Set-theoretic solutions of the Yang-Baxter equation and new classes of R-matrices

Agata Smoktunowicz [a,*], Alicja Smoktunowicz [b,**]

[a] *School of Mathematics, University of Edinburgh, Edinburgh EH9 3JZ, Scotland, United Kingdom*
[b] *Faculty of Mathematics and Information Science, Warsaw University of Technology, Koszykowa 75, 00-662 Warsaw, Poland*

Abstract

We describe several methods of constructing R-matrices that are dependent upon many parameters, for example unitary R-matrices and R-matrices whose entries are functions. As an application, we construct examples of R-matrices with prescribed singular values. We characterise some classes of indecomposable set-theoretic solutions of the quantum Yang-Baxter equation (QYBE) and construct R-matrices related to such solutions. In particular, we establish a correspondence between one-generator braces and indecomposable, non-degenerate involutive set-theoretic solutions of the QYBE, showing that such solutions are abundant. We show that R-matrices related to involutive, non-degenerate solutions of the QYBE have special form. We also investigate some linear algebra questions related to R-matrices.

Keywords: R-matrices, the quantum Yang-Baxter equation, set-theoretic solution, nilpotent rings, braces, singular values
2010 MSC: 15A69, 15A19, 16T25, 16T99, 16N20, 16N20, 16N40

1. Introduction

The quantum Yang-Baxter equation is an important equation in mathematics and physics. It is relevant to statistical mechanics, quantum information science and numerous other research areas. Recall that a nonsingular $n^2 \times n^2$ matrix is called an R-matrix when it satisfies the quantum Yang-Baxter equation:

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

where I is the $n \times n$ identity matrix. In this paper, we will provide examples of R-matrices with prescribed singular values. Many of our R-matrices are

*Principal corresponding author
**Corresponding author
Email addresses: A.Smoktunowicz@ed.ac.uk (Agata Smoktunowicz), smok@mini.pw.edu.pl (Alicja Smoktunowicz)

constructed using set-theoretic solutions of the quantum Yang-Baxter equation, and have only one nonzero element in each column. This type of matrices appear frequently in the literature, for example in [17], where Baxterisation of some R-matrices of this type was obtained, and in [29], where they appear as universal gates for the quantum computation related to the circuit model (see Theorem 1, [29]). In [38, 24, 21] they appear in connection with Braid groups and topological quantum computation (see also [7, 35, 36, 31]). They also appear as *combinatorial R-matrices* in the theory of crystal bases, geometric crystals and box-bell systems. The R-matrices related to involutive, non-degenerate set-theoretic solutions of the QYBE give cocycles into abelian groups [20], therefore they can be given as an input in the construction of universal R-matrices and twists for Hopf algebras, for example as in Theorem 4.2, [18].

Most of the R-matrices constructed in our paper are unitary. A unitary R-matrix leads to a unitary representation of the Braid group, and the resulting unitary matrices associated to braids can be used to process quantum information [38, 15, 21]. In connection with the topological quantum computation, it was conjectured in [24, 42] that a single unitary R-matrix can generate only finite representations of Braid groups, and in [24] it was confirmed in several important classes of R-matrices. In [40], Rowell made the following comment: "From the quantum information point of view, a unitary R-matrix can be used to directly simulate topological quantum computers on the quantum circuit model. More recently people have begun to study what extra gates one needs to supplement braiding with in order to achieve universality (see e.g. [16]). If a single R-matrix can only generate a (nearly) finite group, can an additional small gate lead to a universal gate set?". This question provides the inspiration for our construction of R-matrices with many parameters. All of our examples are locally monomial BVS (we recall the definition in Section 2).

Recall that locally monomial braided vector spaces (BVS) were introduced by Galindo and Rowell in [24], and localisation was introduced by Rowell and Wang in Definition 2.3 in [42]. A related notion of braided vector space of set-theoretic type appeared in [1] in the context of Nichols algebras (note that every braided vector space of set-theoretic type is locally monomial). In [23], Galindo, Hong and Rowell generalized the idea of localisation in two ways, and in [24] Galindo and Rowell remarked that it is feasible that the monomial and Gaussian BVS generate a large proportion of the unitary braided vector spaces (e.g. through quotients and subrepresentations). They also mentioned that they are not aware of any unitary braided vector spaces that do not come from these two families. Recall that Gaussian braided vector spaces were introduced 28 years ago by Goldschmidt and Jones, and since then have been investigated by many authors (see for example [24, 41]). Since only these two classes of unitary R-matrices are known so far, and the Gaussian class is well understood, it seems natural to investigate methods of construction of locally monomial BVS; it is the primary motivation of our paper. We will mainly investigate unitary R-matrices related to locally monomial BVS which are constructed using braces. Recall that braces were introduced by Rump [43] in 2005.

The contents of the chapters are as follows: Section 2 contains background

information. Section 3 investigates linear algebra and matrix theory aspects related to R-matrices. Section 4 gives new examples of unitary R-matrices constructed by using set-theoretic solutions of the QYBE (all of the examples are locally monomial). Section 4 also describes some general methods of constructing unitary locally monomial BVS by using orbits by analogy with cohomology of racks and cycle sets considered in [10, 37], and by introducing I-retraction, as a generalisation of the retraction technique from [20]. In the final section we give concrete examples of R-matrices of small dimension illustrating results obtained in this paper.

An additional motivation for our paper is related to the well-known characterisation of indecomposable solutions of prime order, obtained in [19] and [20]. Recall that in [19], Etingof, Guralnick and Soloviev showed that all indecomposable non-degenerate set-theoretic solutions of the QYBE of prime cardinality are affine, and in [20], Etingof, Schedler and Soloviev showed that all indecomposable involutive non-degenerate solutions of the QYBE of prime cardinality are the cyclic permutation solutions. In Sections 5 and 6 we investigate whether it is possible to obtain an analogous characterisation of indecomposable solutions of arbitrary cardinality. We show that every one-generator brace yields a non-degenerate, involutive, indecomposable solution of the QYBE, and for multipermutation solutions all indecomposable solutions are of this form. We also show that one-generator braces and hence non-degenerate, involutive, indecomposable solutions of the QYBE are abundant. This gives a strong indication that it would be impossible to generalise the results from [19] and [20] to arbitrary cardinalities. As an application, in Section 7 we use our results to construct unitary R-matrices related to indecomposable solutions. In Section 8, we give a simple criterion for whether a given R-matrix is related to a brace; this observation relies on the result of Jespers and Okniński that finite involutive, set-theoretic solutions of the QYBE are left non-degenerate if and only if they are right non-degenerate.

In integrable systems a different type of the quantum Yang-Baxter equation is used, called the parametrized quantum Yang-Baxter equation (see pages 295-297, [30]). Often, the following form of this equation is used $(R(u) \otimes I)(I \otimes R(u+v))(R(v) \otimes I) = (I \otimes R(v))(R(u+v) \otimes I)(I \otimes R(u))$ where u and v are complex variables. Many of the examples of R-matrices obtained in our paper satisfy $R^2 = I$. By using analogous methods as on page 296 [30] it can be shown that if R is an R-matrix such that $R^2 = I$ then $I + uR$ is a solution of the above parametrized QYBE (see Proposition 18). Applications of such R-matrices are discussed in Section 8.7.3 [30].

Observe also that, by combining Proposition 2.9 from [9] (and its proof) with Examples 7, 8 from our paper, we can construct extensions of set-theoretic solutions of the QYBE, in particular we can embed involutive solutions in non-involutive solutions of the QYBE. In [47, 4, 37] extensions of set-theoretic solutions have been used to construct special types of involutive solutions.

In this paper we use the connection of non-degenerate, involutive set-theoretic solutions with nilpotent rings and braces discovered by Rump in 2007 [43]. A related concept of F-braces, introduced in [12], has recently found applications

in cryptography [8]. In [11] examples of F-braces have been constructed by using 2-cocycles.

2. Background information

Here we recall basic information about braces, skew braces, locally monomial braided vector spaces and indecomposable solutions of the quantum Yang-Baxter equation.

We say that $X \in \mathbb{C}^{\mathrm{n}^2 \times \mathrm{n}^2}$ satisfies the quantum Yang-Baxter Equation (QYBE) if

$$(X \otimes I_n)(I_n \otimes X)(X \otimes I_n) = (I_n \otimes X)(X \otimes I_n)(I_n \otimes X), \tag{1}$$

where I_n denotes the $n \times n$ identity matrix, and $A \otimes B$ is the Kronecker product (tensor product) of the matrices A and B: $A \otimes B = (a_{i,j}B)$. That is, the Kronecker product $A \otimes B$ is a block matrix whose (i, j) blocks are $a_{i,j}B$.

Solutions of the quantum Yang-Baxter equation (1) have many interesting properties:

- If $X \in \mathbb{C}^{\mathrm{n}^2 \times \mathrm{n}^2}$ satisfies the QYBE (1), then X^* also satisfies (1).
- If $X \in \mathbb{C}^{\mathrm{n}^2 \times \mathrm{n}^2}$ is an R-matrix, then X^{-1} is an R-matrix.
- If $X \in \mathbb{C}^{\mathrm{n}^2 \times \mathrm{n}^2}$ satisfies the QYBE (1), then $\alpha\, X$ satisfies the QYBE (1) for every $\alpha \in \mathbb{C}$.
- If $X \in \mathbb{C}^{n^2 \times n^2}$ satisfies the QYBE (1) and $P \in \mathbb{C}^{n \times n}$ is arbitrary nonsingular matrix, then
$$\hat{X} = (P \otimes P)X(P \otimes P)^{-1}$$
also satisfies the QYBE (1).

The references to the above properties can be found, for example, in [22, 34].

However, it is not true that if $X \in \mathbb{C}^{n^2 \times n^2}$ is an R-matrix and $P, Q \in \mathbb{C}^{n \times n}$, $P \neq Q$ are arbitrary nonsingular matrices, then $\bar{X} = (P \otimes Q)X(P \otimes Q)^{-1}$ is an R-matrix.

2.1. Set-theoretic solutions

Let X be a non-empty set. Let $r : X \otimes X \to X \otimes X$ be a bijective map and write

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

We say that (X, r) is a set-theoretic solution of the quantum Yang-Baxter equation if

$$r_1 r_2 r_1 = r_2 r_1 r_2,$$

where $r_1 = r \times id_X : X \times X \times X \to X \times X \times X$ and $r_2 = id_X \times r : X \times X \times X \to X \times X \times X$. We say that (X, r) is right non-degenerate if $\sigma_x \in Sym(X)$, for all $x \in X$, (Sym (X) denotes the set of all permutations of the set X); similarly (X, r) is left non-degenerate if $\tau_x \in Sym(X)$, for all $x \in X$. We say that (X, r) is

a non-degenerate involutive set-theoretic solution of the quantum Yang-Baxter equation if $r^2 = id_{X\times X}$ and $\sigma_x, \tau_x \in Sym(X)$, for all $x \in X$.

Let V be the linear space spanned by the elements of X over the field of complex numbers. By $\bar{r} : V \otimes V \to V \otimes V$ we will denote the *linearisation* of r, i.e. the linear map such that

$$\bar{r}(x \otimes y) = \sigma_x(y) \otimes \tau_y(x).$$

Let (X, r) be a set-theoretic solution of the quantum Yang-Baxter equation, then $(V, \bar{r})$ is a solution of the QYBE.

Let (X, r) be a non-degenerate solution of the QYBE. We say that (X, r) is *decomposable* if there exist non-empty subsets $X_1, X_2 \subseteq X$ such that $X = X_1 \cup X_2$ and $r(X_i, X_j) = (X_j, X_i)$ for all $i, j \leq 2$. If it is not possible to find such subsets $X_1, X_2 \subseteq X$ the solution (X, r) is *indecomposable*. In [20] Etingof, Schedler and Soloviev proved that a finite non-degenerate solution (X, r) is indecomposable if and only if X cannot be presented as a union of two non-empty sets Y_1, Y_2 such that $r(Y_1, Y_1) = (Y_1, Y_1)$ and $r(Y_2, Y_2) = (Y_2, Y_2)$. Let $z \in X$. By the *orbit* of z we will mean the smallest set $Y \subseteq X$ such that $z \in Y$ and $\sigma_x(y) \in Y$ and $\tau_x(y) \in Y$, for all $y \in Y, x \in X$.

2.2. Locally monomial BVS

Let V be a linear space over a field F, where, unless otherwise specified, $F = \mathbb{C}$. Let $I_V : V \to V$ be the identity map on V. Recall that a linear authomorphism $c : V \otimes V \to V \otimes V$ satisfies the quantum Yang-Baxter equation if

$$(c \otimes I_V)(I_V \otimes c)(c \otimes I_V) = (I_V \otimes c)(c \otimes I_V)(I_V \otimes c).$$

In this case the pair (V, r) will be called a braided vector space (BVS).

Let (X, r) be a set-theoretic solution of the QYBE, and denote as usually

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

Definition 1. *[Definition 5.8, [1]] Let (X, r) be a set-theoretic solution of the QYBE and let $D = \{d_{(x,y)}\}_{x,y\in X}$, where $0 \neq d_{i,j} \in \mathbb{C}$. Let V be the linear space over $\mathbb{C}$ spanned by elements of X. We say that the data (X, r^D) is* **a braided vector space of set-theoretic type** *if the linear map $r_D : V \otimes V \to V \otimes V$ defined by*

$$r_D(x \otimes y) = d_{(x,y)}\sigma_x(y) \otimes \tau_y(x)$$

satisfies the QYBE. Given (X, r) and D by (X, r^D), we will always mean the linear space V and map r^D as above.

Let (X, r) be a set-theoretic solution of the QYBE. In the remainder of this subsection we will also use the following notation

$$r(x, y) = ({}^x y, x^y)$$

so ${}^x y = \sigma_x(y)$ and $x^y = \tau_y(x)$. We will use it because it is easier to read in Lemma 2. This notation appears in many papers, for example [27].

We recall a special case of Lemma 5.7 from [1]:

Lemma 2. *[Lemma 5.7, [1]] Let (X, r) be a non-degenerate, set-theoretic solution of the quantum Yang-Baxter equation. Let $f : X \otimes X \to \mathbb{C}$ be a mapping, and assume that f takes only nonzero values. Then the following statements are equivalent:*

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

$$f(x, y) \cdot f(x^y, z) \cdot f({}^x y, {}^{x^y} z) = f(y, z) \cdot f(x, {}^y z) \cdot f(x^{{}^y z}, y^z).$$

- *The linear mapping $c : V \otimes V \to V \otimes V$ given by $c(x \otimes y) = f(x, y)^x y \otimes x^y$ satisfies the quantum Yang-Baxter equation.*

The R-matrix of a braided vector space (X, r^D) of set-theoretic type is obtained in the following way (see [6] pages 94, 95).

Definition 3. *Let (X, r^D) be a braided vector space of set-theoretic type, where (X, r) is a set-theoretic solution of the QYBE and $D = \{d_{(x,y)}\}_{x,y \in X}$. Let $X = \{x_1, \ldots, x_n\}$ and let Y be the set of pairs (i, j), with $1 \leq i, j \leq n$, written in the lexicographical ordering. Then M has rows and columns indexed by the set Y, and the entry at the intersection of the column indexed by (i, j) and the row indexed by (k, l) equals $d_{(x_i, x_j)}$ if $r(x_i, x_j) = (x_k, x_l)$ and 0 otherwise. This entry will be denoted by $m_{i,j}^{k,l}$.*

The method of writing the R-matrix related to a set-theoretic solution (X, r) of the QYBE is the same, as for (X, r^D) where all elements $d_{x,y}$ in D are 1.

We now recall the definition of *locally monomial BVS* from [24].

Definition 4. *Let V be a vector space over a field F. Let (V, c) be a braided vector space. We say that (V, r) is a* **locally monomial BVS** *if there is a basis $X = \{x_1, \ldots, x_n\}$ of V such that for each $i, j \leq n$ there are $k, l \leq n$ and $d_{i,j} \in F$ such that $c(x_i \otimes x_j) = d_{i,j}(x_k \otimes x_l)$. Note that, with respect to the base X, (V, r) is a braided vector space of set-theoretic type (X, r^D) for some bijective map $r : X \times X \to X \times X$ and some $D = \{d_{(x,y)}\}_{x,y \in X}$.*

Let (V, c) be a braided vector space, then the matrix of the map $c : V \otimes V \to V \otimes V$ in the base V will be called a *locally monomial R-matrix*. Note that an n^2 by n^2 R-matrix A is *locally monomial* if $A = (P \otimes P)B(P^{-1} \otimes P^{-1})$ for some nonsingular n by n matrix P and where B is an R-matrix of some braided vector space (X, r^D) of set-theoretic type. Notice that B is obtained by modifying nonzero entries of a permutation matrix.

Definition 5. *Let (X, r^D) be a braided vector space of set-theoretic type. We say that (X, r^D) is trivial if there are nonzero complex numbers α_x for $x \in X$ and a constant c such that*

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

Notice that this is equivalent to the condition that there is a nonsingular diagonal n by n matrix P and a constant c such that $\bar{M} = c \cdot (P^{-1} \otimes P^{-1}) M (P \otimes P)$,

where M is the matrix associated to the solution (X,r) (as below Definition 3) and $\bar{M}$ its matrix related to braided vectors space of set-theoretic type (X,r^D) (as in Definition 3).

Lemma 6. *Let (X,r) be an involutive set-theoretic solution of the QYBE, and let (X,r^D) be a braided vector space of set-theoretic type; then $d_{(x,y)}d_{(\sigma_x(y),\tau_y(x))} = c^2$ for all $x,y \in X$ for some constant c (this can be also written as $d_{(x,y)}d_{r(x,y)} = c^2$).*

Proof. It follows from Definition 5 and the fact that $r(r(x,y)) = (x,y)$ since r is involutive. □

Lemma 7. *Let (X,r) be a set-theoretic solution of the QYBE. Let $f : X \times X \to \mathbb{C}$ be a mapping such that, for all $x,y,z \in X$,*

$$f(x,y) = f(x^{{}^{y}z}, y^z), f(x^y, z) = f(x, {}^{y}z), f({}^{x}y, {}^{x^y}z) = f(y,z).$$

Denote $D = \{d_{(x,y)}\}_{\{x,y\in X\}}$, where $d_{(x,y)} = f(x,y)$ for $x,y \in X$; then (X,r^D) is a braided vectors space of set-theoretic type. If (X,r) is a non-degenerate involutive solution of the QYBE, and $f(x,y)f({}^{x}y, x^y)$ is not constant for $x,y \in X$, then (X,r^D) is not trivial.

Proof. It follows from Lemmas 2 and 6. □

2.3. Braces and skew braces

We now recall some basic information about braces and skew-braces. The research area started around 2005, when Wolfgang Rump showed some surprising connections between Jacobson radical rings and solutions to the quantum Yang-Baxter equation. In [44], Rump introduced braces, a generalisation of Jacobson radical rings, as a tool to investigate non-degenerate, involutive set-theoretic solutions of the quantum Yang-Baxter equation, and showed the correspondence between such solutions and braces. Skew braces were recently introduced by Guarnieri and Vendramin to investigate set-theoretic solutions of the QYBE which are not involutive. In [43] Rump showed that every solution (X,r) can be in a good way embedded in a brace.

Definition 8 (Proposition 4, [43]). *A* left brace *is an abelian group $(A;+)$ together with a multiplication $\cdot$ such that the circle operation $a \circ b = a \cdot b + a + b$ makes A into a group, and $a \cdot (b+c) = a \cdot b + a \cdot c$.*

In many papers, the following equivalent definition from [14] is used:

Definition 9 ([14]). *A* left brace *is a set G together with binary operations $+$ and $\circ$ such that $(G,+)$ is an abelian group, $(G,\circ)$ is a group, and $a \circ (b+c) + a = a \circ b + a \circ c$ for all $a,b,c \in G$.*

The additive identity of a brace A will be denoted by 0 and the multiplicative identity by 1. In every brace $0 = 1$. The same notation will be used for skew braces (in every skew brace $0 = 1$). Let A be a left brace. The *socle* of A is $Soc(A) = \{a \in A : a \circ b = a + b \text{ for all } b \in A\} = \{a \in A : a \cdot b = 0 \text{ for all } b \in A\}$.

Remark 1. *Some authors use the notation $\cdot$ instead of $\circ$ and $*$ instead of $\cdot$ (see for example [14, 27]).*

It was observed by Rump that every nilpotent ring is a brace. Let R be a nilpotent ring (associative, and not necessarily commutative) and let n be such that $R^n = 0$. It was shown by Rump [43] that R yields a solution $r : R \times R \to R \times R$ to the quantum Yang-Baxter equation with $r(x, y) = (u, v)$, where $u = x \cdot y + y$, $v = z \cdot x + x$ and $z = \sum_{i=1}^{n} (-1)^i u^i$.

Let R be either a left brace or a ring, and let $C, D \subseteq R$; then CD denotes the set consisting of finite sums of elements cd with $c \in C, d \in D$.

Definition 10. *A left brace R is left nilpotent if $R^n = 0$ for some n where $R^1 = R$ and $R^{i+1} = R \cdot R^i$. A left brace is right nilpotent if $R^{(n)} = 0$ for some n where $R^{(1)} = R$ and $R^{(i+1)} = R^{(i)} \cdot R$. Radical chains R^i and $R^{(i)}$ were introduced by Rump in [43].*

Theorem 11. *[43] Let (X, r) be a non-degenerate, involutive, set-theoretic solution of the QYBE. Then there exists a left brace A with multiplication $\cdot$ and addition $+$ such that $X \subseteq A$ and*

$$r(x, y) = (x \cdot y + y, z \cdot x + x),$$

for $x, y \in A$, where $z \cdot (x \cdot y + y) + z + x \cdot y + y = 0$ for $x, y \in A$ (in each left brace A such z exists and is unique). Moreover, the groups $(A, \circ)$ and $(A, +)$ are generated by elements from X.

Proposition 12. *[13] Let notation be as in Theorem 11, if X is finite then A can be chosen to be finite.*

The fact that $(A, \circ)$ is generated by X follows because A is a factor of the structure group of X [13, 14]. The structure group of a non-degenerate set-theoretic solution (X, r) is the group generated by elements of X subject to all relations $xy = uv$ where $r(x, y) = (u, v)$ (this group was introduced in [20]). The permutation group of a solution (X, r) is the group generated by mappings σ_x where $r(x, y) = (\sigma_x(y), \tau_y(x))$. The permutation group first appeared as a tool in the proof of Theorem 2.15 in [20], without a concrete name but with the notation G_X^0. In [25] the name *permutation group* was introduced and this group was explicitly investigated.

Definition 13. *Let A be a brace, and for $x, y \in A$ define*

$$r'(x, y) = (x \cdot y + y, z \cdot x + x),$$

where z is such that $z \cdot (x \cdot y + y) + z + x \cdot y + y = 0$ for $x, y \in A$. We will say that $r' : A \times A \to A \times A$ is the **Yang-Baxter map associated to** *A. Let $X \subseteq A$; we will say that $r : X \times X \to X \times X$ is a* **restriction of** *r' if $r(x, y) = r'(x, y)$ for all $x, y \in X$.*

In [20], Etingof, Schedler and Soloviev introduced the retract relation for any solution (X, r). Denote $X = \{x_1, \dots, x_n\}$ and $r(x, y) = (\sigma_x(y), \tau_y(x))$. Recall that the retract relation $\sim$ on X is defined by $x_i \sim x_j$ if $\sigma_i = \sigma_j$. The induced solution $Ret(X, r) = (X/\sim, r^{\sim})$ is called the *retraction* of X. A solution (X, r) is called a *multipermutation solution of level m* if m is the smallest nonnegative integer such that after m retractions we obtain the solution with one element. By $mpl(X, r)$ we will denote the multipermutation level of (X, r).

We now recall the definition of a skew brace. Skew braces also yield non-degenerate solutions of the QYBE (see [28]).

Definition 14. *[28] A* skew brace *is a set G together with binary operations $+$ and $\circ$ such that $(G, +)$ is a group, $(G, \circ)$ is a group, and $a \circ (b + c) = a \circ b + (-a) + a \circ c$ for all $a, b, c \in G$. Here $(-a)$ is the inverse of a in the additive group of G, so $a + (-a) = 0$.*

Notice that the group $(A, +)$ need not be commutative; for this reason some authors prefer to use the notation $\cdot$ instead of $+$ in the definition of skew braces [28, 46].

3. Matrix theory observations

In this section we consider the Hadamard product of $A, B \in \mathbb{C}^{\mathrm{m}\times\mathrm{n}}$: $A \circ B = (a_{i,j} b_{i,j})$.

Proposition 15. *Let A, B be R-matrices, such that when we put all nonzero entries of these matrices to 1 the obtained matrix is the same for both matrices A and B, and it is a permutation matrix. Then the Hadamard product of A and B is also an R-matrix.*

Proof. A is an n^2 by n^2 matrix for some n. We can assume that the rows and columns of A are indexed by the set of pairs (i, j) with $i, j \leq n$ in the lexicographical ordering. Denote $X = \{1, \dots, n\}$. Recall that A satisfies QYBE, is non-singular and has exactly one nonzero-element in each column. It follows that A can be obtained as in Definition 3 from some braided vectors space of set-theoretic type (X, r^D) for some $D = \{f(x, y)\}_{x,y\in X}$. Denote by $a_{i,j}^{k,l}$ the entry at the intersection of the (i, j)-th column and (k, l)-th row of A. By Definition 3, $r(i, j) = (k, l)$ if and only if $a_{i,j}^{k,l} \neq 0$. Denote $r(x, y) = ({}^x y, x^y)$. Since A is an R-matrix, the linear mapping $c(x \otimes y) = f(x, y)^x y \otimes x^y$ satisfies QYBE where $f(x, y) = a_{x,y}^{r(x,y)}$.

Similarly, B is the matrix related to some braided vector space of set-theoretic type $(X, \tilde{r}^{D'})$ for some $\tilde{r}$ and some $D' = \{f'(x, y)\}_{x,y\in X}$, where rows and columns of B are indexed by pairs (i, j) with $i, j \leq n$. Denote by $b_{i,j}^{k,l}$ the entry at the intersection of the (i, j)-th column and (k, l)-th row of B. By Definition 3, $\tilde{r}(i, j) = (k, l)$ if and only if $b_{i,j}^{k,l} \neq 0$, hence $r = \tilde{r}$ (by assumption A and B have non-zero entries at the same places). Recall that $r(x, y) = ({}^x y, x^y)$. Since A is an R-matrix, the linear mapping $c'(x \otimes y) = f'(x, y)^x y \otimes x^y$ satisfies QYBE where $f'(x, y) = b_{x,y}^{r(x,y)}$.

By Lemma 2, for every $x, y, z \in X$

$$f(x,y) \cdot f(x^y, z) \cdot f({}^x y, {}^{x^y} z) = f(y,z) \cdot f(x, {}^y z) \cdot f(x^{{}^y z}, y^z).$$

Similarly,

$$f'(x,y) \cdot f'(x^y, z) \cdot f'({}^x y, {}^{x^y} z) = f'(y,z) \cdot f'(x, {}^y z) \cdot f'(x^{{}^y z}, y^z).$$

By multiplying these two equations, we get

$$g(x,y) \cdot g(x^y, z) \cdot g({}^x y, {}^{x^y} z) = g(y,z) \cdot g(x, {}^y z) \cdot g(x^{{}^y z}, y^z)$$

where $g(x,y) = f'(x,y)f'(x,y) = a_{(x,y)}^{r(x,y)} b_{(x,y)}^{r(x,y)}$. Denote $D'' = \{g(x,y)\}_{x,y \in X}$. By Lemma 2, $(X, r^{D''})$ is a braided vector space of set-theoretic type. By Definition 3, the R-matrix related to $(X, r^{D''})$ equals $A \circ B$, consequently the matrix $A \circ B$ satisfies the QYBE. $\square$

Proposition 16. *Let A be an R-matrix such that when we put all its nonzero entries to 1 the obtained matrix is a permutation matrix. Let $G : \mathbb{C} \to \mathbb{C}$ be a function with nonzero values such that $G(pq) = G(p)G(q)$ for all $p, q \in \mathbb{C}$. If A has entries $a_{i,j}$, then the matrix whose i,j-th entry is $G(a_{i,j})$ (for each i,j) is an R-matrix.*

Proof. Let the first 9 lines be as in the proof of Proposition 15. By Lemma 2, for every $x, y, z \in X$

$$f(x,y) \cdot f(x^y, z) \cdot f({}^x y, {}^{x^y} z) = f(y,z) \cdot f(x, {}^y z) \cdot f(x^{{}^y z}, y^z).$$

By applying function G to both sides of this equation we get

$$G(f(x,y)) \cdot G(f(x^y, z)) \cdot G(f({}^x y, {}^{x^y} z)) = G(f(y,z)) \cdot G(f(x, {}^y z)) \cdot G(f(x^{{}^y z}, y^z)).$$

By Lemma 2, $(X, r^{D'})$ is a braided vector space of set-theoretic type, where $D' = \{G(f(x,y))\}_{x,y \in X}$. Therefore the matrix whose i,j-th entry is $G(a_{i,j})$ (for each i,j) is an R-matrix. $\square$

The next example shows that Propositions 15 and 16 need not hold in general for arbitrary R-matrices A and B.

Example 1. *Let*

$$X = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -3 & 2 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Then $detX = -4$ and X is an R-matrix. We can verify that the Hadamard product $X \circ X$ is not an R-matrix.

It is a simple matter to prove the following facts using known properties of the Kronecker products.

Proposition 17. *Let $C, D \in \mathbb{C}^{n\times n}$. Then $X = C \otimes D$ satisfies the quantum Yang-Baxter equation (1) if and only if $C^2 \otimes DCD \otimes D = C \otimes CDC \otimes D^2$.*

Notice that Proposition 17 implies that the Kronecker product of locally monomial matrices need not be an R-matrix.

The next example shows that if $X \in \mathbb{C}^{n^2\times n^2}$ is a singular solution of the QYBE (1) then $X^\dagger$, called the Moore-Penrose pseudo-inverse of X, may not satisfy (1). We recall the $X^\dagger$ is uniquely determined by the following conditions: $XX^\dagger X = X$, $X^\dagger XX^\dagger = X^\dagger$, $X^\dagger X = (X^\dagger X)^*$ and $XX^\dagger = (XX^\dagger)^*$.

Example 2. *Let*

$$C = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

It is easily seen at once that $C^2 = C$, so C is an idempotent matrix (a projection). Now we define $X = C \otimes I_4$. By Propositon 17 X satisfies the QYBE (1) and we have $X^\dagger = C^\dagger \otimes I_4$, where

$$C^\dagger = \frac{1}{3}\begin{pmatrix} 2 & -1 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

A simple verification show that $C^\dagger$ is not an idempotent matrix, so by Proposition 17, $X^\dagger$ is not a solution of the QYBE (1).

By I_n we will denote the $n \times n$ identity matrix. Notice that, by proceeding analogously as on page 296 [30], we get the following observation:

Proposition 18. *Let n be a natural number and let A be an $n^2 \times n^2$ R-matrix such that A^2 is the identity matrix. For each $\alpha \in \mathbb{C}$ the matrix $R(x) = I_{n^2} + \alpha x A$ is a solution of the parameter-dependent Yang-Baxter equation (where x is the variable):*

$$(R(x) \otimes I_n)(I_n \otimes R(x+y))(R(y) \otimes I_n) = (I_n \otimes R(y))(R(x+y) \otimes I_n)(I_n \otimes R(x)).$$

Proof. Observe that $I_n \otimes I_{n^2} = I_{n^2} \otimes I_n = I_{n^3}$. Note that $(\alpha x R \otimes I_n) = \alpha x (R \otimes I_n)$ and hence

$$(\alpha x R \otimes I_n)(I_n \otimes \alpha(x+y)R)(I_{n^2} \otimes I_n) = (I_n \otimes I_{n^2})(\alpha(x+y)R \otimes I_n)(I_n \otimes \alpha x R).$$

Similarly,

$$(I_{n^2} \otimes I_n)(I_n \otimes \alpha(x+y)R)(\alpha y R \otimes I_n) = (I_n \otimes \alpha y R)(\alpha(x+y)R \otimes I_n)(I_n \otimes I_{n^2}),$$

$$(\alpha x R \otimes I_n)(I_n \otimes I_{n^2})(\alpha y R \otimes I_n) = \alpha^2 xy I_{n^3} = (I_n \otimes \alpha y R)(I_{n^2} \otimes I_n)(I_n \otimes \alpha x R).$$

Observe also that $(\alpha x R \otimes I_n)(I_n \otimes I_{n^2})(I_{n^2} \otimes I_n) + (I_{n^2} \otimes I_n)(I_n \otimes I_{n^2})(\alpha y R \otimes I_n) = (I_n \otimes I_{n^2})(\alpha(x+y)R \otimes I_n)(I_n \otimes I_{n^2})$ and $(I_{n^2} \otimes I_n)(I_n \otimes \alpha(x+y)R)(I_{n^2} \otimes I_n) = (I_n \otimes \alpha y R)(I_{n^2} \otimes I_n)(I_n \otimes I_{n^2}) + (I_n \otimes I_{n^2})(I_{n^2} \otimes I_n)(I_n \otimes \alpha x R)$. We can sum all of these equations. The thesis now follows from the fact that R and I_{n^2} are R-matrices, and from the fact that the Kronecker product is distributive. □

4. Some methods of constructing locally monomial R-matrices

4.1. Orbits of set-theoretic solutions and related R-matrices

The following Proposition 19 was inspired by results on to the second cohomology group of racks [10] (see Proposition 3.8) and on the second Yang-Baxter cohomology group of left non-degenerate cycle sets [37] (see Lemma 9.17). Notice however that our proposition also holds for solutions which are not necessarily left non-degenerate.

Let notation be as in subsections 2.2 and 2.3. By $\mathbb{C}$ we will denote the field of complex numbers.

Proposition 19. *Let F be a field. Let (X, r) be a set-theoretic solution of the quantum Yang-Baxter equation, $\bar{r} : V \otimes V \to V \otimes V$ be the linearisation of r and let $X_1, \dots, X_m \subseteq X$ be such that*

- *$X = \bigcup_{i=1}^{m} X_i$ and $X_i \cap X_j = \emptyset$ for all $i < j \leq m$ and*
- *$r(X_i, X_j) = (X_j, X_i)$ for all $i, j \leq m$.*

Let $0 \neq \alpha_{i,j} \in F$ and let $r' : V \otimes V \to V \otimes V$ be the linear mapping such that $r'(x, y) = \alpha_{i,j}\bar{r}(x \otimes y)$ for $x \in X_i$ and $y \in X_j$. Then r' satisfies the quantum Yang-Baxter equation.

Proof. It follows from Lemma 2 (Lemma 5.7 in [1]). □

Example 3 illustrates the use of orbits as sets X_i, vis-à-vis Proposition 19 (the definition of orbits is recalled in Subsection 2.1).

Which subsets of braces give solutions of the quantum Yang-Baxter equation? Below we give some examples of such sets and construct braided vector spaces of set-theoretic type on them using Proposition 19. Some answers to this question can also be found in [3].

Example 3. Let R be a finite left brace and let r' be the associated Yang-Baxter map (defined as in Section 2.3). For $b \in R$, define $Q_b = \{b + ab : a \in R\}$. Notice that for $b, c \in R$ either $Q_b = Q_c$ or $Q_b \cap Q_c = \emptyset$. Let $b_1, b_2, \dots, b_m \in R$ be such that the sets $Q_{b_1}, Q_{b_2}, \dots, Q_{b_m}$ are pairwise distinct. For $i \leq m$ denote $X_i = Q_{b_i}$ and $X = \bigcup_{i \leq m} X_i$. Then $r'(X_i, X_j) = (X_j, X_i)$ for all $i, j \leq m$ and $X_i \cap X_j = 0$ for $i < j \leq m$. Let $r : X \times X \to X \times X$ be a restriction of r', then (X, r) is a non-degenerate involutive solution of the QYBE.

Example 4. Let A be a finite left brace which is a left nilpotent brace (for example a nilpotent ring) and r' be the associated Yang-Baxter map. Let m be a natural number such that $A^m = 0$ and $A^{m-1} \neq 0$. For $i \leq m$ denote $X_i = \{x \in A : x \in A^i, x \notin A^{i+1}\}$ and $X = \bigcup_{i \leq m} X_i$. Then $r'(X_i, X_j) = (X_j, X_i)$ for all $i, j \leq m$ and $X_i \cap X_j = 0$ for $i < j$ since A is a left nilpotent brace. Let $r : X \times X \to X \times X$ be a restriction of r', then (X, r) is a non-degenerate involutive solution of the QYBE.

Example 5. Let R be a finite left brace which is a left nilpotent brace (for example a nilpotent ring) and let r' be the associated Yang-Baxter map. For $b \in R^i, b \notin R^{i+1}$ define $Q_b = b + R^{i+1}$. Notice that for $b, c \in R$ either $Q_b = Q_c$ or $Q_b \cap Q_c = \emptyset$ since R is a left nilpotent brace. Let $b_1, b_2, \ldots, b_m \in R$ be such that the sets $Q_{b_1}, Q_{b_2}, \ldots, Q_{b_m}$ are pairwise distinct. For $i \leq m$ denote $X_i = Q_{b_i}$ and $X = \bigcup_{i \leq m} X_i$. Then $r(X_i, X_j) = (X_j, X_i)$ for all $i, j \leq m$ and $X_i \cap X_j = 0$ for for all $i < j \leq m$. Let $r : X \times X \to X \times X$ be a restriction of r', then (X, r) is a non-degenerate involutive solution of the QYBE.

The decomposition of a left brace into the Sylow subgroups of its additive group is important in the construction of simple braces (see [2, 5]). A similar decomposition can also be used to construct braided vector spaces of set-theoretic type.

Example 6. Let A be a finite left brace and r' be the associated Yang-Baxter map (defined as in Section 2.3). Let $A_1, \ldots, A_m$ be the Sylow subgroups of the additive group of the brace A. Let $0 \neq \alpha_{i,j} \in \mathbb{C}$ for $i, j \leq m$. For each $i \leq m$ let $X_i \subseteq A_i$ contain all elements of A_i except the zero element. Denote $X = \bigcup_{i \leq m} X_i$. Then $r'(X_i, X_j) = (X_j, X_i)$ for all $i, j \leq m$ and $X_i \cap X_j = 0$ for $i < j$ since A is a left nilpotent brace. Let $r : X \times X \to X \times X$ be a restriction of r', then (X, r) is a non-degenerate involutive solution of the QYBE.

We get the following corollary from Proposition 19:

Corollary 20. *Let (X, r) and X_i be as in Example 3, Example 4, Example 5 or Example 6. Let $0 \neq \alpha_{i,j} \in \mathbb{C}$ for all $i, j \leq m$. Let $D = \{d_{x,y}\}_{x,y \in X}$ where $d_{x,y} = \alpha_{i,j}$ for $x \in X_i$, $y \in X_j$, then (X, r^D) is a braided vector space of set-theoretic type. If $\alpha_{i,j}\bar{\alpha}_{i,j} = 1$ for all $i, j \leq m$ then the R-matrix associated to (X, r^D) (as in Definition 3) is a unitary matrix.*

4.2. Some other methods of constructing braided vector spaces of set-theoretic type

Notice that a braided vector spaces of set-theoretic type (BVST) can be obtained by a diagonal similarity (as in the case of trivial BVST in Section 2.2) and by the decomposition of a set-theoretic solution into invariant subsets as in Proposition 19. In this section we give some examples of braided vector spaces of set-theoretic type which cannot be obtained by combining these two methods. All examples in this subsection satisfy the assumptions of Lemma 7 and therefore can be used to construct extensions of set-theoretic solutions as in Proposition 2.9 in [9].

Example 7. Let $X = \{[i, j] : i, j \in \frac{\mathbb{Z}}{2 \cdot \mathbb{Z}}\}$, and define $r : X \otimes X \to X \otimes X$ as

$$r([i, j], [m, n]) = ([m + 1, n + m + i], [i + 1, j + i + m]).$$

Let $g : \frac{\mathbb{Z}}{2 \cdot \mathbb{Z}} \times \frac{\mathbb{Z}}{2 \cdot \mathbb{Z}} \to \mathbb{C}$ be an arbitrary function with non-zero values such that $g(1, 0) = g(0, 1)$. Define $f([i, j], [m, n]) = g(i + j + n, m + j + n)$. Let $D = \{d_{x,y}\}_{x,y \in X}$ be such that $d_{x,y} = f(x, y)$ for all $x, y \in X$; then (X, r^D) is a braided vector space of set-theoretic type. Since $|X| = 4$, this example yields a 16×16 R-matrix, given in Example 14, which can be verified by hand.

Example 8. Let $X = \frac{\mathbb{Z}}{n\cdot\mathbb{Z}}$ and $r(x,y) = (y{+}1, x{-}1)$, for $x, y \in X$. Observe that (X,r) is a non-degenerate, involutive, indecomposable set-theoretic solution of the QYBE. Let $g : \frac{\mathbb{Z}}{n\cdot\mathbb{Z}} \to \mathbb{C}$ be any mapping with nonzero values, and define

$$d_{i,j} = f(i,j) = g(i-j)$$

for $i, j \in \frac{\mathbb{Z}}{n\cdot\mathbb{Z}}$. We will show that (X, r^D) is a braided vectors space of set-theoretic type, where $D = \{d_{i,j}\}_{i,j\in\frac{\mathbb{Z}}{n\cdot\mathbb{Z}}}$. Notice that f satisfies the assumptions of Lemma 7, since $f(x,y) = g(x-y) = f(x-1,y-1) = f({}^{y}z, y^{z})$, $f(x^{y}, z) = f(x-1,z) = g(x-1-z) = f(x,z+1) = f(x, {}^{y}z)$, $f({}^{x}y, {}^{x^{y}}z) = f(y+1, z+1) = g(y-z) = f(y,z)$.

We can assume that $g(1)^2 \neq g(0)g(0)$, then $f(1,0)f(1,0) \neq f(0,0)f(1,1)$, and by Lemma 6 (X, r^D) is a a braided vector space of set-theoretic type, moreover (X, r^D) is non-trivial. This example is illustrated by Examples 12 and 13.

Example 8 yields the following corollary.

Corollary 21. *For every natural number $n > 1$ there exists a non-degenerate, involutive, indecomposable solution (X,r) of the QYBE of cardinality n with a non-trivial braided vectors space of set-theoretic type (X, r^D), for some D.*

4.3. Unitary R-matrices obtained by I-retraction

Recall that a subset I of left brace A is an ideal if $x+y \in I$ and $z\cdot x, z\cdot x \in I$ for all $x, y \in I$ and $z \in A$, see [43]. For $x \in X$ let $[x]_I = \{x+i : i \in I\}$.

On page 160 in [43], Rump showed that if I is an ideal in a brace R then the factor brace $\frac{R}{I}$ is well defined. We will use this fact to introduce the I-retraction; the I-retraction can be viewed as a generalisation of the retraction technique. We will use the I-retraction for construction of locally monomial BVS.

Proposition 22. *[I-retraction] Let A be a left brace and let (X,r) be a set-theoretic solution of the QYBE such that $X \subseteq A$ and r is a restriction of the Yang-Baxter map associated to A. Let I be an ideal in A, and denote $[x]_I = \{x+i : i \in I\}$ for $x \in X$. Define the relation $\sim$ on sets $[x]_I$ by saying that $[x]_I \sim [y]_I$ if and only if $x - y \in I$. Then $\sim$ is an equivalence relation. Let X_I be the set of equivalence classes of this relation. Denote $r(x,y) = ({}^{x}y, x^{y})$ for $x, y \in X$. Define $\tilde{r}([x]_I, [y]_I) = ([{}^{x}y]_I, [x^{y}]_I)$. Then $(X_I, \tilde{r})$ is a non-degenerate involutive set-theoretic solution of the QYBE.*

Proof. This follows from the result that the factor brace A/I is well defined, which was proved by Rump (page 160, end of section 2 in [43]). □

Recall that factors of A/I are well defined for any skew brace A and any ideal I in A, see [28], therefore Remark 22 can be generalised for non-degenerate solutions which can be embedded in skew braces.

Lemma 23. *Let (X,r) be a solution of a finite multipermutation level. If $([X]_I, r_I)$ is an I-retraction of solution (X,r), then $([X]_I, r_I)$ is a solution of a finite multipermutation level and $mpl([X]_I, r_I) \leq mpl(X,r)$.*

Proof. It follows from Proposition 4.7 [27], since if the property from Proposition 4.7 [27] holds for all $a, b, y_1, \ldots, y_m \in X$ then it holds for all $[a]_I, [b]_I, [y_1]_I, \ldots, [y_m]_I \in [X]_I$. $\square$

The proof of the following proposition follows from Lemma 5.7 in [1] (see Lemma 2 in Section 4.2).

Proposition 24. *Let A be a left brace, I be an ideal in A and (X, r), $(X_I, \tilde{r})$ be as in Proposition 22. Let $D = \{d_{[x]_I,[y]_I}\}_{[x]_I,[y]_I \in X_I}$ for some $d_{[x]_I,[y]_I} \in \mathbb{C}$. Define $D' = \{d'_{x,y}\}_{x,y \in X}$, where $d'_{x,y} = d_{[x]_I,[y]_I}$ for all $x, y \in X$. If $(X_I, \tilde{r}^D)$ is a braided vector space of set-theoretic type then $(X, r^{D'})$ is a braided vector space of set-theoretic type.*

Notice that Proposition 24 also holds if instead of I-retraction we consider the classical retraction (for some related results on extensions and retraction of cycle sets see Proposition 10 [37]).

Example 9. Let $n \geq 2$ be a natural number. Let F be the two-elements field and let A be the free (non-unital) F-algebra generated by one generator x subject to relation x^n, then A is a nilpotent algebra. Let $X = \{x + xf : f \in A\}$, and let r be a restriction of the Yang-Baxter map associated to A. Let $g : \frac{\mathbb{Z}}{2\cdot\mathbb{Z}} \times \frac{\mathbb{Z}}{2\cdot\mathbb{Z}} \to \mathbb{C}$ be an arbitrary function with non-zero values such that $g(1, 0) = g(0, 1)$.

Let $g, h \in A, i, j, m, n \in \frac{\mathbb{Z}}{2\cdot\mathbb{Z}}$. For $u = x + ix^2 + jx^3 + gx^3$ and $v = x + mx^2 + nx^3 + hx^3$ define $f(u, v) = g(i + j + n, m + j + n)$. Define $D = \{d_{u,v}\}_{u,v \in X}$ as $d_{u,v} = f(u, v)$, then (R, r^D) is a braided vector space of set-theoretic type. It follows from Proposition 24 because Example 7 is the I-retraction of Example 9 for $I = A^4$.

Example 10. Let X, A, r, n be as in Example 9. Let $g : \frac{\mathbb{Z}}{2\cdot\mathbb{Z}} \to \mathbb{C}$ be any mapping with nonzero values. Let $g, h \in A, i, j \in \frac{\mathbb{Z}}{2\cdot\mathbb{Z}}$. For $u = x + ix^2 + x^2g$ and $v = x + jx^2 + hx^2$ define $f(u, v) = g(i - j)$. Define $D = \{d_{u,v}\}_{u,v \in X}$ as $d_{u,v} = f(u, v)$, then (R, r^D) is a braided vectors space of set-theoretic type. It follows from Proposition 24 because Example 8, with $p = 2$, is the I-retraction of Example 10 for $I = A^3$.

5. Indecomposable solutions

In [20], Etingof, Schedler and Soloviev showed that each involutive non-degenerate indecomposable solution of cardinality p, for each prime number p, is isomorphic to the permutation solution (X, r) where $X = \frac{\mathbb{Z}}{p\cdot\mathbb{Z}}$ and $r(x, y) = (y - 1, x + 1)$. In [19] Etingof, Guralnick and Soloviev showed that all non-degenerate indecomposable solutions of the QYBE whose cardinality is a prime number are affine.

The purpose of this section is to show that for other cardinalities the situation is more complicated. We will introduce one-generator braces to show that every finite one-generator brace yields an indecomposable solution of the QYBE:

Definition 25. *[one-generator brace] Let A be a left brace and $x \in A$, and by $A(x)$ we will denote the smallest left brace which contains x (under the same operations of $+$ and $\circ$ as in A). If $A = A(x)$ for some $x \in A$ then we say that A is a left brace generated by one element x, or a* one-generator left brace. *Notice that if A is a finite brace, then every element from $A(x)$ can be obtained by applying several times operations $+$ and $\circ$ to element x; since inverses of elements in groups $(G, +)$ and $(G, \circ)$ are powers of these elements since these groups are finite.*

Notice that one-generator braces which are Jacobson radical rings are commutative. The following examples show that one-generator braces are abundant and need not be not commutative:

Example 11. *Let $(S, \bullet, +)$ be the brace constructed in Proposition 2.24 in [46], then any element in S generates a finite one-generator brace. Moreover, the obtained one-generator braces have a finite multipermutation level and usually are not commutative.*

Recall that a group A factorises through two subgroups B, C is $A = BC = \{bc : b \in B, c \in C\}$. The factorisation is exact if $B \cap C = 1$. The following example is inspired by Theorem 2.3 and Proposition 2.24 from [46] but has a different additive group. This example is useful for constructing examples of one-generator braces. Recall that for a ring $(R, +, \cdot)$ operation $\circ$ is defined as $a \circ b = a + b + a \cdot b$ for $a, b \in R$.

Proposition 26. *Let N be a nilpotent ring whose group $(N, \circ)$ admits an exact factorisation through two subgroups B and C, so $N = B \circ C$. Then N with the binary operations $+$ and $\odot$ is a brace where $+$ is the usual addition in the ring N and $\odot$ is defined for $a, a' \in N$ as $a \odot a' = b \circ a' \circ c$, where $a = b \circ c$ with $b \in B$, $c \in C$.*

Proof. It was shown in Theorem 2.3 [46] that $(N, \odot)$ is a group. Observe that for $a, e, f \in N$ with $a = b \circ c$ with $b \in B$, $c \in C$ we have $a \odot (e + f) + a = b \circ (e + f) \circ c + a = 2b + 2c + 2bc + e + f + be + bf + ec + fc + bec + bfc = b \circ (e) \circ c + b \circ (f) \circ c = a \odot e + a \odot f$. Therefore $(N, +, \odot)$ is a brace. □

Theorem 27. *Let (X, r) be a finite non-degenerate, involutive solution of the QYBE. The following are equivalent:*

1. *(X, r) is an indecomposable solution.*
2. *There exist a brace A and $x \in A$ such that $X = \{x + ax : a \in A\}$ and every element of A is a sum of elements from X. Moreover r is a restriction of the Yang-Baxter map associated to A.*

Proof. $1 \to 2$. Let (X, r) be an indecomposable solution. By Proposition 12 there exists a left brace A such that $X \subseteq A$ and r is a restriction of the Yang-Baxter map associated to A. Moreover every element of A is a sum of some elements from X, and X generates the group $(A, \circ)$. Observe that since the

brace A is finite then the inverse of an element x in a group $(A,\circ)$ equals some power of this element in this group. Fix $x \in X$, and let $y \in X$. Since (X,r) is indecomposable, there are $r_1,\dots,r_n \in X$ such that $\sigma_{r_1}\sigma_{r_2}\dots\sigma_{r_n}(x) = y$, so $\sigma_r(x) = y$ where $r = r_1 \circ \dots \circ r_n$. Recall that $\sigma_r(x) = x + rx$. It follows that $X \subseteq \{x + rx : r \in A\}$.

It remains to show that $\{x + rx : r \in A\} \subseteq X$. Recall that X generates the group $(A,\circ)$. Observe that since the brace A is finite then the inverse of an element x in a group $(A,\circ)$ equals some power of this element in this group. Therefore every element of A can be written as $r = r_1 \circ \dots \circ r_n$ where $r_i \in X$, and since $\sigma_y(x) \in X$ for $x, y \in X$ we get $\sigma_r(x) = \sigma_{r_1}\sigma_{r_2}\dots\sigma_{r_n}(x) \in X$, hence $\{x + rx : r \in A\} \subseteq X$.

$2 \to 1$. We will first show that $r(X,X) \subseteq (X,X)$. Notice that for each $r, r_1 \in A$ we have $\sigma_{r_1}(x + rx) = \sigma_{r_1 \circ r}(x) = x + (r_1 \circ r)x \in X$. Let a^{-1} denote the inverse of a in the group $(A,\circ)$. By the definition $\tau_y(z) = \sigma_{\sigma_z(y)^{-1}}(z)$ for all $y, z \in A$, hence $\tau_y(z) \in X$. Therefore $r(X,X) \subseteq (X,X)$. We will show that every element $r \in A$ can be written as $r = r_1 \circ \dots \circ r_n$ for some $r_1,\dots,r_n \in X$. By assumption $r = \sum_{i=1}^{n} x_i$ for some n and some $x_i \in X$, where $x_i = s_i x + x$ for some $s_i \in A$. By Theorem 3.8 [27] $a + b = a \circ \sigma_{a^{-1}}(b)$ for $a, b \in A$. We will proceed by induction on n, and assume that if $r = \sum_{i=1}^{n} x_i$ then $r = y_1 \circ \dots \circ y_m$ for some $y_i \in X$; let $r' = \sum_{i=1}^{n+1} x_i = r + x_{n+1} = r \circ \sigma_{r^{-1}}(x_{n+1}) = y_1 \circ \dots \circ y_{m+1}$ where $y_{m+1} = \sigma_{r^{-1}}(x_{n+1}) = \sigma_{r_1} \cdots \sigma_{r_1}(x_{n+1}) \in X$ by the first part of this proof. We have shown that if $r \in A$ then $r = r_1 \circ \dots \circ r_n$ for some $r_1,\dots,r_n \in X$. Therefore $x + rx = \sigma_r(x) = \sigma_{r_1}\sigma_{r_2}\dots\sigma_{r_n}(x)$ where $r_i \in X$, hence (X,r) is indecomposable. $\square$

Theorem 28. *Let A be a finite left brace, let $x \in A$ and let $A(x)$ be as in Definition 25. Denote $X = \{x + ax : a \in A(x)\}$, and let $r : X \times X \to X \times X$ be a restriction of the Yang-Baxter map associated to A. Then (X,r) is an indecomposable, non-degenerate, involutive solution of the quantum Yang-Baxter equation.*

Proof. Notice that since A is finite then $-x$ is a sum of n copies of x for some x. By Theorem 27 it suffices to show that every element in $A(x)$ is a sum of elements from the set $\{x, ax : a \in A\}$. Let $c \in A(x)$, since every element of $A(x)$ can be obtained by applying operations $+$ and $\cdot$ to x, and the number of elements is finite, then $A(x) = \bigcup_{i=1}^{n} R_i$ for some n where $R_1 = \{x\}$ and inductively $R_{j+1} = \{r = \sum_k r_k : r_k \in \bigcup_{i=1}^{j} R_i\} \cup \{r = r_1 r_2 : r_1, r_2 \in \bigcup_{i=1}^{j} R_i\}$.

Let $y \in A(x)$; we will show that $y = k \cdot x + \sum_i s_i x$ for some natural number k and for some $s_i \in A(x)$, where $k \cdot x$ denotes the sum of k copies of x. We will proceed by induction on n where $y \in R_n$. If $n = 1$ then $y = x$ so the result holds. Suppose the result folds for all $y \in R_i$ for $i \leq n$ and let $y \in R_{n+1}$. Then by the definition either $r = \sum_k r_k : r_k \in \bigcup_{i=1}^{n} R_i$ and the result holds by the inductive assumption or $r = r_1 r_2$ for some $r_1, r_2 \in \bigcup_{i=1}^{n} R_i$. By the inductive assumption $r_2 = k' \cdot x + \sum_{i=1}^{m} s_i x$ for some $s_i \in A(x)$ and some natural number k'. Hence $r = k' \cdot (r_1 x) + \sum_{i=1}^{m} r_1 \cdot (s_i x)$. Notice that $r_1(s_i x) = (r_1 + s_i + r_1 s_i)x - r_1 x - s_i x$, and since $A(x)$ is finite $-r_1 x = \sum_{i=1}^{k} r_1 x$ and $-s_i x = \sum_{j=1}^{k'} s_i x$ for some k, k'.

Therefore $r_1(s_i x)$ is a sum of elements from the set $\{x, ax : a \in A\}$, concluding the proof. $\square$

Question 29. *Characterise one-generator braces of the multipermutation level 2.*

Question 30. *Is Theorem 28 also true for infinite one-generator braces?*

6. Nilpotent braces and related solutions

In this this section a non-degenerate, involutive set-theoretic solution (X, r) of the quantum Yang-Baxter equation will simply be referred to as *a solution*. We will investigate solutions which can be embedded into nilpotent braces. It was shown in Proposition 5.15 [27] that if $G(X, r)$ is the structure group of (X, r), then $mpl(G, r) \leq mpl(X, r) + 1$, where $mpl(G, r)$ denotes the multipermutation level of solution associated to $G(X, r)$. We obtain a similar result.

Lemma 31. *Let (X, r) be a finite solution and let A be a finite left brace such that $X \subseteq A$ and r is a restriction of the Yang-Baxter map associated to A. Assume that every element of A is a sum of some elements from X. If (X, r) has a finite multipermutation level, then A is a right nilpotent brace and $A^{(m+2)} = 0$ where $m = mpl(X, r)$.*

Proof. Let $[x]$ denote the retraction of element $x \in X$. Notice that by the definition of the retraction for $x, y \in X$ we have $[x] = [y]$ if and only if $x \cdot r = y \cdot r$ for all $r \in X$. Since every element of A is a sum of elements from X, this is equivalent to say that $x \cdot s = y \cdot s$ for all $s \in A$. Therefore the retraction of the solution (X, r) embeds into the retraction of the solution associated to brace A. By Proposition 7 [43] this implies that the retraction of (X, r) embeds into brace $A/Soc(A)$. Notice also that every element in $A/Soc(A)$ is a sum of elements from the set [X]-the retraction of X. Therefore, the fact that $A^{(m+2)} = 0$ can be proved by induction on m (by Proposition 6 [13]). $\square$

Lemma 32. *Let (X, r) be a solution which is the retraction of a finite solution whose permutation group (X, r) is nilpotent. Then there exists a finite left brace A such that $X \subseteq A$ and every element of A is a sum of elements from X and A is a left nilpotent brace, where r is a restriction of the Yang-Baxter map associated to A.*

Proof. Let (X, r) be the retraction of solution (Y, r') and denote $r'(x, y) = (\sigma_x(y), \tau_y(x))$. By Theorem 11 and Corollary 12, there is a finite left brace B such that $Y \subseteq B$ and every element of B is a sum of elements from Y, and elements from Y generate the multiplicative group $(B, \circ)$; moreover r' is the restriction of $r'' : B \times B \to B \times B$ - the Yang-Baxter map associated to B. Denote $r''(x, y) = (\sigma'_x(y), \tau'_y(x))$. By assumption r' is the restriction of r'', so $\sigma'_y(x) = \sigma_y(x)$ for $x, y \in Y$.

Let $\mathcal{G}(Y, r')$ be the permutation group of (Y, r'), so it is the group generated by maps $\sigma_x : Y \to Y$ for $x \in Y$ with the operation of the composition of maps.

Let T be the group generated by maps $\sigma'_x : B \to B$ for $x \in Y$. Recall that elements from Y generate the multiplicative group $(B, \circ)$ and $\sigma_x\sigma_y = \sigma_{x\circ y}$, therefore T equals the group generated by maps $\sigma'_b : B \to B$ for $b \in b$.

Let $f \in T$, then f is the identity map if and only if $f(b) = b$ for all $b \in B$. This is equivalent to saying that $f(y) = y$ for all $y \in Y$, since every element of B is a sum of elements from Y and $\sigma_y(a + b) = \sigma(a) + \sigma(b)$. Therefore, T is isomorphic to the group $\mathcal{G}(Y, r')$, which implies that T is nilpotent (since T and $\mathcal{G}(Y, r')$ have corresponding generators and $\mathcal{G}(Y, r')$ is nilpotent).

Notice that by the definition of the retraction for $x, y \in Y$ we have $[x] = [y]$ if and only if $x \cdot r = y \cdot r$ for all $r \in Y$. Since every element of B is a sum of elements from Y, this is equivalent to saying that $x \cdot s = y \cdot s$ for all $s \in B$. Therefore the retraction of the solution (Y, r') embeds into the retraction of the solution associated to the left brace B. By Proposition 7 [43] this implies that the retraction of (X, r) embeds into brace $A = B/Soc(B)$. Notice also that every element in A is a sum of elements from [X]-the retraction of X.

It remains to show that the multiplicative group $(A, \circ)$ of A is nilpotent. Recall that T is nilpotent, therefore there is n such that for every $b_1, \ldots, b_n \in B$ $\sigma'_{[[\ldots[[b_1,b_2]b_3]\ldots]b_n]}$ is the identity map, therefore $\sigma'_{[[\ldots[[b_1,b_2]b_3]\ldots]b_n]}(b) = b$ for all $b \in B$, consequently $[[\ldots[[b_1, b_2]b_3]\ldots]b_n]$ is in the socle of B. It follows that A° is a nilpotent group (since $A = B/Soc(B)$). By Theorem 1 from [45] A is a left nilpotent brace, so $A^n = 0$ for some n. $\square$

If (X, r) is a solution of a finite multipermutation level and the permutation group of (X, r) is nilpotent then (X, r) need not to embed in a left nilpotent left brace; for example a right nilpotent left brace of cardinality 6 whose multiplicative group is not nilpotent and whose permutation group is nilpotent can be obtained by taking the opposite multiplication in Example 3 [43].

Lemma 33. *Let s be a natural number and let A be a left brace which is right nilpotent, so $A^{(s)} = 0$ for some s. Let $a, b \in A$. Define inductively elements $d_i = d_i(a, b), d'_i = d'_i(a, b)$ as follows: $d_0 = a$, $d'_0 = b$, and for $i \leq 1$ define $d_{i+1} = d_i + d'_i$ and $d'_{i+1} = d'_i d_i$. Then for every $c \in A$ we have*

$$(a + b)c = ac + bc + \sum_{i=0}^{2s} (-1)^{i+1}((d'_i d_i)c - d'_i(d_i c)).$$

Proof. We can prove by induction that $d'_i \in A^{(i+1)}$, hence almost all d'_i are zero. We can use the same proof as in Lemma 15 in [45] where instead of $d_j d'_j$ we write at each place $d'_j d_j$ for every j (for various j), and instead of ab we write ba. $\square$

Lemma 34. *Let (X, r) be a solution of a finite multipermutation level and $Y \subseteq X$ be such that $r(Y, Y) \subseteq (Y, Y)$, then (Y, r') is also a solution of a finite multipermutation level and $mpl(Y, r') \leq mpl(X, r)$, where r' is a restriction of r to $Y \times Y$.*

Proof. This follows from Proposition 4.7 [27], since if the property from Proposition 4.7 [27] holds for all $a, b, y_1, \ldots, y_m \in X$ then it holds for all $a, b, y_1, \ldots, y_m \in Y$. $\square$

The first part of Lemma 34 was proved in [14] under the additional assumption that (Y, r') is invariant under the permutation group of (X, r).

Theorem 35. *Let (X, r) be a finite solution. The following are equivalent:*

1. *(X, r) is an indecomposable solution of a finite multipermutation level, and x is an element of X.*
2. *There is a finite one-generator left brace A generated by some element $x \in A$ such that $X = \{x + ax : a \in A\}$ and r is a restriction of the Yang-Baxter map associated to A. Moreover, $A^{(m)} = 0$ for some m.*

Proof. If point 2 holds then by Theorem 28 (X, r) is an indecomposable solution. By Lemma 34 (X, r) has a finite multipermutation level, as it is a subsolution of the solution associated to a right nilpotent left brace. Recall that by Proposition 5 from [13] the solution associated to a right nilpotent brace has a finite multipermutation level. This shows implication $2 \to 1$.

Assume that point 1 holds, and let A be as in Theorem 11 and Corollary 12. By Lemma 31, A has a finite multipermutation level. Let $x \in X$, it suffices to show that $A = A(x)$-the brace generated by x. Recall that $A^{(n)}$ is an ideal in A, by a result of Rump [43]. We will show by induction that $A \subseteq A(x) + A^{(n)}$ for every n. For $n = 1$ it is true as $A^{(1)} = A$. Suppose the result holds for some n, and let $y \in A$, since every element of A is a sum of elements from X, then y is a sum of some elements from X so $y = k \cdot x + \sum_i r_i x$ for some natural number k and for some $r_i \in A$, where $k \cdot x$ denotes the sum of k copies of x. By assumption $r_i \in A(x) + A^{(n)}$ hence $r_i = x_i + s_i$, where $x_i \in A(x)$, $s_i \in A^{(n)}$. Notice that $r_i x = (x_i + s_i)x \in x_i x + A^{(n+1)} \subseteq A(x) + A^{(n+1)}$ by Lemma 33 applied for $a = x_i$ and $b = s_i$. It follows that $y \in A(x) + A^{(n+1)}$. By the assumptions, $A^{(m)} = 0$ for some m, therefore $A \subseteq A(x)$, as required. $\square$

A solution (X, r) is square-free if $r(x, x) = (x, x)$ for all $x \in X$. It was shown by Rump in [44] that every finite square-free solution of the QYBE is decomposable.

Corollary 36. *Let (X, r) be a finite solution of a finite multipermutation level. If for every $x \in X$ there is $y \in X$ such that $r(x, y) = (y, x)$, then the solution (X, r) is decomposable, provided that the cardinality of X is larger than 1.*

Proof. Let $x \in X$, then by Theorem 35 $X = \{x + ax : a \in A\}$ where A is a left brace generated by x. Let $r(x, y) = (y, x)$, since $y \in X$ then $y = x + rx$ for some $r \in A$. Notice that $r(y, x) = (x, y)$ since r is involutive, this implies $yx + x = x$, hence $0 = yx = (x + rx)x = x^2 + a$ for some $a \in A^{(3)}$ by applying Lemma 33 for $a = x$ and $b = rx$. Therefore, $x^2 \in A^{(3)}$ which implies $A^{(2)} \subseteq A^{(3)} \subseteq A^{(4)} \cdots \subseteq A^{(n)} = 0$ for some n, hence $x^2 = 0$, and so the cardinality of X is 1. $\square$

Question 37. *Are Theorem 35 and Corollary 36 also true without the assumption that the multipermutation level of (X,r) is finite?*

Question 38. *Is there a connection between one-generator skew-braces and indecomposable non-degenerate set-theoretic solutions of the QYBE?*

7. *R*-matrices constructed using indecomposable solutions and nilpotent braces

In this section we will use results from Sections 5 and 6 to construct R-matrices related to indecomposable set-theoretic solutions of the QYBE.

Proposition 39. *Let X be a set which has more than one element. Let (X,r) be a non-degenerate, involutive, indecomposable set-theoretic solution of the QYBE of a finite multipermutation level. Suppose that (X,r) is the retraction of a finite solution whose permutation group is nilpotent. Then there exists an I-retraction of (X,r) such that (X_I,r_I) is a solution isomorphic to the solution $(Y,\tilde{r})$ where $Y=\frac{\mathbb{Z}}{n\cdot\mathbb{Z}}$ for some $n>1$ and $\tilde{r}(x,y)=(y+1,x-1)$, for $x,y\in Y$.*

Proof. By Lemma 32, there is a left nilpotent brace A such that $X\subseteq A$ and every element of A is a sum of elements from X, and r is a restriction of the Yang-Baxter map associated to A. We can use this particular brace A in the proof of implication $1\rightarrow 2$ of Theorem 35 and get that $X=\{ax+x : a\in A\}$ for some $x\in A$, A is generated as a brace by x and $A^{(m)}=0$ for some m. Since A is both a left nilpotent and right nilpotent left brace, by Theorem 3 from [45] we have $A^{[t]}=0$ for some t, where $A^{[1]}=A$ and $A^{[n+1]}$ is defined inductively as $A^{[n+1]}=\sum_{i=1}^{n}A^{[i]}\cdot A^{[n+1-i]}$.

Notice that $A^2=0$ implies $r(x,y)=(y,x)$; then (X,r) is decomposable, since each element in X is an orbit, hence $A^2\neq 0$. Let $I=A\cdot A^2+A^2\cdot A$, then it is easy to see that I is an ideal in A. Notice that A/I is a ring, since $(a+b)c=((a+b)+ab+ab(a+b))c=(a+b+ab)c=ac+bc$ for all $a,b,c\in A/I$. Let $\bar{x}=x+I\in A/I$, then $X_I=\{\bar{x}+r\bar{x} : r\in A/I\}$ and A/I is a ring generated by element $\bar{x}$ where $\bar{x}^3=0$. Hence every element of X_I equals $\bar{x}+k\cdot\bar{x}^2$ for some k (where $k\cdot\bar{x}$ is a sum of k copies of $\bar{x}$). Notice that $\bar{x}^2\neq 0$, since otherwise $A^2\subseteq I=A^{[3]}$. Notice that $A^2\subseteq A^{[3]}$ yields $A^2\subseteq A^{[3]}\subseteq A^{[4]}\subseteq\ldots=0$ since $A^{[t]}=0$. Therefore $A^2=0$, a contradiction, hence $x^2\notin I$.

Notice that $r_I(\bar{x}+i\cdot\bar{x}^2,\bar{x}+j\cdot\bar{x}^2)=(\bar{x}+(j+1)\cdot\bar{x}^2,\bar{x}+(i-1)\cdot\bar{x}^2)$, hence X_I has more than 1 element (since $x^2\neq 0$ in A/I). Let n be the smallest natural number such that $n\cdot\bar{x}^2=0$; then (X_I,r_I) is isomorphic to the solution $(Y,\tilde{r})$. □

As an application of Proposition 24 we obtain:

Theorem 40. *Let (X,r) be a solution of a finite multipermutation level. Suppose that (X,r) is the retraction of a finite solution whose permutation group is nilpotent. If the cardinality of X is larger than 1 then there exists a non-trivial braided vector space of set-theoretic type (X,r^D) for some $D=\{d_{x,y}\}_{x,y\in X}$.*

Proof. If (X, r) is decomposable the result follows from Proposition 19. If the solution (X, r) is indecomposable then (X_I, r_I) is indecomposable, for any ideal I. By Proposition 24, any locally monomial BVS can be lifted from (X_I, r_I) to (X, r). The result now follows from Proposition 39 and Example 8 in Section 5. □

Question 41. *Is it possible to construct a non-trivial braided vector space of set-theoretic type (X, r^D) for every finite, involutive, non-degenerate set-theoretic solution (X, r) of a finite multipermutation level? Especially of a multipermutation level 2?*

8. *R*-matrices associated to involutive set-theoretic solutions of the QYBE

In [39], Okniński remarked that it would be interesting to know what types of R-matrices correspond to non-degenerate, involutive, set-theoretic solutions of the quantum Yang-Baxter equation. We answer this question below.

Proposition 42. *Let (X, r) be a set-theoretic solution of the QYBE. Let A be the matrix associated to (X, r) as in Definition 3. The following is equivalent:*

1. *The solution (X, r) is involutive and non-degenerate.*
2. *If we divide A in a natural way into n by n blocks then each block has exactly one entry equal to 1, and all the other entries zero (for $n = 3$ this decomposition is illustrated on matrix A in Examples 13, 15 and 16). Moreover, A is a permutation matrix which is symmetric, and A^2 is the identity matrix. In particular, A is unitary.*

Proof. Denote $X = \{x_1, \ldots, x_n\}$. By Definition 3, every column of M has only one nonzero entry equal to one, and the $a_{i,j}^{k,l}$ entry of A is nonzero if and only if $r(x_i, x_j) = (x_k, x_l)$. By assumption r is an involutive solution then $r(x_i, x_j) = (x_k, x_l)$ implies $r(x_k, x_l) = (x_i, x_j)$, hence the $a_{i,j}^{k,l}$ entry of A is nonzero if and only if the $a_{k,l}^{i,j}$ entry of A is nonzero (and it happens exactly when $r(x_i, x_j) = (x_k, x_l)$). It follows that A is a symmetric matrix. Moreover, A^2 equals the identity matrix, so A is a permutation matrix. It follows that every row in A has exactly one nonzero entry.

By Corollary 2.3 from [32] and Corollary 8.2.4 from [33], if X is finite, then an involutive solution (X, r) is right non-degenerate if and only if it is left non-degenerate.

It remains to consider the property that r is right non-degenerate. Assume that the solution (X, r) is right non-degenerate.

Fix element i; then we know that, for every j, there are $t_j, q_j \leq n$ such that $r(x_i, x_j) = (x_{t_j}, x_{q_j})$. Recall that right non-degeneracy of r means exactly that among elements $t_1, t_2, \ldots, t_n$ we can find every positive integer not exceeding n. For $i = 1$ the above property implies that (because A is written in a basis

$x_i \otimes x_j$ with lexicographical order) if the first n columns of A are divided into $n \times n$ blocks then each block has a nonzero entry (and since each column has only one nonzero entry, then each such block has exactly one nonzero entry). By applying it for different j, we get that when A is divided in the natural way into n by n blocks, then each block has exactly one entry equal to 1, and all other entries equal to 0.

By repeating the above reasoning in the reverse order we see that every matrix satisfying assumption 2 gives rise to a non-degenerate involutive set-theoretic solution of the QYBE. □

Proposition 43. *Let $X = \{1, 2, \ldots, n\}$. Let (X, r) be a non-degenerate, involutive, set-theoretic solution of the quantum Yang-Baxter equation and let (X, r^D) be a braided vector space of set-theoretic type where $D = \{d_{i,j}\}_{i,j \in X}$ for some $d_{i,j} \in \mathbb{C}$. Let M be the R-matrix associated to (X, r^D) as in Definition 3. Then the singular values of the M are $|d_{i,j}|$. If $|d_{i,j}| = 1$ for all $i, j \leq m$ then M is a unitary matrix.*

Proof. By Definition 3 the entry at the intersection of the column indexed by $[i, j]$ and the row indexed by $[k, l]$ of M equals $d_{i,j}$ if $r(i, j) = (k, l)$ and 0 otherwise. Let M^* denote the conjugate transpose of M. Notice that $M \cdot M^*$ is a diagonal matrix with entries $|d_{i,j}|^2$ on the diagonal (in some order). This implies that M is unitary, provided that $|d_{i,j}| = 1$. □

9. Concrete examples

In this section we provide some examples of some of the R-matrices and locally monomial BVS constructed in this paper.

Example 12. *This example gives the R-matrix obtained in Example 8 in the case when $n = 4$.*

$$A = \begin{pmatrix} dE_{44} & aE_{1,4} & bE_{2,4} & cE_{3,4} \\ cE_{4,1} & dE_{1,1} & aE_{2,1} & bE_{3,1} \\ bE_{4,2} & cE_{1,2} & dE_{2,2} & aE_{3,2} \\ aE_{4,3} & bE_{1,3} & cE_{2,3} & dE_{3,3} \end{pmatrix}.$$

Here $E_{i,j}$ is the 4×4 matrix which has all zeros entries except the element (i, j) which equals 1.

Example 13. *This example gives the R-matrix obtained in Example 8 in the*

case when $n = 3$.

$$A = \left(\begin{array}{ccc|ccc|ccc} 0 & 0 & 0 & 0 & 0 & a & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & c \\ 0 & 0 & b & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & b & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & a & 0 & 0 \\ c & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & c & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & b & 0 \\ 0 & a & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right).$$

We see that

$$A = \begin{pmatrix} bE_{3,3} & aE_{1,3} & cE_{2,3} \\ cE_{3,1} & bE_{1,1} & aE_{2,1} \\ aE_{3,2} & cE_{1,2} & bE_{2,2} \end{pmatrix}.$$

Example 14. *This example gives the R-matrix obtained in Example 7.*

$$A = \begin{pmatrix} cE_{4,4} & cE_{3,4} & aE_{1,3} & bE_{2,3} \\ cE_{4,3} & cE_{3,3} & bE_{1,4} & aE_{2,4} \\ bE_{3,1} & aE_{4,1} & cE_{2,2} & cE_{1,2} \\ aE_{3,2} & bE_{4,2} & cE_{2,1} & cE_{1,1} \end{pmatrix}.$$

Here $E_{i,j}$ *are defined as in Example 12.*

Example 15. *This example gives the R-matrix obtained as in Proposition 19 in the case when the cardinality of* X *is* 3*, and* X *has* 2 *orbits.*

$$A = \left(\begin{array}{ccc|ccc|ccc} 0 & 0 & 0 & 0 & a & 0 & 0 & 0 & 0 \\ 0 & a & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & b & 0 & 0 \\ \hline 0 & 0 & 0 & a & 0 & 0 & 0 & 0 & 0 \\ a & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & b & 0 \\ \hline 0 & 0 & c & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & c & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & d \end{array}\right).$$

Example 16. *This example produces the R-matrix obtained as in Proposition 19 in the case when the cardinality of* X *is* n *and when* X *has* n *orbits; the obtained matrix is* $n^2 \times n^2$*. The method uses matrix* S *which is the* $n \times n$ *matrix with consecutive entries and a matrix* $D = diag(d_1, d_2, \ldots, d_n)$ *where* $d_1, \ldots, d_n$ *are arbitrary. The method is analogous for distinct* n*, so we present it in the case when* $n = 3$*. We will obtain the R-matrix obtained as in Proposition 19 in*

the case when the cardinality of X is 3, and when X has 3 orbits. Let $n = 3$ and $D = diag(d_1, d_2, \ldots, d_9)$. Let

$$S = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}.$$

Let s_1, s_2, s_3 denote the columns of S, i.e. $s_1 = (1, 4, 7)^T$, $s_2 = (2, 5, 8)^T$ and $s_3 = (3, 6, 9)^T$. We define a permutation vector $p = (p_1, p_2, \ldots, p_9)^T$, taking $p = (s_1^T, s_2^T, s_3^T)^T$. We see that $p = (1, 4, 7, 2, 5, 8, 3, 6, 9)^T$. Then we form $A = DP$, where P is the permutation matrix $P = (e_{p_1}, \ldots, e_{p_9})$ (we permute the columns of the 9 times 9 identity matrix). Denote $d = (d_1, d_2, \ldots, d_9)^T$. We have $A = (d_1 e_1, d_4 e_4, d_7 e_7, d_2 e_2, d_5 e_5, d_8 e_8, d_3 e_3, d_6 e_6, d_9 e_9)$ and

$$A = A(d) = \left(\begin{array}{ccc|ccc|ccc} d_1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & d_2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & d_3 & 0 & 0 \\ \hline 0 & d_4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & d_5 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & d_6 & 0 \\ \hline 0 & 0 & d_7 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & d_8 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & d_9 \end{array}\right). \tag{2}$$

Notice that if $d_2 = d_3 = d_4 = d_6 = d_7 = d_8 = 0$ then A is a diagonal matrix.

If $d_1 \geq d_2 \geq \ldots d_{n^2} > 0$, then the matrix A constructed above is an R-matrix with prescribed singular values $d_1, d_2, \ldots, d_{n^2}$. We recall that the singular values of A are the positive square roots of the eigenvalues of A^*A, and they play a significant role in many practical applications. If $|d_i| = 1$ for $i = 1, 2, \ldots, n^2$, then A is unitary.

Now we present another example of a unitary R-matrix.

Example 17. *Let $n = 3$ and define $H = I - \alpha e e^T$, where $e = (1, 1, \ldots, 1)^T \in R^9$, $\alpha = 2/n^2$. H is called a reflection (Householder's transformation). We can check that H is not an R-matrix, but if we apply the same permutation P as in Example 16 then we get that $A_1 = HP$ is a unitary R-matrix.*

We have

$$A_1 = \frac{1}{9}\left(\begin{array}{ccc|ccc|ccc} 7 & -2 & -2 & -2 & -2 & -2 & -2 & -2 & -2 \\ -2 & -2 & -2 & 7 & -2 & -2 & -2 & -2 & -2 \\ -2 & -2 & -2 & -2 & -2 & -2 & 7 & -2 & -2 \\ \hline -2 & 7 & -2 & -2 & -2 & -2 & -2 & -2 & -2 \\ -2 & -2 & -2 & -2 & 7 & -2 & -2 & -2 & -2 \\ -2 & -2 & -2 & -2 & -2 & -2 & -2 & 7 & -2 \\ \hline -2 & -2 & 7 & -2 & -2 & -2 & -2 & -2 & -2 \\ -2 & -2 & -2 & -2 & -2 & 7 & -2 & -2 & -2 \\ -2 & -2 & -2 & -2 & -2 & -2 & -2 & -2 & 7 \end{array}\right).$$

Notice that $A_1 = P - \alpha E$, where E is a matrix with all entries equal 1. Let $P(3 \times 3)$ be a Vandermonde matrix formed for roots of unity, i.e.

$$P = \begin{pmatrix} 1 & 1 & 1 \\ w_3 & w_2 & w_1 \\ w_3^2 & w_2^2 & w_1^2 \end{pmatrix},$$

where $w_j = \omega^j$ and $\omega = e^{\frac{2\Pi i}{3}}$. Then we can check that $(P \otimes P)^{-1} A_1 (P \otimes P) = A(d)$, where $d = (-1, 1, 1, \ldots, 1)^T$ and $A = A(d)$ is defined in (2). Note that the columns of P form the set of orthogonal eigenvectors of the ones matrix of size 3×3. We have $P^* P = 3I$. We obtain that A_1 is a locally monomial matrix.

Example 18. *Let E be a matrix where all entries equal 1. Let B be a locally monomial BVS which was obtained in Example 8, with the additional assumption that all non-zero entries of B are equal to 1. Assume that B and E are n^2 by n^2 matrices for some n, and $\alpha, \beta \in \mathbb{C}$ then the matrix $\alpha B + \beta E$ satisfies the QYBE. For example, we obtain the following unitary R-matrix when $\alpha = \frac{-2}{9}$ and $\beta = \frac{7}{9}$.*

$$A_2 = \frac{1}{9} \left(\begin{array}{ccc|ccc|ccc} -2 & -2 & -2 & -2 & -2 & 7 & -2 & -2 & -2 \\ -2 & -2 & -2 & -2 & -2 & -2 & -2 & -2 & 7 \\ -2 & -2 & 7 & -2 & -2 & -2 & -2 & -2 & -2 \\ \hline -2 & -2 & -2 & 7 & -2 & -2 & -2 & -2 & -2 \\ -2 & -2 & -2 & -2 & -2 & -2 & 7 & -2 & -2 \\ 7 & -2 & -2 & -2 & -2 & -2 & -2 & -2 & -2 \\ \hline -2 & -2 & -2 & -2 & 7 & -2 & -2 & -2 & -2 \\ -2 & -2 & -2 & -2 & -2 & -2 & -2 & 7 & -2 \\ -2 & 7 & -2 & -2 & -2 & -2 & -2 & -2 & -2 \end{array} \right).$$

Surprisingly, this matrix is locally monomial. Using the same similarity matrix P as in Example 17, we find that $(P \otimes P)^{-1} A_2 (P \otimes P) = A(d)$, where $A = A(d)$ is defined in (2), and $d = (-w_3, w_2, w_1, w_1, w_3, w_2, w_2, w_1, w_3)^T$.

Acknowledgements

The authors would like to thank Cesar Galindo, Eric Rowell, Leandro Vendramin, Robert Weston and Harry Braden for their helpful and enlightening comments. The first author was supported by ERC Advanced grant 320974. We would also like to thank the paper's anonymous referee for providing many useful suggestions as to how to improve the original version.

References

[1] N. Andruskiewitsch, M. Graña, *From racks to pointed Hopf algebras*, Adv. Math. 178 2 (2003), 177–243.

[2] D. Bachiller, *Extensions, matched products, and simple braces*, arXiv:1511.08477v3 [math.GR], 13 June 2016.

[3] D. Bachiller, F. Cedó, E. Jespers, *Solutions of the Yang-Baxter equation associated with a left brace*, J. Algebra 463 (2016), 80–102.

[4] D. Bachiller, F. Cedó, E. Jespers, J. Okniński, *A family of inretractable square-free solutions of the Yang-Baxter equation*, to appear in Fundamenta Math.

[5] D. Bachiller, F. Cedó, E. Jespers, J. Okniński, *Iterated matched products of finite braces and simplicity; new solutions of the Yang-Baxter equation*, to appear in Trans. Amer. Math. Soc.

[6] K.A. Brown, K. R. Goodearl, Lectures on Algebraic Quantum Groups, Advanced Courses in Mathematics CRB Barcelona, Birkhäuster, 2002.

[7] T. Brzeziński, F. F. Nichita, *Yang-Baxter systems and entwined structures*, Commun. Algebr. 2005, 33, 1083–1093.

[8] M. Calderini, M. Sala, *Elementary abelian regular subgroups as hidden sum for cryptographic trapdoors*, arXiv:1702.00581v1 (2017).

[9] J. S. Carter, M. Elhamdadi, M. Saito *Homology theory for the set-theoretic Yang-Baxter equation and knot invariants from generalizations of quandles*, Fundamenta Mathematicae, 184 (2004), 31–54.

[10] J. S. Carter, D. Jelsovsky, S. Kamada, and M. Saito, *Quandle homology groups, their Betti numbers, and virtual knots*, J. Pure Appl. Algebra, 157(2-3) 2001, 135–155.

[11] F. Catino, I. Colazzo, P. Stefanelli, *Regular subgroups of the affine group*, Bull. Aust. Math. Soc. 91 (2015), 76–85.

[12] F. Catino, R. Rizzo, *Regular subgroups of the affine group and radical circle algebras*, Bull. Aust. Math. Soc. 79 (2009), 103–107.

[13] F. Cedó, Tatiana Gateva-Ivanova, Agata Smoktunowicz, *On the Yang-Baxter equation and left nilpotent left braces*, Journal of Pure and Applied Algebra, 221, (2016), 751–756.

[14] F. Cedó, E. Jespers, J. Okniński, *Braces and the Yang-Baxter Equation*, Communications in Mathematical Physics April 2014, Volume 327, Issue 1, 101–116.

[15] R. S. Chen, *Generalized Yang-Baxter equations and braiding quantum gates*, Journal of Knot Theory and Its Ramifications, 21 (2012), No. 9, Article No. 1250087, arXiv:1108.5215v1.

[16] S. X. Cui, S.M. Hong, Z. Wang, *Universal quantum computation with weakly integral anyons*, Quantum Information Processing, Volume 14, Issue 8, (2015), 2687–2727.

[17] K. A. Dancer, P. E. Finch and P. S. Isaac, *Universal Baxterisation for Z-graded Hopf algebras*, Journal of Physics A: Mathematical and Theoretical. Volume 40, Number 50 (2007), 1069–1075.

[18] P. Etingof and S. Gelaki, *A method of construction of finite-dimensional triangular semisimple Hopf algebras*, Mathematical Research Letters 5 (1998), 551–561.

[19] P. Etingof, R. Guralnick, A. Soloviev, *Indecomposable set-theoretical solutions to the quantum Yang-Baxter equation on a set with a prime number of elements*, J. Algebra 249 (2001), 709–719.

[20] P. Etingof, T. Schedler, T. Soloviev, *A set theoretical solutions to the quantum Yang-Baxter equation,* Duke. Math. J. 100 (1999), 169–209.

[21] J. M. Franko, *Braid group representations arising from the Yang-Baxter equation*, Journal of Knot theory and its Ramifications, Vol. 19, 525, (2010).

[22] J. M. Franko, *Braid group representations via the Yang Baxter equation*, Indiana University, ProQuest Dissertations Publishing, 2007.

[23] C. Galindo, S. M. Hong, E. C. Rowell, *Generalized and quasi-localization of braid group representations*, Int. Math. Res. Not. no. 3, (2013), 693–731.

[24] C. Galindo, E. C. Rowell, *Braid representations from unitary braided vector spaces*, J. Math. Phys. 55 (2014), 061702.

[25] T. Gateva-Ivanova, *A combinatorial approach to the set-theoretic solutions of the Yang-Baxter equation*, J. Math. Phys., 45 (2004), pp. 3828–3858.

[26] T. Gateva-Ivanova and S. Majid, *Quantum spaces associated to multipermutation solutions of level two*, Algebr. Represent. Theor. 14 (2), 2011, 341–376.

[27] T. Gateva-Ivanova, *Set-theoretic solutions of the Yang-Baxter equation, Braces, and Symmetric groups* (2015), arXiv:1507.02602 [math.QA].

[28] L. Guarnieri, L. Vendramin, *Skew braces and the Yang-Baxter equation*, to appear in Mathematics of Computation, arXiv:1511.03171v3 [math.QA], 16 March 2016.

[29] L. H. Kauffman and S.J. Lomonaco Jr, *Braiding operators are universal quantum gates*, New Journal of Physics 6 (2004) 134, Online at http://www.njp.org/.

[30] A. Klimyk, K. Schmudgen, Quantum groups and their representations, Springer, 1997.

[31] R. Iordanescu, F. F. Nichita, I. M. Nichita, *The Yang-Baxter Equation, (Quantum) Computers and Unifying Theories*, Axioms 2014, 3, 360-368; doi:10.3390/axioms3040360.

[32] E. Jespers and J. Okniński, *Monoids and group of I-type*, Algebr. Represent. Theory 8 (2005), 709–729.

[33] E. Jespers and J. Okniński, Noetherian Semigroup Rings, Springer, Dordrecht, 2007.

[34] C. Kassel, Quantum Groups, Graduate Text in Mathematics 155, Springer–Verlag, New York, 1995.

[35] V. Kharchenko, Quantum Lie Theory, a Multilinear Approach, Lecture Notes in Mathematics, Vol. 2150, Springer International Publishing, 2015.

[36] M. Larsen, E. C. Rowell, *Unitary braid representations with finite image*, Algebraic and Geometric Topology, 8, (2008), 2063–2079.

[37] V. Lebed, L. Vendramin, *Homology of left non-degenerate set-theoretic solutions to the Yang-Baxter equation*, to appear in Advances in Mathematics.

[38] C. Nayak, S. H. Simon, A. Stern, M. Freedman, S. Das Sarma, *Non-Abelian Anyons and Topological Quantum Computation*, Rev. Mod. Phys. 80, 1083 (2008), arXiv:condmat/0707.1889.

[39] Jan Okniński, private communication, January 2017.

[40] Eric Rowell, private communication, February 2017.

[41] Eric Rowell, *Parameter dependent Gaussian (z, N)-generalized Yang-Baxter operators*, Quantum Inf. Comp. 16 (2016), no. 1, 2, 0105–0114.

[42] E. C. Rowell, Z. Wang, *Localization of unitary braid group representations*, Comm. Math. Phys. no. 3 (2012), 595–615.

[43] Wolfgang Rump, *Braces, radical rings, and the quantum Yang-Baxter equation*, Journal of Algebra, Volume 307 (2007), 153–170.

[44] Wolfgang Rump, *A decomposition theorem for square-free unitary solutions of the Yang-Baxter equation*, Advances in Mathematics, 193 (2005), 40–55.

[45] A. Smoktunowicz, *On Engel groups, nilpotent groups, braces and the Yang-Baxter equation*, to appear in Trans. Amer. Math.Soc.

[46] A. Smoktunowicz, L.Vendramin, *On skew braces*, to appear in Combinatorial Algebra (also arXiv:1705.06958v1 [math.GR] 19 May 2017).

[47] L. Vendramin, *Extensions of set-theoretic solutions of the Yang-Baxter equation and a conjecture of Gateva-Ivanova*, J. Pure Appl. Alg. 220 (2016), no. 5, 1681–2076.