x) = y ^ x.  [assumption].
14 x v (y v x) = x v y.  [assumption].
15 ((x ^ y) ^ x) v ((((x v y) v x) ^ (z ^ ((x v y) v x))) v ((x ^ y) ^ x)) = ((x v ((y ^ z) ^ y))
↪  v x) ^ (((y v z) v y) ^ ((x v ((y ^ z) ^ y)) v x)).  [assumption].
16 (x ^ y) v (z ^ (y v x)) = (x v z) ^ (y v (z ^ x)).
↪  [copy(15),rewrite([6(2),13(2),8(3),14(3),8(4),14(4),13(5),6(5),13(5),14(6),6(6),13(6),8(7),14⌋
↪  (7),8(8),14(8),6(9),13(9),8(10),14(10),13(11)])].
17 (c1 ^ (c2 ^ c1)) v (c1 ^ (c3 ^ c1)) != c1 ^ ((c2 v c3) ^ c1).  [deny(1)].
18 (c2 ^ c1) v (c3 ^ c1) != (c2 v c3) ^ c1.  [copy(17),rewrite([13(5),13(8),13(14)])].
21 x ^ (x ^ y) = x ^ y.  [para(6(a,1),3(a,1)),rewrite([13(2)])].
23 x ^ ((x v y) ^ z) = x ^ z.  [para(9(a,1),6(a,1,1)),flip(a)].
26 (x ^ y) v (x ^ (y ^ z)) = x ^ y.  [para(6(a,1),10(a,1,2))].
27 x v ((x ^ y) v z) = x v z.  [para(10(a,1),8(a,1,1)),flip(a)].
30 (x v (y v z)) ^ z = z.  [para(8(a,1),11(a,1,1))].
32 (x ^ y) v (y v z) = y v z.  [para(12(a,1),8(a,1,1)),flip(a)].
36 (x v y) ^ x = x.  [para(9(a,1),13(a,1,2)),rewrite([9(4)])].
37 x v (y ^ x) = x.  [para(13(a,1),10(a,1,2))].
38 x v (y v (x v z)) = x v (y v z).  [para(14(a,1),8(a,1,1)),rewrite([8(2),8(4)]),flip(a)].
40 x v (y v (z v x)) = x v (y v z).  [para(8(a,1),14(a,1,2))].
41 (x v y) ^ (y v x) = y v x.  [para(14(a,1),11(a,1,1))].
47 x v (y ^ (x v z)) = (x v y) ^ (x v (z v (y ^ x))).
↪  [para(9(a,1),16(a,1,1)),rewrite([8(2),14(2),8(7)])].
```

```
49 (x ^ y) v (z ^ y) = ((y ^ x) v z) ^ (y v (z ^ (y ^ x))).
 ↪  [para(10(a,1),16(a,1,2,2)),rewrite([6(2),13(2)])].
52 (x v (y v z)) ^ (z v x) = z v x.
 ↪  [para(11(a,1),16(a,1,2)),rewrite([32(3),40(4),30(6)]),flip(a)].
59 (x v y) ^ (x ^ z) = x ^ z.  [para(36(a,1),6(a,1,1)),flip(a)].
60 (x v (y v z)) ^ (x v y) = x v y.  [para(8(a,1),36(a,1,1))].
64 x v (y ^ (z ^ x)) = x.  [para(6(a,1),37(a,1,2))].
65 x v ((y ^ x) v z) = x v z.  [para(37(a,1),8(a,1,1)),flip(a)].
67 (x ^ y) v (z ^ y) = ((x ^ y) v z) ^ y.  [para(37(a,1),16(a,1,2,2)),rewrite([6(2),3(1),64(8)])].
69 ((x ^ y) v z) ^ (x v (z ^ (x ^ y))) = ((y ^ x) v z) ^ x.
 ↪  [back_rewrite(49),rewrite([67(3)]),flip(a)].
70 ((c2 ^ c1) v c3) ^ c1 != (c2 v c3) ^ c1.  [back_rewrite(18),rewrite([67(7)])].
77 (x v y) ^ (z ^ y) = z ^ y.  [para(37(a,1),30(a,1,1,2))].
78 x ^ (y ^ (((x ^ y) v z) ^ u)) = x ^ (y ^ u).  [para(23(a,1),6(a,1)),rewrite([6(2)]),flip(a)].
79 (x v y) ^ ((x v (y v z)) ^ u) = (x v y) ^ u.  [para(8(a,1),23(a,1,2,1))].
80 (x v (y v z)) ^ y = y.  [para(11(a,1),23(a,2)),rewrite([8(3),77(5)])].
96 x v (y v (z ^ x)) = x v y.  [para(9(a,1),64(a,1,2,2)),rewrite([8(3)])].
101 x v (y ^ (x v z)) = (x v y) ^ (x v z).  [back_rewrite(47),rewrite([96(7)])].
119 x v (y ^ (x ^ z)) = x.  [para(37(a,1),27(a,1,2)),rewrite([10(2)]),flip(a)].
123 ((x ^ y) v z) ^ y = ((y ^ x) v z) ^ y.  [back_rewrite(69),rewrite([119(5)]),flip(a)].
146 (x ^ y) v (((x v z) ^ y) v u) = ((x v z) ^ y) v u.  [para(23(a,1),32(a,1,1))].
147 (x v (y v z)) ^ (u ^ y) = u ^ y.  [para(32(a,1),80(a,1,1,2))].
180 (x v (y v z)) ^ (x v (z ^ y)) = (x v z) ^ (x v y).
 ↪  [para(16(a,1),65(a,1,2)),rewrite([101(5),101(8)])].
182 ((x v y) ^ z) v ((x ^ z) v u) = ((x v y) ^ z) v u.  [para(23(a,1),65(a,1,2,1))].
207 (x ^ y) v (y ^ x) = x ^ y.  [para(3(a,1),26(a,1,2)),rewrite([6(2),13(2),6(5),13(5)])].
264 ((x v (y ^ z)) ^ z) v (u ^ (z v x)) = (x v ((y ^ z) v u)) ^ (z v (u ^ (x v (y ^ z)))).
 ↪  [para(96(a,1),16(a,1,2,2)),rewrite([8(9)])].
321 x ^ ((y ^ x) v y) = y ^ x.  [para(207(a,1),16(a,2,2)),rewrite([21(2),101(5),12(2),59(6)])].
339 x ^ (((y ^ x) v y) ^ z) = y ^ (x ^ z).  [para(321(a,1),6(a,1,1)),rewrite([6(2)]),flip(a)].
368 (x ^ y) v (z v (y ^ x)) = (x ^ y) v z.  [para(207(a,1),38(a,1,2,2)),rewrite([14(4)]),flip(a)].
413 ((x ^ y) v z) ^ (y ^ x) = y ^ x.  [para(207(a,1),52(a,1,2)),rewrite([368(4),207(7)])].
427 (x v (y v z)) ^ (x v (u ^ y)) = x v (u ^ y).  [para(32(a,1),60(a,1,1,2))].
431 x v (y ^ z) = (x v y) ^ (x v z).  [back_rewrite(180),rewrite([427(5)])].
478 (((x v y) ^ z) v u) ^ (z v x) = (x v ((y ^ z) v u)) ^ ((z v u) ^ (z v x)).  [back_rewrite(264⌋
 ↪  ),rewrite([431(2),6(4),11(3),431(5),32(7),431(10),431(13),431(13),14(13),60(13)])].
564 x ^ (((x ^ (y v z)) v u) ^ z) = x ^ z.  [para(11(a,1),78(a,2,2)),rewrite([77(6)])].
860 ((x ^ (y v x)) v z) ^ x = x.  [para(11(a,1),413(a,1,2)),rewrite([11(6)])].
906 (x ^ (y v x)) v (z v (x v u)) = (x ^ (y v x)) v (z v u).
 ↪  [para(860(a,1),27(a,1,2,1)),rewrite([8(5),8(9)])].
1143 ((c1 ^ c2) v c3) ^ c1 != (c2 v c3) ^ c1.  [para(123(a,1),70(a,1))].
2417 ((x ^ (y v z)) v x) ^ z = x ^ z.  [para(339(a,1),77(a,1)),rewrite([11(2)]),flip(a)].
2488 (((x v y) ^ (z v u)) v x) ^ ((x v y) ^ u) = (((x v y) ^ (z v u)) v x) ^ u.
 ↪  [para(2417(a,1),79(a,1,2))].
3387 (x ^ (y v x)) v (y v z) = y v (x v z).
 ↪  [para(41(a,1),146(a,1,2,1)),rewrite([8(4),906(5),41(7),8(6)])].
3783 ((x ^ (y v z)) v u) ^ (x ^ z) = x ^ z.
 ↪  [para(564(a,1),13(a,1,2)),rewrite([6(6),13(5),564(10)])].
3884 (((x v y) ^ (z v u)) v x) ^ u = (x v y) ^ u.
 ↪  [back_rewrite(2488),rewrite([3783(7)]),flip(a)].
6688 (x ^ (y v x)) v y = y v x.  [para(4(a,1),3387(a,1,2)),rewrite([14(5)])].
8213 ((x v y) ^ (z v x)) v z = z v x.  [para(6688(a,1),182(a,1,2)),rewrite([12(5)]),flip(a)].
8233 ((x v y) ^ ((z v u) ^ (z v x))) v z = (z v u) ^ (z v x).
 ↪  [para(32(a,1),8213(a,1,1,1)),rewrite([431(3),431(8)])].
27126 (((x v y) ^ z) v u) ^ x = (z v u) ^ x.
 ↪  [para(478(a,1),3884(a,1,1,1)),rewrite([431(10),8233(17),6(14),6(13),11(12),147(12)]),flip(a)].
27152 ((x ^ y) v z) ^ x = (y v z) ^ x.  [para(4(a,1),27126(a,1,1,1,1))].
27153 $F.  [resolve(27152,a,1143,a)].

============================== end of proof ==========================
```

Code 10: Any weak distributive solution is simply cancellative. A proof is given, first for the left-handed case, and then for the right-handed case.

```
============================== INPUT =================================

formulas(sos).
x ^ x = x.
x v x = x.
x ^ (y ^ z) = (x ^ y) ^ z.
x v (y v z) = (x v y) v z.
x ^ (x v y) = x.
x v (x ^ y) = x.
(x ^ y) v y = y.
(x v y) ^ y = y.
((x ^ y) ^ x) v ((((x v y) v x) ^ (z ^ ((x v y) v x))) v ((x ^ y) ^ x)) = ((x v ((y ^ z) ^ y)) v
↪  x) ^ (((y v z) v y) ^ ((x v ((y ^ z) ^ y)) v x)).
x ^ (y ^ x) = x ^ y.
x v (y v x) = y v x.
end_of_list.

formulas(goals).
x v (y v x) = z v (y v z) & x ^ (y ^ x) = z ^ (y ^ z) -> x = z.
end_of_list.

============================== end of input ==========================

============================== PROOF =================================

% -------- Comments from original proof --------
% Proof 1 at 0.01 (+ 0.03) seconds.
% Length of proof is 27.
% Level of proof is 7.
% Maximum clause weight is 19.
% Given clauses 32.

1 x v (y v x) = z v (y v z) & x ^ (y ^ x) = z ^ (y ^ z) -> x = z # label(non_clause) #
↪  label(goal).  [goal].
4 x ^ (y ^ z) = (x ^ y) ^ z.  [assumption].
5 (x ^ y) ^ z = x ^ (y ^ z).  [copy(4),flip(a)].
6 x v (y v z) = (x v y) v z.  [assumption].
7 (x v y) v z = x v (y v z).  [copy(6),flip(a)].
9 x v (x ^ y) = x.  [assumption].
10 (x v y) ^ y = y.  [assumption].
11 (x ^ y) v y = y.  [assumption].
12 x ^ (y ^ x) = x ^ y.  [assumption].
13 x v (y v x) = y v x.  [assumption].
14 ((x ^ y) ^ x) v ((((x v y) v x) ^ (z ^ ((x v y) v x))) v ((x ^ y) ^ x)) = ((x v ((y ^ z) ^ y))
↪  v x) ^ (((y v z) v y) ^ ((x v ((y ^ z) ^ y)) v x)).  [assumption].
15 ((x v y) ^ z) v (y ^ x) = ((x ^ z) v y) ^ (z v x).
↪  [copy(14),rewrite([5(2),12(2),7(3),13(3),7(4),13(4),12(5),5(5),12(5),13(6),5(6),12(6),7(7),13⌋
↪  (7),7(8),13(8),5(9),12(9),7(10),13(10),12(11)])].
16 c3 v (c2 v c3) = c1 v (c2 v c1).  [deny(1)].
17 c2 v c3 = c2 v c1.  [copy(16),rewrite([13(5),13(8)])].
18 c3 ^ (c2 ^ c3) = c1 ^ (c2 ^ c1).  [deny(1)].
19 c3 ^ c2 = c1 ^ c2.  [copy(18),rewrite([12(5),12(8)])].
20 c3 != c1.  [deny(1)].
41 (x ^ y) v x = x.  [para(9(a,1),13(a,1,2)),rewrite([9(4)])].
58 (c2 v c1) ^ c3 = c3.  [para(17(a,1),10(a,1,1))].
62 c3 v (c1 ^ c2) = c3.  [para(19(a,1),9(a,1,2))].
63 c2 ^ c3 = c2 ^ c1.  [para(19(a,1),12(a,1,2)),rewrite([12(5)]),flip(a)].
82 c1 ^ (c3 v c2) = c3.  [para(58(a,1),15(a,1,1)),rewrite([62(5),63(4),11(6)]),flip(a)].
90 (c2 ^ c1) v c3 = c3.  [para(63(a,1),11(a,1,1))].
```

```
102 c3 v c1 = c1.  [para(82(a,1),41(a,1,1))].
130 c3 ^ (c1 v c2) = c1.  [para(90(a,1),15(a,2,1)),rewrite([17(3),10(5),19(4),9(5)]),flip(a)].
132 c3 = c1.  [para(130(a,1),9(a,1,2)),rewrite([102(3)]),flip(a)].
133 $F.  [resolve(132,a,20,a)].

============================== end of proof ==========================


============================== INPUT =================================

formulas(sos).
x ^ x = x.
x v x = x.
x ^ (y ^ z) = (x ^ y) ^ z.
x v (y v z) = (x v y) v z.
x ^ (x v y) = x.
x v (x ^ y) = x.
(x ^ y) v y = y.
(x v y) ^ y = y.
((x ^ y) ^ x) v ((((x v y) v x) ^ (z ^ ((x v y) v x))) v ((x ^ y) ^ x)) = ((x v ((y ^ z) ^ y)) v
 ↪  x) ^ (((y v z) v y) ^ ((x v ((y ^ z) ^ y)) v x)).
x ^ (y ^ x) = y ^ x.
x v (y v x) = x v y.
end_of_list.

formulas(goals).
x v (y v x) = z v (y v z) & x ^ (y ^ x) = z ^ (y ^ z) -> x = z.
end_of_list.

============================== end of input ==========================

============================== PROOF =================================

% -------- Comments from original proof --------
% Proof 1 at 0.05 (+ 0.00) seconds.
% Length of proof is 26.
% Level of proof is 6.
% Maximum clause weight is 19.
% Given clauses 51.

1 x v (y v x) = z v (y v z) & x ^ (y ^ x) = z ^ (y ^ z) -> x = z # label(non_clause) #
 ↪  label(goal).  [goal].
4 x ^ (y ^ z) = (x ^ y) ^ z.  [assumption].
5 (x ^ y) ^ z = x ^ (y ^ z).  [copy(4),flip(a)].
6 x v (y v z) = (x v y) v z.  [assumption].
7 (x v y) v z = x v (y v z).  [copy(6),flip(a)].
8 x ^ (x v y) = x.  [assumption].
9 x v (x ^ y) = x.  [assumption].
10 (x v y) ^ y = y.  [assumption].
11 (x ^ y) v y = y.  [assumption].
12 x ^ (y ^ x) = y ^ x.  [assumption].
13 x v (y v x) = x v y.  [assumption].
14 ((x ^ y) ^ x) v ((((x v y) v x) ^ (z ^ ((x v y) v x))) v ((x ^ y) ^ x)) = ((x v ((y ^ z) ^ y))
 ↪  v x) ^ (((y v z) v y) ^ ((x v ((y ^ z) ^ y)) v x)).  [assumption].
15 (x ^ y) v (z ^ (y v x)) = (x v z) ^ (y v (z ^ x)).
 ↪  [copy(14),rewrite([5(2),12(2),7(3),13(3),7(4),13(4),12(5),5(5),12(5),13(6),5(6),12(6),7(7),13⌋
 ↪  (7),7(8),13(8),5(9),12(9),7(10),13(10),12(11)])].
16 c3 v (c2 v c3) = c1 v (c2 v c1).  [deny(1)].
17 c3 v c2 = c1 v c2.  [copy(16),rewrite([13(5),13(8)])].
18 c3 ^ (c2 ^ c3) = c1 ^ (c2 ^ c1).  [deny(1)].
19 c2 ^ c3 = c2 ^ c1.  [copy(18),rewrite([12(5),12(8)])].
```

```
20 c3 != c1.  [deny(1)].
59 c3 ^ (c1 v c2) = c3.  [para(17(a,1),8(a,1,2))].
60 c2 v c3 = c2 v c1.  [para(17(a,1),13(a,1,2)),rewrite([13(5)]),flip(a)].
62 c2 ^ (c3 ^ x) = c2 ^ (c1 ^ x).  [para(19(a,1),5(a,1,1)),rewrite([5(4)]),flip(a)].
63 (c2 ^ c1) v c3 = c3.  [para(19(a,1),11(a,1,1))].
82 (c2 v c1) ^ (c1 v (c3 ^ c2)) = c3.  [para(59(a,1),15(a,1,2)),rewrite([63(5),60(4)]),flip(a)].
310 c3 ^ c2 = c1 ^ c2.  [para(62(a,1),12(a,1)),rewrite([12(5)]),flip(a)].
323 c3 = c1.  [back_rewrite(82),rewrite([310(7),9(8),10(5)]),flip(a)].
324 $F.  [resolve(323,a,20,a)].

============================== end of proof ==========================
```

Code 11: Any weak distributive solution is lower symmetric. A proof is given, first for the left-handed case, and then for the right-handed case.

```
============================== INPUT =================================

formulas(sos).
x ^ x = x.
x v x = x.
x ^ (y ^ z) = (x ^ y) ^ z.
x v (y v z) = (x v y) v z.
x ^ (x v y) = x.
x v (x ^ y) = x.
(x ^ y) v y = y.
(x v y) ^ y = y.
((x ^ y) ^ x) v ((((x v y) v x) ^ (z ^ ((x v y) v x))) v ((x ^ y) ^ x)) = ((x v ((y ^ z) ^ y)) v
 ↪  x) ^ (((y v z) v y) ^ ((x v ((y ^ z) ^ y)) v x)).
x ^ (y ^ x) = x ^ y.
x v (y v x) = y v x.
end_of_list.

formulas(goals).
x v y = y v x -> x ^ y = y ^ x.
end_of_list.

============================== end of input ==========================

============================== PROOF =================================

% Proof 1 at 0.01 (+ 0.00) seconds.
% Length of proof is 19.
% Level of proof is 6.
% Maximum clause weight is 51.000.
% Given clauses 18.

1 x v y = y v x -> x ^ y = y ^ x # label(non_clause) # label(goal).  [goal].
2 x ^ x = x.  [assumption].
3 x v x = x.  [assumption].
4 x ^ (y ^ z) = (x ^ y) ^ z.  [assumption].
5 (x ^ y) ^ z = x ^ (y ^ z).  [copy(4),flip(a)].
6 x v (y v z) = (x v y) v z.  [assumption].
7 (x v y) v z = x v (y v z).  [copy(6),flip(a)].
11 (x v y) ^ y = y.  [assumption].
12 ((x ^ y) ^ x) v ((((x v y) v x) ^ (z ^ ((x v y) v x))) v ((x ^ y) ^ x)) = ((x v ((y ^ z) ^ y))
 ↪  v x) ^ (((y v z) v y) ^ ((x v ((y ^ z) ^ y)) v x)).  [assumption].
13 (x v ((y ^ (z ^ y)) v x)) ^ ((y v (z v y)) ^ (x v ((y ^ (z ^ y)) v x))) = (x ^ (y ^ x)) v (((x
 ↪  v (y v x)) ^ (z ^ (x v (y v x)))) v (x ^ (y ^ x))).
 ↪  [copy(12),rewrite([5(2),7(4),7(6),5(10),5(14),7(16),7(18),5(20),7(22)]),flip(a)].
14 x ^ (y ^ x) = x ^ y.  [assumption].
```

```
15 x v (y v x) = y v x.  [assumption].
16 c2 v c1 = c1 v c2.  [deny(1)].
17 c2 ^ c1 != c1 ^ c2.  [deny(1)].
18 ((x ^ y) v z) ^ (y v x) = ((x v z) ^ y) v (z ^ x).  [back_rewrite(13),rewrite([14(2),15(3),15(⌋
 ↪  4),14(5),15(6),14(7),14(6),15(7),15(8),14(9),14(9),15(10)])].
41 (c1 v c2) ^ c1 = c1.  [para(16(a,1),11(a,1,1))].
73 c1 v (c2 ^ c1) = c1.  [para(41(a,1),18(a,2,1)),rewrite([2(3),3(6),41(5)]),flip(a)].
76 c2 ^ c1 = c1 ^ c2.  [para(73(a,1),11(a,1,1)),rewrite([14(5)]),flip(a)].
77 $F.  [resolve(76,a,17,a)].

============================== end of proof ==========================


============================== INPUT =================================

formulas(sos).
x ^ x = x.
x v x = x.
x ^ (y ^ z) = (x ^ y) ^ z.
x v (y v z) = (x v y) v z.
x ^ (x v y) = x.
x v (x ^ y) = x.
(x ^ y) v y = y.
(x v y) ^ y = y.
((x ^ y) ^ x) v ((((x v y) v x) ^ (z ^ ((x v y) v x))) v ((x ^ y) ^ x)) = ((x v ((y ^ z) ^ y)) v
 ↪  x) ^ (((y v z) v y) ^ ((x v ((y ^ z) ^ y)) v x)).
x ^ (y ^ x) = y ^ x.
x v (y v x) = x v y.
end_of_list.

formulas(goals).
x v y = y v x -> x ^ y = y ^ x.
end_of_list.

============================== end of input ==========================

============================== PROOF =================================

% -------- Comments from original proof --------
% Proof 1 at 0.00 (+ 0.05) seconds.
% Length of proof is 18.
% Level of proof is 5.
% Maximum clause weight is 19.
% Given clauses 18.

1 x v y = y v x -> x ^ y = y ^ x # label(non_clause) # label(goal).  [goal].
2 x ^ x = x.  [assumption].
3 x v x = x.  [assumption].
4 x ^ (y ^ z) = (x ^ y) ^ z.  [assumption].
5 (x ^ y) ^ z = x ^ (y ^ z).  [copy(4),flip(a)].
6 x v (y v z) = (x v y) v z.  [assumption].
7 (x v y) v z = x v (y v z).  [copy(6),flip(a)].
8 x ^ (x v y) = x.  [assumption].
12 x ^ (y ^ x) = y ^ x.  [assumption].
13 x v (y v x) = x v y.  [assumption].
14 ((x ^ y) ^ x) v ((((x v y) v x) ^ (z ^ ((x v y) v x))) v ((x ^ y) ^ x)) = ((x v ((y ^ z) ^ y))
 ↪  v x) ^ (((y v z) v y) ^ ((x v ((y ^ z) ^ y)) v x)).  [assumption].
15 (x v y) ^ (z v (y ^ x)) = (x ^ z) v (y ^ (z v x)).
 ↪  [copy(14),rewrite([5(2),12(2),7(3),13(3),7(4),13(4),12(5),5(5),12(5),13(6),5(6),12(6),7(7),13⌋
 ↪  (7),7(8),13(8),5(9),12(9),7(10),13(10),12(11)]),flip(a)].
16 c2 v c1 = c1 v c2.  [deny(1)].
```

```
17 c2 ^ c1 != c1 ^ c2.  [deny(1)].
57 c2 ^ (c1 v c2) = c2.  [para(16(a,1),8(a,1,2))].
74 (c2 ^ c1) v c2 = c2.  [para(57(a,1),15(a,2,2)),rewrite([3(3),2(5),57(5)]),flip(a)].
76 c2 ^ c1 = c1 ^ c2.  [para(74(a,1),8(a,1,2)),rewrite([5(5),12(5)]),flip(a)].
77 $F.  [resolve(76,a,17,a)].

============================== end of proof ==========================
```

List of symbols

Symbol	Description	Page
$(A,+,+,\iota,\sigma)$	A trivial YB-semitruss.	59
$(A,+,\circ,\lambda,\sigma)$	A YB-semitruss.	58
$(A,+,\circ,\lambda)$	A left semitruss.	57
$(B,+,\circ)$	A (skew) left brace or semi-brace.	30
$(G(X,r),r_{G(X,r)})$	The extended solution of (X,r) on $G(X,r)$.	39
$(M(X,r),r_{M(X,r)})$	The extended solution of (X,r) associated to $M(X,r)$, as defined in Theorem 2.1.1.	39
$(S,\cdot^{\mathrm{op}})$	The opposite semigroup of a semigroup $(S,\cdot)$.	37
$(X,\triangleleft)$	A shelf, rack or quandle.	33
(X,r)	A set-theoretic solution of the Yang-Baxter equation, with $r: X\times X\to X\times X:(x,y)\mapsto(\lambda_x(y),\rho_y(x))$.	28
(X,s')	The right derived solution of (X,r).	40
(X,s)	The left derived solution of (X,r).	40
$[G,G]$	The commutator subgroup of the group G.	127
$\mathrm{Aut}(S)$	The automorphism group of an algebraic structure S.	37
$\mathrm{End}(S)$	The set of all endomorhisms of an algebraic structure S.	37
$\mathrm{FM}(X)$	The free monoid generated by the set X.	37
$\mathrm{gr}(X\mid R)$	The group presented with set of generators X and with set of relations R.	37
$\mathrm{gr}(B)$	The subgroup of a group A generated by the set $B\subseteq A$.	37
id_X	The identity map $X\to X:x\mapsto x$ on a set X.	37
$\mathrm{Im}(f)$	The image of a function f.	36
$\mathrm{Inj}(X,r)$	The induced set-theoretic solution $(\iota(X),r_{\iota(X)})$.	39
ι	The natural map $\iota: X\to G$.	39
$\langle B\rangle$	The subsemigroup of a semigroup A generated by the set $B\subseteq A$.	37
$\langle B\rangle^1$	The submonoid of a monoid A generated by the set $B\subseteq A$.	37
$\langle X\mid R\rangle$	The semigroup presented with set of generators X and with	

	set of relations R.	37
$\langle X \mid R\rangle^1$	The monoid presented with set of generators X and with set of relations R.	37
$\mathrm{Map}(X,X)$	The set of all maps $X \to X$.	37
$\mathbb{N}$	The set of non-negative integers.	37
π	1-cocycle $\pi : M(X,r) \to A(X,r)$.	44
π'	1-cocycle $\pi : M(X,r) \to A'(X,r)$.	44
$\mathrm{Ret}(X,r)$	The retract solution of (X,r).	149
$\mathrm{Soc}(B)$	The socle of a skew left brace $(B,+,\circ)$.	31
$\mathrm{Sym}(X)$	The symmetric group of a set X.	37
Sym_n	The symmetric group on n elements.	14
$\mathbb{Z}$	The set of integers.	24
$A'(X,r)$	The right derived (structure) monoid associated to the solution (X,r).	40
$A(X,r)$	The left derived (structure) monoid associated to the solution (X,r).	40
$A'_{\mathrm{gr}}(X,r)$	The right derived (structure) group associated to the solution (X,r).	41
$A_{\mathrm{gr}}(X,r)$	The left derived (structure) group associated to the solution (X,r).	41
B^e	$B^e = \{(b, \lambda'_{\pi^{-1}(b)}) \mid b \in B\}$, for a subset B of $A(X,r)$.	133
$E_*(S)$	The subset of idempotents of a semigroup $(S,*)$.	82
$G(X,r)$	The structure group associated to the solution (X,r).	37
K	A field.	35
$K[(A(X,r),+)]$	The derived structure algebra associated to (X,r).	102
$K[(M(X,r),\circ)]$	The structure algebra associated to (X,r).	102
$K[G(X,r)]$	The structure group algebra associated to (X,r).	35
$M(X,r)$	The structure monoid associated to the solution (X,r).	37
$S(X,r)$	The structure semigroup associated to the solution (X,r).	37
S^1	The smallest monoid containing the semigroup S.	37
$T(G)$	The torsion subgroup of the group G.	127
$Z(S)$	The center of a semigroup S.	37

Index