Left Braces and the Solutions of the Yang-Baxter Equation

Patrick Kinnear, Ivan Lau, Dora Puljic

Year 4 Project

School of Mathematics

University of Edinburgh

08/03/2019

Abstract

In this paper, we study the solutions of the Yang-Baxter equation (YBE) and the theory of left braces. For the YBE, we provide three new conditions for constructing particular types of R-matrices. In addition, we establish an explicit formula for the characteristic polynomial of all R-matrices arising from non-degenerate set-theoretic solution of Yang-Baxter equation.

For left braces, we prove that a left brace with the operation $*$ associative is a two-sided brace. Finally, we show that the properties of being solvable and semiprime are both preserved under semidirect product and wreath products.

Contents

Abstract **2**

Introduction **7**

1 Solutions of the Yang-Baxter Equation **10**

1.1 The Yang-Baxter Equation 10

1.1.1 The Tensor and Kronecker Products 10

1.1.2 The Yang-Baxter Equation 11

1.2 R-matrices 12

2 Set-Theoretic Solutions of the Yang Baxter Equation **18**

2.1 Set-Theoretic Solutions of the Yang-Baxter Equation 18

2.2 Obtaining R-matrices from Set-Theoretic Solutions 19

2.3 Non-Degenerate Set-Theoretic Solutions 21

2.4 Involutive Set-Theoretic Solutions 22

3 Jacobson Radical Rings **25**

3.1 Jacobson Radical Rings 25

3.2 Jacobson Radical Rings and the Circle Operation $\circ$ 26

3.3 Set-Theoretic Solutions of the Yang-Baxter Equation Associated to Jacobson Radical Rings 27

4 Left Braces **29**

4.1 Left Braces 29

4.2 Arithmetic on Left Braces 32

4.3 Set-Theoretic Solutions of the Yang-Baxter Equation Associated to Left Braces . . . 33

5 Constructions of Left Braces 37

5.1 Subbraces, Ideals and Quotients . . . 37

5.1.1 Brace Morphisms . . . 39

5.2 Semidirect and Wreath Products of Braces . . . 40

6 Left Braces Associated to Solutions 43

6.1 Constructing Left Braces from Set-Theoretic Solutions . . . 43

6.2 Embedding Solutions in Braces . . . 49

6.3 Using Left Braces to Obtain All Finite Solutions of the YBE . . . 51

7 Other Relaxations of Jacobson Radical Rings 53

7.1 Right Braces . . . 53

7.2 Two-Sided Braces . . . 54

7.3 One-Sided Braces with Associative $*$ Operation . . . 55

8 Algebraic Properties of Left Braces 58

8.1 Solvable Braces . . . 58

8.2 Semiprime Braces . . . 62

Conclusion 68

Bibliography 70

List of Figures

5.1 First Isomorphism Theorem 40

6.1 The map $\psi\colon \mathbb{Z}^X \to \mathrm{Sym}_X$. 47

List of Tables

4.1 Cayley table of $(A, \circ)$ in Example 4.1.5, where the intersection of row a and column b is $a \circ b$. 31

4.2 Table of $(A, *)$ in Example 4.1.5, where the intersection of row a and column b is $a * b$. 31

7.1 Comparing different axioms held by each algebraic structure . . . 57

Introduction

The Yang-Baxter equation (YBE) first appeared in theoretical physics papers by Yang [Yan67] and Baxter [Bax72]. It has since developed into an indispensable tool in modern physics, with connections to many areas such as statistical mechanics [GY94, Bax82], integrable systems [Jim90, Skl90] and quantum field theory [Frö88, ZZ79]. More recently, it has also found applications in quantum computation and quantum information processing [KL04, GKZ05, GZ07].

Beyond its physical significance, the YBE is also of great mathematical interest since its investigation led to the inception of quantum groups [Jim85, Dri88]. Quantum groups have asserted their influence in various mathematical areas such as category theory [Tur92, Wen98], representation theory [Yet90, KS97], topology [BS04], combinatorics [Ari02, Jin03], non-commutative geometry [Man18] and algebraic geometry [MO12], to name a few.

Given a vector space V, we say that a linear operator $R\colon V \otimes V \to V \otimes V$ is a solution of the YBE if and only if

$$(R \otimes I)(I \otimes R)(R \otimes I) = (I \otimes R)(R \otimes I)(I \otimes R).$$

where I is the identity on V. When the dimension of V is finite, we call R an R-matrix. It is a central open problem to find all the solutions of the YBE. Unitary solutions to the YBE, in particular, lead to braid group representations which can be used in quantum information processing [KL02]. While many solutions have been found [Pou18], the problem of finding all the solutions of the YBE is still open for vector spaces of dimension $n > 2$.

If X is a basis of the vector space V, then a map $r\colon X^2 \to X^2$ such that

$$(r \times \mathrm{Id}_X)(\mathrm{Id}_X \times r)(r \times \mathrm{Id}_x) = (\mathrm{Id}_X \times r)(r \times \mathrm{Id}_x)(\mathrm{Id}_X \times r),$$

induces a solution of YBE. We call the pair (X, r) a set-theoretic solution of the YBE. The study of these solutions of the YBE was proposed by Drinfeld in [Dri92]. If we denote the components of the map r by $r(x, y) = (\sigma_x(y), \tau_y(x))$ for all $x, y \in X$, then we say the solution (X, r) is non-degenerate if both σ_x and τ_x are bijective for any $x \in X$. If $r^2 = \mathrm{Id}_{X^2}$, then we say (X, r) is an involutive solution. The subclass of non-degenerate, involutive set-theoretic solutions has received considerable attention [ESS99, GIdB98] due to its applications in physics as well as its connections to other topics in mathematics such as bijective 1-cocycles

[ESS99], Bieberbach groups [GIdB98], racks and Hopf algebras [AG03, EG98].

Following Drinfeld's proposal to study set-theoretic solutions of the YBE, early studies (see, for instance, [ESS99, GIdB98]) tended to use techniques from group theory. In [Rum07], Rump introduced a new algebraic structure, now known as a left brace, to help study non-degenerate involutive set-theoretic solutions of the YBE. In the same paper, it was shown that many of the earlier results in [ESS99, GIdB98] can be interpreted as consequences of the algebraic properties of this structure. Moreover, using left braces to investigate these solutions have led to many new and significant results [Rum08, BC14, CJO14, BCJ16, BCJO17a, CGIS17, Smo18b]. In particular, [BCJ16] has reduced the open problem of classification of non-degenerate involutive set-theoretic solutions of the Yang–Baxter equation to the open problem of classification of left braces. As left braces generalise Jacobson radical rings [Rum07], they have also been studied solely for their algebraic properties [Bac15, Brz18, CGIS18].

Our aim

As the theory of left braces is a recent and fast-developing area of research, the existing literature consists mainly of research papers. In fact, there is only one survey written to date [Ced18]. This paper aims to provide an accessible and self-contained overview of the theory of left braces, aimed at late undergraduate or early graduate students.

We set out to provide strong motivation for the study of braces by showing how they are intimately related to the solutions of the YBE. We will look in depth at the YBE and its solutions, supplying concrete examples and background material when necessary. With all this set up, we will introduce left braces and give an account of how the problem of finding all non-degenerate involutive set-theoretic solutions of the YBE can be reduced to that of finding all left braces. Finally, we will proceed to study the braces in their own right: for instance, examining certain algebraic properties of braces which have familiar analogues in undergraduate level group and ring theory.

We emphasise that our layout is complementary to the survey of [Ced18], in which left braces are introduced in the abstract and thoroughly examined, with their relationship to solutions of the YBE being a culminating rather than a motivating moment.

Contributions

Our contributions to the existing literature are as follows:

(i) We present three new conditions for constructing particular types of R-matrices. (See Proposition 1.2.6, Proposition 1.2.8, Proposition 1.2.10.)

(ii) We establish an explicit formula for the characteristic polynomial of any R-matrix arising from a non-degenerate set-theoretic solution of the YBE. (See Proposition 1.2.11.)

(iii) We prove that a left brace with an associative operation $*$ is a two-sided brace. (See Theorem 7.3.1.) This answers the problem proposed in [CGIS18, Question 2.1(2)].

(iv) We show that brace properties of being solvable and semiprime are invariant under the semidirect and wreath product of braces. (See Lemma 8.1.5, Lemma 8.1.6, Lemma 8.2.5, Lemma 8.2.10.)

Organisation of the Paper

This paper is organised as follows. In Chapter 1, we formally introduce the YBE. We review past results regarding R-matrices and also present our new results. In Chapter 2, we introduce non-degenerate involutive set-theoretic solutions of the YBE. We then illustrate the method to obtain R-matrices from these set-theoretic solutions. Chapter 3 studies Jacobson radical rings and their associated non-degenerate involutive set-theoretic solutions of the YBE. Left braces, which generalise Jacobson radical rings, are introduced in Chapter 4 along with their associated non-degenerate involutive set-theoretic solutions of the YBE. In Chapter 5, we introduce familiar algebraic notions in the context of left braces such as subbraces, quotients, ideals, products, and morphisms. In Chapter 6 we show that any set-theoretic solution (X, r) is embedded in the solution (A, r_A) associated to some left brace A. In particular, we explain how any finite solution can be embedded in that of a finite brace. In Chapter 7, we define right braces and show that a left brace with associative operation $*$ is a two-sided brace. In Chapter 8, we define solvable and semiprime braces and show that these properties are preserved by the semidirect and wreath products.

Chapter 1

Solutions of the Yang-Baxter Equation

In this chapter, we introduce the celebrated Yang-Baxter Equation and its solutions, which are called R-matrices in a finite-dimensional setting. We give results on R-matrices and their characteristic polynomials, and we show how to obtain R-matrices from a set X and a map $r\colon X^2 \to X^2$.

1.1 The Yang-Baxter Equation

The Yang-Baxter equation is an important equation concerning linear operators. To fully understand it we will require the notions of tensor and Kronecker products, which we briefly outline here.

1.1.1 The Tensor and Kronecker Products

Given two vector spaces V and W over $\mathbb{C}$, with respective bases $\{e_i\}_{i\in I}$ and $\{f_j\}_{j\in J}$, we may ask how to combine them to form a new vector space. One construction is the direct sum $V \oplus W$, which has dimension $\dim V + \dim W$. In contrast, the **tensor product** is a way to combine V and W to form a new vector space, $V \otimes W$, of dimension $\dim V \times \dim W$. For our purposes, the details of this construction are not important, and interested readers are referred to [Gri07, XI.5] for a more detailed discussion of the tensor product.

In the finite dimensional case, we may express $V \otimes W$ using coordinate vectors. If $\{e_i\}_{i=1}^m$ is a basis for V and $\{f_j\}_{j=1}^n$ a basis for W, then $V \otimes W$ will be a vector space of dimension mn, hence isomorphic to $\mathbb{C}^{mn}$. We will denote the basis of $V \otimes W$ as the set $\{e_i \otimes f_j\}_{1\le i\le m, 1\le j\le n}$. When this set is taken to have the lexicographical ordering, then $e_i \otimes f_j$ is the column vector of size mn, with 1 in the $(i,j)^{\text{th}}$ entry and zeros elsewhere.

Since all $\mathbb{C}$-vector spaces of dimension mn are isomorphic, it is natural to ask what makes $V \otimes W$ different from $\mathbb{C}^{mn}$? The answer is that we have a notion of how to combine elements of V and W to obtain elements of $V \otimes W$. For $v = \sum_{i=1}^{m} \lambda_i e_i \in V, w \in W$, we can define a map $\otimes \colon V \times W \to V \otimes W$ by

$$v \otimes w = \begin{bmatrix} \lambda_1 w \\ \vdots \\ \lambda_n w \end{bmatrix}. \tag{1.1}$$

It should be noted that in general, elements of $V \otimes W$ need not have the form $v \otimes w$ for $v \in V, w \in W$.

Now, suppose that we are given vector spaces V, W, X, Y and linear maps $S \colon V \to X$ and $T \colon W \to Y$. Then, we can define $S \otimes T \colon V \otimes W \to X \otimes Y$ to be the map acting on the basis of $V \otimes W$ as

$$(S \otimes T)(e_i \otimes f_j) = (Se_i) \otimes (Tf_j).$$

The definition of $S \otimes T$ is well-defined regardless of the dimensions of the vector spaces involved. In the case where V, W, X, Y are all finite-dimensional, say they have dimensions m, n, k, l respectively, then we can represent the maps S, T and $S \otimes T$ as matrices. Let

$$S = \begin{bmatrix} s_{11} & \dots & s_{1m} \\ \vdots & \ddots & \vdots \\ s_{k1} & \dots & s_{km} \end{bmatrix}$$

be the matrix of S, and $T \in \mathbb{C}^{l \times n}$ be the matrix of T. Then the matrix representing $S \otimes T$ is

$$S \otimes T = \begin{bmatrix} s_{11}T & \dots & s_{1m}T \\ \vdots & \ddots & \vdots \\ s_{k1}T & \dots & s_{km}T \end{bmatrix}. \tag{1.2}$$

Given any two matrices A, B, the above construction gives a way of taking their product $A \otimes B$, which we shall refer to as the **Kronecker product** of A and B.

1.1.2 The Yang-Baxter Equation

We are now ready to define the Yang-Baxter equation. Let V be a vector space over $\mathbb{C}$, and $R \colon V \otimes V \to V \otimes V$ a linear operator. We say that R is **a solution of Yang-Baxter equation** if and only if

$$(R \otimes I)(I \otimes R)(R \otimes I) = (I \otimes R)(R \otimes I)(I \otimes R). \tag{1.3}$$

where I is the identity map on V.

For finite dimensional V, we call solutions of the YBE R-matrices. We will now

give an indication of why finding (all) solutions of the YBE is difficult. Suppose $\dim V = n < \infty$. Then a naïve approach to finding R-matrices $R\colon V \otimes V \to V \otimes V$ would be to treat each entry of R as an unknown. This gives n^4 unknowns, since R is $n^2 \times n^2$. We could try to form a system of simultaneous equations by equating the entries of the left- and right-hand-side of (1.3). But the left- and right-hand-sides of (1.3) are products of the matrices $R \otimes I$ and $I \otimes R$, each of which is $n^3 \times n^3$. So we would form n^6 equations. Each equation would involve a product of up to 3 terms coming from each side of the (1.3), yielding an equation of degree ≤ 3. Therefore, this apporach of forming simultaneous equations and solving for the entries of R could mean solving n^6 cubics in n^4 variables. This makes the potential difficulty of solving the YBE apparent.

While many solutions have been found for vector spaces of dimension n (in fact an infinite family of solutions for each dimension was given in [Pou18]), the problem of finding all solutions is far from solved. Beside the trivial dimensions 0 and 1, the only dimension for which all solutions of the YBE have been found is dimension 2. This was achieved with the help of a computer in [Hie93]. Based on this work, all unitary solutions of dimension 2 have been classified in [Dye03] [1]. Solutions to YBE for higher dimensions remain unclassified [Che12].

In the next section, we will outline some basic results regarding R-matrices. We will state and prove other relevant results regarding R-matrices and their characteristic polynomials. In the final section of this chapter we show how to obtain an R-matrix from a mapping of sets (a so-called set-theoretic solution of the YBE).

1.2 R-matrices

In this section we will explore the properties of R-matrices. For this task, we will require the following properties of the Kronecker product. The following properties are straightforward from (1.2).

Lemma 1.2.1. [Bro06, Theorem 5] *Let $A \in \mathbb{C}^{m\times n}$. Then the following hold:*

(i) $(\lambda A) \otimes B = \lambda(A \otimes B) = A \otimes (\lambda B)$ *for* $\lambda \in \mathbb{C}$;

(ii) $(A \otimes B) \otimes C = A \otimes (B \otimes C)$ *for* $B \in \mathbb{C}^{p\times q}$, $C \in \mathbb{C}^{r\times s}$;

(iii) $(A + B) \otimes C = A \otimes C + B \otimes C$ *for* $B \in \mathbb{C}^{m\times n}$, $C \in \mathbb{C}^{r\times s}$;

(iv) $A \otimes (B + C) = A \otimes B + A \otimes C$ *for* $B, C \in \mathbb{C}^{p\times q}$;

(v) $I_m \otimes I_n = I_{mn}$.

[1] In [Dye03], dimension is defined as the dimension of the R-matrix mapping $V \otimes V \to V \otimes V$, where $\dim R = (\dim V)^2$.

Lemma 1.2.2. [Bro06, Theorem 7] *Let $A \in \mathbb{C}^{m\times n}$, $B \in \mathbb{C}^{p\times q}$, $C \in \mathbb{C}^{n\times k}$ and $D \in \mathbb{C}^{q\times r}$. Then we have*

$$(A \otimes B)(C \otimes D) = (AC) \otimes (BD).$$

Lemma 1.2.3. [Bro06, Theorem 15] *Let $A \in \mathbb{C}^{n\times n}$, $B \in \mathbb{C}^{m\times m}$. If the eigenvalues of A are λ_i for $i \in \{1, \ldots, n\}$ and eigenvalues of B are μ_j for $j \in \{1, \ldots, m\}$, then the eigenvalues of $A \otimes B$ are*

$$\{\lambda_i \mu_j \mid i \in \{1, \ldots, n\}, j \in \{1, \ldots, m\}\}.$$

Now that we are acquainted with the Kronecker product of matrices, we give some important properties of R-matrices.

Proposition 1.2.4. [SS18, Proposition 3.3] *If $C, D \in \mathbb{C}^{n\times n}$, then $X = C \otimes D$ satisfies YBE if and only if $C^2 \otimes DCD \otimes D = C \otimes CDC \otimes D^2$.*

Proof. In the following proof we will repeatedly use Lemma 1.2.1 (ii) and Lemma 1.2.2. We have that X satisfies the YBE if and only if

$$\begin{aligned}
&(C \otimes D \otimes I)(I \otimes C \otimes D)(C \otimes D \otimes I) = (I \otimes C \otimes D)(C \otimes D \otimes I)(I \otimes C \otimes D) \\
\iff\ & C^2 \otimes (D \otimes I)(C \otimes D)(D \otimes I) = C \otimes (C \otimes D)(D \otimes I)(C \otimes D) \\
\iff\ & C^2 \otimes DCD \otimes D = C \otimes CDC \otimes D^2.
\end{aligned}$$

□

Proposition 1.2.5. [SS17, Proposition 4] *Let $C \in \mathbb{C}^{s\times s}$ and $X = C \otimes I_{pn}$, where $n = ps$. Then X satisfies YBE if and only if $C^2 \otimes I_p \otimes C = C \otimes I_p \otimes C^2$.*

Proof. In the following proof we will repeatedly use Lemma 1.2.1 (ii), Lemma 1.2.1 (v) and Lemma 1.2.2. We have that X satisfies the YBE if and only if

$$(C\otimes I_{p^2s}\otimes I_{ps})(I_{ps}\otimes C\otimes I_{p^2s})(C\otimes I_{p^2s}\otimes I_{ps}) = (I_{ps}\otimes C\otimes I_{p^2s})(C\otimes I_{p^2s}\otimes I_{ps})(I_{ps}\otimes C\otimes I_{p^2s})$$

which is true if and only if

$$(C \otimes I_{ps})(I_{ps} \otimes C)(C \otimes I_{ps}) \otimes I_{p^2s} = (I_{ps} \otimes C)(C \otimes I_{ps})(I_{ps} \otimes C) \otimes I_{p^2s}.$$

The above equality is equivalent to

$$(C \otimes I_p \otimes I_s)(I_s \otimes I_p \otimes C)(C \otimes I_p \otimes I_s) = (I_p \otimes I_s \otimes C)(C \otimes I_p \otimes I_s)(I_p \otimes I_s \otimes C)$$

which is true if and only if $C^2 \otimes I_p \otimes C = C \otimes I_p \otimes C^2$, proving the result. □

In a similar vein to the above results, we obtained a sufficient condition for R-matrices of a particular form.

Proposition 1.2.6. *Let $Y \in \mathbb{C}^{n\times n}$. Then the matrix $X = (I_n \otimes Y) + (Y \otimes I_n)$ is an R-matrix if Y satisfies*

$$Y^2 \otimes I_n = I_n \otimes Y^2. \tag{1.4}$$

Proof. We let $I_n = I$ to simplify the notation.

Substituting the given expression for X, we arrive at

$$X \otimes I = Y \otimes I \otimes I + I \otimes Y \otimes I,$$

$$I \otimes X = I \otimes Y \otimes I + I \otimes I \otimes Y,$$

using Lemma 1.2.1 (ii), (iii), and (iv) and Lemma 1.2.2. Then we calculate $(X \otimes I)(I \otimes X) = Y \otimes Y \otimes I + I \otimes Y^2 \otimes I + Y \otimes I \otimes Y + I \otimes Y \otimes Y$, which implies that

$$\begin{aligned}(I \otimes X)(X \otimes I)(I \otimes X) = {} & Y \otimes Y^2 \otimes I + I \otimes Y^3 \otimes I + 2Y \otimes Y \otimes Y + I \otimes Y^2 \otimes Y \\ & + I \otimes Y^2 \otimes Y + Y \otimes I \otimes Y^2 + I \otimes Y \otimes Y^2,\end{aligned}$$

and

$$\begin{aligned}(X \otimes I)(I \otimes X)(X \otimes I) = {} & Y^2 \otimes Y \otimes I + Y \otimes Y^2 \otimes I + Y^2 \otimes I \otimes Y + 2Y \otimes Y \otimes Y \\ & + Y \otimes Y^2 \otimes I + I \otimes Y^3 \otimes I + I \otimes Y^2 \otimes Y.\end{aligned}$$

From (1.4) it follows that

$$\begin{aligned}(I \otimes X)(X \otimes I)(I \otimes X) = {} & Y \otimes Y^2 \otimes I + I \otimes Y^3 \otimes I + 2Y \otimes Y \otimes Y + Y^2 \otimes I \otimes Y \\ & + I \otimes Y^2 \otimes Y + Y \otimes I \otimes Y^2 + I \otimes Y \otimes Y^2 \\ = {} & (X \otimes I)(I \otimes X)(X \otimes I).\end{aligned}$$

□

It would be interesting to know whether the converse holds. This motivates the following question.

Question 1.2.7. Are there any matrices $Y \in \mathbb{C}^{n\times n}$ such that $Y^2 \otimes I_n \neq I_n \otimes Y^2$, but the matrix $X = (I_n \otimes Y) + (Y \otimes I_n)$ is an R-matrix?

We can apply the above propositions to obtain matrices which satisfy the YBE. We can use Proposition 1.2.4 to find solutions of the YBE by taking an idempotent matrix D and letting $X = D \otimes D$, or also by choosing $X = C \otimes I_n$ for idempotent $C \in \mathbb{C}^{n\times n}$. Similarly, we can let $X = C \otimes I_{pn}$ for idempotent $C \in \mathbb{C}^{s\times s}$ and use Proposition 1.2.5.

The sufficiency condition in Proposition 1.2.6 requires Y^2 and I_n to commute under Kronecker product. However, given $A, B \in \mathbb{C}^{m\times n}$, we have $A \otimes B = B \otimes A$ if and only if one of the matrices is a scalar multiple of the other [Bro06, Theorem 24]. Therefore, the condition in the proposition requires Y^2 to be a scalar matrix λI for some $\lambda \in \mathbb{C}$. It follows that we can let $Y = \mu I$ where μ is the principal square root of λ.

Lemma 1.2.3 tells us how to find eigenvalues of $A \otimes B$ given the eigenvalues of A and B. It provides a simple way of calculating the eigenvalues of the R-matrices constructed using Propositions 1.2.4, 1.2.5 and 1.2.6.

We will now explore "near idempotent" matrices, that is, matrices $Y \in \mathbb{C}^{n\times n}$ which satisfy $Y^2 = cY$ for some $c > 0$.

Proposition 1.2.8. *A matrix $Y \in \mathbb{C}^{n\times n}$ satisfies $Y^2 = cY$ if and only if it is a scalar multiple of an idempotent matrix.*

Proof. Notice that $Y^2 = cY \iff \frac{1}{c}Y$ is idempotent.

Suppose $c = 1$. Then $\frac{1}{c}Y$ is idempotent if and only if Y is idempotent. If $c \neq 1$ then $\frac{1}{c}Y$ is idempotent if and only if Y is a scalar multiple of an idempotent matrix. □

We will now give a sufficient condition for such near idempotent matrices to satisfy the YBE.

First, note that for a scalar matrix Y we have $Y \otimes I_n = I_n \otimes Y$, therefore it satisfies the YBE.

Now we show that if $K \coloneqq \operatorname{diag}(a, \dots, a, 0, \dots, 0)$ for some scalar a, then K satisfies the YBE. Observe that K is the Jordan normal form of an idempotent matrix when $a = 1$, and it is the Jordan normal form of a scalar multiple of an idempotent matrix when $a \neq 1$.

Let $K = \operatorname{diag}(\underbrace{a, \dots, a}_{k \text{ times}}, \underbrace{0, \dots, 0}_{s \text{ times}})$, be an $n^2 \times n^2$ matrix. Then we have

$$K \otimes I_n = \operatorname{diag}(\underbrace{a, \dots, a}_{nk \text{ times}}, \underbrace{0, \dots, 0}_{ns \text{ times}})$$

and

$$I_n \otimes K = \operatorname{diag}(\underbrace{K, \dots, K}_{n \text{ times}}).$$

Further, we have that the diaginal entries of $(K \otimes I_n)(I_n \otimes K)$ are

$$[(K \otimes I_n)(I_n \otimes K)]_{ii} = \begin{cases} 0 & \text{if} \quad (K \otimes I_n)_{ii} = 0 \quad \text{or} \quad (I_n \otimes K)_{ii} = 0 \\ a^2 & \text{if} \quad (K \otimes I_n)_{ii} = (I_n \otimes K)_{ii} = a. \end{cases}$$

So we have

$$\begin{aligned} [(I_n \otimes K)(K \otimes I_n)(I_n \otimes K)]_{ii} &= \begin{cases} 0 & \text{if} \quad [(K \otimes I_n)(I_n \otimes K)]_{ii} = 0 \\ & \quad \text{or} \quad (I_n \otimes K)_{ii} = 0 \\ a^3 & \text{if} \quad [(K \otimes I_n)(I_n \otimes K)]_{ii} = (I_n \otimes K)_{ii} = a \end{cases} \\ &= [(K \otimes I_n)(I_n \otimes K)(K \otimes I_n)]_{ii}. \end{aligned}$$

Therefore K satisfies the YBE.

We remark that it is not true that matrices similar to K satisfy the YBE, which can be seen in the following example.

Example 1.2.9. Let

$$B = \begin{bmatrix} -62 & -96 & -192 & -224 \\ 64 & 98 & 192 & 224 \\ -16 & -24 & -46 & -56 \\ 4 & 6 & 12 & 16 \end{bmatrix},$$

which is similar to $\mathrm{diag}(2, 2, 2, 0)$. It is easily checked that B doesn't satisfy YBE.

Proposition 1.2.10. *If $A \in \mathbb{C}^{n^2 \times n^2}$ is a non-singular diagonal R-matrix, then it is equal to cI for $c \in \mathbb{C}$.*

Proof. Let $A = \mathrm{diag}(a_1, \ldots, a_{n^2})$, where $a_i \in \mathbb{C}$. Then it follows that

$$A \otimes I = \mathrm{diag}(\underbrace{a_1, \ldots, a_1}_{n \text{ times}}, \underbrace{a_2, \ldots, a_2}_{n \text{ times}}, \ldots, \underbrace{a_{n^2}, \ldots, a_{n^2}}_{n \text{ times}})$$

and

$$I \otimes A = \mathrm{diag}\Big(\underbrace{a_1, \ldots, a_{n^2}, a_1, \ldots, a_{n^2}, \ldots, a_1, \ldots, a_{n^2}}_{n \text{ times}}\Big).$$

Therefore,

$$(A \otimes I)(I \otimes A)(A \otimes I) =$$
$$\mathrm{diag}(a_1^3, \ldots, a_1^2 a_n, a_2^2 a_{n+1}, \ldots, a_2^2 a_{2n}, \ldots, a_n^2 a_{n^2-n}, \ldots, a_n^2 a_{n^2}, \ldots, a_{n^2}^2 a_1, \ldots, a_{n^2}^3),$$

and

$$(I \otimes A)(A \otimes I)(I \otimes A) =$$
$$\mathrm{diag}(a_1^3, \ldots, a_1 a_n^2, a_2 a_{n+1}^2, \ldots, a_2 a_{2n}^2, \ldots, a_n a_{n^2-n}^2, \ldots, a_n a_{n^2}^2, \ldots, a_{n^2} a_{n^2-n}^2, \ldots, a_{n^2}^3).$$

Therefore we have $a_1^2 a_2 = a_1 a_2^2, \ldots, a_1^2 a_n = a_1 a_n^2$, implying that $a_1, \ldots, a_n$ are all equal. Further, we have $a_{n+1} a_2^2 = a_{n+1}^2 a_2, \ldots, a_{2n} a_2^2 = a_{2n}^2 a_2$, and analogous equations up to $a_{n^2}^2 a_{n^2-n} = a_{n^2} a_{n^2-n}^2$. These imply that $a_1, \ldots, a_{n^2}$ are all equal. □

We conclude this section with a result on the characteristic polynomial of a matrix $A \in \mathbb{C}^{n \times n}$ having precisely 1 non-zero entry in each row and column. In Section 2.2 we will see that matrices associated with non-degenerate set-theoretic solutions are of this form. We let the entry in the i-th row be equal to a_i for $i \in \{1, \ldots, n\}$. Then it is easy to see that $A = DP$, where $D = \mathrm{diag}(a_1, \ldots, a_n)$ and P is a permutation matrix. Recall that there is a bijective correspondence between $n \times n$ permutation matrices and the group Sym_n of permutations of $\{1, \ldots, n\}$, where each element of Sym_n is represented by a permutation of columns of I_n. For the

following result, we will characterise the permutation matrices P using elements of Sym_n written as disjoint cycles.

Proposition 1.2.11. *Let $A \in \mathbb{C}^{n\times n}$ have precisely 1 non-zero entry in each row and column, and let the entry in the i-th row equal to a_i for $i \in 1, \ldots, n$. Suppose $A = DP$ where $D = diag(a_1, \ldots, a_n)$ and P is a permutation matrix. Then the characteristic polynomial $\chi(x)$ of A is given by*

$$\chi(x) = \pm(x^{k_1} - a_{l_1} \ldots a_{l_{k_1}}) \ldots (x^{k_m} - a_{l_1} \ldots a_{l_{k_m}}),$$

where k_i are the cycle lengths of disjoint cycles of P and $l_i, \ldots, l_{k_i}$ are the numbers in the cycle decomposition of the corresponding cycle of length k_i.

Proof. We calculate the characteristic polynomial of an $n \times n$ matrix $M = [m_{i,j}]$ using the following formula;

$$\chi_M(x) = \det(M - xI) = \sum_{\sigma\in \mathrm{Sym}_n} \Big(\mathrm{sgn}(\sigma) \prod_{i=1}^{n} (m_{i,\sigma(i)} - \delta_{i,\sigma(i)}x\Big) \tag{1.5}$$

for $\delta_{i,j}$ the Kronecker delta.

We first calculate the characteristic polynomial of a matrix $B \in \mathbb{C}^{r\times r}$ which has precisely 1 non-zero entry in each row and column, with the entry in the i-th row equal to b_i for $i \in \{1, \ldots, r\}$, and which is such that $B = D_B P_B$ where $D_B = \mathrm{diag}(b_1, \ldots, b_r)$ and P_B is a permutation matrix corresponding to a single r-cycle. Note that no number in $\{1, \ldots, r\}$ is fixed by P_B, that is, the matrix P_B has zeros on the diagonal.

Notice that the only permutations that will contribute to the sum in (1.5) are the identity permutation and the permutation corresponding to P_B. It follows that

$$\chi_B(x) = (-1)^r(x^r - b_1 \ldots b_r).$$

Now we consider $\chi_A(x)$. We claim that the first disjoint cycle of P, of length k_1, contributes a factor $x^{k_1} - a_{l_1} \ldots a_{l_{k_1}}$ to $\chi_A(x)$, and likewise for k_i for $i \in \{1, \ldots, m\}$. This can bee seen by noting that the only permutations that contribute to the sum (1.5), are those that contain any number of the same disjoint cycles as P does, and that act as the identity on the elements not contained in those cycles.

Now, the proposition follows. □

Chapter 2

Set-Theoretic Solutions of the Yang Baxter Equation

In this chapter, we will see how to obtain a solution of the Yang-Baxter equation from a set X and a map $r\colon X^2 \to X^2$ which satisfies certain properties. This approach to the study of the Yang-Baxter equation was first suggested in [Dri92, Section 9].

2.1 Set-Theoretic Solutions of the Yang-Baxter Equation

Let X be a non-empty set and let $r\colon X^2 \to X^2$ be such that

$$(r \times \mathrm{Id}_X)(\mathrm{Id}_X \times r)(r \times \mathrm{Id}_X) = (\mathrm{Id}_X \times r)(r \times \mathrm{Id}_X)(\mathrm{Id}_X \times r). \tag{2.1}$$

Then we call (X, r) a **set-theoretic solution to the Yang-Baxter equation**. This is is because, as we will describe in the next section, we may obtain solutions of the Yang-Baxter equation from the pair (X, r).

Remark 2.1.1. It will be notationally useful for us to denote r as $r(x, y) = (\sigma_x(y), \tau_y(x))$. In this case, by expanding (2.1) and comparing first entries, we can show that for $x, y \in X$,

$$\sigma_x\sigma_y = \sigma_{\sigma_x(y)}\sigma_{\tau_y(x)}.$$

Notation 2.1.2. For ease of notation, we will write $r \times \mathrm{Id}_X$ as $r_{12}\colon X^3 \to X^3$, and $\mathrm{Id}_X \times r$ as $r_{23}\colon X^3 \to X^3$.

Example 2.1.3. Let X be any set, and $r\colon X^2 \to X^2$ be defined by $r(x, y) = (y, x)$ Then for $x, y, z \in X$ we have

$$r_{12}r_{23}r_{12}(x, y, z) = r_{12}r_{23}(y, x, z) = r_{12}(y, z, x) = (z, y, x)$$

and

$$r_{23}r_{12}r_{23}(x, y, z) = r_{23}r_{12}(x, z, y) = r_{23}(z, y, y) = (z, y, x),$$

so (X, r) is a set-theoretic solution of the YBE. Since this (X, r) is a solution for any set, we call it the **trivial solution**.

Example 2.1.4. Let $X = \{1, \dots n\}$, and $r\colon X^2 \to X^2$ be defined by $r(x, y) = (y + 1, x - 1)$ where addition is performed modulo n. Then for $x, y, z \in X$, we have

$$r_{12}r_{23}r_{12}(x, y, z) = r_{12}r_{23}(y+1, x-1, z) = r_{12}(y+1, z+1, x-2) = (z+2, y, x-2)$$

while

$$r_{23}r_{12}r_{23}(x, y, z) = r_{23}r_{12}(x, z+1, y-1) = r_{23}(z+2, x-1, y-1) = (z+2, y, x-2).$$

Therefore (X, r) is a set-theoretic solution of the Yang-Baxter Equation. Here, $\sigma_x(y) = y + 1$ and $\tau_y(x) = x - 1$.

2.2 Obtaining R-matrices from Set-Theoretic Solutions

The Yang-Baxter equation (1.3) is an equation concerning linear operators on a vector space, while our so-called set-theoretic solutions are defined in terms of a set X. To obtain a solution of the YBE from X, we will need to be able to form a vector space from X. The construction of a free vector space makes this possible.

Given a set X, we can construct an abstract vector space $\mathcal{F}(X)$ by treating X simply as a collection of symbols, with no linear dependencies between them, and letting $\mathcal{F}(X)$ denote the space of all finite $\mathbb{C}$-linear combinations of these symbols which satisfy the axioms of a vector space. By construction, $\mathcal{F}(X)$ is a vector space whose dimension is the cardinality of X, and we call it the free vector space (over $\mathbb{C}$) with basis X. The tensor product of free vector spaces $\mathcal{F}(X) \otimes \mathcal{F}(Y)$ for sets X, Y is isomorphic to the free vector space $\mathcal{F}(X \times Y)$. By convention, we will denote the basis of $\mathcal{F}(X) \otimes \mathcal{F}(Y)$ by $\{x \otimes y\}_{x \in X, y \in Y}$, where $x \otimes y$ is simply a symbol for the basis element of $\mathcal{F}(X) \otimes \mathcal{F}(Y)$ isomorphic to $(x, y) \in X \times Y$.

Now, given sets X, Y and a map $r : X \to Y$, we immediately obtain a linear map $\widetilde{r}\colon \mathcal{F}(X) \to \mathcal{F}(Y)$, by taking

$$\widetilde{r}\left(\sum_{x \in X} \lambda_x x\right) = \sum_{x \in X} \lambda_x r(x).$$

We will use this idea to obtain a linear operator on $\mathcal{F}(X) \otimes \mathcal{F}(X)$ which satisfies the YBE, given a set-theoretic solution of the YBE.

Specifically, we let (X, r) be a set-theoretic solution and we let V denote the free vector space over $\mathbb{C}$ with basis X. Then we define $\widetilde{r}\colon V \otimes V \to V \otimes V$ be the linear map acting on the basis X by $\widetilde{r}(x \otimes y) = \sigma_x(y) \otimes \tau_y(x)$. Then it is clear that the map $\widetilde{r}$ is a solution of the YBE.

If $X = \{x_1, \ldots, x_n\}$ is a finite set, then the matrix associated to $\widetilde{r}$ is an R-matrix. We call it the **R-matrix associated to the solution** (X, r). Note that this matrix has rows and columns indexed by pairs (i, j) for $1 \leq i, j \leq n$. By convention, these pairs are considered to be ordered lexicographically. Then, considering the definition of $\widetilde{r}$, it is easy to see that this matrix is a permutation matrix. In particular, its nonzero entries have the value 1.

Example 2.2.1. Consider the set-theoretic solution (X, r) from Example 2.1.3, and let $X = \{x_1, x_2, x_3\}$. Then we can write the R-matrix associated to this solution as

$$R = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

To construct an R-matrix from a set-theoretic solution, with nonzero entries that may differ from 1, we could try changing the values of the nonzero entries (without, of course, setting them to zero). Sometimes this will produce a new R-matrix, and sometimes it will not. We describe a valid change of nonzero values in the following definition.

Definition 2.2.2. Let (X, r) be a set-theoretic solution of the Yang-Baxter equation. Then consider the vector space V, defined to be the free vector space over $\mathbb{C}$ with basis X. Then let $D = \{d_{(x,y)}\}_{x,y \in X}$ where $0 \neq d_{(x,y)} \in \mathbb{C}$. We call (X, r^D) a **braided vector space of set-theoretic type** if the linear map $\widetilde{r^D} \colon V \otimes V \to V \otimes V$ defined for $x, y \in X$ by

$$\widetilde{r^D}(x \otimes y) = d_{(x,y)}(\sigma_x(y) \otimes \tau_y(x))$$

satisfies the Yang-Baxter equation.

Given a braided vector space of set-theoretic type (X, r^D), with the set $X = \{x_1, \ldots, x_n\}$ finite, we may form an R-matrix as follows. Let M be the matrix with rows and columns indexed by pairs (i, j) in lexicographical order, for $1 \leq i, j \leq n$. Then the intersection of column (i, j) and row (k, l) is defined to be

$$m_{i,j}^{k,l} = \begin{cases} d_{(x_i, x_j)} & \text{if } r(x_i, x_j) = (x_k, x_l) \\ 0 & \text{otherwise.} \end{cases}$$

Then clearly M is an R-matrix, since M is the matrix of a linear map $r^D \colon V \otimes V \to V \otimes V$ satisfying the YBE. In the case where $D = \{d_{(x,y)}\}_{x,y \in X}$ with $d_{(x,y)} = 1$ for all $x, y \in X$, we recover the R-matrix associated to the set-theoretic solution (X, r).

In the next section, we will give sufficient conditions on the solution (X, r) under which we may obtain a braided vector space of set-theoretic type. We will see that it is sufficient that (X, r) has the property of being non-degenerate. Finally, we will show that when (X, r) has the additional property of being involutive, we may obtain R-matrices as above which are in some sense non-trivial.

2.3 Non-Degenerate Set-Theoretic Solutions

We now know how to construct an R-matrix given a braided vector space of set-theoretic type. However, it remains to consider when we can obtain a braided vector space of set-theoretic type from a set-theoretic solution (X, r). In this section, we show that if (X, r) has the property of being non-degenerate, then we can construct a braided vector space (X, r^D).

Definition 2.3.1. If (X, r) is a set-theoretic solution of the Yang-Baxter equation, we say the solution is **left non-degenerate** if $\sigma_x \in \mathrm{Sym}_X$ for all $x \in X$, where Sym_X denotes the symmetric group on the elements of X (i.e. the group of permutations of the elements of X). Similarly, the solution (X, r) is called **right non-degenerate** if $\tau_x \in \mathrm{Sym}_X$ for all $x \in X$. A solution which is both left and right non-degenerate is simply called **non-degenerate**.

With the notion of a non-degenerate solution of the YBE, we now recall the following lemma, a special case of [AG03, Lemma 5.7].

Lemma 2.3.2. [SS18, Lemma 2.2] *Let (X, r) be a non-degenerate set-theoretic solution of the YBE. Let $f\colon X^2 \to \mathbb{C}$ be a mapping, and assume that f takes only nonzero values. Then the following statements are equivalent:*

- *For all $x, y, z \in X$,*

  $$f(x,y)\cdot f(\tau_y(x),z)\cdot f(\sigma_x(y),\sigma_{\tau_y(x)}(z)) = f(y,z)\cdot f(x,\sigma_y(z))\cdot f(\tau_{\sigma_y(z)}(x),\tau_z(y)).$$

- *The linear mapping $c\colon V \otimes V \to V \otimes V$ given by*

  $$c(x \otimes y) = f(x,y)\cdot \sigma_x(y) \otimes \tau_y(x)$$

  satisfies the YBE for $x, y \in X$.

Given the above result, the following lemma is clear.

Lemma 2.3.3. *Let (X, r) be a non-degenerate set-theoretic solution of the YBE. Then let $f : X^2 \to \mathbb{C}$ be any map which never has the value zero, such that for all $x, y, z \in X$,*

(i) $f(x,y) = f(\tau_{\sigma_y(z)}(x), \tau_z(y))$;

(ii) $f(\tau_y(x), z) = f(x, \sigma_y(z))$;

(iii) $f(\sigma_x(y), \sigma_{\tau_y(x)}(z)) = f(y, z)$.

Then letting $D = \{d_{(x,y)}\}_{x,y\in X}$ *with* $d_{(x,y)} = f(x, y)$*, it follows that* (X, r^D) *is a braided vector space of set-theoretic type.*

Proof. This follows immediately from Definition 2.2.2 and Lemma 2.3.2. □

Example 2.3.4. Consider the solution (X, r) from Example 2.1.3. Then for any $x \in X$, the map $\sigma_x \colon X \to X$ is the identity on X, which is a bijection. So (X, r) is left non-degenerate. Similarly, $\tau_x = \mathrm{Id}_X$ for all $x \in X$, so that (X, r) is right non-degenerate. Then it is easy to see that any map $f \colon X^2 \to \mathbb{C}$ which is never zero satisfies the conditions of Lemma 2.3.3. Let $X = \{x_1, x_2, x_3\}$, and let $f(x, y) = i$ if $x = y$ and 3 otherwise. Then putting $D = \{d_{(x,y)}\}_{x,y\in X}$ such that $d_{(x,y)} = f(x, y)$ we have that (X, r^D) is a braided vector space of set-theoretic type. The associated matrix

$$\hat{R} = \begin{bmatrix} i & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 3 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 3 & 0 & 0 \\ 0 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & i & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 3 & 0 \\ 0 & 0 & 3 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 3 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & i \end{bmatrix}.$$

is an R-matrix.

In this section, we have seen that from any non-degenerate set-theoretic solution (X, r) of the YBE, it is possible to obtain a braided vector space of set-theoretic type by simply choosing a map $f : X^2 \to \mathbb{C}$ appropriately. Previously, we saw how to construct an R-matrix given any such braided vector space. In the next section, we will see that the additional property of involutivity ensures that this R-matrix is sufficiently different to the R-matrix associated to the solution (X, r).

2.4 Involutive Set-Theoretic Solutions

In this section, we give a sufficient condition for a braided vector space (X, r^D) to be non-trivial, where trivial is defined as follows.

Definition 2.4.1. [SS18, Definition 2.5] Let (X, r^D) be a braided vector space of set-theoretic type. Then we say (X, r^D) is **trivial** if there exists nonzero $\alpha_x \in \mathbb{C}$ for all $x \in X$ and a constant $c \in \mathbb{C}$ with

$$d_{(x,y)} = c \cdot \alpha_x \cdot \alpha_y \cdot (\alpha_{\sigma_x(y)})^{-1} \cdot (\alpha_{\tau_y(x)})^{-1}.$$

Remark 2.4.2. Observe that this is equivalent to there existing an invertible n by n diagonal matrix P such that $\bar{M} = (P^{-1} \otimes P^{-1})M(P \otimes P)$, where $\bar{M}$ is the R-matrix associated to (X, r^D) and M is the R-matrix associated to (X, r). In other words, (X, r^D) is trivial if and only if its R-matrix is similar to that of (X, r) by $(P \otimes P)$, for P a diagonal $n \times n$ matrix.

It turns out that, when (X, r) has the property of being involutive, there is an easy condition ensuring (X, r^D) is non-trivial.

Definition 2.4.3. Let (X, r) be a set-theoretic solution of the Yang-Baxter equation. Then we say the solution is **involutive** if $r^2 = \mathrm{Id}_{X^2}$.

Remark 2.4.4. We observe that if (X, r) is an involutive, left non-degenerate solution of the YBE with $r(x, y) = (\sigma_x(y), \tau_y(x))$, then

$$\sigma_{\sigma_x(y)}(\tau_y(x)) = x,$$

which implies $\tau_y(x) = \sigma^{-1}_{\sigma_x(y)}(x)$. So if (X, r) is a set-theoretic solution of the YBE which is both involutive and left non-degenerate, then the map r can be defined just in terms of the left component σ_x. In this paper, we will often characterise the map r of such a set-theoretic solution (X, r) by its left component σ_x.

With the notion of an involutive set-theoretic solution of the YBE, we now have the following lemma which essentially re-formulates Lemma 2.6 from [SS18].

Lemma 2.4.5. *Let (X, r) be an involutive set-theoretic solution of the Yang-Baxter equation, and suppose (X, r^D) is a braided vector space of set-theoretic type. If $d_{(x,y)}d_{r(x,y)} = d_{(x,y)}d_{(\sigma_x(y),\tau_y(x))}$ is not constant, then (X, r^D) is non-trivial.*

Proof. Suppose that (X, r^D) is trivial. Then from Definition 2.4.1, we have that

$$d_{(x,y)} = c \cdot \alpha_x \cdot \alpha_y \cdot (\alpha_{\sigma_x(y)})^{-1} \cdot (\alpha_{\tau_y(x)})^{-1}$$

and

$$d_{(\sigma_x(y),\tau_y(x))} = c \cdot \alpha_{\sigma_x(y)} \cdot \alpha_{\tau_y(x)} \cdot (\alpha_{\sigma_{\sigma_x(y)}(\tau_y(x))})^{-1} \cdot (\alpha_{\tau_{\tau_y(x)}(\sigma_x(y))})^{-1}$$

for some α_k nonzero complex numbers, and $c \in \mathbb{C}$ a nonzero fixed constant. Then since r is involutive, we have that

$$\sigma_{\sigma_x(y)}(\tau_y(x)) = x, \quad \tau_{\tau_y(x)}(\sigma_x(y)) = y$$

and so $d_{(\sigma_x(y),\tau_y(x))} = c \cdot (\alpha_{\sigma_x(y)}) \cdot (\alpha_{\tau_y(x)}) \cdot \alpha_x^{-1} \cdot \alpha_y^{-1}$, from which it is clear that

$$d_{(x,y)} \cdot d_{(\sigma_x(y),\tau_y(x))} = c^2.$$

Thus $d_{(x,y)} \cdot d_{(\sigma_x(y),\tau_y(x))} = d_{(x,y)}d_{r(x,y)}$ is constant. By the contrapositive, if $d_{(x,y)}d_{r(x,y)}$ is non-constant, then (X, r^D) is non-trivial. □

Example 2.4.6. It is clear that the solution (X, r) as in Example 2.1.3 is involutive. Taking $X = \{x_1, x_2, x_3\}$, we can consider the braided vector space (X, r^D)

given in Example 2.3.4. Note that if $x = y$, then $d_{(x,y)}d_{r(x,y)} = -1$, while if $x \neq y$, then $d_{(x,y)}d_{r(x,y)} = 9$. Then by Lemma 2.4.5, the braided vector space (X, r^D) is nontrivial. In other words the matrix $\hat{R}$ from Example 2.3.4 is not similar, in the sense of Remark 2.4.2, to the matrix R associated to (X, r) given in Example 2.2.1

Example 2.4.7. Consider the solution (X, r) from Example 2.1.4, with $n = 3$. This is clearly involutive. For any $x \in X$, the map $\sigma_x \colon X \to X$ is the map sending $y \mapsto y + 1 \mod 3$, which is a bijection. So (X, r) is left non-degenerate. Similarly, we can check that (X, r) is right non-degenerate. Now consider $f \colon X^2 \to \mathbb{C}$ given by $f(x, y) = (x - y) \mod 3 + 1$. It is easy to check that f satisfies the conditions of Lemma 2.3.3, so putting $D = \{d_{(x,y)}\}_{x,y \in X}$ such that $d_{(x,y)} = f(x, y)$ we have that (X, r^D) is a braided vector space of set-theoretic type. Then the associated matrix

$$R = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 3 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 3 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 \\ 0 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

is an R-matrix. Further, we have that $d_{(0,1)} \cdot d_{r(0,1)} = 3 \cdot 1 = 3$ but $d_{(0,2)} \cdot d_{r(0,2)} = 4$, so $d_{(x,y)}d_{r(x,y)}$ is not constant. Then by Lemma 2.4.5, (X, r^D) is nontrivial, so the matrix R is not similar, in the sense of Remark 2.4.2, to the matrix associated to (X, r).

Combining our results so far: we know that if we have a set-theoretic solution (X, r) of the Yang-Baxter equation which is non-degenerate and involutive, then under mild conditions we can form braided vector spaces (X, r^D) which are not trivial, and hence we can produce R-matrices which are not trivially similar to the R-matrix associated to (X, r). Further, it was shown in [SS18, Proposition 8.1] that any such R-matrix is a unitary matrix, and hence has useful properties for applications such as quantum information processing.

For these reasons, our exploration the exploration of set-theoretic solutions (X, r) will be restricted to the exploration of non-degenerate, involutive set-theoretic solutions of the YBE. For the remainder of this paper, we will consider such set-theoretic solutions. Unless stated otherwise, we will use the convention that a solution of the YBE, or simply a *solution*, refers to a non-degenerate, involutive set-theoretic solution of the Yang-Baxter equation.

Chapter 3

Jacobson Radical Rings

In this chapter we turn our attention to Jacobson radical rings, which will, remarkably, turn out to give rise to solutions of the YBE. We study the properties of Jacobson radical rings, and show how we can construct solutions of the YBE from Jacobson radical rings.

3.1 Jacobson Radical Rings

Before we study Jacobson radical rings, we first state the formal definition of a ring.

Definition 3.1.1. A **ring** is a set R equipped with two binary operations $+$ and $*$ satisfying the following set of axioms:

(A1) $a + b = b + a$ for every $a, b \in R$.
(A2) $(a + b) + c = a + (b + c)$ for every $a, b, c \in R$.
(A3) There exists $0 \in R$ such that $0 + a = a$ for every $a \in R$.
(A4) For every $a \in R$ there exists $-a \in R$ such that $a + (-a) = 0$.
(M2) $a * (b * c) = (a * b) * c$ for every $a, b, c \in R$.
(D1) $a * (b + c) = a * b + a * c$ for every $a, b, c \in R$.
(D2) $(a + b) * c = a * c + b * c$ for every $a, b, c \in R$.

Remark 3.1.2. In particular, throughout this paper, a ring R does not necessarily have a multiplicative identity.

Definition 3.1.3. A **Jacobson radical ring** is a ring $(R, +, *)$ that satisfies the following property:

(JR1) For every $a \in R$ there exists some $b \in R$ such that $a * b + a + b = 0$.

We now look at a few concrete examples of Jacobson radical rings.

Example 3.1.4. Consider the ring of all 3×3 strictly upper-triangular matrices with integer entries, equipped with the usual matrix addition and multiplication. Denote this set by $T_3(\mathbb{Z})$. Each element in $T_3(\mathbb{Z})$ has the form

$$A = \begin{bmatrix} 0 & a & b \\ 0 & 0 & c \\ 0 & 0 & 0 \end{bmatrix}$$

where $a, b, c \in \mathbb{Z}$. Notice that for each A as above, there exists a matrix B, given by

$$B = \begin{bmatrix} 0 & -a & ac-b \\ 0 & 0 & -c \\ 0 & 0 & 0 \end{bmatrix} \in T_3(\mathbb{Z}),$$

which satisfies $A * B + A + B = 0$. In fact, one can show that B is the unique matrix with this property. Furthermore, one can also compute and verify that $B * A + B + A = 0$.

Example 3.1.5. Using mathematical induction and block multiplication, we can check that $T_n(\mathbb{Z})$ is also a Jacobson radical ring. This generalises Example 3.1.4.

Example 3.1.6. Let $(G, +)$ be an abelian group with identity 0. We equip G with a binary operation such that $g_1 * g_2 = 0$ for every $g_1, g_2 \in G$. We can check that

$$g * (-g) + g + (-g) = 0$$

for all $g \in G$. Hence, $(G, +, *)$ is a Jacobson radical ring. We refer to a ring of this type as a **trivial ring**.

3.2 Jacobson Radical Rings and the Circle Operation $\circ$

Let R be a Jacobson radical ring. Unlike in the case of Example 3.1.4, it is not immediately obvious from Definition 3.1.3 whether for each $a \in R$, there exists a unique $b \in R$ such that $a * b + a + b = 0 = b * a + b + a$. The answer to this is positive, which we will show in this section.

For any Jacobson radical ring R, we define the operation $\circ \colon R \times R \to R$ by

$$a \circ b = a * b + a + b. \tag{3.1}$$

We will show that $(R, \circ)$ is a group with 0 being the identity. Due to the group structure, we have that for any $a \in R$, there exists a unique $b \in R$ such that

$$a * b + a + b = a \circ b = 0 = b \circ a = b * a + b + a.$$

Proposition 3.2.1. *Let R be a Jacobson radical ring. Then $(R, \circ)$ is a group.*

Proof. We need to show that $(R, \circ)$ satisfies the group axioms, i.e., (i) associativity, (ii) existence of identity and (iii) existence of inverse.

(i) For all $a, b, c \in R$, we have

$$\begin{aligned}(a \circ b) \circ c &= (a * b + a + b) * c + (a * b + a + b) + c \\ &= a * b * c + a * c + b * c + a * b + a + b + c \\ &= a * (b * c + b + c) + a + (b * c + b + c) \\ &= a \circ (b \circ c).\end{aligned}$$

Thus, the operation $\circ$ is associative.

(ii) It is clear that 0 is the identity since for all $a \in R$, $a \circ 0 = 0 \circ a = a$.

(iii) It is clear that right inverse exists by the definition of Jacobson radical ring, i.e. for all $a \in R$, there exists some $b \in R$ such that

$$a \circ b = a * b + a + b = 0.$$

Similarly, there exists some $c \in R$ such that $b \circ c = 0$. But the associativity of operation $\circ$ implies

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

Therefore, for each $a \in R$, there exists $b \in R$ such that $a \circ b = b \circ a = 0$.

We conclude that $(R, \circ)$ is a group. □

3.3 Set-Theoretic Solutions of the Yang-Baxter Equation Associated to Jacobson Radical Rings

With the machinery built so far, we are ready to study how each Jacobson radical ring naturally yields a solution of the YBE.

Proposition 3.3.1. *Let R be a Jacobson radical ring. Define $r : R^2 \to R^2$ to be the map*

$$r(x, y) = (x \circ y - x, z \circ x - z),$$

where $z \circ (x \circ y - x) = 0$. Then, (R, r) is a solution of the YBE.

The proof is conceptually straightforward but consists of tedious manipulations. Moreover, the above result can be seen as a special case of Lemma 4.3.7 which will be proved in the next Chapter. We will merely provide a proof sketch here.

Proof Sketch. Non-degeneracy is clear since $(R, +)$ and $(R, \circ)$ are groups. It is not hard to show that $r^2(x, y) = (x, y)$. It is straightforward albeit tedious to show that (R, r) is non-degenerate and is indeed a solution. □

Example 3.3.2. Let $(T_3(\mathbb{Z}), +, *)$ be the matrix ring as in Example 3.1.4. Let the map $r(x, y) = (x \circ y - x, z \circ x - z) = (x * y + y, z * x + x)$ where $z * (x * y + y) = 0$. It is straightforward to verify that (R, r) is a non-degenerate involutive set-theoretic solution.

We now show the connection between trivial ring and trivial solution through the following proposition.

Proposition 3.3.3. *Let R be a Jacobson radical ring and let (R, r) be the solution of the YBE associated to R. Suppose that $r(x, y) = (y, x)$, for all $x, y \in R$. Then R is a trivial ring.*

Proof. If $r(x, y) = (y, x)$ for all $x, y \in R$, then $x * y = x \circ y - x - y = y - y = 0$. □

Chapter 4

Left Braces

It is remarkable that Jacobson radical rings give rise to solutions of the Yang-Baxter equation. In fact, since all $T_n(\mathbb{Z})$ (for any $n \geq 2$) are Jacobson radical rings, we immediately have an infinite family of solutions.

However, this is far from giving us *all* solutions. A much more significant result is, in layman's terms: if (X, r) is a solution, then X is always "part of" an algebraic structure which is "almost like" a Jacobson radical ring. In this chapter, we will formalise the notion of "almost like". In Chapter 6, we will formalise the notion of "part of".

4.1 Left Braces

A new algebraic structure known as a left brace was first introduced by Rump in [Rum07, Definition 2] to help study the solutions of the YBE. In the Proposition 4 of the same paper, Rump gave an equivalent definition as follows:

Definition 4.1.1. A **left brace** is a set A equipped with two binary operations $+$ and $*$ satisfying the following set of axioms:

(B1) $(A, +)$ is an abelian group.

(B2) $(A, \circ)$ is a group.

(D1) $a * (b + c) = a * b + a * c$ for all $a, b, c \in A$.

Remark 4.1.2. It follows immediately from Definition 3.1.1 and Theorem 3.2.1 that any Jacobson radical ring $(R, +, *)$ satisfies the brace axioms. As we will see later, there are left braces which are not Jacobson radical rings. Hence, one can view left braces as a generalisation of Jacobson radical rings. We will study how left braces generalise Jacobson radical rings in detail in Chapter 7.

It is clear that once we have the binary operations $+$ and $*$ defined on a left brace A, the binary operation $\circ$ will be totally determined. Conversely, one can choose

to define the binary operations $+$ and $\circ$ first, and then induce the operation $*$ as

$$a * b = a \circ b - a - b. \tag{4.1}$$

However, we need to ensure that operation $*$ satisfies (D1). Notice that this condition can be reformulated with respect to operations $+$ and $\circ$ since

$$\begin{aligned} & a * (b + c) = a * b + a * c \\ \iff & a * (b + c) + a + b + c = a * b + a * c + a + b + c \\ \iff & a \circ (b + c) = a \circ b + a \circ c - a. \end{aligned}$$

Reformulating (D1) of Definition 4.1.1, we have a definition of a left brace which is defined with respect to the operations $+$ and $\circ$. The following is the definition of left braces used in the recent literature, first defined in [CJO14, Definition 1].

Definition 4.1.3. A **left brace** is a set A equipped with two binary operations $+$ and $\circ$ satisfying the following set of axioms:

(B1) $(A, +)$ is an abelian group.

(B2) $(A, \circ)$ is a group.

(D1) $a \circ (b + c) = a \circ b + a \circ c - a$ for every $a, b, c \in A$.

In the introduction of [Rum07], it is remarked that the name *brace* is a reference to "the property that A combines two different equations or groups to a new entity." This is easily seen by the formulation of Definition 4.1.3, where it is clear that a left brace structure $(A, +, \circ)$ draws together two group structures, related via axiom (D1).

We will now look at some examples of left braces. From Remark 4.1.2, we know that any Jacobson radical ring $(A, +, *)$ gives rise to a left brace $(A, +, \circ)$. Therefore, we immediately have Examples 3.1.5 and 3.1.6 as left braces.

Example 4.1.4. Let $(A, +)$ be an abelian group with identity 0. Equip A with a binary operation $\circ$ such that $a_1 \circ a_2 = a_1 + a_2$ for every $a_1, a_2 \in A$. It is clear that $(A, \circ)$ is a left brace. Notice that $(A, +, *)$ is a trivial ring as defined in Example 3.1.6, since

$$a_1 * a_2 = a_1 \circ a_2 - a_1 - a_2 = 0$$

for all $a_1, a_2 \in A$. We refer to a left brace of this type as a **trivial brace**.

We will now look at an example of left brace which is *not* a Jacobson radical ring.

Example 4.1.5. Let $(A, +)$ be the direct product of groups $(\mathbb{Z}_3, +)$ and $(\mathbb{Z}_2, +)$. Note that $(A, +)$ is a group with the underlying set

$$\{(0,0), (1,0), (2,0), (0,1), (1,1), (2,1)\}.$$

Equip A with a binary operation $\circ$ as defined in Table 4.1. One can verify that

(i) $(A, \circ)$ is a group;

(ii) $a \circ (b + c) = a \circ b + a \circ c - a$ for all $a, b, c \in A$.

Therefore, we have that $(A, +, \circ)$ is a left brace. It is easy to compute $(A, *)$, which is given in Table 4.2. Notice that $((0,1) + (1,1)) * (1,0) = (1,0) * (1,0) = (0,0)$, but $(0,1) * (1,0) + (1,1) * (1,0) = (1,0) + (1,0) = (2,0)$. Therefore, $(A, *)$ does not satisfy (D2). Hence, $(A, +, *)$ is not a Jacobson radical ring.

$\circ$	(0,0)	(1,0)	(2,0)	(0,1)	(1,1)	(2,1)
(0,0)	(0,0)	(1,0)	(2,0)	(0,1)	(1,1)	(2,1)
(1,0)	(1,0)	(2,0)	(0,0)	(1,1)	(2,1)	(0,1)
(2,0)	(2,0)	(0,0)	(1,0)	(2,1)	(0,1)	(1,1)
(0,1)	(2,1)	(2,1)	(1,1)	(0,0)	(2,0)	(1,0)
(1,1)	(1,1)	(0,1)	(2,1)	(1,0)	(0,0)	(2,0)
(2,1)	(2,1)	(1,1)	(0,1)	(2,0)	(1,0)	(0,0)

Table 4.1: Cayley table of $(A, \circ)$ in Example 4.1.5, where the intersection of row a and column b is $a \circ b$.

$*$	(0,0)	(1,0)	(2,0)	(0,1)	(1,1)	(2,1)
(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)
(1,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)
(2,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)
(0,1)	(0,0)	(1,0)	(2,0)	(0,0)	(1,0)	(2,0)
(1,1)	(0,0)	(1,0)	(2,0)	(0,0)	(1,0)	(2,0)
(2,1)	(0,0)	(1,0)	(2,0)	(0,0)	(1,0)	(2,0)

Table 4.2: Table of $(A, *)$ in Example 4.1.5, where the intersection of row a and column b is $a * b$.

Remark 4.1.6. Alert readers may have noticed that the multiplicative group $(A, \circ)$ in Example 4.1.5 is isomorphic to D_3, the dihedral group of 6 elements.

In the next example, we generalise Example 4.1.5 from $(A, \circ) \cong D_3$ to $(A, \circ) \cong D_p$, where p is an odd prime.

Example 4.1.7. Let $(A, +) = \mathbb{Z}_{2p}$ for some odd prime p. Equip A with a binary operation $\circ$ such that $a \circ b \coloneqq a + (-1)^a(b)$ for all $a, b \in A$. It is straightforward to show that $(A, +, \circ)$ is a left brace. On the other hand,

$$(1 + 1) * 1 = 2 * 1 = 2 \circ 1 - 2 - 1 = 2 + (-1)^2(1) - 2 - 1 = 0,$$

but

$$1 * 1 + 1 * 1 = 2(1 \circ 1 - 1 - 1) = 2\big(1 + (-1)^1(1) - 1 - 1\big) = -4 \neq 0.$$

Therefore, $(A, +, *)$ is not a Jacobson radical ring. It is also clear that $1 \circ 2 \neq 2 \circ 1$. Hence $(A, \circ)$ is not abelian. It follows from [Gri07, Proposition 6.1][1] that $(A, \circ) \cong D_p$.

4.2 Arithmetic on Left Braces

In this section, we will look at some arithmetical identities of the additive and multiplicative groups of left braces, which will be used in the rest of the paper. All these identities can be found in [Lau18, Section 2]. For the sake of completeness, we will give a sketch proof for each identity.

We first fix the notation for the group $(A, +)$ of any left brace A.

Notation 4.2.1. For any left brace $(A, +, \circ)$, we call $(A, +)$ the additive group of A and denote the additive identity by 0. For each $a \in A$, we denote its additive inverse by $-a$. Let a be any element of a left brace A and $n \geq 0$ be an integer. We write na to denote $\underbrace{a + a + \cdots + a}_{n \text{ times}}$. Similarly, if $m < 0$ is a negative integer, we write ma to represent $\underbrace{-a - a - \cdots - a}_{-m \text{ times}}$.

Proposition 4.2.2. *Let $(A, +, \circ)$ be a left brace. Then for all $a, b, c \in A$, we have the following identities.*

(i) $a \circ 0 = 0 \circ a = a$;

(ii) $a \circ (-b) = 2a - a \circ b$;

(iii) $a \circ (b - c) = a \circ b - a \circ c + a$.

Proof Sketch.

(i) It follows from (D1) that $a \circ 0 = a \circ (0 + 0) = a \circ 0 + a \circ 0 - a$. Rearranging shows that 0 is the right identity, hence the identity of $(A, \circ)$.

(ii) It follows from (D1) that $a = a \circ 0 = a \circ \big(b + (-b)\big) = a \circ b + a \circ (-b) - a$. Rearranging gives us the claim.

(iii) It follows from (D1) that $a \circ (b - c) = a \circ \big(b + (-c)\big) = a \circ b + a \circ (-c) - a$. Applying result (ii) gives us the claim. □

In particular, observe that 0 is the identity of $(A, \circ)$, which is not too surprising given Theorem 3.2.1. We now fix the notation for the group $(A, \circ)$.

Notation 4.2.3. For any left brace $(A, +, \circ)$, we call $(A, \circ)$ the multiplicative group of A. By convention, we will write the multiplicative identity as $1 \in A$. However, it should be noted that $0 = 1$, which follows from Proposition 4.2.2(i). Furthermore, we write a^{-1} as the multiplicative inverse of a.

[1] [Gri07] denotes dihedral group of size $2p$ by D_{2p}, while we denote it by D_p in this paper

The following two lemmas can be seen as a generalisation of (D1). They allow us to do arithmetic on left braces conveniently.

Lemma 4.2.4. *Let $(A, +, \circ)$ be a left brace. Let $n \geq 1$ be an integer. For any $a, b_1, b_2, \ldots b_n \in A$, we have*

$$a \circ (b_1 + b_2 + \cdots + b_n) = a \circ b_1 + a \circ b_2 + \cdots + a \circ b_n - (n-1)a.$$

Proof Sketch. This is straightforward by mathematical induction on n, where the inductive step follows from (D1). □

Lemma 4.2.5. *Let $(A, +, \circ)$ be a left brace. Let $m, n \geq 1$ be integers. For any $a, b_1, \ldots, b_m, c_1, \cdots, c_n \in A$, we have*

$$\begin{aligned} &a \circ (b_1 + \cdots + b_m - c_1 - \cdots - c_n) \\ &= a \circ b_1 + \cdots + a \circ b_m - a \circ c_1 - \cdots - a \circ c_n + (n - m + 1)a. \end{aligned}$$

Proof Sketch. We first rewrite the term as

$$a \circ \big((b_1 + \cdots + b_m) - (c_1 + \cdots + c_n)\big).$$

The claim now follows from Proposition 4.2.2(iii) and Lemma 4.2.4. □

The following identity comes from Rump's original definition of left braces in [Rum07, Definition 2]. We show that this can be derived from Definition 4.1.3.

Lemma 4.2.6. *Let $(A, +, \circ)$ be a left brace. Then for all $a, b, c \in A$, we have*

$$(a * b + a + b) * c = a * (b * c) + a * c + b * c.$$

Proof Sketch. We have

$$\begin{aligned} (a * b + a + b) * c &= (a \circ b) \circ c - a \circ b - c \\ &= a \circ (b \circ c) - a * b - a - b - c \\ &= a * (b * c + b + c) + (b * c + b + c) - a * b - b - c \\ &= a * (b * c) + a * c + b * c. \end{aligned}$$

□

4.3 Set-Theoretic Solutions of the Yang-Baxter Equation Associated to Left Braces

The central motivation for Rump's introduction of left braces is that left braces give rise to solutions of the YBE. In this section, we make explicit the construction of a solution of the YBE given a left brace, following the exposition of [CJO14].

We first introduce the following notation to ease our constructions later in this section.

Notation 4.3.1. For any set X, we denote by Sym_X the symmetric group on the elements of X (that is, the group of permutations of the elements of X).

Notation 4.3.2. Let $(A, +, \circ)$ be a left brace. Then for any $a \in A$, we define $\lambda_a \colon A \to A$ by

$$\lambda_a(b) = a \circ b - a$$

for all $b \in A$.

It is easy to verify that for all $a \in A$, the inverse of λ_a is the map $\lambda_a^{-1} \colon A \to A$ defined by

$$\lambda_a^{-1}(b) = a^{-1} \circ (b + a)$$

for all $b \in A$. Therefore, $\lambda_a \colon A \to A$ is bijective and $\lambda_a \in \mathrm{Sym}_A$ for all $a \in A$. Moreover, the maps λ_a have the following elementary properties.

Lemma 4.3.3. [CJO14, Lemma 1] *Let $(A, +, \circ)$ be a left brace. Then*

(i) *$\lambda_a(x + y) = \lambda_a(x) + \lambda_a(y)$, that is, λ_a is an automorphism of the abelian group $(A, +)$;*

(ii) *$\lambda_a \lambda_b = \lambda_{a \circ b}$, that is, the map $\lambda \colon A \to \mathrm{Sym}_A$, defined by $\lambda(a) = \lambda_a$ is a homomorphism of groups.*

Proof.

(i) Let $a, x, y \in A$. We have

$$\begin{aligned} \lambda_a(x + y) &= a \circ (x + y) - a \\ &= a \circ x + a \circ y - a - a \\ &= \lambda_a(x) + \lambda_a(y), \end{aligned}$$

where the second equality follows from (D1).

(ii) Let $a, b, x \in A$. We have

$$\begin{aligned} (\lambda_a \lambda_b)(x) &= a \circ (b \circ x - b) - a \\ &= a \circ (b \circ x) - a \circ b + a - a \\ &= (a \circ b) \circ x - a \circ b \\ &= \lambda_{a \circ b}(x), \end{aligned}$$

where the second equality follows from Proposition 4.2.2(iii). □

The homomorphism $\lambda \colon A \to \mathrm{Sym}_A$, defined by $\lambda(a) = \lambda_a$ is not necessarily injective. This motivates the following definition.

Definition 4.3.4. Let A be a left brace. The socle of A is

$$\mathrm{Soc}(A) = \mathrm{Ker}(\lambda) = \{a \in A \mid \lambda_a = \lambda_0 = \mathrm{Id}_A\}.$$

Remark 4.3.5. For any left brace A, we have $a \in \mathrm{Soc}(A)$ if and only if $a \circ b = a + b$ for all $b \in A$. To see this, notice that $\lambda_a = \mathrm{Id}_A$ if and only if $\lambda_a(b) = b$ for all $b \in A$. This is true if and only if $a \circ b - a = b$. Rearranging yields $a \circ b = a + b$.

We are now ready to examine how a left brace gives rise to a solution of the YBE, beginning with the following proposition characterising the left non-degenerate involutive solutions.

Proposition 4.3.6. [CJO14, Proposition 2] *Let X be a non-empty set and $r\colon X^2 \to X^2$ be a map such that $r(x,y) = \big(\sigma_x(y), \tau_y(x)\big)$. Then (X, r) is a solution of the YBE if and only if*

(i) $r^2 = \mathrm{Id}_{X^2}$;

(ii) $\sigma_x, \tau_x \in \mathrm{Sym}_X$ *for all* $x \in X$;

(iii) $\sigma_x\left(\sigma_{\sigma_x^{-1}(y)}\right) = \sigma_y\left(\sigma_{\sigma_y^{-1}(x)}\right)$ *for all* $x, y \in X$.

Proof. Omitted, see [CJO06, Theorem 4.1]. □

Lemma 4.3.7. [CJO14, Lemma 2] *Let A be a left brace. Then*

(i) $a \circ \lambda_a^{-1}(b) = b \circ \lambda_b^{-1}(a)$ *for all* $a, b \in A$,

(ii) $\lambda_a\left(\lambda_{\lambda_a^{-1}(b)}\right) = \lambda_b\left(\lambda_{\lambda_b^{-1}(a)}\right)$ *for all* $a, b \in A$,

(iii) *the map $r\colon A^2 \to A^2$ defined by $r(x,y) = \big(\lambda_x(y), \lambda^{-1}_{\lambda_x(y)}(x)\big)$ is a solution of the Yang-Baxter equation.*

Proof.

(i) For all $a, b \in A$, we have that

$$a \circ \lambda_a^{-1}(b) = a \circ a^{-1} \circ (b + a) = b + a = b \circ b^{-1} \circ (a + b) = b \circ \lambda_b^{-1}(a).$$

(ii) For all $a, b \in A$, we have that

$$\lambda_a\left(\lambda_{\lambda_a^{-1}(b)}\right) = \lambda_{a \circ \lambda_a^{-1}(b)} = \lambda_{b \circ \lambda_b^{-1}(a)} = \lambda_b\left(\lambda_{\lambda_b^{-1}(a)}\right),$$

where the first and third equalities come from Lemma 4.3.3, and the second equality comes from part (i).

(iii) We first check that the map r is indeed involutive. We have

$$\begin{aligned} r^2(x,y) &= r\left(\lambda_x(y), \lambda^{-1}_{\lambda_x(y)}(x)\right) \\ &= \left(\lambda_{\lambda_x(y)}\left(\lambda^{-1}_{\lambda_x(y)}(x)\right), \lambda^{-1}_{\lambda_{\lambda_x(y)}\left(\lambda^{-1}_{\lambda_x(y)}(x)\right)}\left(\lambda_x(y)\right)\right) \\ &= \left(x, \lambda_x^{-1}\left(\lambda_x(y)\right)\right) \\ &= (x, y). \end{aligned}$$

Hence $r^2 = \mathrm{Id}_{X^2}$.

Now, the left component of $r(x, y)$ is $\lambda_x(y)$, and we know that $\lambda_x \in \mathrm{Sym}_A$. Further, $\lambda^{-1}_{\lambda_x(y)}(x)$ is clearly bijective since it is the inverse of a bijection, so $\lambda^{-1}_{\lambda_x(y)}(x) \in \mathrm{Sym}_A$. Then, by part (ii), we know that all conditions (i), (ii) and (iii) of Proposition 4.3.6 are met. Hence, we know that (A, r) is a solution of the YBE. □

Notation 4.3.8. Let A be a left brace. We call the set-theoretic solution (A, r) of the YBE defined in Lemma 4.3.7 the solution of the YBE associated to the left brace A. For clarity, we may denote the map r as in the statement of Lemma 4.3.7 by r_A.

Chapter 5

Constructions of Left Braces

We have seen in the previous chapter that left braces are useful in the study of solutions of the YBE. In particular, every left brace A gives rise to a solution of the YBE. We will now provide some useful constructions to allow us to obtain new braces from old. We will introduce standard algebraic constructions such as substructures, quotients, and products in a brace-theoretic context.

5.1 Subbraces, Ideals and Quotients

In many mathematical structures there is an obvious notion of sub-structure: in sets we have subsets, in groups we have subgroups, and in rings we have subrings. There may also be a notion of quotient structures arising from a suitable equivalence relation. In topological spaces, any equivalence relation gives rise to a quotient topological space. In a ring R, the relation $x \sim y \iff x - y \in I$ for some ideal I of R and elements $x, y \in R$ gives rise to a factor ring R/I. In left braces both of these constructions exist.

There is an immediate notion of subbrace, given here as defined in [Rum07, page 160].

Definition 5.1.1. Let $(A, +, \circ)$ be a left brace. A subset $B \subseteq A$ is a **subbrace** of A if $(B, +)$ is a subgroup of $(A, +)$ and $(B, \circ)$ is a subgroup of $(A, \circ)$.

The definition of a quotient or factor brace is analogous to the definition from ring theory. As such, we first require the definition of a brace ideal.

Definition 5.1.2. [CJO14, p. 103] Let $(A, +, \circ)$ be a left brace. Then a subset $I \subseteq A$ is an **ideal** of A if $(I, \circ)$ is a normal subgroup of $(A, \circ)$ and $\lambda_a(I) \subseteq I$ for all $a \in A$.

Remark 5.1.3. It is clear that any ideal I of a brace A is also a subbrace of A. This is because for $a, b \in I$ we have that $a - b = b \circ b^{-1} \circ a - b = \lambda_b(b^{-1} \circ a) \in I$, so $(I, +)$ is a subgroup of $(A, +)$

At first glance, Definition 5.1.2 looks quite different to the ring-theoretic definition of an ideal. In fact, the above definition can be characterised similarly to the ring-theoretic notion of an ideal as an additive subgroup which absorbs multiplication. Such a characterisation of brace ideals appeared in [MBBER18, Lemma 4].

Proposition 5.1.4. *Let $(A, +, \circ)$ be a left brace. Then a subset $I \subseteq A$ is an ideal of A if and only if I is a subbrace of A such that*

$$i * a \in I \text{ for all } i \in I, a \in A$$

and

$$a * i \in I \text{ for all } i \in I, a \in A.$$

Proof. Let I be an ideal of A. By Remark 5.1.3, we know I is a subbrace of A. It is clear that

$$a * i = \lambda_a(i) - i \in I.$$

Meanwhile, we have

$$\begin{aligned} i * a &= i \circ a - i - a \\ &= \big(a \circ a^{-1} \circ (i \circ a) - a\big) - i \\ &= \lambda_a(a^{-1} \circ i \circ a) - i \in I. \end{aligned}$$

We will now show the converse. Let I be a subbrace of A such that for all $i \in I, a \in A$, we have $i * a \in I$ and $a * i \in I$. It is clear that

$$\lambda_a(i) = a * i - i \in I,$$

so $\lambda_a(I) \subseteq I$ for all $a \in A$. It remains to show that $(I, \circ)$ is a normal subgroup of $(A, \circ)$. Notice that we have

$$\begin{aligned} a \circ i \circ a^{-1} &= a \circ (i * a^{-1} + i + a^{-1}) \\ &= a \circ (i * a^{-1}) + a \circ i + a \circ a^{-1} - a - a \\ &= a \circ i' + a * i + i - a \\ &= a * i' + i' + a * i + i \in I, \end{aligned}$$

where $i' = i * a^{-1}$ is an element in I. □

The proposition above allows us to understand a brace ideal as in ring theory: a subbrace that absorbs the $*$ operation from the left and the right.

With the notion of ideal, we are now prepared to define the notion of factor braces. Given an ideal I of a left brace B, we may define the relation $\sim$ on B by

$$a \sim b \iff a - b \in I$$

for $a, b \in B$. It is easy to check that $\sim$ is an equivalence relation. We refer to the equivalence classes of $\sim$ as the cosets of I in B; and for $b \in B$, we denote the coset

of I containing b by $b + I$. Then we may define the factor brace B/I as follows.

Definition 5.1.5. Let B be a left brace and I an ideal of B. Then B/I is the set of cosets of I in B with the operations $+$ and $\circ$ defined by

$$(a + I) + (b + I) = (a + b) + I$$

and

$$(a + I) \circ (b + I) = (a \circ b) + I.$$

We call B/I the **quotient** of B by I.

It is straightforward to check that the quotient B/I is itself a left brace under the operations $+$ and $\circ$ given in Definition 5.1.5. We will refer to such a construction as a quotient brace, or factor brace.

Example 5.1.6. Let A be the brace as in Example 4.1.5, and consider $I = \{(a, 0) \mid a \in \{0, 1, 2\}\}$. It is clear that $(I, +)$ is a subgroup of $(A, +)$, and from Table 4.1, we can see that $(I, \circ) \leq (A, \circ)$. So I is a subbrace of A. Then, inspection of Table 4.2 shows that I absorbs left- and right-multiplication by elements of A, so I is an ideal of A by Proposition 5.1.4. Then I and A/I are left braces. Since I has 3 elements, and the only group of order 3 up to isomorphism is $\mathbb{Z}_3$, it follows that I is isomorphic to G_3, the trivial brace with 3 elements. Similarly, A/I has only 2 elements, and since $\mathbb{Z}_2$ is the only group of order 2 up to isomorphism, A/I is isomorphic to G_2, the trivial brace with 2 elements.

Example 5.1.7. It was shown in [Rum07, Proposition 7] that if A is a brace, then $\operatorname{Soc}(A)$ is an ideal of A. Therefore, $A/\operatorname{Soc}(A)$ is a brace. This will be important to our constructions later in this paper.

5.1.1 Brace Morphisms

In ring theory, we obtain ideals of rings as the kernels of ring homomorphisms. The same idea works in the context of braces. Brace morphisms are defined naturally as follows.

Definition 5.1.8. [CJO14, Definition 2] Let B_1 and B_2 be two left braces. A map $f : B_1 \to B_2$ is a **homomorphism of left braces** if

$$f(a + b) = f(a) + f(b)$$

and

$$f(a \circ b) = f(a) \circ f(b)$$

for all $a, b \in B_1$. The kernel of f is $\operatorname{Ker}(f) = \{a \in B_1 | f(a) = 1\}$.

A bijective homomorphism of left braces is called an **isomorphism of left braces**, and a brace isomorphism $f \colon B \to B$ is called a **brace automorphism** of the left brace B.

It is easy to check that the kernel of a brace homomorphism $f\colon B_1 \to B_2$ is an ideal of B_1, so the kernels of homomorphisms give us one way of forming factor braces. As with groups and rings, there is a First Isomorphism Theorem for braces.

Theorem 5.1.9. [Ced18, Theorem 2.17](First Isomorphism Theorem) *Given any homomorphism of left braces $f\colon B_1 \to B_2$, there exists a unique isomorphism*

$$\tilde{f}\colon B_1/\operatorname{Ker}(f) \to \operatorname{Im}(f)$$

such that the diagram in Figure 5.1 commutes, that is $f = \iota \circ \tilde{f} \circ \pi$, where $\pi\colon B_1 \to B_1/\operatorname{Ker}(f)$ is the natural homomorphism and ι is the inclusion map.

$$\begin{array}{ccc} B_1 & \xrightarrow{\quad f \quad} & B_2 \\ \downarrow{\scriptstyle \pi} & & \uparrow{\scriptstyle \iota} \\ B_1/\operatorname{Ker}(f) & \xrightarrow{\quad \tilde{f} \quad} & \operatorname{Im}(f) \end{array}$$

Figure 5.1: First Isomorphism Theorem

The proof of this theorem mirrors the corresponding proofs for the group and ring-theoretic results.

5.2 Semidirect and Wreath Products of Braces

As well as looking at subbraces within a brace, or arriving at new braces via the ideals and quotients of a brace, we may ask how to combine two left braces to produce a new brace. One obvious construction would be to take a direct product: given braces G and H, this is the set of tuples (g, h) in $G \times H$ with operations $+$ and $\circ$ defined element-wise. In this section, we will introduce the semidirect product of left braces, a construction from group theory which generalises the direct product. We will also consider the wreath product, a specific kind of semidirect product.

The semidirect product originated in group theory, and is a generalisation of the direct product. The group-theoretic construction is as follows.

Definition 5.2.1. Let $(G, \cdot), (H, \cdot)$ be groups, and $\sigma\colon H \to \operatorname{Aut}(G)$ be a group homomorphism, with $\operatorname{Aut}(G)$ the group of automorphisms of G. Then the **semidirect product** $G \rtimes H$ of G and H **via** σ is the set $G \times H$ equipped with the group operation

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1 \cdot \sigma(h_1)(g_2), h_1 \cdot h_2)$$

for all $(g_1, h_1), (g_2, h_2) \in G \times H$.

If the group H acts on G in a natural way (for instance, if $H = \mathrm{Aut}(G)$), then the homomorpism σ may not be explicitly defined. The semidirect product of braces was introduced by Rump in [Rum08].

Definition 5.2.2. Let $(G, +, \circ), (H, +, \circ)$ be left braces and $\sigma : H \to \mathrm{Aut}(G)$ be a group homomorphism from $(H, \circ)$ to the group of brace automorphisms of G. Then the **semidirect product** $G \rtimes H$ of G and H **via** σ is the set $G \times H$ equipped with the following addition

$$(g_1, h_1) + (g_2, h_2) = (g_1 + g_2, h_1 + h_2)$$

and the following circle operation

$$(g_1, h_1) \circ (g_2, h_2) = (g_1 \circ \sigma(h_1)(g_2), h_1 \circ h_2)$$

for all $(g_1, h_1), (g_2, h_2) \in G \times H$.

It is clear that when $\sigma : H \to \mathrm{Aut}(G)$ is defined by $\sigma(h) = \mathrm{Id}_G$ for all $h \in H$, then $G \rtimes H$ via σ is the direct product of G and H. The semidirect product may be used to define a related notion of wreath product. The wreath product of braces was investigated in Corollaries 3.5 and 3.6 of [CJDR10], and in Corollary 1 of [CJO14].

Definition 5.2.3. Let G, H be left braces and consider the set

$$W = \{f \colon H \to G \text{ such that } |\{h \in H : f(h) \neq 1\}| < \infty\}$$

which is a left brace when we define addition and circle operations as

$$(f_1 + f_2)(h) = f_1(h) + f_2(h),$$
$$(f_1 \circ f_2)(h) = f_1(h) \circ f_2(h)$$

for $f_1, f_2 \in W, h \in H$. Then the **wreath product** $G \wr H$ of G and H is the brace $W \rtimes H$ via $\sigma \colon H \to \mathrm{Aut}(W)$ defined by $\sigma(h)(f)(x) = f(hx)$ for all $x, h \in H, f \in W$.

It should be remarked that, while the semidirect and wreath product constructions arose in group theory, a matrix wreath product of algebras was recently introduced in [AAJZ17] in order to study Jacobson radical, nil and primitive algebras.

It is easy to check that if G, H are left braces then so is $G \rtimes H$. It was shown in ([CJO14], Corollary 1) that $G \wr H$ is also a left brace.

Example 5.2.4. Let G_3 denote the trivial brace with additive group isomorphic to $\mathbb{Z}_3$, and G_2 denote the trivial brace with additive group isomorphic to $\mathbb{Z}_2$. Then consider a group homomorphism $\sigma \colon (G_2, \circ) \to \mathrm{Aut}(G_3)$. If $\mathrm{Ker}(\sigma) = G_2$, then $G_3 \rtimes G_2$ via σ is a direct product, and its is clear that this has trivial brace structure.

Then consider σ with $\mathrm{Ker}(\sigma) \subsetneq G_2$. Since σ is a group homomorphism, then $\sigma(0) = \mathrm{Id}_{G_3}$, and also $\sigma^2(1) = \mathrm{Id}_{G_3}$. The only possibility for $\sigma(1)$ to be a non-identity automorphism of G_3 is that $\sigma(1)$ fixes $0 \in G_3$, and swaps 1 and 2. Then denote $G_6 = G_3 \rtimes G_2$ via σ. It is straightforward to check that Table 4.1 is the multiplication table for $(G_6, \circ)$, and it follows that G_6 is simply the brace A defined in Example 4.1.5.

Chapter 6

Left Braces Associated to Solutions

In Section 4.3, we showed that given a left brace, we can construct a solution of the YBE. In this chapter, we will show that we can reverse this process: given a set-theoretic solution (X, r), we can construct a left brace A such that $X \subseteq A$. Furthermore, we will show that (X, r) is embedded in the set theoretic solution (A, r_A), in the sense that restricting the domain of r_A to X^2 gives us exactly the map $r\colon X^2 \to X^2$. Finally, we will show that, when X is finite, we can obtain a finite brace B as a factor brace of A, such that (X, r) embeds in (B, r_B).

6.1 Constructing Left Braces from Set-Theoretic Solutions

Given a solution (X, r) of the YBE, we will show in this section how to construct a left brace A. In the next section, we will show how to embed (X, r) in the solution (A, r_A), and how to replace A with a finite quotient brace when X is finite.

Our first brace construction will be based on the structure group of a solution (X, r) of the YBE. This concept was first introduced in [ESS99, Section 2].

Definition 6.1.1. Let (X, r) be a solution of the YBE. Then the **structure group** of (X, r) is the group denoted by $G(X, r)$, with presentation

$$G(X, r) = \langle X \mid xy = \sigma_x(y)\tau_y(x), \forall x, y \in X \rangle, \tag{6.1}$$

where $r(x, y) = (\sigma_x(y), \tau_y(x))$.

Example 6.1.2. If (X, r) is as in Example 2.1.3, then $G(X, r)$ is the free abelian group generated by the elements of X.

It is clear that $X \subseteq G(X, r)$, and we now seek to give $G(X, r)$ the structure of a

left brace. The overall strategy to produce such a brace structure is as follows. We let $\mathbb{Z}^X$ be the additive free abelian group with basis X, i.e. the group with presentation

$$\mathbb{Z}^X = \langle X \mid x + y = y + x, \forall x, y \in X \rangle,$$

and a typical element $t \in \mathbb{Z}^X$ denoted as $t = \sum_{y \in X} n_y y$ for $n_y \in \mathbb{Z}$. We let

$$M = \mathbb{Z}^X \rtimes \mathrm{Sym}_X$$

where $\sigma \in \mathrm{Sym}_X$ acts naturally on $\mathbb{Z}^X$ via $\sigma\left(\sum_{y \in X} n_y y\right) = \sum_{y \in X} n_y \sigma(y)$. We will show that $G(X, r)$ is isomorphic to a subgroup B of M, before defining an addition operation on B such that B is a left brace. We may then use this additive structure on B to induce an addition operation on $G(X, r)$, which makes $G(X, r)$ a left brace.

We will construct an isomorphism from $G(X, r)$ to $B \leq M$ by constructing an injective homomorphism $G(X, r) \to M$, and taking B as the image of this homomorphism.

Proposition 6.1.3. [ESS99, Proposition 2.3] *The map $\phi\colon X \to M$ given by $\phi(x) = (x, \sigma_x)$, for any $x \in X$, can be extended to a group homomorphism $\widetilde{\phi}\colon G(X, r) \to M$.*

Proof. Defining $\widetilde{\phi}(x) = (x, \sigma_x)$ for $x \in X$ and $\widetilde{\phi}(1) = (0, \mathrm{Id}_X)$, then we may define the map $\widetilde{\phi}\colon G(X, r) \to M$ to be the map that satisfies

$$\widetilde{\phi}(xy) = \widetilde{\phi}(x)\widetilde{\phi}(y)$$

for all $x, y \in X$. This clearly defines $\widetilde{\phi}$ on all of $G(X, r)$. Moreover, from (6.1), we see that $\widetilde{\phi}$ is a group homomorphism provided that

$$\widetilde{\phi}(x)\widetilde{\phi}(y) = \widetilde{\phi}\big(\sigma_x(y)\big)\widetilde{\phi}\big(\tau_y(x)\big).$$

Note that

$$\widetilde{\phi}(x)\widetilde{\phi}(y) = (x, \sigma_x)(y, \sigma_y) = \big(x + \sigma_x(y), \sigma_x\sigma_y\big),$$

while on the other hand,

$$\begin{aligned}\widetilde{\phi}\big(\sigma_x(y)\big)\widetilde{\phi}\big(\tau_y(x)\big) &= \big(\sigma_x(y), \sigma_{\sigma_x(y)}\big)\big(\tau_y(x), \sigma_{\tau_y(x)}\big) \\ &= \big(\sigma_x(y) + \sigma_{\sigma_x(y)}\tau_y(x), \sigma_{\sigma_x(y)}\sigma_{\tau_y(x)}\big).\end{aligned}$$

Now, by Remark 2.4.4, $\sigma_{\sigma_x(y)}\tau_y(x) = x$. By Remark 2.1.1, $\sigma_{\sigma_x(y)}\sigma_{\tau_y(x)} = \sigma_x\sigma_y$. Then it follows that

$$\widetilde{\phi}\big(\sigma_x(y)\big)\widetilde{\phi}\big(\tau_y(x)\big) = \big(x + \sigma_x(y), \sigma_x\sigma_y\big) = \widetilde{\phi}(x)\widetilde{\phi}(y),$$

so $\widetilde{\phi}\colon G(X, r) \to M$ is a group homomorphism. □

Now, summarising the proofs of Proposition 2.4 and 2.5 in [ESS99], we will show

that $\widetilde{\phi}$ is injective.

We define $\pi\colon G(X,r) \to \mathbb{Z}^X$ by $\pi(g) = t$ if $\widetilde{\phi}(g) = (t,s) \in M$. Thus if $\widetilde{\phi}(g) = (0, \mathrm{Id}_X)$, then $\pi(g) = 0$. Clearly $\widetilde{\phi}(1) = (0, \mathrm{Id}_X)$, so $\pi(1) = 0$. Suppose π is a bijection. Then $\widetilde{\phi}(g) = (0, \mathrm{Id}_X)$ implies $\pi(g) = 0 = \pi(1)$, so $g = 1$. Therefore $\mathrm{Ker}(\widetilde{\phi}) = \{1\}$, so $\widetilde{\phi}$ is injective.

We will now prove that π is a bijection, by explicitly constructing the inverse h of π inductively.

Let $X^+ = X \subseteq \mathbb{Z}^X$, and $X^- = \{-x \in \mathbb{Z}^X \mid x \in X\}$, and $Y = X^+ \cup X^-$. For $k \in \mathbb{Z}^{\geq 0}$ we let $\mathbb{Z}^X_k \subseteq \mathbb{Z}^X$ be the set of all elements in $\mathbb{Z}^X$ that are a sum of at most k elements of Y. Then $\mathbb{Z}^X \subseteq \cup_{k=0}^{\infty} \mathbb{Z}^X_k$. Similarly, let $G(X,r)^k$ be the set of all elements of $G(X,r)$ which can be written as a product of at most k elements from $X \cup X^{-1} \subseteq G(X,r)$.

For $x \in X$ and $t = \sum_{y \in X} n_y y \in \mathbb{Z}^X$, we may define the action $x \star t = \sum_{y \in X} n_y \sigma_x(y)$. This action can be extended in the obvious way to a group action of $G(X,r)$ on $\mathbb{Z}^X$ (and the group action is well-defined by Remark 2.1.1).

We will now define h inductively on each $\mathbb{Z}^X_k$ in a compatible way. We start by setting $h(0) = 1$, $h(x) = x$ and $h(-x) = \big(\tau_x^{-1}(x)\big)^{-1}$. For the next step we will need the following lemma.

Lemma 6.1.4. [ESS99, Lemma 2.6] *If $\xi, \eta \in Y$, then $h(\xi)h\big(h(\xi)^{-1} \star \eta\big) = h(\eta)h\big(h(\eta)^{-1} \star \xi\big)$.*

Proof Sketch. We must consider three cases: (i) η and ξ both in X^+; (ii) one of η and ξ is in X^+ while the other is in X^-; (iii) η and ξ both in X^-. Each case follows from the fact that (X,r) is involutive and non-degenerate, and the full details are given in [ESS99]. □

Now we start the inductive step. We assume that h is defined for $\mathbb{Z}^X_k$, and we consider $\eta \in \mathbb{Z}^X_{k+1}$ and $\xi \in Y$. Then we can write $\eta = a + \xi$, where $a \in \mathbb{Z}^X_k$. We define $h(\eta) = h(h(a) \star \xi)h(a)$.

Lemma 6.1.5. [ESS99, Lemma 2.7] *The map h is well defined on each $\mathbb{Z}^X_k$ and therefore on the whole of $\mathbb{Z}^X$.*

Proof. This is proven by induction on k.

Clearly, h is well-defined for $k = 0, 1$. Suppose h is well-defined on $\mathbb{Z}^X_{k-1}$. Then for $a \in \mathbb{Z}^X_{k-2}$, and $\xi, \eta \in Y$, we have

$$\begin{aligned} h((a+\xi)+\eta) &= h(a+\xi)h(h(a+\xi)^{-1} \star \eta) \\ &= h(a)h(h(a)^{-1} \star \xi)h((h(a)h(h(a)^{-1} \star \xi))^{-1} \star \eta) \\ &= h(a)h(h(a)^{-1} \star \xi)h((h(h(a)^{-1} \star \xi)^{-1} \star h(a)^{-1} \star \eta). \end{aligned}$$

We must show the last expression is symmetric in ξ, η and is equal to $h(a)$ when $\xi = -\eta$. Setting $\xi' = h(a)^{-1} \star \eta$ and $\eta' = h(a)^{-1} \star \eta$, the above becomes

$$h\big((a+\xi)+\eta\big) = h(a)h(\xi')h\big(h(\xi')^{-1} \star \eta'\big)$$

which is symmetric in η', ξ' by Lemma 6.1.4, and hence in η, ξ. Then suppose that $\xi = -\eta$, then $\xi' = z \in X^+$ and $\eta' = -z \in X^-$. Then we have

$$\begin{aligned} h(a)h(z)h\big(h(z)^{-1} \star (-z)\big) &= h(a)zh\big(z^{-1} \star (-z)\big) \\ &= h(a)zh\big(-\sigma_z(z)\big) \\ &= h(a)z\big(\tau^{-1}_{\sigma_z(z)}\sigma_z(z)\big)^{-1}. \end{aligned}$$

Observe that $r\big(z, \sigma_z^{-1}(z)\big) = \big(z, \tau_{\sigma_z^{-1}(z)}(z)\big)$ and then by involutivity,

$$\big(z, \sigma_z^{-1}(z)\big) = r\Big(z, \tau_{\sigma_z^{-1}(z)}(z)\Big) = \Big(\sigma_z\tau_{\sigma_z^{-1}(z)}(z), \tau_{\tau_{\sigma_z^{-1}(z)}(z)}(z)\Big).$$

In particular, $z = \sigma_z\tau_{\sigma_z^{-1}(z)}(z)$ and it follows that $\tau^{-1}_{\sigma_z^{-1}}\sigma_z^{-1}(z) = z$. Then we have that $h\big(h(z) \star (-z)\big)h(z)h(a) = h(a)$ and the lemma is proved. □

We are now almost ready to show that h is the inverse of π. First, notice the following. If $g_1, g_2 \in G(X, r)$ and $\widetilde{\phi}(g_1) = (t_1, s_1), \widetilde{\phi}(g_2) = (t_2, s_2)$ then we have

$$\widetilde{\phi}(g_1g_2) = \widetilde{\phi}(g_1)\widetilde{\phi}(g_2) = (t_1, s_1)(t_2, s_2) = (t_1 + s_1t_1, s_1, s_2)$$

and so

$$\pi(g_1g_2) = t_1 + s_1t_1 = \pi(g_1) + s_1\pi(g_2) = \pi(g_1) + g_1 \star \pi(g_2), \tag{6.2}$$

where the final equality follows from the definition of the group action. Using this result, together with our previous lemmas, the following is straightforward.

Lemma 6.1.6. *The maps h and π are inverses to each other.*

Proof. We will check that $\pi\big(h(a)\big) = a$ for $a \in \mathbb{Z}_k^X$ and that $h\big(\pi(b)\big) = b$ for $b \in G(X, r)^k$.

For $k = 0, 1$ this is trivial. Suppose that the maps are inverse to one another on $\mathbb{Z}_k^X$ and $G(X, r)^k$. Then for any element $\eta \in \mathbb{Z}_{k+1}^X$, we have $\eta = a + \xi$ for $a \in \mathbb{Z}_k^X, \xi \in Y$. Then we have

$$\begin{aligned} \pi\big(h(a+\xi)\big) &= \pi(h(a)h\big(h(a)^{-1} \star \xi)\big) \\ &= \pi\big(h(a)\big) + h(a) \star \pi\big(h(h(a)^{-1} \star \xi)\big) \\ &= a + h(a) \star h(a)^{-1} \star \xi \\ &= a + \xi, \end{aligned}$$

since $a \in \mathbb{Z}_k^X, \xi \in Y$.

Let $b \in G(X,r)^k, y \in X \cup X^{-1}$. Then we have

$$h\big(\pi(yb)\big) = h\big(\pi(y) + y \star \pi(b)\big) = h\big(\pi(y)\big)h\Big(h\big(\pi(y)\big)^{-1} \star y \star \pi(b)\Big) = yh\big(\pi(b)\big) = yb,$$

since $b \in G(X,r)^k$ and $y \in X \cup X^{-1}$. □

Then we have that π is bijective, so by our previous discussion it follows that $\widetilde{\phi}$ is injective, and as such $\widetilde{\phi}$ is an isomorphism onto its image. The maps π and h provide a bijection between $G(X,r)$ and $\mathbb{Z}^X$, which we will use to define an additive structure on $G(X,r)$ in terms of the natural additive structure on $\mathbb{Z}^X$. We may also use this bijection to understand the structure of $\mathrm{Im}\big(\widetilde{\phi}\big)$. We define $\rho\colon M \to \mathrm{Sym}_X$ by $\rho(t,s) = s$. Then we define $\psi\colon \mathbb{Z}^X \to \mathrm{Sym}_X$ by $\psi(t) = \rho\Big(\widetilde{\phi}\big(h(t)\big)\Big)$. The definition of this map is illustrated in Figure 6.1. If $(t,s) \in \mathrm{Im}(\widetilde{\phi})$, say $(t,s) = \widetilde{\phi}(g)$ for $g \in G(X,r)$, then $s = \rho\Big(\widetilde{\phi}(g)\Big) = \rho\Big(\widetilde{\phi}\big(h(t)\big)\Big) = \psi(t)$. Therefore, $\mathrm{Im}(\widetilde{\phi}) = \{\big(t, \psi(t)\big) \mid t \in \mathbb{Z}^X\}$.

$$\begin{array}{ccc} G(X,r) & \xrightarrow{\quad\widetilde{\phi}\quad} & M \\ {\scriptstyle h}\uparrow & & \downarrow{\scriptstyle \rho} \\ \mathbb{Z}^X & \xrightarrow{\quad\psi\quad} & \mathrm{Sym}_X \end{array}$$

Figure 6.1: The map $\psi\colon \mathbb{Z}^X \to \mathrm{Sym}_X$.

To summarise, we have shown that the map ϕ as in Proposition 6.1.3 induces a group isomorphism $\widetilde{\phi}\colon G(X,r) \to B$, where

$$B = \{\big(t, \psi(t)\big) \mid t \in \mathbb{Z}^X\} \leq M \tag{6.3}$$

for an appropriate map $\psi\colon \mathbb{Z}^X \to \mathrm{Sym}_X$. In particular, restricting the domain of ψ to only the set X, we have $\psi(x) = \phi(x) = \sigma_x$ for all $x \in X$.

Note that the form of B as given in (6.3) shows that we can identify B with $\mathbb{Z}^X$, which in turn is in bijection with $G(X,r)$. We will use the natural additive structure on $\mathbb{Z}^X$ to define an addition on B which makes B a left brace.

Proposition 6.1.7. [Ced18, page 59] *Let B be the subgroup of M as above, and denote its multiplication by $\circ$. Equip B with operation $+$ defined as*

$$\big(x, \psi(x)\big) + \big(y, \psi(y)\big) = \big(x + y, \psi(x+y)\big)$$

Then $(B, +, \circ)$ is a left brace.

Proof. It is clear that $(B,+)$ and $(B,\circ)$ are groups. Note that, since $\big(x,\psi(x)\big) \circ \big(y,\psi(y)\big) = \big(x + \psi(x)(y), \psi(x)\psi(y)\big)$, it follows that $\psi\big(x + \psi(x)(y)\big) = \psi(x)\psi(y)$.

For $x, y, z \in B$, we then have

$$\begin{aligned}
&\big(x, \psi(x)\big) \circ \Big(\big(y, \psi(y)\big) + \big(z, \psi(z)\big)\Big) + \big(x, \psi(x)\big) \\
&= \big(x, \psi(x)\big) \circ \big(y + z, \psi(y + z)\big) + \big(x, \psi(x)\big) \\
&= \Big(x + \psi(x)(y + z), \psi\big(x + \psi(x)(y + z)\big) + \big(x, \psi(x)\big)\Big) \\
&= \Big(x + \psi(x)(y + z) + x, \psi\big(x + \psi(x)(y + z) + x\big)\Big) \\
&= \Big(x + \psi(x)(y) + \psi(x)(z) + x, \psi\big(x + \psi(x)(y) + \psi(x)(z) + x\big)\Big) \\
&= \Big(x + \psi(x)(y), \psi\big(x + \psi(x)(y)\big)\Big) + \Big(x + \psi(x)(z), \psi\big(x + \psi(x)(z)\big)\Big) \\
&= \big(x + \psi(x)(y), \psi(x)(y)\big) + \big(x + \psi(x)(z), \psi(x)(z)\big) \\
&= \big(x, \psi(x)\big) \circ \big(y, \psi(y)\big) + \big(x, \psi(x)\big) \circ \big(z, (z)\big),
\end{aligned}$$

where the fourth equality follows from the natural action of Sym_X on $\mathbb{Z}^X$ as defined at the start of this section. □

We are now in a position to define the structure of a left brace on $G(X, r)$.

Proposition 6.1.8. *Let multiplication in $G(X, r)$ be denoted by $\circ$. Then $G(X, r)$ has the structure of a left brace with addition defined as*

$$g + h = \widetilde{\phi}^{-1}\Big(\widetilde{\phi}(g) + \widetilde{\phi}(h)\Big),$$

for all $g, h \in G(X, r)$.

Proof. It is clear that $G(X, r)$ is a group under $+$ and $\circ$. For any $x, y, z \in G(X, r)$, we have

$$\begin{aligned}
x \circ (y + z) + x &= \widetilde{\phi}^{-1}\Big(\widetilde{\phi}\big(x \circ (y + z)\big) + \widetilde{\phi}(x)\Big) \\
&= \widetilde{\phi}^{-1}\Big(\big(x, \psi(x)\big) \circ \big(y + z, \psi(y + z)\big) + \big(x, \psi(x)\big)\Big) \\
&= \widetilde{\phi}^{-1}\Big(\Big(x + \psi(x)(y + z), \psi\big(x + \psi(x)(y + z)\big)\Big) + \big(x, \psi(x)\big)\Big) \\
&= \widetilde{\phi}^{-1}\Big(\Big(2x + \psi(x)(y + z), \psi\big(\psi(x)(y + z) + 2x\big)\Big)\Big) \\
&= \widetilde{\phi}^{-1}\Big(\Big(2x + \psi(x)(y) + \psi(x)(z), \psi\big(\psi(x)(y) + \psi(x)(z) + 2x\big)\Big)\Big) \\
&= \widetilde{\phi}^{-1}\Big(\Big(x + \psi(x)(y), \psi\big(x + \psi(x)(y)\big)\Big) + \Big(x + \psi(x)(z), \psi\big(x + \psi(x)(z)\big)\Big)\Big) \\
&= \widetilde{\phi}^{-1}\Big(\big(x, \psi(x)\big) \circ \big(y, \psi(y)\big) + \big(x, \psi(x)\big) \circ \big(z, \psi(z)\big)\Big) \\
&= \widetilde{\phi}^{-1}\Big(\widetilde{\phi}(x \circ y) + \widetilde{\phi}(x \circ z)\Big) \\
&= x \circ y + x \circ z.
\end{aligned}$$

□

Note it follows that

$$\begin{aligned}
\lambda_x(y) &= x \circ y - x \\
&= \widetilde{\phi}^{-1}\Big(\widetilde{\phi}(x \circ y) - \widetilde{\phi}(x)\Big) \\
&= \widetilde{\phi}^{-1}\Big(\big(x, \psi(x)\big) \circ \big(y, \psi(y)\big) - \big(x, \psi(x)\big)\Big) \\
&= \widetilde{\phi}^{-1}\Big(\Big(x + \psi(x)(y), \psi\big(x + \psi(x)(y)\big)\Big) - \big(x, \psi(x)\big)\Big) \\
&= \widetilde{\phi}^{-1}\Big(\Big(\psi(x)(y), \psi\big(\psi(x)(y)\big)\Big)\Big) \\
&= \psi(x)(y),
\end{aligned}$$

for all $x, y \in G(X, r)$.

Therefore we have shown that any for any solution (X, r) of the YBE, we may form a left brace A, with multiplicative group $G(X, r)$. Moreover, we can identify X as a subset of this brace, so we are justified in viewing X as being embedded in A. In fact, as we will see in the next section, (X, r) is a subsolution of the solution (A, r_A).

6.2 Embedding Solutions in Braces

Having constructed a brace A from the structure group $G(X, r)$ of a solution, we will now see that (X, r) can be seen as a subsolution of the solution (A, r_A) associated to the brace A as in Section 4.3. Moreover, we will show how to adapt the construction of the previous section when X is finite, to embed (X, r) in the solution associated to a finite brace.

Given two solutions (X, r) and (Y, s) of the YBE with $Y \subseteq X$, we say that (Y, s) is a **subsolution** of (X, r) if $r(Y, Y) \subseteq (Y, Y)$ and $r_{\restriction_{Y^2}} = s$.

Now, for any solution (X, r) of the YBE we can consider the brace A obtained from $G(X, r)$ as above. Then we can show that (X, r) is a subsolution of the solution (A, r_A) associated to A. To see this, let $x, y \in X \subseteq A$. We have

$$\begin{aligned}
r_A(x, y) &= \big(\lambda_x(y), \lambda^{-1}_{\lambda_x(y)}(x)\big) \\
&= \Big(\psi(x)(y), \psi^{-1}\big(\psi(x)(y)\big)(x)\Big) \\
&= \big(\sigma_x(y), \sigma^{-1}_{\sigma_x(y)}(x)\big) \\
&= \big(\sigma_x(y), \tau_y(x)\big) \\
&= r(x, y),
\end{aligned}$$

using the characterisation of Remark 2.4.4 for the fourth equality. So restricting the domain of the map r_A to X^2, we recover the original solution (X, r), and (X, r) is a subsolution of (A, r_A). Hence any solution of the YBE can be embedded in a left brace as a subsolution.

In fact, if (X, r) is a finite solution (that is, the set X is finite), we can embed (X, r) in a finite left brace. To see this, we will need the following construction.

Definition 6.2.1. The **permutation group** of the solution (X, r) denoted by $\mathcal{G}(X, r)$ is the subgroup of Sym_X generated by $\{\sigma_x \mid x \in X\}$.

Proposition 6.2.2. *The map $\widetilde{\psi} : G(X, r) \to \mathcal{G}(X, r)$ given by $\widetilde{\psi}(x) = \rho(\widetilde{\phi}(x))$is a group homomorphism.*

Proof. It is straightforward to calculate that

$$\widetilde{\psi}(x \circ y) = \rho\Big(\big(x, \psi(x)\big) \circ \big(y, \psi(y)\big)\Big) = \rho\Big(\big(x + \psi(x)(y), \psi(x)\psi(y)\big)\Big) = \widetilde{\psi}(x)\widetilde{\psi}(y).$$

□

As remarked in [Ced18, page 60], there is a natural addition on $\mathcal{G}(X, r)$ giving rise to a left brace structure: namely, the addition which makes $\widetilde{\psi}$ a brace homomorphism. Further $\mathrm{Ker}(\widetilde{\psi}) = \mathrm{Soc}\big(G(X, r)\big)$, so $\mathcal{G}(X, r) \cong G(X, r)/\mathrm{Soc}\big(G(X, r)\big)$.

It is clear that, for X finite, then $\mathcal{G}(X, r) \subseteq \mathrm{Sym}_X$ is finite, from which it follows that $[G(X, r) : \mathrm{Soc}(G(X, r))] = n$ for some $n < \infty$. Through the following two results, which restate [CGIS17, Remark 7], we will show that we can embed X in a finite left brace B.

Lemma 6.2.3. *Let (X, r) be a finite solution of the YBE, such that $[G(X, r) : \mathrm{Soc}\big(G(X, r)\big)] = n < \infty$. Then the set $I = \{ng : g \in G(X, r)\}$ is an ideal of $G(X, r)$ and moreover, $G(X, r)/I$ is a finite left brace of order $n^{|X|}$.*

Proof. Denote $G = G(X, r)$ as a left brace. Observe that $I \subseteq \mathrm{Soc}(G)$. This can be seen from the fact that $[G : \mathrm{Soc}(G)] = n$, so $G/\mathrm{Soc}(G)$ has n elements. When $g + \mathrm{Soc}(G)$ is the coset of g in $G/\mathrm{Soc}(G)$, it follows that the order of $g + \mathrm{Soc}(G)$ in $G/\mathrm{Soc}(G)$, call it k, divides n. Say $n = kl$. Therefore, $kg + \mathrm{Soc}(G) = k(g + \mathrm{Soc}(G)) = \mathrm{Soc}(G)$ and $kg \in \mathrm{Soc}(G)$. Then $ng + \mathrm{Soc}(G) = (kl)g + \mathrm{Soc}(G) = l(kg + \mathrm{Soc}(G)) = l(\mathrm{Soc}(G)) = \mathrm{Soc}(G)$, so $ng \in \mathrm{Soc}(G)$.

It is straightforward to verify that I is a subbrace of G. Furthermore, if $ng, nh \in I$, then $h * (ng) = n * (hg) \in I$ by left-distributivity. Also, since $ng \in I \subseteq \mathrm{Soc}(G)$, it follows from Remark 4.3.5 that $(ng) * h = 0 = n0 \in I$. So I is an ideal of G, by Proposition 5.1.4.

Now, $(G, +)$ is isomorphic to the free abelian group on the elements of X. It is clear that we can represent an element of $(G, +)$ as an m-tuple of integers, where $m = |X|$. Then it follows that elements of G/I can be represented as m-tuples of integers modulo n, so G/I has order n^m, which is finite. □

Proposition 6.2.4. *If (X, r) is a finite set-theoretic solution of the YBE, then there exists a finite left brace B with associated solution (B, r_B) such that X can be embedded in B, and $r_B(X, X) \subseteq (X, X)$ and, moreover, $r_{B|_{X^2}} = r$.*

Proof. Let $B = G/I$ for G, I as defined in Lemma 6.2.3. Note that if $x, y \in X$ and $x \neq y$, then $x - y \notin I$ since $I \subseteq G$, and $(G, +)$ is the free abelian group on the elements of X. Then the natural map $can : G \to G/I$ is injective on $X \subseteq G$, so $can_{\restriction X} : X \to B$ is an embedding of X in B. Furthermore, for $x, y \in X$, we have

$$r_B(x + I, y + I) = r_G(x, y) + I \in X + I$$

so X is preserved under r_B. It is also clear that $r_B = r$ on X^2. □

Therefore, not only can we embed a solution (X, r) in a left brace A such that (X, r) is a subsolution of (A, r_A): when X is a finite solution, we may take A to be a finite brace.

6.3 Using Left Braces to Obtain All Finite Solutions of the YBE

We have seen in Section 4.3 that any left brace gives rise to a solution of the YBE. In Section 6.1, we saw that any solution (X, r) of the YBE gives rise to a left brace A obtained from the structure group $G(X, r)$. In section 6.2, we saw that (X, r) is a subsolution of (A, r_A) and moreover, when X is finite, we can embed (X, r) as a subsolution of a finite quotient brace A/I.

Therefore, to find all solutions of the YBE it is sufficient to first find all left braces, and then for each left brace B to find the subsets $X \subseteq B$ such that $r(X, X) \subseteq (X, X)$

Example 6.3.1. Consider the brace A of Example 4.1.5. We saw in Example 5.2.4 that $A = G_6 = G_3 \rtimes G_2$ for G_3, G_2 the trivial braces on 3 and 2 elements respectively; and in Example 5.1.6 that $(G_3, 0)$ is an ideal of A. Then from Section 4.3, we know (G_6, r_{G_6}) is a set-theoretic solution of the YBE. However, consider also the subset $I = (G_3, 0) \subseteq G_6$. It is easy to check that $r_{G_6}(I, I) \subseteq (I, I)$. Letting r'_{G_6} denote the restriction of r_{G_6} to I^2, we see that (I, r'_{G_6}) is a solution of the YBE.

It is clear that the solution (I, r'_{G_6}) in the example above is isomorphic to the solution (G_3, r_{G_3}) associated to the trivial brace G_3. In general, if B_1 is a subbrace of B_2, then if (X, r) is a subsolution of (B_1, r_{B_1}), we have that (X, r) is also a subsolution of (B_2, r_{B_2}). This follows from the fact that (B_1, r_{B_1}) is a subsolution of (B_2, r_{B_2}). So the method of first finding all left braces, and then finding all solutions (X, r) arising as subsets of each brace, will involve considerable over-counting and is not an optimal way to find all solutions of the YBE. Indeed, even finding all the subsolutions of a single left brace B may not be an easy task - naïvely, we may need to check $2^{|B^2|}$ subsets of B^2 for closure under r_B.

In [BCJ16], a method was presented for classifying all solutions (X, r) in a systematic way, using the permutation group of a solution. Given a left brace

B, the method of [BCJ16] allows us to classify all solutions (X, r) such that $\mathcal{G}(X, r) \cong B$.

In this chapter, we have seen that the task of finding all solutions of the YBE can be reduced to the problem of finding all left braces B, and considering the subsolutions of each associated solution (B, r_B). Moreover, if we are seeking finite solutions of the YBE, it suffices to consider only finite braces since every finite solution can be embedded as a subsolution of a finite left brace. There is some redundancy in this method, but using the construction of the permutation group $\mathcal{G}(X, r)$, a method was presented in [BCJ16] to classify all solutions (X, r) in a systematic way. This motivates our interest in the study of left braces. In the remainder of this paper, we will look in greater detail at left braces as well as at related brace-theoretic constructions.

Chapter 7

Other Relaxations of Jacobson Radical Rings

In this chapter we come back to the defining axioms of braces and examine whether there was any arbitrariness in their choice. As a consequence, we introduce the notion of right braces and show that they are in bijective correspondence with left braces. Moreover, we show that a left brace with associative $*$ operation is a two-sided brace.

7.1 Right Braces

Recall from Chapter 4.1 that in comparison to Jacobson radical rings, left braces relax two of the ring axioms - (M2) and (D2) - but they assume the extra axiom (B2). Alert readers may have wondered if there is a "deeper" motivation for the choice of retaining (D1) as compared to (D2). Alternatively, one may ask questions such as: What would be the resulting algebraic structure had we chosen to retain (D2)? Is this algebraic structure helpful in the study of solutions of the Yang-Baxter equation?

We will answer this question fully by showing that this choice is purely cosmetic, in the sense that there is a bijective correspondence between left braces and this "other" algebraic structure. We first define this algebraic structure formally.

Definition 7.1.1. [CJO14, Definition 1] A **right brace** is a set A equipped with two binary operations $+$ and $\circ$ satisfying the following set of axioms:

(B1) $(A, +)$ is an abelian group.

(B2) $(A, \circ)$ is a group.

(D2) $(a + b) \circ c = a \circ c + b \circ c - c$ for every $a, b, c \in A$.

For any right brace $(A, +\circ)$, we define the binary operation $*$ by

$$a * b = a \circ b - a - b$$

for any $a, b \in A$. It is also easy to verify that

$$(a + b) * c = a * c + b * c.$$

We now show the bijective correspondence between left braces and right braces through the following definition.

Definition 7.1.2. Let $(A, +, \circ)$ be a left brace. The **opposite brace** of A is the right brace $(A, +, \odot)$ having the same underlying set and same additive group, but multiplicative group $(A, \odot)$ equal to the opposite group of $(A, \circ)$, that is

$$a \odot b = b \circ a$$

for all $a, b \in A$. The opposite brace of a right brace is defined similarly.

It is straightforward to verify from Definition 7.1.2 that this map is involutive, i.e. opposite brace of the opposite of a brace B is simply B itself. Hence, we have that left braces and right braces are in one-to-one correspondence.

Due to this bijective correspondence, everything that we have studied for left braces can be studied in a similar fashion in the context of right braces.

7.2 Two-Sided Braces

In this section, we will show that a set that is both a left brace and right brace is precisely a Jacobson radical ring. Consequently, we can view left braces as a strict relaxation of axiom (D2) of Jacobson radical rings, without the need to add any further axioms.

Definition 7.2.1. A **two-sided brace** is a left brace which is also a right brace.

It is clear that a Jacobson radical ring $(R, +, *)$ is a left brace and a right brace, hence is a two-sided brace. We now show that the converse is in fact true as well by showing the following lemma.

Lemma 7.2.2. *If $(A, +, \circ)$ is a two-sided brace, then the operation $*$ on A is associative.*

Proof. Let $a, b, c \in A$. Since A is a left brace, we have from Lemma 4.2.6 that

$$(a * b + a + b) * c = a * (b * c) + a * c + b * c.$$

But since A is a right brace, it follows from (D2) that

$$(a * b + a + b) * c = (a * b) * c + a * c + b * c.$$

Therefore, we have $a * (b * c) = (a * b) * c$ for all $a, b, c \in A$. Hence, the operation $*$ is associative. □

Proposition 7.2.3. *If $(A, +, \circ)$ is a two-sided brace, then $(A, +, *)$ is a Jacobson radical ring.*

Proof. It is sufficient to check that $(A, +, *)$ satisfies (JR1). Since $(A, \circ)$ is a group, for every $a \in A$, we have

$$a * a^{-1} + a + a^{-1} = a \circ a^{-1} = 1 = 0.$$

Hence, $(A, +, *)$ is a Jacobson radical ring. □

7.3 One-Sided Braces with Associative $*$ Operation

The correspondence of two-sided braces and Jacobson radical rings in Proposition 7.2.3 tell us that the algebraic structure defined by axioms (B1), (M2), (D1), (D2) and (JR1) is exactly the algebraic structure defined by axioms (B1), (B2), (D1) and (D2). One can interpret the relaxation of (M2) and (JR1) from Jacobson radical rings as being "compensated" for by the addition of axiom (B2).

It's natural to ask if similar "compensations" exist. In this section, we will show that a left brace with operation $*$ associative is a two-sided brace. This answers the question asked in [CGIS18, Question 2.1(2)].

Theorem 7.3.1. [Lau18, Theorem 1.1] *Let $(A, +, \circ)$ be a left brace. If the operation $*$ is associative, then A is a two-sided brace.*

Due to the correspondence of left braces and right braces apparent from Definition 7.1.2, we immediately have that a right brace with operation $*$ associative is a two-sided brace.

Theorem 7.3.2. *Let $(A, +, \circ)$ be a right brace. If the $*$ operation is associative, then A is a two-sided brace.*

To prove Theorem 7.3.1, we will develop two algebraic manipulation identities that hold for left braces with operation $*$ associative. We remark that these identities do not hold for general left braces.

Proposition 7.3.3 is shown in the last three lines of the proof for [CGIS18, Proposition 2.2].

Proposition 7.3.3. *Let $(A, +, \circ)$ be a left brace with associative $*$ operation. Then for all $a, b \in A$, we have*

$$(-a) * b = -(a * b).$$

Proof. We have

$$\begin{aligned}\big(a * (-a)\big) * b &= \big(a * (-a) + a + (-a)\big) * b \\ &= a * \big((-a) * b\big) + a * b + (-a) * b,\end{aligned}$$

where the second equality follows from Lemma 4.2.6. Due to the associativity of operation $*$, we have

$$\big(a * (-a)\big) * b = a * \big((-a) * b\big),$$

which implies

$$0 = a * b + (-a) * b.$$

Hence, we have $(-a) * b = -(a * b)$ for all $a, b \in A$. □

Substituting (4.1) into Proposition 7.3.3, we immediately get the following corollary. This corollary will be used in our proof for Theorem 7.3.1.

Corollary 7.3.4. *Let $(A, +, \circ)$ be a left brace such that the operation $*$ is associative. Then for all $a, b \in A$, we have*

$$(-a) \circ b = -(a \circ b) + 2b.$$

We now show the proof of Theorem 7.3.1.

Proof of Theorem 7.3.1. Suppose the operation $*$ is associative. Then for all $a, b, c \in A$, we have

$$(a * b) * c = a * (b * c).$$

Applying (4.1) to both sides twice and rearranging, we see that

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

This implies

$$\begin{aligned}&a^{-1} \circ \Big((a \circ b - a - b) \circ c - a \circ b\Big) \\ &= a^{-1} \circ \Big(a \circ (b \circ c - b - c) - a - a - b \circ c + c + c\Big).\end{aligned}$$

Applying Lemma 4.2.5, rearranging and substituting $a^{-1} \circ a$ with 0 gives us

$$a^{-1} \circ \big(a \circ b - a + (-b)\big) \circ c = b \circ c - c - a^{-1} \circ b \circ c + a^{-1} \circ c + a^{-1} \circ c.$$

Applying similar manipulations gives us

$$\big(b + a^{-1} \circ (-b)\big) \circ c + c = b \circ c + (a^{-1} \circ c + a^{-1} \circ c - a^{-1} \circ b \circ c).$$

Using Lemma 4.2.5 to factorise the last term on RHS gives us

$$\big(b + a^{-1} \circ (-b)\big) \circ c + c = b \circ c + a^{-1} \circ (2c - b \circ c).$$

Applying Corollary 7.3.4 and associativity of the operation $\circ$ gives us

$$\big(b + a^{-1} \circ (-b)\big) \circ c + c = b \circ c + a^{-1} \circ (-b) \circ c.$$

Since $(A, \circ)$ is a group, for each $d \in A$, we can find the associated $a \in A$ such that $d = a^{-1} \circ (-b)$. Hence, we have for all $b, c, d \in A$,

$$(b + d) \circ c + c = b \circ c + d \circ c.$$

We conclude that A is a two-sided brace. □

Therefore, we have shown that the following four algebraic structures are exactly the same:

(i) Jacobson radical ring;

(ii) Two-sided brace;

(iii) Left brace with operation $*$ associative;

(iv) Right brace with operation $*$ associative.

	(B1)	(B2)	(D1)	(D2)	(M2)	(JR1)
Jacobson radical ring	✓		✓	✓	✓	✓
Two-sided brace	✓	✓	✓	✓		
Left brace with operation $*$ associative	✓	✓	✓		✓	
Right brace with operation $*$ associative	✓	✓		✓	✓	
Left brace	✓	✓	✓			
Right brace	✓	✓		✓		

Table 7.1: Comparing different axioms held by each algebraic structure

Chapter 8

Algebraic Properties of Left Braces

In this chapter, we will introduce some properties of braces and examine how these properties interact with the semidirect and wreath product of braces.

In group theory the class of solvable groups plays an important role, through the Feit-Thompson Theorem, in the classification theory of finite simple groups [Gri07, page 83]. In ring theory, there are several important classes of rings. These include nil and nilpotent rings, as well as prime and semiprime rings, and simple rings. These ring-theoretic properties are important to the structure theory of rings and algebras, and a full account of these properties can be found in [Bre14].

In braces, there are analogues of these group-theoretic and ring-theoretic properties. Understanding these properties in a brace-theoretic context may provide useful insight for the classification theory of left braces.

In Section 5 of [Smo18a], it was shown that the property of being a right nilpotent brace is preserved by the semidirect and wreath products. In this chapter, we show that the brace properties of being solvable, and of being semiprime, are invariant under the semidirect and wreath products.

8.1 Solvable Braces

The definition of a solvable left brace is an analogue of the definition for solvable groups. Just as the definition for solvable groups involves considering normal subgroups and quotient groups, the definition of a solvable left brace is based on brace ideals and quotient braces.

Recall that a brace B is trivial if $a \circ b = a + b$ for all $a, b \in B$. Note that this is equivalent to saying $B^2 = B * B = 0$. Then observe that B/I is trivial if and only if $B^2 \subseteq I$.

Definition 8.1.1. [BCJO17b, Definition 2.2] A **solvable brace** is any left brace

B which has a series $\{0\} = B_0 \subseteq B_1 \subseteq \cdots \subseteq B_m = B$ such that B_i is an ideal of B_{i+1}, and such that B_{i+1}/B_i is a trivial brace for any $i \in \{0, 1, \ldots, m-1\}$.

We will often abuse notation by denoting the zero brace $\{0\}$ with the symbol 0.

Example 8.1.2. Consider the brace A from Example 4.1.5. We saw in Example 5.2.4 that we can write $A = G_3 \rtimes G_2$, where G_3, G_2 are the trivial braces on 3 and 2 elements respectively; and we saw in Example 5.1.6 that $I = \{G_3, 0\}$ is an ideal of A. Note that, A/I has order 2, so $A/I \cong G_2$ since there is only one group of order 2 up to isomorphism. Since G_2 is trivial, A/I is trivial. Also, $I \cong G_3$ which is trivial, so $I/\{0\}$ is a trivial brace. Then the sequence of ideals $0 \subseteq I \subseteq G_6$ shows G_6 is a solvable brace.

Example 8.1.3. Let p be an odd prime and let A be the brace as described in Example 4.1.7. Then consider the set $I = \{2n : 0 \leq n \leq p-1\}$. $(I, +)$ is clearly a subgroup of $(A, +)$. If $2n, 2m \in I$, then

$$2n \circ 2m = 2n + (-1)^{2n} 2m = 2n + 2m.$$

It follows, since I is a subgroup of A under $+$, that I is also a subgroup under $\circ$ and thus I is a subbrace of A. Clearly, from the above, we see I is a trivial brace so $I/\{0\}$ is a trivial brace. Further, the order of A/I is 2, and there is only one brace of order 2, the trivial brace with two elements. Then A/I is a trivial brace, and the series of ideals $0 \subseteq I \subseteq A$ shows that A is a solvable brace.

We will use the following result from [BCJO17b] to show that solvability is preserved by semidirect and wreath products.

Proposition 8.1.4. [BCJO17b, Proposition 2.4]

(a) Define $d_1(B) = B^2 = B * B$, and $d_{i+1}(B) = d_i(B)^2$ for every positive integer i. Then, B is a solvable brace if and only if $d_k(B) = 0$ for some k.

(b) Let B be a left brace, and let I be an ideal of B. If I and B/I are solvable braces, then B is also solvable.

(c) Any sub-brace, and any quotient of a solvable brace is solvable.

Proof. For part (a), suppose B is solvable. Then there is a series $0 = B_0 \subseteq B_1 \subseteq \cdots \subseteq B_m = B$ such that B_i is an ideal of B_{i+1}, and such that B_{i+1}/B_i is trivial. Then $d_1(B) = B^2 \subseteq B_{m-1}$, and $d_2(B) \subseteq B_{m-1}^2 \subseteq B_{m-2}$ and so on, until we obtain that $d_m(B) \subseteq B_0 = 0$. Thus for $k = m$, we have $d_k(B) = 0$. Conversely, suppose there is k such that $d_k(B) = 0$. Note that $d_{i+1}(B)$ is an ideal of $d_i(B)$, and that $d_i(B)/d_{i+1}(B)$ is trivial since $d_i(B)^2 \subseteq d_i(B)$. Then the series of ideals $0 = d_k(B) \subseteq \cdots \subseteq d_1(B) \subseteq d_0(B) = B$ shows that B is solvable.

For parts (b) and (c), the proofs directly mirror the corresponding group theoretic results. □

Lemma 8.1.5. *The semidirect product $N \rtimes H$ of braces N and H is solvable if and only if N and H are solvable.*

Proof. Let $N \rtimes H$ be a semidirect product of braces via $\sigma : H \to \mathrm{Aut}(N)$, and suppose $N \rtimes H$ is solvable. It is clear that

$$(0, H) = \{(0, h) : h \in H\} \subseteq N \rtimes H$$

is a sub-brace of $N \rtimes H$. Then note that for any $n_1, n_2 \in N$, we have

$$(n_1, 0) \circ (n_2, 0) = (n_1 \circ n_2, 0)$$

showing that

$$(N, 0) = \{(n, 0) : n \in N\} \subseteq N \rtimes H$$

is also a sub-brace of $N \rtimes H$. By Proposition 8.1.4, part (c), we see that $(0, H), (N, 0)$ are solvable left braces, and it is clear that these braces are isomorphic to H, N respectively. Thus H, N are solvable left braces.

Now suppose that N, H are solvable, and consider $N \rtimes H$ via $\sigma : H \to \mathrm{Aut}(N)$. Then consider $f : N \rtimes H \to H$ defined by $f(n, h) = h$ for all $h \in H$. Note that for $(n_1, h_1), (n_2, h_2) \in N \rtimes H$, we have

$$f((n_1, h_1) + (n_2, h_2)) = f(n_1 + n_2, h_1 + h_2) = h_1 + h_2 = f(n_1, h_1) + f(n_2, h_2)$$

and, for some $d \in N$,

$$f((n_1, h_1) \circ (n_2, h_2)) = f((d, h_1 \circ h_2)) = h_1 \circ h_2 = f(n_1, h_1) \circ f(n_2, h_2).$$

Thus f is a homomorphism. Note that $(n, h) \in \mathrm{Ker}(f)$ if and only if $h = 0$, which is the case if and only if $(n, h) \in (N, 0)$. Thus $\mathrm{Ker}(f) = (N, 0)$, and furthermore $(N, 0)$ is an ideal of $N \rtimes H$. It is clear that f is surjective, thus applying Theorem 5.1.9 gives that $N \rtimes H/(N, 0)$ and H are isomorphic braces.

Then, by Proposition 8.1.4, part (b), we have that since $N \cong (N, 0)$ and $H \cong N \rtimes H/(N, 0)$ are solvable, $N \rtimes H$ is solvable. □

To show that the wreath product of braces G, H is solvable if and only if G, H are solvable, it suffices to show the following result.

Lemma 8.1.6. *Let G, H be braces, and*

$$W = \{f : H \to G \text{ s.t. } |\{h \in H : f(h) \neq 1\}| < \infty\}$$

Then G is solvable if and only if W is solvable.

Proof. Suppose that W is solvable. Let $\phi : G \to W$ be defined for all $g \in G$ by

$\phi(g) = \alpha_g : H \to G$, where

$$\alpha_g(h) = \begin{cases} g \text{ if } h = 1 \\ 0 \text{ otherwise} \end{cases}$$

for all $h \in H$. Now, it is easy to check that ϕ is a homomorphism of braces, and it is clear that $g \in \mathrm{Ker}(\phi)$ if and only if $\alpha_g(1) = 0$, i.e. if and only if $g = 0$. Thus $\mathrm{Ker}(\phi) = 0$, so $G \cong \mathrm{Im}(\phi)$ by Theorem 5.1.9. Since $\mathrm{Im}(\phi)$ is a sub-brace of W, it follows from Proposition 8.1.4 that $\mathrm{Im}(\phi) \cong G$ is a solvable brace.

Now suppose G is a solvable brace. Then it has a series $0 = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_m = G$ for some m, as in Definition 8.1.1. Define the set

$$W_i = \{f \in W : f(H) \subseteq G_i\}.$$

It is clear that that W_i form the chain $0 = W_0 \subseteq \cdots \subseteq W_m = W$. It is also easy to check that each W_i is an ideal of W, from which it follows that W_i is an ideal of W_{i+1}. It remains to show that W_{i+1}/W_i is trivial for all $0 \leq i \leq m-1$.

For any such i, let $\alpha, \beta \in W_{i+1}$. Then for all $h \in H$,

$$(\alpha * \beta)(h) = \alpha(h) * \beta(h) \in G_{i+1}^2 \subseteq G_i$$

using that G is solvable. This shows that $W_{i+1}^2 \subseteq W_i$, that is, W_{i+1}/W_i is trivial. Then it follows that W is a solvable brace. □

Lemma 8.1.7. *The wreath product $G \wr H$ of two braces G and H is solvable if and only if G and H are solvable braces.*

Proof. Let G, H be left braces. Then G, H are solvable if and only if W, H are solvable by Lemma 8.1.6, where W is such that $G \wr H = W \rtimes H$. Then W, H are solvable if and only if $W \rtimes H$ is solvable by Lemma 8.1.5. Since $G \wr H = W \rtimes H$, we have that G, H are solvable if and only if $G \wr H$ is solvable. □

The constructions and results presented here have closely related analogues in group theory. Indeed, there are equivalent statements of Lemmas 8.1.5 and 8.1.7 for groups, whose proofs directly mirror those given here. It is tempting to ask whether the results of this section are implied by these existing group-theoretic results: however, this is not the case.

This is because a brace G may have solvable additive and multiplicative groups but not itself be a solvable brace. In [CJDR10, Theorem 2.1] it is shown that the multiplicative group of any finite brace is a particular kind of group called an IYB group. In [ESS99, Theorem 2.15], it was shown that any IYB group is a solvable group. Thus the $\circ$ group of any finite brace is solvable. But there exist non-solvable finite left braces. Indeed, any non-trivial brace B whose only ideals are $\{0\}$ and B is not solvable. A brace B whose only ideals are $\{0\}$ and B is called a simple brace, and it has been shown in [CJO18], [BCJO17b] and [BCJO18] that

there exist an abundance of nontrivial simple left braces. Therefore, a brace with solvable additive and multiplicative groups need not be a solvable brace.

8.2 Semiprime Braces

Another property which is preserved under semidirect and wreath products is semiprimality. This concept originates in ring theory: we say a ring R is prime if, for any nonzero ideals I, J of R, we have that $IJ \neq 0$. Similarly, a ring R is semiprime if $I^2 \neq 0$ for all nonzero ideals I of R. The definitions of prime and semiprime braces are direct analogues of the ring-theoretic concepts, and were introduced in [KSV18].

Definition 8.2.1. Let G be a left brace. Then G is called **prime** if for any nonzero ideals I, J of G, we have that $I * J \neq 0$.

Definition 8.2.2. Let G be a left brace. Then G is called **semiprime** if for any nonzero ideal I of G, we have that $I * I \neq 0$.

It is clear that any prime left brace is semiprime, and it should also be clear that any nontrivial simple left brace is prime (and hence semiprime). As remarked in previous section, the papers [CJO18], [BCJO17b] and [BCJO18] construct infinite families of simple left braces - hence there exist many prime and semiprime left braces. In [KSV18, Question 4.4], it was asked whether there exist finite prime non-simple left braces. In Section 5 of [CJO18], it is shown how to construct a finite prime left brace which is not a simple left brace, answering the question in the affirmative.

In the structure theory of noncommutative algebras, prime and semiprime rings play a central role. In particular, a series of lemmas concerning prime and semiprime rings are used in the proofs of Wedderburn's structure theorems (see [Bre14], Sections 2.2 and 2.9). This suggests that prime and semiprime braces may be useful tools in the task of classifying all left braces. In the remainder of this section, we show that the wreath and semidirect product of two semiprime left braces is semiprime. This allows us to generate an abundance of semiprime left braces.

Before proceeding to show how semiprimality interacts with the semidirect product, we will require the notion of the projection of an ideal of a semidirect product of braces, and the following lemma regarding it.

Definition 8.2.3. Let G, H be left braces, and $G \rtimes H$ be their semidirect product via $\sigma : H \to \mathrm{Aut}(G)$. Let $S \subseteq G \rtimes H$. The we define the **right projection** of S as the set

$$\pi_H(S) = \{h \in H : (g, h) \in S \text{ for some } g \in G\}$$

and the **left projection** of S as the set

$$\pi_G(S) = \{g \in G : (g, h) \in S \text{ for some } h \in H\}.$$

Lemma 8.2.4. *Let G, H be left braces, and $G \rtimes H$ be their semidirect product via $\sigma : H \to \mathrm{Aut}(G)$. Let I be an ideal of $G \rtimes H$. Then $\pi_H(I)$ is an ideal of H. Furthermore, if $\pi_H(I) = 0$, then $\pi_G(I)$ is an ideal of G.*

Proof. First, let $Q = \pi_H(I)$, and let $q_1, q_2 \in Q$, with $g_1, g_2 \in G$ such that $(g_1, q_1), (g_2, q_2) \in I$. Then $q_1^{-1} \in Q, 0 \in Q$ since $(I, \circ)$ is a subgroup of $(G \rtimes H, \circ)$. Also, there exists some $d \in G$ so that

$$(d, q_1 \circ q_2) = (g_1, q_1) \circ (g_2, q_2) \in I$$

so $q_1 \circ q_2 \in Q$ and $(Q, \circ) \leq (H, \circ)$. Now let $x \in H$. Note that, since $(I, \circ)$ is normal in $(G \rtimes H, \circ)$, we have that for some $d' \in G$,

$$(d', x \circ q_1 \circ x^{-1}) = (0, x) \circ (g_1, q_1) \circ (0, x^{-1}) = (0, x) \circ (g_1, q_1) \circ (0, x)^{-1} \in I.$$

Then it follows that $x \circ q_1 \circ x^{-1} \in Q$, so $(Q, \circ) \lhd (H, \circ)$.

Now, let $b \in H$. Consider (a, b) for some $a \in G$. Note that, as I is an ideal of $G \rtimes H$, we have that for some $d'' \in G$,

$$(d'', \lambda_b(q_1)) = \lambda_{(a,b)}(g_1, q_1) \in I.$$

So it is clear that $\lambda_b(Q) \subseteq Q$ for all $b \in H$. Thus $\pi_H(I) = Q$ is indeed an ideal of H.

Then let $Q = 0$, and consider $P = \pi_G(I)$. We claim that this is an ideal of G. This follows by noting that if $p_1, p_2 \in P$ then $(p_1, h_1), (p_2, h_2) \in I$ for some $h_1, h_2 \in H$. Then $h_1, h_2 \in Q = 0$, so $h_1 = h_2 = 0$. Then, noting that $\sigma(0) = id$, we have that for $g_1, g_2 \in G$,

$$(g_1, 0) \circ (g_2, 0) = (g_1 \circ g_2, 0)$$

and the proof is then similar to the proof that Q is an ideal of H. □

We now have sufficiently developed tools to explore how the semidirect product interacts with semiprime braces.

Lemma 8.2.5. *Let G and H be semiprime left braces. Then the semidirect product $G \rtimes H$ via $\sigma \colon H \to \mathrm{Aut}(G)$, is a semiprime left brace.*

Proof. First, suppose that G, H are semiprime. It is known that $G \rtimes H$ is a left brace. Suppose for a contradiction that $G \rtimes H$ is not semiprime. Then there exists some nonzero ideal I of $G \rtimes H$ such that $I * I = 0$.

Let $Q = \pi_H(I)$, and let $q_1, q_2 \in Q$ with $g_1, g_2 \in G$ such that $(g_1, q_1), (g_2, q_2) \in I$. Then for some $d \in G$,

$$(d, q_1 * q_2) = (g_1, q_1) * (g_2, q_2) \in I * I = 0.$$

Then $q_1 * q_2 = 0$, and it follows that $Q * Q = 0$. Supposing Q is nonzero, then by Lemma 8.2.4 it is a nonzero ideal of H. But this contradicts that H is a semiprime

left brace. So we assume $Q = 0$.

Then by Lemma 8.2.4, we have that $P = \pi_G(I)$ is an ideal of G. Observe that if $p_1, p_2 \in P$ it must be that $(p_1, 0), (p_2, 0) \in I$. Then notice that

$$(p_1 * p_2, 0) = (p_1, 0) * (p_2, 0) \in I * I = 0$$

and so $p_1 * p_2 = 0$, and it follows that $P * P = 0$. If P is nonzero, it is a nonzero ideal of G and this contradicts that G is semiprime. But if $P = 0$, this contradicts that I is nonzero (as we assume Q is zero). In either case, we have a contradiction. Thus no such ideal I of $G \rtimes H$ exists, so $G \rtimes H$ is semiprime. □

As with solvable braces, we can use our lemma on the semidirect product of semiprime braces to obtain a result on the wreath product of semiprime braces. To achieve this, we will require require the following lemmas relating ideals in G to ideals in the brace W, as in Definition 5.2.3. We begin with the following which relates inverses in G to inverses in W.

Lemma 8.2.6. *Let G, H be left braces and W as in Definition 5.2.3. If $h \in H$, $g \in G$ and $f \in W$ are such that $g = f(h)$, then $g^{-1} = f^{-1}(h)$.*

Proof. Let h, g, f be as above and note that the identity in W is the function $0_W : H \to G$ such that $0_W(k) = 1_G$ for all $k \in H$. Then by definition,

$$1_G = (f^{-1} \circ f)(h) = f^{-1}(h) \circ f(h) = f^{-1}(h) \circ g.$$

So $f^{-1}(h)$ is a left inverse for g, and similarly it is a right inverse. So $f^{-1}(h) = g^{-1}$, since group inverses are unique. □

Given left braces G, H, the following lemma allows us to construct ideals of G from ideals of the corresponding wreath product brace W.

Lemma 8.2.7. *Let G, H be left braces and W be as in* Definition 5.2.3, and I an ideal of W. Then for any $h \in H$, the set

$$J_h = \{g \in G : f(h) = g \text{ for some } f \in I\}$$

is an ideal of G.

Proof. Since $0_W \in I$, we have $1_G \in J_h$ for any $h \in H$, by the definition of 0_W.

Then let $g_1 \in J_h$, so $g_1 = f_1(h)$ for $f_1 \in I$. Then, as I is an ideal of W, there is a function $f_1^{-1} \in I$ and by Lemma 8.2.6, we have $f_1^{-1}(h) = g_1^{-1}$. So $g_1^{-1} \in J_h$.

Now let $g_2 \in J_h$, with $g_2 = f_2(h)$ for $f_2 \in I$. Then

$$g_1 \circ g_2 = f_1(h) \circ f_2(h) = (f_1 \circ f_2)(h) \in J_h$$

since $f_1 \circ f_2 \in I$, as I is an ideal of W. So we see $(J_h, \circ) \leq (G, \circ)$.

Now, let $x \in G$. Then define $\alpha_x : H \to G$ by

$$\alpha_x(k) = \begin{cases} x \text{ if } k = h \\ 1 \text{ otherwise} \end{cases}$$

so $\alpha_x \in W$. Then

$$x \circ g_1 \circ x^{-1} = \alpha_x(h) \circ f_1(h) \circ \alpha_x^{-1}(h) = (\alpha_x \circ f_1 \circ \alpha_x^{-1})(h) \in J_h$$

since $(I, \circ)$ is a normal subgroup of $(W, \circ)$. This shows that $(J, \circ)$ is normal in $(G, \circ)$.

Finally, let $a \in G$. Then for $g_1 \in J_h$, we have

$$\begin{aligned} \lambda_a(g_1) &= a \circ g_1 - a \\ &= \alpha_a(h) \circ f_1(h) - \alpha_a(h) \\ &= (\alpha_a \circ f_1 - \alpha_a)(h) \\ &= (\lambda_{\alpha_a}(f_1))(h) \\ &\in J_h \end{aligned}$$

since I is an ideal. This shows $\lambda_a(J_h) \subseteq J_h$ for any $a \in G$, so J_h is an ideal of G. □

In fact, an analogue of the above lemma also allows us to obtain ideals of the wreath product brace W, given an ideal of G.

Lemma 8.2.8. *Let G, H left braces and W as in the Definition 5.2.3, and let P be an ideal of G. Then for any $h \in H$, the set*

$$Q_h = \{f \in W : f(h) \in P\}$$

is an ideal of W.

Proof. Clearly $0_W \in Q_h$. Let $f_1 \in Q_h$, say $f_1(h) = p_1 \in P$. Then by Lemma 8.2.6, $f_1^{-1}(h) = p_1^{-1} \in P$, so $f_1^{-1} \in Q_h$.

Now let $f_2 \in Q_h$, so $f_2(h) = p_2$ for some $p_2 \in P$. Then

$$(f_2 \circ f_1)(h) = f_2(h) \circ f_1(h) = p_2 \circ p_1 \in P$$

so $f_2 \circ f_1 \in Q_h$. So $(Q_h, \circ) \leq (W, \circ)$.

Now let $\phi \in W$. Then

$$(\phi \circ f_1 \circ \phi^{-1})(h) = \phi(h) \circ f_1(h) \circ \phi^{-1}(h) = x \circ p_1 \circ x^{-1} \in P$$

using Lemma 8.2.6 and that $(P, \circ)$ is normal in $(G, \circ)$. Thus $\phi \circ f_1 \circ \phi^{-1} \in Q_h$, so $(Q_h, \circ) \lhd (W, \circ)$.

Finally, let $\alpha \in W$. Then

$$\begin{aligned}(\lambda_\alpha(f_1))(h) &= (\alpha \circ f_1 - \alpha)(h) \\ &= \alpha(h) \circ f_1(h) - \alpha(h) \\ &= \lambda_{\alpha(h)}(f_1(h)) \\ &= \lambda_{\alpha(h)}(p_1) \\ &\in P\end{aligned}$$

since P is an ideal of G. This shows $\lambda_\alpha(Q_h) \subseteq Q_h$ for any $\alpha \in W$, and so Q_h is an ideal of W. □

We may now observe the following regarding the wreath product brace W.

Lemma 8.2.9. *If G and H are left braces, then the left brace*

$$W = \{f : H \to G \text{ such that } |\{h \in H : f(h) \neq 1\}| < \infty\}$$

is semiprime if and only if G is semiprime.

Proof. Let G be semiprime, and suppose that W is not semiprime. Then there exists a nonzero ideal I of W with $I * I = 0$. Then for any $h \in H$ we may associate to I the set J_h as in Lemma 8.2.7, which by this lemma is an ideal of G.

Let $h \in H$ be fixed and consider $g_1, g_2 \in J_h$, so $g_1 = f_1(h), g_2 = f_2(h)$ for some $f_1, f_2 \in I$. Then

$$g_1 * g_2 = f_1(h) * f_2(h) = (f_1 * f_2)(h) = 0_W(h) = 1_G = 0_G$$

which shows that $J_h * J_h = 0$. If J_h is nonzero, then this contradicts that G is a semiprime left brace. This implies that $J_h = 0$ for all $h \in H$. But this in turn contradicts that I is a nonzero ideal of W. So no such ideal I exists, and W is a semiprime left brace.

Now let that W be semiprime, and suppose G is not. Then there exists a nonzero ideal P of G such that $P * P = 0$. Then given any $h \in H$, we may construct the set Q_h as in Lemma 8.2.8, which by this lemma is an ideal of W. Note that Q_h is nonzero. This is since P is nonzero, so there is some nonzero $g \in P$, and the function $\alpha_g : H \to G$ defined by

$$\alpha_g(k) = \begin{cases} g \text{ if } k = h \\ 1_G \text{ otherwise} \end{cases}$$

for all $k \in H$ is nonzero.

Let $h \in H$ be fixed and consider $f_1, f_2 \in Q_h$, so $f_1(h) = p_1, f_2(h) = p_2$ for some $p_1, p_2 \in P$. Then

$$(f_1 * f_2)(h) = f_1(h) * f_2(h) = p_1 * p_2 = 0_G = 1_G$$

since $P * P = 0$. This shows that $Q_h * Q_h = 0$, which contradicts that W is semiprime. So no such ideal P exists, and G is a semiprime left brace. □

We now combine Lemma 8.2.5 and Lemma 8.2.9 to give the following result concerning the wreath product of braces.

Lemma 8.2.10. *If G, H are semiprime left braces, then their wreath product $G \wr H$ is a semiprime left brace.*

Proof. Let G, H be semiprime left braces. Then by Lemma 8.2.9, we have that the left brace

$$W = \{f \colon H \to G \text{ such that } \ |\{h \in H : f(h) \neq 1\}| < \infty\}$$

is semiprime. Then by Lemma 8.2.5, the semidirect product $W \rtimes H$ is a semiprime left brace. Then by definition, $G \wr H = W \rtimes H$ is a semiprime left brace. □

The above Lemma is a one-way implication. However, if the converse of Lemma 8.2.5 is true, then using Lemma 8.2.9 we would be able to extend Lemma 8.2.10 to a biconditional statement. This motivates the following question.

Question 8.2.11. If G, H are left braces and their semidirect product $G \rtimes H$ via σ is semiprime, are G and H semiprime?

Conclusion

In this paper, we have surveyed left braces and their connection to the Yang-Baxter equation.

To motivate our exposition we introduced the Yang-Baxter equation and its solutions, called R-matrices in a finite-dimensional setting, in Chapter 1. We introduced three new results characterising certain kinds of R-matrices (Proposition 1.2.6, Proposition 1.2.8, Proposition 1.2.10). We outlined how R-matrices may be obtained from set-theoretic solutions in Chapter 2, highlighting the importance of non-degenerate involutive set-theoretic solutions for this construction. We also gave an explicit formula for the characteristic polynomial of any R-matrix obtained from a non-degenerate set-theoretic solution (Proposition 1.2.11).

We have given a detailed account of how left braces are connected with non-degenerate set-theoretic solutions of the YBE. In Chapter 3, we introduced Jacobson radical rings, to illustrate how an abstract algebraic structure may give rise to a set-theoretic solution of the YBE, before introducing left braces as a generalisation of Jacobson radical rings in Chapter 4. We showed in Section 4.3 that for any left brace A we can construct a solution (A, r_A) of the YBE. Then we explored the opposite problem in Chapter 6, having introduced some useful algebraic constructions in Chapter 5. That is, we showed that given a solution (X, r), we may construct a left brace A such that X embeds in A, and the solution (X, r) is a subsolution of (A, r_A). Moreover, we showed that when the set X is finite, we may embed (X, r) as a subsolution of a quotient brace of A which is finite. Thus, we saw that the problem of finding all finite solutions of the YBE can be reduced to the classification of finite left braces.

In Chapter 7, we related left braces to other algebraic structures: in particular, we saw that there is a natural construction of a right brace analogous to that of the left brace, and that these two classes of objects are in bijection. Therefore, all of our theory could be equivalently re-stated in terms of right braces. We saw that two-sided braces are exactly Jacobson radical rings, and we further showed that when the operation $*$ of a left brace is associative, then the brace is two-sided. This answers a question posed in [CGIS18, Question 2.1(2)]. Finally, we explored some algebraic properties of left braces. In analogy with group theory, we introduced solvable left braces, and in analogy with ring theory, we introduced prime and semiprime left braces. We showed that the semidirect product of two braces is solvable if and only if each brace is solvable, and that the same is true

for the wreath product. We also showed that if G, H are semiprime braces then so is their semidirect product, as well as their wreath product.

Future Work

The possibilities for future work are abundant in the study of the Yang-Baxter equation and brace theory. R-matrices can frequently be found in literature, as they have important applications in quantum computing, representation theory, integrable systems and other fields, and therefore finding new types of R-matrices is certainly a worthwhile endeavour. All solutions of the YBE remain to be determined for vector spaces of dimension 3 and higher [Hie93], and solutions remain to be fully classified for dimension 2 and higher [Dye03]. In the area of braces, one new direction of research is in skew braces, initiated in [GV17]. These are a generalisation of braces in which axiom (B1) is relaxed, removing the requirement that the additive group be abelian. Such structures give rise to non-degenerate set-theoretic solutions of the YBE which need not be involutive.

Acknowledgements

We would sincerely like to thank Agata Smoktunowicz, our supervisor for this project, for introducing us to the wonderful theory of braces, and for her continual patience and support throughout the project. Her encouragement and insights were indispensable for the completion of this project.

Bibliography

[AAJZ17] Adel Alahmadi, Hamed Alsulami, SK Jain, and Efim Zelmanov. Matrix wreath products of algebras and embedding theorems. arXiv: 1703.08734v2 [math.RA], March 2017. (Cited on page 41.)

[AG03] Nicolás Andruskiewitsch and Matías Graña. From racks to pointed Hopf algebras. *Advances in Mathematics*, 178(2):177 – 243, September 2003. doi: 10.1016/S0001-8708(02)00071-3. (Cited on pages 8 and 21.)

[Ari02] Susumu Ariki. *Representations of Quantum Algebras and Combinatorics of Young Tableaux*. University lecture series. American Mathematical Society, July 2002. doi: 10.1090/ulect/026/01. (Cited on page 7.)

[Bac15] David Bachiller. Classification of braces of order p^3. *Journal of Pure and Applied Algebra*, 219(8):3568 – 3603, August 2015. doi: 10.1016/j.jpaa.2014.12.013. (Cited on page 8.)

[Bax72] Rodney Baxter. Partition function of the eight-vertex lattice model. *Annals of Physics*, 70(1):193–228, March 1972. doi: 10.1016/0003-4916(72)90335-1. (Cited on page 7.)

[Bax82] Rodney Baxter. *Exactly Solved Models in Statistical Mechanics*. Academic Press London, February 1982. (Cited on page 7.)

[BC14] David Bachiller and Ferran Cedó. A family of solutions of the Yang–Baxter equation. *Journal of Algebra*, 412:218 – 229, May 2014. doi: 10.1016/j.jalgebra.2014.05.011. (Cited on page 8.)

[BCJ16] David Bachiller, Ferran Cedó, and Eric Jespers. Solutions of the Yang–Baxter equation associated with a left brace. *Journal of Algebra*, 463:80 – 102, October 2016. doi: 10.1016/j.jalgebra.2016.05.024. (Cited on pages 8, 51, and 52.)

[BCJO17a] David Bachiller, Ferran Cedó, Eric Jespers, and Jan Okniński. A family of irretractable square-free solutions of the Yang–Baxter

equation. In *Forum Mathematicum*, volume 29, pages 1291–1306. De Gruyter, January 2017. doi: 10.1515/forum-2015-0240. (Cited on page 8.)

[BCJO17b] David Bachiller, Ferran Cedó, Eric Jespers, and Jan Okniński. Asymmetric product of left braces and simplicity; new solutions of the Yang–Baxter equation. *Communications in Contemporary Mathematics*, page 1850042, May 2017. doi: 10.1142/S0219199718500426. (Cited on pages 58, 59, 61, and 62.)

[BCJO18] David Bachiller, Ferran Cedó, Eric Jespers, and Jan Okniński. Iterated matched products of finite braces and simplicity; new solutions of the Yang-Baxter equation. *Transactions of the American Mathematical Society*, 370(7):4881–4907, February 2018. doi: 10.1090/tran/7180. (Cited on pages 61 and 62.)

[Bre14] Matej Brešar. *Structure of Finite Dimensional Algebras*, pages 25–51. Springer International Publishing, Cham, March 2014. doi: 10.1007/978-3-319-08693-4. (Cited on pages 58 and 62.)

[Bro06] Bobbi Broxson. The Kronecker Product. 2006. URL https://digitalcommons.unf.edu/etd/25. (Cited on pages 12, 13, and 14.)

[Brz18] Tomasz Brzezinski. Trusses: Between braces and rings. *Transactions of the American Mathematical Society*, November 2018. doi: 10.1090/tran/7705. (Cited on page 8.)

[BS04] Philippe Bonneau and Daniel Sternheimer. Topological Hopf algebras, quantum groups and deformation quantization. *Hopf algebras in noncommutative geometry and physics*, 239:55–70, November 2004. (Cited on page 7.)

[Ced18] Ferran Cedó. Left Braces: Solutions of the Yang-Baxter Equation. *Advances in Group Theory and Applications*, 5:33–90, June 2018. doi: 10.4399/97888255161422. (Cited on pages 8, 40, 47, and 50.)

[CGIS17] Ferran Cedó, Tatiana Gateva-Ivanova, and Agata Smoktunowicz. On the Yang–Baxter equation and left nilpotent left braces. *Journal of Pure and Applied Algebra*, 221(4):751–756, April 2017. doi: 10.1016/j.jpaa.2016.07.014. (Cited on pages 8 and 50.)

[CGIS18] Ferran Cedó, Tatiana Gateva-Ivanova, and Agata Smoktunowicz. Braces and symmetric groups with special conditions. *Journal of Pure and Applied Algebra*, 222(12):3877–3890, December 2018. doi: 10.1016/j.jpaa.2018.02.012. (Cited on pages 8, 9, 55, and 68.)

[Che12] Rebecca Chen. Generalized Yang–Baxter Equations and Braiding Quantum Gates. *Journal of Knot Theory and Its Ramifications*, 21(09):1250087, 2012. doi: 10.1142/S0218216512500873. (Cited on page 12.)

[CJDR10] Ferran Cedó, Eric Jespers, and Angel Del Rio. Involutive Yang-Baxter groups. *Transactions of the American Mathematical Society*, 362(5):2541–2558, May 2010. doi: 10.1090/S0002-9947-09-04927-7. (Cited on pages 41 and 61.)

[CJO06] Ferran Cedó, Eric Jespers, and Jan Okniński. The gelfand-kirillov dimension of quadratic algebras satisfying the cyclic condition. *Proceedings of the American Mathematical Society*, 134(3):653–663, 2006. (Cited on page 35.)

[CJO14] Ferran Cedó, Eric Jespers, and Jan Okniński. Braces and the Yang–Baxter equation. *Communications in Mathematical Physics*, 327(1):101–116, April 2014. doi: 10.1007/s00220-014-1935-y. (Cited on pages 8, 30, 33, 34, 35, 37, 39, 41, and 53.)

[CJO18] Ferran Cedó, Eric Jespers, and Jan Okniński. An abundance of simple left braces with abelian multiplicative sylow subgroups. arXiv: 1807.06408v1 [math.QA] , July 2018. (Cited on pages 61 and 62.)

[Dri88] Vladimir Drinfeld. Quantum groups. *Journal of Soviet Mathematics*, 41(2):898–915, Apr 1988. doi: 10.1007/BF01247086. (Cited on page 7.)

[Dri92] Vladimir Drinfeld. On some unsolved problems in quantum group theory. In Petr P. Kulish, editor, *Quantum Groups*, pages 1–8, Berlin, Heidelberg, 1992. Springer Berlin Heidelberg. doi: 10.1007/BFb0101175. (Cited on pages 7 and 18.)

[Dye03] Heather Dye. Unitary Solutions to the Yang–Baxter Equation in Dimension Four. *Quantum Information Processing*, 2(1):117–152, April 2003. doi: 10.1023/A:1025843426102. (Cited on pages 12 and 69.)

[EG98] Pavel Etingof and Shlomo Gelaki. A method of construction of finite-dimensional triangular semisimple hopf algebras. *Mathematical Research Letters*, 5, July 1998. doi: 10.4310/MRL.1998.v5.n4.a12. (Cited on page 8.)

[ESS99] Pavel Etingof, Travis Schedler, and Alexandre Soloviev. Set-theoretical solutions to the quantum Yang–Baxter equation. *Duke Mathematical Journal*, 100(2):169–209, November 1999. doi: 10.1215/S0012-7094-99-10007-X. (Cited on pages 7, 8, 43, 44, 45, and 61.)

[Frö88] Jürg Fröhlich. *Statistics of Fields, the Yang-Baxter Equation, and the Theory of Knots and Links*, pages 71–100. Springer US, Boston, MA, 1988. doi: 10.1007/978-1-4613-0729-7$_4$. (Cited on page 7.)

[GIdB98] Tatiana Gateva-Ivanova and Michel Van den Bergh. Semigroups of I-Type. *Journal of Algebra*, 206(1):97 – 112, August 1998. doi: 10.1006/jabr.1997.7399. (Cited on pages 7 and 8.)

[GKZ05] Mo-Lin Ge, Louis Kauffman, and Yong Zhang. Yang–Baxterizations, Universal Quantum Gates and Hamiltonians. *Quantum Information Processing*, 4(3):159–197, August 2005. doi: 10.1007/s11128-005-7655-7. (Cited on page 7.)

[Gri07] Pierre Grillet. *Abstract Algebra*. Springer, New York, July 2007. doi: 10.1007/978-0-387-71568-1. (Cited on pages 10, 32, and 58.)

[GV17] Leandro Guarnieri and Leandro Vendramin. Skew braces and the yang–baxter equation. *Mathematics of Computation*, 86(307):2519–2534, 2017. doi: 10.1090/mcom/3161. (Cited on page 69.)

[GY94] Mo-Lin Ge and Chen-Ning Yang. *Braid Group, Knot Theory and Statistical Mechanics II*. World Scientific Publishing, February 1994. doi: 10.1142/2138. (Cited on page 7.)

[GZ07] Mo-Lin Ge and Yong Zhang. GHZ States, Almost-Complex Structure and Yang–Baxter Equation. *Quantum Information Processing*, 6(5):363–379, October 2007. doi: 10.1007/s11128-007-0064-3. (Cited on page 7.)

[Hie93] Jarmo Hietarinta. Solving the two-dimensional constant quantum Yang-Baxter equation. *Journal of Mathematical Physics*, 34:1725–1756, May 1993. doi: 10.1063/1.530185. (Cited on pages 12 and 69.)

[Jim85] Michio Jimbo. A q-difference analogue of $U(\mathfrak{g})$ and the Yang-Baxter equation. *Letters in Mathematical Physics*, 10(1):63–69, July 1985. doi: 10.1007/BF00704588. (Cited on page 7.)

[Jim90] Michio Jimbo. *Yang-Baxter Equation In Integrable Systems*. Advanced Series In Mathematical Physics. World Scientific Publishing, March 1990. doi: 10.1142/1021. (Cited on page 7.)

[Jin03] Naihuan Jing. *Algebraic Combinatorics and Quantum Groups*. World Scientific Publishing, July 2003. doi: 10.1142/5331. (Cited on page 7.)

[KL02] Louis Kauffman and Samuel Lomonaco. Quantum entanglement and topological entanglement. *New Journal of Physics*, 4(1):73,

October 2002. doi: 10.1088/1367-2630/4/1/373. (Cited on page 7.)

[KL04] Louis Kauffman and Samuel Lomonaco. Braiding operators are universal quantum gates. *New Journal of Physics*, 6(1):134, October 2004. doi: 10.1088/1367-2630/6/1/134. (Cited on page 7.)

[KS97] Anatoli Klimyk and Konrad Schmüdgen. *Quantum Groups and Their Representations*. Texts and monographs in physics. Springer, March 1997. doi: 10.1007/978-3-642-60896-4. (Cited on page 7.)

[KSV18] Alexander Konovalov, Agata Smoktunowicz, and Leandro Vendramin. On skew braces and their ideals. *Experimental Mathematics*, pages 1–10, December 2018. doi: 10.1080/10586458.2018.1492476. (Cited on page 62.)

[Lau18] Ivan Lau. An Associative Left Brace is a Ring. arXiv: 1811.04894v3 [math.RA], November 2018. (Cited on pages 32 and 55.)

[Man18] Yuri Manin. *Quantum groups and non-commutative geometry (CRM Short Courses)*. Springer International Publishing, October 2018. doi: 10.1007/978-3-319-97987-8. (Cited on page 7.)

[MBBER18] Hang Yang Meng, Adolfo Ballester-Bolinches, and Ramon Esteban-Romero. Left Braces and the Quantum Yang–Baxter Equation. *Proceedings of the Edinburgh Mathematical Society*, page 1–14, December 2018. doi: 10.1017/S0013091518000664. (Cited on page 38.)

[MO12] Davesh Maulik and Andrei Okounkov. Quantum groups and quantum cohomology. arXiv: 1211.1287v3 [math.AG], November 2012. (Cited on page 7.)

[Pou18] Arash Pourkia. Solutions to the constant Yang–Baxter equation in all dimensions. arXiv: 1806.08400v1 [quant-ph], June 2018. (Cited on pages 7 and 12.)

[Rum07] Wolfgang Rump. Braces, radical rings, and the quantum Yang-Baxter equation. *Journal of Algebra*, 307(1):153 – 170, January 2007. doi: 10.1016/j.jalgebra.2006.03.040. (Cited on pages 8, 29, 30, 33, 37, and 39.)

[Rum08] Wolfgang Rump. Semidirect products in algebraic logic and solutions of the quantum Yang–Baxter equation. *Journal of Algebra and Its Applications*, 7(04):471–490, 2008. doi: 10.1142/S0219498808002904. (Cited on pages 8 and 41.)

[Skl90] Evgeny Sklyanin. Quantum version of the method of inverse scattering problem. In *Yang-Baxter Equation In Integrable Systems*, pages 121–171. World Scientific Publishing, 1990. doi: 10.1007/BF01091462. (Cited on page 7.)

[Smo18a] Agata Smoktunowicz. A note on set-theoretic solutions of the Yang–Baxter equation. *Journal of Algebra*, 500:3 – 18, April 2018. doi: 10.1016/j.jalgebra.2016.04.015. (Cited on page 58.)

[Smo18b] Agata Smoktunowicz. On Engel groups, nilpotent groups, rings, braces and the Yang-Baxter equation. *Transactions of the American Mathematical Society*, 370(9):6535–6564, March 2018. doi: 10.1090/tran/7179. (Cited on page 8.)

[SS17] Agata Smoktunowicz and Alicja Smoktunowicz. Set-theoretic solutions of the Yang-Baxter equation and new classes of R-matrices. arXiv: 1704.03558v3 [math.RA], April 2017. (Cited on page 13.)

[SS18] Agata Smoktunowicz and Alicja Smoktunowicz. Set-theoretic solutions of the Yang–Baxter equation and new classes of R-matrices. *Linear Algebra and its Applications*, 546:86–114, 2018. doi: 10.1016/j.laa.2018.02.001. (Cited on pages 13, 21, 22, 23, and 24.)

[Tur92] Vladimir Turaev. Modular categories and 3-manifold invariants. *International Journal of Modern Physics B*, 06(11-12):1807–1824, 1992. doi: 10.1142/S0217979292000876. (Cited on page 7.)

[Wen98] Hans Wenzl. C^*-tensor categories from quantum groups. *Journal of the American Mathematical Society*, 11(2):261–282, April 1998. doi: 10.1090/S0894-0347-98-00253-7. (Cited on page 7.)

[Yan67] Chen-Ning Yang. Some exact results for the many-body problem in one dimension with repulsive delta-function interaction. *Physical Review Letters*, 19(23):1312–1315, December 1967. doi: 10.1103/PhysRevLett.19.1312. (Cited on page 7.)

[Yet90] David Yettera. Quantum groups and representations of monoidal categories. *Mathematical Proceedings of the Cambridge Philosophical Society*, 108(2):261–290, 1990. doi: 10.1017/S0305004100069139. (Cited on page 7.)

[ZZ79] Alexander Zamolodchikov and Alexey Zamolodchikov. Factorized s-matrices in two dimensions as the exact solutions of certain relativistic quantum field theory models. *Annals of Physics*, 120(2):253 – 291, 1979. doi: 10.1016/0003-4916(79)90391-9. (Cited on page 7.)