MATCHED PAIRS APPROACH TO SET THEORETIC SOLUTIONS OF THE YANG-BAXTER EQUATION

TATIANA GATEVA-IVANOVA AND SHAHN MAJID

ABSTRACT. We study set-theoretic solutions (X, r) of the Yang-Baxter equations on a set X in terms of the induced left and right actions of X on itself. We give a characterization of involutive square-free solutions in terms of cyclicity conditions. We characterise general solutions in terms of abstract matched pair properties of the associated monoid $S(X, r)$ and we show that r extends as a solution $(S(X, r), r_S)$. Finally, we study extensions of solutions both directly and in terms of matched pairs of their associated monoids. We also prove several general results about matched pairs of monoids S of the required type, including iterated products $S \bowtie S \bowtie S$ equivalent to r_S a solution, and extensions $(S \bowtie T, r_{S\bowtie T})$. Examples include a general 'double' construction $(S \bowtie S, r_{S\bowtie S})$ and some concrete extensions, their actions and graphs based on small sets.

1. INTRODUCTION

It was established in the last two decades that solutions of the linear braid or 'Yang-Baxter equations' (YBE)

$$r^{12}r^{23}r^{12} = r^{23}r^{12}r^{23}$$

on a vector space of the form $V^{\otimes 3}$ lead to very remarkable algebraic structures. Here $r : V \otimes V \to V \otimes V$, $r^{12} = r \otimes \mathrm{id}, r^{23} = \mathrm{id} \otimes r$ is a notation and structures include coquasitriangular bialgebras $A(r)$, their quantum group (Hopf algebra) quotients, quantum planes and associated objects at least in the case of specific standard solutions, see [23, 22]. On the other hand, the variety of all solutions on vector spaces of a given dimension has remained rather elusive in any degree of generality. Some years ago it was proposed by V.G. Drinfeld[1] to consider the same equations in the category of sets, and in this setting several general results are now known. It is clear that a set-theoretic solution extends to a linear one, but more important than this is that set-theoretic solutions lead to their own remarkable algebraic and combinatoric structures, only somewhat analogous to quantum group constructions. In the present paper we develop a systematic approach to set-theoretic solutions based on the monoid that they generate and on a theory of matched pairs or factorisation of monoids. We present results both at the level of (X, r), at the level

Date: 21.11.2006.

1991 *Mathematics Subject Classification.* Primary 81R50, 16W50, 16S36.

Key words and phrases. Yang-Baxter, Semigroups, Quantum Groups.

The first author was partially supported by the Royal Society, UK, by Grant MI 1503/2005 of the Bulgarian National Science Fund of the Ministry of Education and Science, and by The Abdus Salam International Centre for Theoretical Physics (ICTP). Both authors were supported by the Isaac Newton Institute during completion of the work.

of unital semigroups (monoids) and on the 'exponentiation problem' from one to the other.

Let X be a nonempty set and let $r : X \times X \longrightarrow X \times X$ be a bijective map. In this case we shall use notation (X, r) and refer to it as a *quadratic set* or set with quadratic map r. We present the image of (x, y) under r as

$$r(x,y) = ({}^x y, x^y). \tag{1.1}$$

The formula (1.1) defines a "left action" $\mathcal{L} : X \times X \longrightarrow X$, and a "right action" $\mathcal{R} : X \times X \longrightarrow X$, on X as:

$$\mathcal{L}_x(y) = {}^x y, \quad \mathcal{R}_y(x) = x^y, \tag{1.2}$$

for all $x, y \in X$. The map r is *non-degenerate*, if the maps $\mathcal{R}_x$ and $\mathcal{L}_x$ are bijective for each $x \in X$. In this paper we shall often assume that r is non-degenerate, as will be indicated. Also, as a notational tool, we shall often identify the sets $X \times X$ and X^2, the set of all monomials of length two in the free monoid $\langle X \rangle$.

As in [8] to each quadratic map $r : X^2 \to X^2$ we associate canonically algebraic objects (see Definition 2.1) generated by X and with quadratic defining relations $\Re = \Re(r)$ naturally determined as

$$xy = zt \in \Re(r), \quad \text{whenever} \quad r(x,y) = (z,t). \tag{1.3}$$

Note that in the case when X is finite, the set $\Re(r)$ of defining relations is also finite, therefore the associated algebraic objects are finitely presented. Furthermore in many cases they will be standard finitely presented with respect to the degree-lexicographic ordering. It is known in particular that the algebra generated by the monoid $S(X, r)$ defined in this way has remarkable homological properties when r obeys the braid or Yang-Baxter equations in $X \times X \times X$ and other restrictions such as square-free, involutive. Set-theoretic solutions were introduced in [1, 27] and studied in [4, 5, 6, 10, 13, 2, 17, 14, 16] as well as more recently in [11, 7, 3, 8, 9, 24] and other works. We say that a set X is 'braided' when it is equipped with an invertible solution.

In this paper we study the close relations between the combinatorial properties of the defining relations, i.e. of the map r, and the structural properties of the associated algebraic objects, particularly through the 'actions' above. Section 2 contains preliminary material and some elementary results based on direct calculation with $\mathcal{R}_x, \mathcal{L}_x$. These include cancellation properties in $S(X, r)$ (Proposition 2.13 and related results) that will be needed later and a full characterisation of when (X, r) obeys the Yang-Baxter equations under the assumption of square free, involutive and nondegenerate. In particular we find that they are equivalent to a cyclicity condition

$$^{({}^y x)}({}^y z) = {}^{({}^x y)}({}^x z)$$

for all $x, y, z \in X$ (see Theorem 2.36). Cyclicity conditions, originally called "cyclic conditions" were discovered in 1990 while the first author was looking for new classes of Noetherian Artin-Shelter regular rings, [4, 5, 6], and have already played an important role in the theory, see [4, 5, 6, 8, 9, 10, 11, 14, 24]. The cyclic conditions are used in the proof of the nice algebraic and homological properties of the binomial skew polynomial rings, such as being Noetherian, [4, 5], Gorenstein (Artin-Schelter regular), [6, 9], and for their close relation with the set-theoretic solutions of YBE [10, 9]. The cycle sets, as Rump calls them have essential role in his decomposition theorem, [24].

In Section 3 we show that when (X,r) is a braided set the 'actions' $\mathcal{R}_x, \mathcal{L}_x$ indeed extend to actions of the monoid $S = S(X,r)$ on itself to form a matched pair (S,S) of monoids in the sense of [20, 22]. This means that S acts on itself from the left and the right in a compatible way to construct a new monoid $S \bowtie S$. We also have an induced map $r_S(u,v) = ({}^uv, u^v)$ and moreover

$$uv = {}^uvu^v$$

holds in S for all $u, v \in S$ (in other words, r_S-commutative). This result is in Theorem 3.6 and leads us also to introduce a general theory of monoids S with these properties, which we call an '**M3**-monoid'. We remark that matched pairs of groups are a notion known in group theory since the 1910s and also known [17] to be connected with set-theoretic solutions of the YBE. There is also a nice review of the main results in [17, 2] from a matched pair of groups point of view in [26], among them a good way to think about the properties of the group $G(X,r)$ universally generated from (X,r). In particular it is known that the group $G(X,r)$ is itself a braided set in an induced manner and this is the starting point of the these works. Our own goals and methods are certainly very different and in particular for an **M3**-monoid one cannot automatically deduce that r_S is invertible and obeys the YBE as would be true in the group case. When it does, we say that (S, r_S) is a 'braided monoid' and we eventually show in Theorem 3.14 that this is nevertheless the case for $S = S(X,r)$. Most of this section is concerned with these two theorems. Theorem 3.23 at the end of the section provides the converse under a mild 2-cancellative assumption on the quadratic set (X,r); this is braided if and only if $(S(X,r), r_S)$ is a braided monoid.

Among results at the level of a general **M3**-monoid S we give some explicit criteria for r_S to obey the YBE and a complete characterisation for this in Theorem 3.22 as $(S, S \bowtie S)$ forming a matched pair by extending the actions. In this case we find iterated double crossproduct monoids $S \bowtie S$, $S \bowtie S \bowtie S$ etc., as the analogue of the construction for bialgebras $A(r)$ of iterated double cross products $A(r) \bowtie A(r), A(r) \bowtie A(r) \bowtie A(r)$, etc. in [21]. We also provide an interpretation of the YBE as zero curvature for 'surface-transport' around a cube and this is related to the 'labelled square' construction for the bicrossproduct Hopf algebras associated to (finite) group matched pairs introduced in [22].

In Section 4 we use our matched pair characterisation to study a natural notion of 'regular extension' $Z = X \sqcup Y$ of set theoretic solutions. Our first main result, Theorems 4.9 and 4.13 provide explicit if and only if conditions for such an extension to obey the YBE. Theorem 4.15 finds similarly explicit but slightly weaker if and only if conditions for a matched pair (S,T) and monoid $S \bowtie T$ where S, T are the associated braided monoids built from X, Y using the results of Section 3. Our inductive construction from the (X, r_X) and (Y, r_Y) data here (and also the construction of (S,S) in Section 3) is somewhat analogous to the construction of a Lie group matched pair from a Lie algebra one by integrating vector fields and connections [19].

Finally in Section 4 we bring these results together with a complete if and only if characterisation of when is a regular extension obeys the YBE as equivalent to $U = S(Z, r_Z)$ being a double cross product $U = S \bowtie T$ and forming matched pairs with S, T. This is Theorem 4.28 and is the main result of the section. We also provide a corresponding theory of regular extensions at the level of abstract **M3**-monoids in Theorem 4.31 and Corollary 4.32. A further immediate corollary is that every braided monoid S has a 'double' braided monoid $S \bowtie S$, which is an analogue of the induced coquasitriangular structure on the bialgebra $A(R) \bowtie A(R)$ in [22].

Section 5 looks at explicit constructions for extensions using our methods for a pair of initial (X, r_X), (Y, r_Y). We consider particularly a special case which we call 'strong twisted union' and which is a nevertheless a far-reaching generalisaton of the 'generalised twisted union' in [2]. We give characterizations of when a strong twisted union obeys the YBE linking back to our cyclicity results of Section 2. We conclude with some concrete nontrivial examples of extensions. The solutions here are involutive, nondegenerate, square-free with the condition 'lri' also from Section 2. We provide graphs of the initial and extended solutions and illustrate how the methods of the paper translate into very practical tools for their construction. These graphs can also be viewed as a natural source of discrete noncommutative geometries, a point of view to be developed elsewhere.

2. Cancellation and cyclicity properties for quadratic sets

The new results in this section relate to 2-cancellation conditions needed later on and to cyclicity conditions of interest in the theory of quadratic sets. We show in particular that a number of possible such conditions are all equivalent under mild hypotheses.

2.1. **Preliminaries on quadratic and braided sets.** For a non-empty set X, as usual, we denote by $\langle X\rangle$, and ${}_{gr}\langle X\rangle$, respectively the free unital semigroup (i.e., free monoid), and the free group generated by X, and by $k\langle X\rangle$- the free associative k-algebra generated by X, where k is an arbitrary field. For a set $F \subseteq k\langle X\rangle$, (F) denotes the two sided ideal of $k\langle X\rangle$, generated by F.

Definition 2.1. [8] Assume that $r : X^2 \longrightarrow X^2$ is a bijective map.

(i) The monoid

$$S = S(X, r) = \langle X; \Re(r)\rangle,$$

with a set of generators X and a set of defining relations $\Re(r)$, is called *the monoid associated with* (X, r).

(ii) The *group* $G = G(X, r)$ *associated with* (X, r) is defined as

$$G = G(X, r) = {}_{gr}\langle X; \Re(r)\rangle.$$

(iii) For arbitrary fixed field k, *the k-algebra associated with* (X, r) is defined as

$$\mathcal{A} = \mathcal{A}(k, X, r) = k\langle X\rangle/(\Re(r)). \tag{2.1}$$

Clearly $\mathcal{A}$ is a quadratic algebra, generated by X and with defining relations $\Re(r)$. Furthermore, $\mathcal{A}$ is isomorphic to the monoid algebra $kS(X, r)$.

Remark 2.2. [9] When we study the monoid $S = S(X, r)$, the group $G = G(X, r)$, or the algebra $A = A(k, X, r)$ associated with (X, r), it is convenient to use the action of the infinite group, $\mathcal{D}(r)$, generated by maps associated with the quadratic relations, as follows. As usual, we consider the two bijective maps $r^{ii+1} : X^3 \longrightarrow X^3$, $1 \leq i \leq 2$, where $r^{12} = r \times Id_X$, and $r^{23} = Id_X \times r$. Then

$$\mathcal{D} = \mathcal{D}(r) = {}_{\mathrm{gr}}\langle r^{12}, r^{23}\rangle$$

acts on X^3. If r is involutive, the bijective maps r^{12} and r^{23} are involutive as well, so in this case $\mathcal{D}(r)$ is *the infinite dihedral group*,

$$\mathcal{D} = \mathcal{D}(r) = {}_{\mathrm{gr}}\langle r^{12}, r^{23} : (r^{12})^2 = e, \quad (r^{23})^2 = e\rangle$$

Note that all monomials $\omega' \in X^3$ which belong to the same orbit $\mathcal{O}_{\mathcal{D}}(\omega)$ satisfy $\omega' = \omega$ as elements of G (respectively, S, A).

Definition 2.3. (1) r is *square-free* if $r(x, x) = (x, x)$ for all $x \in X$.

(2) A non-degenerate involutive square-free map (X, r) will be called *(set-theoretic) quantum binomial map*.

(3) r is *a set-theoretic solution of the Yang-Baxter equation* (YBE) if the braid relation

$$r^{12}r^{23}r^{12} = r^{23}r^{12}r^{23}$$

holds in $X \times X \times X$. In this case (X, r) is also called *a braided set.* If in addition r is involutive (X, r) is called *a symmetric set.*

The following lemma is straightforward.

Lemma 2.4. *Suppose (X, r) is given, and let ${}^x\bullet$, and $\bullet^x$ be the associated left and right actions. Then*

(1) *r is involutive if and only if*

$$^{^xy}(x^y) = x, \text{ and } (^yx)^{y^x} = x, \text{ for all } x, y \in X.$$

(2) *r is square-free if and only if*

$$^xx = x, \text{ and } x^x = x \text{ for all } x \in X.$$

(3) *If r is non-degenerate and square-free, then*

$$^xy = x \iff x^y = y \iff y = x \iff r(x, y) = (x, y).$$

It is also straightforward to write out the Yang-Baxter equations for r in terms of the actions. This is in [2] but we recall it here in our notations for convenience.

Lemma 2.5. *Let (X, r) be given in the notations above. Then r obeys the YBE (or (X, r) is a braided set)* iff *the following conditions hold*

$$\mathbf{l1}: \quad {}^x({}^yz) = {}^{^xy}({}^{x^y}z), \qquad\qquad \mathbf{r1}: \quad (x^y)^z = (x^{^yz})^{y^z},$$

$$\mathbf{lr3}: \quad ({}^xy)^{({}^{x^y}z)} \; = \; {}^{(x^{^yz})}(y^z),$$

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

Proof. We refer to the diagram (2.2). This diagram contains elements of the orbit of arbitrary monomial $xyz \in X^3$, under the action of the group $\mathcal{D}(r)$. Note that

each two monomials in this orbit are equal as elements of S
(2.2)

$$\begin{array}{ccc}
xyz & \xrightarrow{r_{12}} & r(xy)z = ({}^xyx^y)z \\
{\scriptstyle r_{23}}\downarrow & & \downarrow{\scriptstyle r_{23}} \\
xr(yz) = x({}^yzy^z) & & ({}^xy)r((x^y)z) = ({}^xy)({}^{x^y}z)(x^y)^z \\
{\scriptstyle r_{12}}\downarrow & & \downarrow{\scriptstyle r_{12}} \\
r(x({}^yz))(y^z) = {}^x({}^yz)(x^{{}^yz})(y^z) & & r(({}^xy)({}^{x^y}z))(x^y)^z = [{}^{{}^xy}({}^{x^y}z)][({}^xy)^{({}^{x^y}z)}][(x^y)^z] = w_1 \\
{\scriptstyle r_{23}}\downarrow & & \\
{}^x({}^yz)r((x^{{}^yz})(y^z)) = [{}^x({}^yz)][{}^{(x^{{}^yz})}(y^z)][(x^{{}^yz})^{y^z}] = w_2 & &
\end{array}$$

from which we read off **l1,lr3,r1** for equality of the words in X^3. □

The following proposition was also proved in [2], see 2.1.

Proposition 2.6. [2]. *(a) Suppose that (X,r) is involutive, r is right non-degenerate and the assignment $x \to \mathcal{R}_x$ is a right action of $G(X,r)$ on X. Define the map $T : X \longrightarrow X$ by the formula $T(y) = \mathcal{R}_y^{-1}(y)$, then one has $\mathcal{R}_x^{-1} \circ T = T \circ \mathcal{L}_x$.*

Suppose in addition that $\mathcal{L}_x$ are invertible , i.e. (X,r) is involutive and non-degenerate. Then

(b) T is invertible, and the two left actions of $G(X,r)$ given by $x \to \mathcal{R}_x^{-1}$ and $x \to \mathcal{L}_x$ are isomorphic to each other.

(c) Condition **r1** *implies* **l1** *and* **lr3***. Thus (X,r) is symmetric if and only if* **r1** *is satisfied.*

Remark 2.7. It was shown by a different argument in [8] that if (X,r) is square-free symmetric set, then $\mathcal{R}_x = \mathcal{L}_x^{-1}$ for all $x \in X$

We want to find out now what is the relation between the actions, and the above conditions, if we assume only that r in non-degenerate, without any further restrictions. Compatible left and right actions appear in the notion of matched pairs of groups, see [22], and motivated by this theory we also define their natural extensions:

Definition 2.8. Given (X,r) we extend the actions ${}^x\bullet$ and $\bullet^x$ on X to left and right actions on $X \times X$ as follows. For $x,y,z \in X$ we define:

$${}^x(y,z) := ({}^xy, {}^{x^y}z), \quad \text{and} \quad (x,y)^z := (x^{{}^yz}, y^z)$$

We say that r is respectively left and right invariant if

$$\mathbf{l2}: \qquad r({}^x(y,z)) = {}^x(r(y,z)), \quad \mathbf{r2}: \qquad r((x,y)^z) = (r(x,y))^z$$

hold for all $x,y,z \in Z$.

Lemma 2.9. *Let (X,r) be given in the notations above. Then the following are equivalent*

1. *(X,r) is a braided set.*
2. **l1***,* **r2***.*
3. **r1***,* **l2***.*

Proof. From the formula (1.1) and Definition 2.8:

$$r({}^x(y,z)) = r({}^xy, {}^{(x^y)}z) = ({}^{{}^xy}({}^{(x^y)}z), ({}^xy)^{({}^{(x^y)}z)}). \tag{2.3}$$

$$^x(r(y,z)) = {}^x({}^yz, y^z) = ({}^x({}^yz), {}^{(x^{({}^yz)})}(y^z)). \tag{2.4}$$

Hence condition **l2** is an equality of pairs in $X \times X$:

$$({}^{{}^xy}({}^{(x^y)}z), ({}^xy)^{({}^{(x^y)}z)}) = ({}^x({}^yz), {}^{(x^{({}^yz)})}(y^z))$$

as required. The case of **r2** is similar. We have proved that for any quadratic set

$$\mathbf{l2} \Longleftrightarrow \mathbf{l1}, \mathbf{lr3}; \quad \mathbf{r2} \Longleftrightarrow \mathbf{r1}, \mathbf{lr3} \tag{2.5}$$

and we then use Lemma 2.5. It is also easy enough to see the result directly from the diagram (2.2). Thus

$$w_1 = {}^{{}^xy}({}^{x^y}z)r(x,y)^z, \quad w_2 = {}^x({}^yz)r((xy)^z) \tag{2.6}$$

on computing these expressions as in the proof of Lemma 2.9. Equality of the first factors for all x, y, z is **l1** and of the 2nd factors is **r2** for x, y, z, viewed in X^2. Similarly for **r1**,**l2**. □

These observations will play a role later on. Clearly, all of these conditions and **lr3** hold in the case of a braided set.

2.2. **Cancellation conditions.** To proceed further we require and investigate next some cancellation conditions. A sufficient but not necessary condition for them is if $X \subset G(X,r)$ is an inclusion.

Definition 2.10. Let (X,r) be a quadratic set. We say that r is *2-cancellative* if for every positive integer k, less than the order of r, the following two condition holds:

$$r^k(x,y) = (x,z) \Longrightarrow z = y \text{ (left 2-cancellative)}$$
$$r^k(x,y) = (t,y) \Longrightarrow x = t \text{ (right 2-cancellative)}$$

It follows from Corollary 2.13 that every non-degenerate involutive quadratic map (X,r) is 2-cancellative.

Proposition 2.11. *Let* (X,r) *be a set with quadratic map, with associated monoid* $S = S(X,r)$. *Then:*

(1) S *has (respectively left, right) cancellation on monomials of length 2* if and only if r *is (respectively left, right) 2-cancellative;*

(2) Suppose that (X,r) *is 2-cancellative solution. Then* S *has cancellation on monomials of length 3.*

Proof. We recall that the defining relations of S come from the map r. We do not assume r is necessarily of finite order, so, in general,

$$xy = xz \text{ in } S \Longleftrightarrow xz = r^k(xy), \text{ for some positive integer } k,$$
$$\text{or } xy = r^k(xz) \text{ for some positive integer } k.$$

Assume $xy = xz$ in S. Without loss of generality, we may assume $xz = r^k(xy)$. But r is 2-cancellative, so $z = y$

Clearly if r is not left 2-cancellative, then there is an equality $xz = r^k(xy)$ for some integer $k \geq 1$, and $z \neq y$. This gives $xz = xy$ in S, therefore S is not left cancellative. This proves the left case of (1). The proof of the right case is analogous.

We shall prove (2). Suppose (X,r) is a 2-cancellative solution. Let $xyz = xpq$ be an equality in S. Then the monomial xpq, considered as an element of X^3, is in the orbit $\mathcal{O}_{\mathcal{D}}(xyz)$ of xyz under the action of the group $\mathcal{D}(r)$ on X^3, and therefore occurs in the YB-diagram (2.2). We study the six possible cases. In the first four cases we follow the left vertical branch of the diagram.

$$(a)\ \ (x,p,q) = (x,y,z) \text{ in } X^{\times 3} \implies (p,q) = (y,z) \text{ in } X\times X \implies pq = yz \text{ in } S.$$

$$(b)\ \ (x,p,q) = (x, r(y,z)) \text{ in } X^{\times 3} \implies (p,q) = r(y,z) \text{ in } X\times X \implies pq = yz \text{ in } S.$$

$$(c)\ \ (x,p,q) = (r(x,{}^{y}z), y^{z}) \text{ in } X^3 \implies q = y^z \text{ and } (x,p) = r(x,{}^{y}z)$$
$$\implies^{\text{by } r \text{ 2-cancellative}} p = {}^{y}z \implies (x,p,q) = (x,{}^{y}z, y^z)$$
$$\implies (p,q) = r(y,z) \implies pq = yz \ \text{ in } S.$$

$$(d)\ \ (x,p,q) = ({}^{x}({}^{y}z), r((x^{{}^{y}z}), y^z) \implies x = {}^{x}({}^{y}z) \implies^{\text{by } r \text{ 2-cancellative}} x^{{}^{y}z} = {}^{y}z$$
$$\implies (x,p,q) = (x, r({}^{y}z, y^z) = (x, r^2(y,z)) \implies (p,q) = r^2(y,z) \implies pq = yz \ \text{ in } S.$$

$$(e)\ \ (x,p,q) = (r(x,y),z) \text{ in } X^{\times 3} \implies q = z \text{ and } (x,p) = r(x,y)$$
$$\implies^{\text{by } r \text{ 2-cancellative}} p = y \implies (x,p,q) = (x,y,z) \text{ in } X^{\times 3}$$

$$(f)\ \ (x,p,q) = ({}^{x}y, r(x^y, z)) \text{ in } X^{\times 3} \implies {}^{x}y = x \implies^{\text{by } r \text{ 2-cancellative}}$$
$$x^y = y \implies (x,p,q) = (x, r(y,z)) \implies (p,q) = r(y,z) \implies pq = yz \text{ in } S.$$

We have shown that

$$xyz = xpq \text{ is an equality in } S^3 \implies yz = pq \text{ in } \ S^2$$

Assume now that $xyz = xyt$ is an equality in S^3. It follows from the previous that $yz = yt$, in S^2, therefore by the 2-cancellativeness of S $z = t$.

Analogous argument verifies the right cancellation in S^3. □

The following Lemma 2.12 and Corollary 2.13 show that each non-degenerate involutive quadratic map is 2-cancellative:

Lemma 2.12. *Suppose (X,r) is non-degenerate and involutive quadratic map (not necessarily a solution of YBE), $x,y \in X$. The following conditions are equivalent:*

(1) $r(x,y) = (x,t)$, *for some* $t \in X$;
(2) $r(x,y) = (s,y)$, *for some* $s \in X$;
(3) ${}^{x}y = x$;
(4) $x^y = y$;
(5) $r(x,y) = (x,y)$.

Proof. Suppose $r(x,y) = (x,t)$, for some $t \in X$. Clearly it follows from the standard equality $r(x,y) = ({}^{x}y, y^x)$ that $(5) \implies (1) \iff (3)$, and $(5) \implies (2) \iff (4)$.

We will show $(3) \implies (4)$. Assume ${}^{x}y = x$. Then the equalities

$${}^{x}y = x =^{r \text{ involutive}} {}^{{}^{x}y}(x^y) = {}^{x}(x^y).$$

give ${}^{x}y = {}^{x}(x^y)$, which by the non-degeneracy of r implies $y = x^y$. One analogously proves the implication $(4) \implies (3)$.

We have shown that each of the first four conditions implies the remaining three and hence, clearly (5) also holds. This completes the proof of the lemma. □

Corollary 2.13. *Let (X, r) be non-degenerate and involutive quadratic set. Then r is 2-cancellative and $S = S(X, r)$ has cancellation on monomials of length 2.*

Furthermore, if (X, r) is a solution of YBE, then S has cancellation on monomials of length 3.

The following example gives a non-degenerate bijective solution (X, r) which is not 2-cancellative,

Example 2.14. Let $X = \{x, y, z\}$, $\rho = (xyz)$, be a cycle of length three in $Sym(X)$. Define $r(x, y) := (\rho(y), x)$. Then $r : X \times X \longrightarrow X \times X$ is a non-degenerate bijection of order 6.

$$(x, x) \longrightarrow^r (y, x) \longrightarrow^r (y, y) \longrightarrow^r (z, y) \longrightarrow^r (z, z) \longrightarrow^r (x, z) \longrightarrow^r (x, x),$$
$$(x, y) \longrightarrow^r (z, x) \longrightarrow^r (y, z) \longrightarrow^r (x, y).$$

It is easy to check that r is a solution of YBE, (this is a permutation solution). The two actions satisfy: $\mathcal{L}_x\mathcal{L}_y = \mathcal{L}_z = (xyz); \mathcal{R}_x = \mathcal{R}_y = \mathcal{R}_z = e$, so r is nondegenerate. Note that r^2 fails to be nondegenerate, since $r^2(y, x) = (z, y)$, $r^2(y, y) = (z, z)$. Moreover, r is not 2-cancellative, since $xx = yx$ is an equality in S. Note also that in the group $G(X, r)$ all generators are equal: $x = y = z$.

Lemma 2.15. *Let (X, r) be a 2-cancellative quadratic set. If the monoid $S(X, r)$ has cancellation on monomials of length 3 then*

(i) **l2** $\Longleftrightarrow$ **r2** $\Longleftrightarrow$ **l1** & **r1** $\Longleftrightarrow$ *(X, r) is braided set.*
Furthermore, if r is nondegenerate and involutive then
(ii) **l1** $\Longleftrightarrow$ **r1** $\Longleftrightarrow$ *(X, r) is a symmetric set.*

Proof. We look again at the requirements of the YBE in the proof recalled above. The monoid $S(X, r)$ has cancellation on monomials of length 3. So if we look at this diagram (2.2) in the monoid $S(X, r)$ then as words in $S(X, r)$ we already have equality $w_1 = w_2$. If we assume **l1, lr3** we can cancel the first two factors and deduce **r1** holding in $S(X, r)$. But $X \subset S(X, r)$, so we can conclude **r1** in X. Similarly any two of **l1**, **lr3**, **r1** allows us to conclude the third. It follows from Lemma 2.5 that any two is equivalent in this case to (X, r) braided. This proves (i). Also, if we assume now that r is involutive and nondegenerate then by Proposition 2.6, one has **r1** $\Longrightarrow$ **l1, lr3**, similarly **l1** $\Longrightarrow$ **r1, lr3**, thus we have **l1** $\Longleftrightarrow$ **r1**, which by (i) gives the last part. □

Clearly for the proof of the lemma it is enough to assume $X \subset G(X, r)$ is an inclusion. It is important to note that the condition $X \subset G(X, r)$ or an equivalent one is not empty as shows the following example.

Example 2.16. Consider $X = \{x, y, z\}$ and r on monomials:

$$xy \to xz \to yz \to yy \to xy, \quad xx \to zz \to yx \to zy \to xx, \quad zx \to zx.$$

Clearly, r is non-degenerate and as we show below obeys **l1, r1**. On the other hand it does not obey the YBE. Note that $x = y = z$ in $G(X, r)$ by cancelling in the group, so X is not contained in $G(X, r)$. Here we give some details. It is not difficult to see that for each pair $\xi, \eta \in X$ there is an equality

$$r(\xi\eta) = (\mathcal{L}(\eta), \mathcal{R}(\xi)), \text{ where } \mathcal{L} = (x\ z\ y) \in S_3, \quad \mathcal{R} = (x\ z) \in S_3.$$

In other words r is *a permutational map*, (see Definition 2.21), and in the notation of (1.2) we have $\mathcal{L}_x = \mathcal{L}_y = \mathcal{L}_z = \mathcal{L} = (x\ z\ y)$, a cycle of length three in S_3, and

$\mathcal{R}_x = \mathcal{R}_y = \mathcal{R}_z = \mathcal{R} = (x\ z)$, a transposition in S_3. It is clear then that the left action satisfy

$$ {}^a({}^b\xi) = \mathcal{L}^2(\xi) = {}^{{}^ab}({}^{a^b}\xi), \quad \text{for all } \xi, a, b \in X, $$

therefore **l1** holds. Similarly for the right action one has:

$$ (\xi^a)^b = \mathcal{R}^2(\xi) = \xi = (\xi^{{}^ab})^{a^b}, \text{ for all } \xi, a, b \in X, $$

which verifies **r1** . Furthermore, as a permutational map r obeys all cyclic conditions, see Definition 2.20. Direct computation shows that $r^{12}r^{23}r^{12}(xyz) \neq r^{23}r^{12}r^{23}(xyz)$, so (X, r) does not obey the YBE.

2.3. **Cyclic conditions.** In various cases in a nodegenerate (X, r) the left and the right actions are inverses, i.e. $\mathcal{R}_x = \mathcal{L}_x^{-1}$ and $\mathcal{L}_x = \mathcal{R}_x^{-1}$ for all $x \in X$. For example this is true for every square-free symmetric set (X, r). It is natural then to single out a class of non-degenerate sets (X, r) by a stronger condition **lri** defined below, and study the the relation of this property to the other conditions on the left (resp. right) action.

Definition 2.17. Let (X, r) be a quadratic set. We define the condition

$$ \textbf{lri:} \qquad ({}^xy)^x = y = {}^x(y^x) \text{ for all } x, y \in X. $$

In other words **lri** holds if and only if $\mathcal{R}_x = \mathcal{L}_x^{-1}$ and $\mathcal{L}_x = \mathcal{R}_x^{-1}$.

Lemma 2.18. *Let (X, r) be a quadratic set. Then the following are equivalent:*

(1) **lri** *holds*
(2) $({}^xy)^x = y$ *for all* $x, y \in X$
(3) ${}^x(y^x) = y$ *for all* $x, y \in X$.

In this case (X, r) is nondegenerate.

Proof. Assume (2). We will show first that (X, r) is left non-degenerate. Assume ${}^xy = {}^xz$. Then

$$ y = ({}^xy)^x = ({}^xz)^x = z, $$

which proves the left non-degeneracy. Assume now that $y^x = z^x$. By the left non-degeneracy, there exist unique $s, t \in X$, with $y = {}^xs, z = {}^xt$. Then

$$ y^x = z^x \implies s = ({}^xs)^x = ({}^xt)^x = t \implies y = z, $$

so (X, r) is right non-degenerate, and therefore non-degenerate.

Next we show that (2) $\Rightarrow$ (3). By the nondegeneracy of (X, r) for any $x, y \in X$ there exists unique $z \in X$, with $y = {}^xz$. Then

$$ {}^x(y^x) = {}^x(({}^xz)^x) =^{\text{by assumption}} {}^xz = y. $$

The proof of the implication in the opposite direction is analogous. Thus either part implies **lri**. □

We will show later that under some cyclicity restrictions, the involutiveness of r is equivalent to condition **lri**. The following lemma is straight forward.

Lemma 2.19. *Assume (X, r) satisfies* **lri**. *Then* **l1** $\Longleftrightarrow$ **r1**, *and* **l2** $\Longleftrightarrow$ **r2**.

More generally, clearly, **lri** implies that whatever property is satisfied by the left action, an analogous property is valid for the right action and vice versa. In particular, this is valid for the left and right 'cyclic conditions'. Such conditions were discovered, see [4, 5, 8] when the first author studied binomial rings with skew polynomial relation and square-free solutions of YBE. It is interesting to know that the proofs of the good algebraic and homological properties of these algebras and monoids use in explicit or implicit form the existence of the full cyclic condition in the form below (Definition 2.20). This includes the properties of being Noetherian, Gorenstein, therefore Artin-Shelter regular, and "producing" solutions of YBE, see [4, 5, 6, 8, 9, 10, 11, 14]. Compared with these works, here we do not assume that X is finite, and initially the only restriction on the map r we impose is "r is non-degenerate". We recall first the notion of "cyclic conditions" in terms of the left and right actions and study the implication of the cyclic conditions on the properties of the actions, in particular how are they related with involutiveness of r and and condition **lri**.

Definition 2.20. Let (X, r) be a quadratic set. We define the conditions

$$\begin{array}{llll} \textbf{cl1}: & {}^{y^x}x = {}^{y}x \quad \text{for all } x, y \in X; & \textbf{cr1}: & x^{{}^x y} = x^y, \quad \text{for all } x, y \in X; \\ \textbf{cl2}: & {}^{{}^x y}x = {}^{y}x, \quad \text{for all } x, y \in X; & \textbf{cr2}: & x^{y^x} = x^y \quad \text{for all } x, y \in X. \end{array}$$

We say (X, r) is *weak cyclic* if **cl1,cr1** hold and is *cyclic* if all four of the above hold.

One can also define left-cyclic as **cl1,cl2** and similarly right-cyclic, which is related to cycle sets to be considered later.

Example 2.21. (*Permutational solution*, Lyubashenko, [1]) Let X be nonempty set, let f, g be bijective maps $X \longrightarrow X$, and let $r(x, y) = (g(y), f(x))$. We call r *a permutational map.* Then a) (X, r) is braided if and only if $fg = gf$. Clearly, in this case ${}^x y = {}^z y = g(y)$, and $y^x = y^z = f(y)$ for all $x, z, y \in X$, so $\mathcal{L}_x = g$, and $\mathcal{R}_x = f$ for all $x \in X$, hence (X, r) is cyclic. b) (X, r) is symmetric if and only if $f = g^{-1}$. Note that if $n \geq 2$, and $f \neq \mathrm{id}_X$, or $g \neq \mathrm{id}_X$, the solution (X, r) is never square-free.

The following examples come from Lemma 2.23.

Example 2.22.

(1) Every square-free non-degenerate braided set (X, r) is weak cyclic.
(2) Every square-free left cycle set (see Definition 2.27) satisfies **cl2**.
(3) Every square-free right cycle set (see Def. 2.27) satisfies **cr2**.

Lemma 2.23. *Assume (X, r) is with* **lri**. *Then the following conditions are equivalent*

(1) (X, r) *satisfies* **cl1**;
(2) (X, r) *satisfies* **cl2**;
(3) (X, r) *satisfies* **cr1**;
(4) (X, r) *satisfies* **cr2**;
(5) (X, r) *is cyclic.*

Proof. Note first that by Lemma 2.18 (X, r) is nondegenerate. Suppose first that **cl1** holds, so ${}^{y^x}x = {}^{y}x$ for all $x, y \in X$. In this equality we set $z = y^x$, and (by **lri**) $y = {}^x z$, and obtain by the nondegeneracy ${}^z x = {}^{{}^x z}x$ for all $x, z \in X$, i.e. **cl2**. The implication

$$\textbf{cl2} \Longrightarrow \textbf{cl1}$$

is analogous. It follows then that **cl1** and **cl2** are equivalent. But under the assumption of **lri** one has

$$\mathbf{cl1} \Longleftrightarrow \mathbf{cr1} \text{ and } \mathbf{cl2} \Longleftrightarrow \mathbf{cr2}.$$

We have shown that the conditions **cl1**, **cl2**, **cr1** **cr2**, are equivalent. Clearly, each of them implies the remaining three conditions, and therefore (see Definition 2.20) (X,r) is cyclic. The inverse implications follow straightforwardly from Definition 2.20. □

Proposition 2.24. *Let (X,r) be a quadratic set. Then any two of the following conditions imply the remaining third condition.*

(1) *(X,r) is involutive*
(2) *(X,r) is nondegenerate and cyclic.*
(3) **lri** *holds.*

Proof. (1), (2) $\Longrightarrow$ (3). By assumption r is involutive, hence $({}^yx)^{y^x} = x$, which together with **cl1** in the form ${}^yx = {}^{y^x}x$, implies

$$({}^{y^x}x)^{y^x} = x.$$

By the non-degeneracy of r it follows that given $x \in X$, every $z \in X$ can be presented as $z = y^x$, for appropriate uniquely determined y. We have shown

$$({}^zx)^z = x \text{ for every } x, z \in X.$$

It follows from Lemma 2.18 that ${}^z(x^z) = x$ is also in force for all $x, z \in X$, so **lri** is in force.

(2), (3) $\Longrightarrow$ (1). For the involutiveness of r it will be enough to show $({}^yx)^{y^x} = x$ for all $x, y \in X$. We set

$$z = {}^xy, \text{ so } y =^{\mathbf{lri}} z^x. \tag{2.7}$$

The equalities

$$x =^{\mathbf{lri}} ({}^yx)^y =^{\mathbf{cl2}} ({}^{{}^xy}x)^y = ({}^zx)^{z^x}$$

by (2.7), imply that $({}^zx)^{z^x} = x$, which, by the non-degeneracy of r is valid for all $z, x \in X$. Therefore r is involutive and the implication (2), (3) $\Longrightarrow$ (1) is verified.

(1), (3) $\Longrightarrow$ (2). By Lemma 2.18 (X,r) is nondegenerate. Let $x, y \in X$. We will show **cl1**. Consider the equalities

$$({}^{y^x}x)^{y^x} =^{\mathbf{lri}} x =^{r \text{ involutive}} ({}^yx)^{y^x}.$$

Thus by the nondegeneracy, ${}^{y^x}x = {}^yx$, which verifies **cl1**. The hypothesis of Lemma 2.23 is satisfied, therefore **cl1** implies (X,r) cyclic. The proposition has been proved. □

Remark 2.25. In Proposition 2.24 one can replace (2) by the weaker condition
(2') (X,r) nondegenerate and **cl1** holds.

We give now the definition of *(left) cycle set.*

Remark 2.26. The notion of cycle set was introduced by Rump, see [24] and was used in the proof of the decomposition theorem. In his definition Rump assumes that the left and the right actions on X are inverses (or in our language, condition **lri** holds), and that r is involutive. We keep the name "cycle set" but we suggest a bit more general definition here. We do not assume that r is involutive, neither that **lri** holds. Therefore we have to distinguish left and right cycle sets. Furthermore, Corollary 2.30 shows that for a square-free left cycle set conditions r is involutive and **lri** are equivalent.

Definition 2.27. Let (X, r) be a quadratic set.

a) [24] (X, r) is called *a left cycle set* if

$$\textbf{csl} \qquad {}^{({}^y t)}({}^y x) = {}^{({}^t y)}({}^t x) \text{ for all } x, y, t \in X$$

b) Analogously we define *a right cycle set* by the condition

$$\textbf{csr} \qquad (x^y)^{t^y} = (x^t)^{y^t} \text{ for all } x, y, t \in X.$$

Proposition 2.28. *Let (X, r) be involutive with* **lri**. *Then*

(i) *(X, r) is non-degenerate and cyclic.*
(ii) **csl** $\Longleftrightarrow$ **l1**.
(iii) **csl** $\Rightarrow ({}^x z)^y = {}^{x^y}(z^{y^x})$ *and* ${}^x(z^y) = ({}^{{}^y x} z)^{{}^x y}$ *for all $x, y, z \in X$.*
(iv) *Suppose that (X, r) is 2-cancellative and the monoid $S(X, r)$ has cancellation on monomials of length 3 then* **csl** $\Longleftrightarrow$ **l1** $\Longleftrightarrow$ *(X, r) is a symmetric set.*

Proof. Proposition 2.24 implies (i). To prove (ii) we first show **l1** $\Longrightarrow$ **csl**. Let $x, y, t \in X$. Consider the equalities

$${}^{({}^y t)}({}^y x) =^{\mathbf{l1}} {}^{{}^y t y}({}^{({}^y t)^y} x) =^{\mathbf{cl2,lri}} {}^{({}^t y)}({}^t x).$$

This verifies **csl**. Next we assume **csl** holds in (X, r) and shall verify **l1**. Let $x, y, z \in X$. Set $t = z^y$. Then, by **lri** $z = {}^y t$, and the following equalities verify **l1**

$${}^z({}^y x) = {}^{{}^y t}({}^y x) =^{\mathbf{csl}} {}^{({}^t y)}({}^t x) = {}^{({}^{z^y} y)}({}^{z^y} x) =^{\mathbf{cl1}} {}^{({}^z y)}({}^{z^y} x).$$

We have shown **csl** $\Longleftrightarrow$ **l1**.

We shall prove the first equality displayed in (iii). Assume **l1**. Note that **lri** and (X, r) cyclic imply the following equalities in $S(X, r)$:

$$x.y^x = {}^x(y^x).x^{y^x} = y.x^y, \tag{2.8}$$

and

$${}^y x.y = {}^{{}^y x} y.({}^y x)^y = {}^x y.x \tag{2.9}$$

Consider the equalities:

$${}^x z =^{\mathbf{lri}} {}^x({}^{y^x}(z^{y^x})) =^{\mathbf{l1}} {}^{(xy^x)}(z^{y^x}) = {}^{(yx^y)}(z^{y^x}) = {}^y({}^{x^y}(z^{y^x}))$$

using **l1** and (2.8) followed by **l1**. We apply $\bullet^y$ to both sides to get

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

For the second equality displayed in (iii), we consider

$$z^y =^{\mathbf{lri}} (({}^{{}^y x} z)^{{}^y x})^y =^{\mathbf{r1}} ({}^{{}^y x} z)^{({}^y x.y)} = (({}^{{}^y x} z)^{{}^x y.x} = (({}^{{}^y x} z)^{{}^x y})^x$$

using **r1** and (2.9) followed by **r1**. Then by **lri**, we obtain

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

This verifies (iii).

Assume now (X, r) is 2-cancellative and the monoid $S(X, r)$ has cancellation on monomials of length 3. Then by Lemma 2.15 one has

$$\mathbf{l1}, \mathbf{r1} \iff (X, r) \text{ is a symmetric set.} \tag{2.10}$$

Clearly, **lri** implies **l1** $\Longleftrightarrow$ **r1**, which together with (2.10) and (ii) gives

$$\textbf{csl} \Longleftrightarrow \textbf{l1} \iff (X,r) \text{ is a symmetric set.}$$

The proof of the proposition is now complete. □

We now look at the more general non-degenerate case.

Lemma 2.29. *Assume (X,r) is non-degenerate and square-free. (We do not assume involutiveness.) Then*

$$\begin{array}{lll} \textbf{l1} \implies \textbf{cl1}; & \textbf{r1} \implies \textbf{cr1}; & \textbf{lr3} \implies \textbf{cl1}, \textbf{cr1}; \\ \textbf{csl} \implies \textbf{cl2}; & \textbf{csr} \implies \textbf{cr2}. & \end{array}$$

Proof. We prove first **l1** $\implies$ **cl1**. Suppose (X,r) satisfies **l1**. Consider the equalities

$$ {}^{y}x = {}^{y}({}^{x}x) =^{\mathbf{l1}} {}^{{}^{y}x}({}^{y^{x}}x). \tag{2.11}$$

By Lemma 2.4.3, ${}^{t}x = t$ implies $x = t$, which together with (2.11) gives ${}^{y^{x}}x = {}^{y}x$. We have shown **l1** $\Longrightarrow$ **cl1**. The implication **r1** $\Longrightarrow$ **cr1** is analogous.

Suppose **lr3** holds. We set $z = y$ in the equality

$$ ({}^{x}y)^{({}^{x^{y}}(z))} = {}^{(x^{{}^{y}z})}(y^{z}), \quad \text{for all } x,y,z, \in X, \tag{2.12}$$

and obtain:

$$ ({}^{x}y)^{({}^{x^{y}}(y))} = {}^{(x^{y})}y. \tag{2.13}$$

By hypothesis (X,r) is square-free, therefore (2.13) and Lemma 2.4 imply

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

which proves **cl1**. If we set $x = y$ in (2.12), similar argument proves **cr1**. Therefore **lr3** implies that (X,r) is weakly cyclic as stated.

Assume **csl** is satisfied. So, for all $x, y, t \in X$ one has ${}^{{}^{y}t}({}^{y}x) = {}^{{}^{t}y}({}^{t}x)$ in which we substitute in $y = x$ and obtain

$$ {}^{{}^{x}t}({}^{x}x) = {}^{{}^{t}x}({}^{t}x).$$

This, since r is square-free, yields ${}^{({}^{x}t)}x = {}^{t}x$, which verifies **csl** $\Longrightarrow$ **cl2**. The proof of **csr** $\Longrightarrow$ **cr2** is analogous. □

Lemma 2.29 and Proposition 2.24 imply the following corollary.

Corollary 2.30. *Suppose (X,r) is non-degenerate and square free. If any of the conditions* **l1**, **r1**, **lr3**, **csl**, **csr** *hold then*

$$r \textit{ is involutive} \Longleftrightarrow \textbf{lri}$$

In this case (X,r) is cyclic.

Lemma 2.31. *Suppose (X,r) is non-degenerate, square-free and involutive (i.e. a quantum binomial set). Then condition* **lr3** *implies that (X,r) is symmetric set with* **lri**.

Proof. Note first that by Corollary 2.30 **lri** is in force. By Lemma 2.29 **lr3** implies the weak cyclic conditions **cl1, cl2**. We shall prove the implication

$$\textbf{lr3} \Longrightarrow \textbf{l1}.$$

Let $x, u, t \in X$. We have to show

$$ {}^{x}({}^{u}t) = {}^{{}^{x}u}({}^{x^{u}}t). \tag{2.14}$$

By assumption the equality (2.12) holds. We apply the left action ${}^{{}^{x^y}z}\bullet$, to each side of (2.12), and by **lri** we obtain

$$ {}^{x}y = {}^{({}^{x^y}z)}({}^{(x^{{}^y z})}(y^z)) \tag{2.15}$$

for all $x, y, z \in X$. First we set

$$ z = u^t, \quad y = {}^{z}t, \tag{2.16}$$

hence by **lri**,

$$ y^z = t, \quad {}^{t}z = u; \tag{2.17}$$

$$ {}^{y}z = {}^{y^z}z =^{\mathbf{cl1}} {}^{t}z = u, \qquad x^{{}^y z} = x^u. \tag{2.18}$$

Next

$$ {}^{z}t = {}^{u^t}t =^{\mathbf{cl1}} {}^{u}t; \quad \Rightarrow \qquad x^y = x^{{}^z t} = x^{{}^u t}, \tag{2.19}$$

which together with (2.16) and **lr3** yields

$$ {}^{x^y}z = {}^{x^{{}^u t}}(u^t) = ({}^{x}u)^{x^u t}. \tag{2.20}$$

We now use (2.16), (2.17), and (2.19), to obtain for the left-handside of (2.15)

$$ {}^{x}y = {}^{x}({}^{z}t) = {}^{x}({}^{u}t). \tag{2.21}$$

For right-handside of (2.15), we use (2.17),(2.18), and (2.20) to find

$$ {}^{({}^{x^y}z)}({}^{(x^{{}^y z})}(y^z)) = {}^{({}^x u)^{x^u} t}({}^{x^u}t) =^{\mathbf{cl1}} {}^{({}^x u)}({}^{x^u}t). \tag{2.22}$$

Now (2.21), (2.22), and (2.15) imply (2.14). □

Corollary 2.32. *Let (X, r) be a non-degenerate, square-free involutive set. Then*

$$(X, r) \text{ is symmetric} \iff \mathbf{csl}.$$

In this case (X, r) is cyclic and satisfies **lri**.

Proof. Assume **csl** holds. Note first that both **lri** and the conditions for (X, r) cyclic are satisfied. Indeed, by hypothesis r is involutive, which by Corollary 2.30 implies **lri**. It follows from Lemma 2.29 that **cl2** is satisfied, so **lri** and Lemma 2.23 imply all cyclic conditions for (X, r) cyclic. Now the hypothesis of Proposition 2.28 is satisfied, therefore **csl** $\Longrightarrow$ **l1**. Clearly **l1** and **lri** imply **r1** (see Remark 2.19). It follows by Proposition 2.6 that (X, r) is braided and therefore a symmetric set.

Assume next (X, r) is symmetric set. Clearly then **l1** holds, and since (X, r) is square-free and involutive, Corollary 2.30 implies **lri**. Furthermore, by Lemma 2.29 **l1** implies **cl1**, and therefore by **lri** all the conditions for (X, r) cyclic are satisfied. We use again Proposition 2.28 to deduce **csl**. □

Remark 2.33. Note that in [24] it is shown that under the assumptions that (X, r) is square-free, non-degenerate, involutive and satisfies **lri**, then (X, r) is braided if and only if it is a cycle set. Here we show that a weaker hypothesis is enough: Assuming that (X, r) is square-free, non-degenerate, and involutive, we show that condition **csl** is equivalent to (X, r) braided, and each of them implies **lri**.

Theorem 2.34. *Suppose (X, r) is a quantum binomial set (i.e. non-degenerate, involutive and square-free). Then the following conditions are equivalent:*

(1) *(X, r) is a set-theoretic solution of the Yang-Baxter equation.*
(2) *(X, r) satisfies* **l1**.
(3) *(X, r) satisfies* **l2**.
(4) *(X, r) satisfies* **r1**.
(5) *(X, r) satisfies* **r2**.
(6) *(X, r) satisfies* **lr3**
(7) *(X, r) satisfies* **csl**.

In this case (X, r) is cyclic and satisfies **lri**.

Proof. By Lemma 2.5 and Lemma 2.9

$$(X, r) \text{ symmetric} \Longrightarrow \mathbf{l1}, \mathbf{l2}, \mathbf{r1}, \mathbf{r2}, \mathbf{lr3}$$

By Proposition 2.6 each of the conditions **l1**, **r1** implies "(X, r) is symmetric". Note that **l2** is just **l1** and **lr3**, **r2** is just **r1** and **lr3**. Lemma 2.31 gives **lr3** $\Longrightarrow (X, r)$ is symmetric. This verifies the equivalence of the first six conditions. Finally, Corollary 2.32 implies the equivalence **csl** $\Longleftrightarrow (X, r)$ is symmetric. □

3. Matched pairs of monoids and braided monoids

In this section we shall study the 'exponentiation' of a braided set (X, r) to a matched pair (S, S) of monoids with property **M3**. We shall also study the converse.

3.1. **Strong matched pairs and monoid factorisation.** The notion of matched pair of groups in relation to group factorisation has a classical origin. For finite groups it was used in the 1960s by Kac and Paljutkin in the construction (in some form) of certain Hopf algebras [15]. More recently, such 'bismash product' or 'bicrossproduct' Hopf algebras were rediscovered respectively by Takeuchi [25] and Majid [20]. The latter also extended the theory to Lie group matched pairs [19] and to general Hopf algebra matched pairs [20]. By now there have been many works on matched pairs in different contexts and we refer to the text [22] and references therein. In particular, this notion was used by Lu, Yan and Zhu to study the set-theoretic solution of YBE and the associated 'braided group', see [17] and the excellent review [26].

In fact we will need the notion of a matched pair of monoids [20], to which we shall add some refinements that disappear in the group case.

Definition 3.1. (S, T) is a matched pair of monoids if T acts from the left on S by ${}^{(\ )}\bullet$ and S acts T from the right by $\bullet^{(\ )}$ and these two actions obey

$$\begin{array}{llll} \mathbf{ML0}: & {}^a1 = 1, \quad {}^1u = u; & \mathbf{MR0}: & 1^u = 1, \quad a^1 = a \\ \mathbf{ML1}: & {}^{(ab)}u = {}^a({}^bu), & \mathbf{MR1}: & a^{(uv)} = (a^u)^v \\ \mathbf{ML2}: & {}^a(u.v) = ({}^au)({}^{a^u}v), & \mathbf{MR2}: & (a.b)^u = (a^{{}^bu})(b^u), \end{array}$$

for all $a, b \in T, u, v \in S$.

The following proposition is well-known, though more often for groups rather than monoids. For completeness only, we recall briefly the proof as well.

Proposition 3.2. *A matched pair (S, T) of monoids implies a monoid $S \bowtie T$ (called the* double cross product*) built on $S \times T$ with product and unit*

$$(u, a)(v, b) = (u.{}^av, a^v.b), \quad 1 = (1, 1), \quad \forall u, v \in S, \ a, b \in T$$

and containing S,T as submonoids. Conversely, if there exists a monoid R factorising into S,T in the sense that the product $\mu : S\times T\to R$ is bijective then (S,T) are a matched pair and $R\cong S\bowtie T$ by this identification μ.

Proof. A direct proof immediate, see for example [20] in the monoid case:

$$W_1=[(u,a).(v,b)].(w,c)=(u.({}^av),(a^v).b).(w,c)=(a({}^av)({}^{((a^v)b)}w),(((a^v)b)^w)c)$$
$$=(u[{}^a(v({}^bw))],[((a^v)b)^w]c)$$
$$W_2=(u,a).[(v,b).(w,c)]=(u,a).(v({}^bw),(b^w)c)(u.({}^a(v({}^bw))),a^{(v({}^bw)}.(b^w)c))$$
$$=(u[{}^a(v({}^bw))],[((a^v)b)^w]c)$$

Clearly, $W_1=W_2$, on using the matched pair properties, hence $S\bowtie T$ is a monoid. It is also clear from the construction that the converse is true: for $S\bowtie T$ with product in the form stated to be a monoid we need the matched pair conditions. For example,

$$(u,a).(1,1)=(u.{}^a1,a^1.1)=(u,a)$$

requires $u.{}^a1=u$ and $a^1=a$, for all $u\in S,a\in T$. The first equality implies ${}^a1=1$, similarly the other cases of **ML0, MR0**. Likewise, consider the equalities:

$$W_1=[(1,a)(u,1)](v,1)=({}^au,a^u).(v,1)=({}^au.({}^{a^u}v),(a^u)^v)$$
$$W_2=(1,a)[(u,1)(v,1)]=(1,a)(u.{}^1v,1^v)=(1,a)(uv,1)=({}^a(uv),a^{(uv)}).$$

To be associative we need $W_1=W_2$, therefore **MR1, ML2**. Analogously, we obtain the other requirements for a matched pair from $S\bowtie T$ a monoid.

Now suppose R factors into S,T. Consider $a\in T,u\in S$ and $au\in R$. By the bijectivity it must be the product of some unique elements $u'a'$ for $u'\in S$ and $v'\in T$. We define ${}^{(\,)}\bullet:T\times S\to S$ and $\bullet^{(\,)}:T\times S\to T$ by $u'={}^au$ and $a'=a^u$. It is then easy to see that these are actions and form a matched pair. Indeed, the product map allows us to identify $R\cong S\times T$ by $u.a=(u,a)$. In this case associativity in R implies

$$(u.a).(v.b)=u(a.v)b=u.({}^av.a^v)b=(u.{}^av).(a^v.b)$$

i.e. the product of R has the double cross product form when referred to $S\times T$ for the maps ${}^{(\,)}\bullet,\bullet^{(\,)}$ defined as above. □

Next we introduce the following natural notion in this context. It is automatically satisfied in the group case but is useful in the monoid case:

Definition 3.3. A *strong monoid factorisation* is a factorisation in submonoids S,T as above such that R also factorises into T,S. We say that a matched pair is *strong* if it corresponds to a strong factorisation.

In this case we have two bijections

$$\mu_1:S\times T\to R,\quad \mu_2:T\times S\to R$$

and hence an invertible map

$$r_{T,S}=\mu_1^{-1}\mu_2:T\times S\to S\times T,\quad r_{T,S}(a,u)=\mu_1^{-1}({}^au.a^u)=({}^au,a^u).$$

We also have two double crossed products $S\bowtie T$ and $T\bowtie S$ and two underlying matched pairs. If (S,T) is a strong matched pair we shall denote the actions for

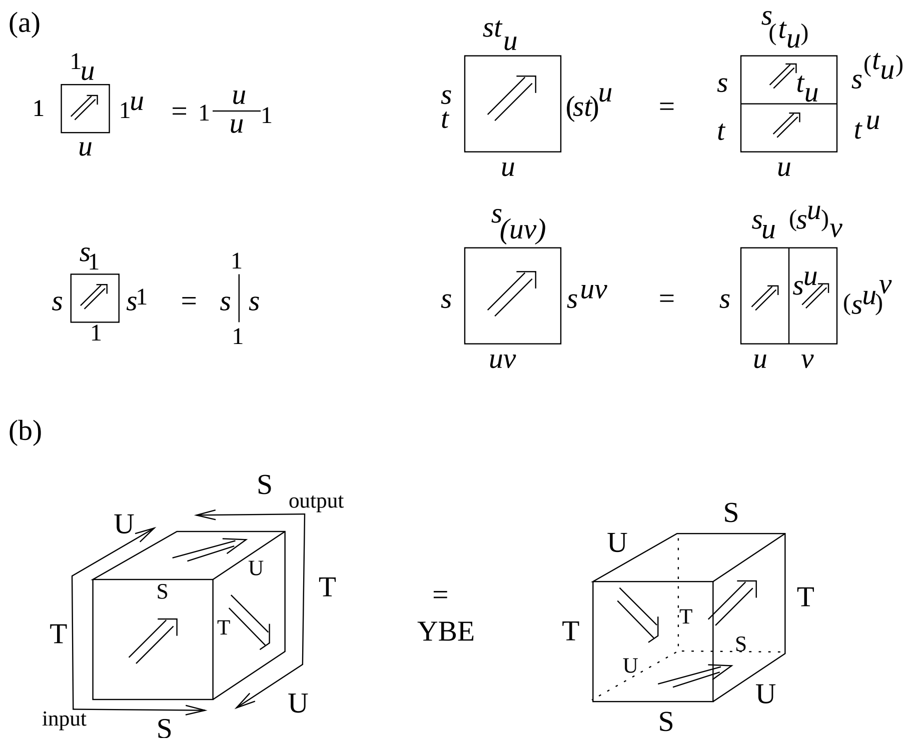

FIGURE 1. Notation (a) and (b) subdivision property encoding the axioms of a matched pair with $\Rightarrow$ the map $r_{T,S}$, and (c) Yang-Baxter equation as surface transport around a cube

the accompanying matched pair (T, S) by different notations $\triangleright : S \times T \to T$ and $\triangleleft : S \times T \to S$ to keep them distinct from the previous ones. They are defined by

$$r^{-1}_{T,S}(u, a) = (u \triangleright a, u \triangleleft a)$$

and are characterised with respect to the original actions by

$$\text{(3.1)} \quad {}^{a}u \triangleright a^{u} = a, \quad {}^{a}u \triangleleft a^{u} = u, \quad {}^{u \triangleright a}(u \triangleleft a) = u, \quad (u \triangleright a)^{u \triangleleft a} = a, \quad \forall u \in S, a \in T.$$

We note also that the axioms Definition 3.1 of a matched pair (S, T) have the nice interpretation and representation as a subdivision property, see [18, 22]. Thus is recalled in Figure 1 where a box is labelled on the left and lower edge by T, S and the other two edges are determined by the actions. This operation $\Rightarrow$ is exactly the map $r_{T,S}$ above. If one writes out the subdivision property as a composition of maps, it says

$$r_{T,S}(ab, u) = (\mathrm{id} \times \cdot) r_{12} r_{23}(a, b, u), \quad r_{T,S}(a, uv) = (\cdot \times \mathrm{id}) r_{23} r_{12}(a, u, v)$$

where $r = r_{T,S}$ and the numerical suffices denote which factors it acts on. This is just the subdivision property written out under a different notation, but is suggestive of the axioms of a coquasitriangular structure in the case when $T = S$, a point of view used in [17]. Finally, returning to Figure 1, if the matched pair is strong it means precisely that $\Rightarrow$ is reversible. The reversed map evidently obeys the same subdivision property and therefore corresponds exactly to another matched pair, namely (T, S). This proves that a matched pair is strong in the sense $r_{T,S}$ invertible if an only if (T, S) is another matched pair with actions related by (3.1).

We also define a braided monoid analogously to the term 'braided group' in the sense of [26], [17]. (This term should not be confused with its use to describe Hopf algebras in braided categories in another context).

Definition 3.4. An **M3**-*monoid* is a monoid S forming part of a matched pair (S, S) for which the actions are such that

$$\mathbf{M3}: \quad {}^{u}v u^{v} = uv$$

holds in S for all $u, v \in S$. We define the *associated map* $r_S : S \times S \to S \times S$ by $r_S(u, v) = ({}^{u}v, u^{v})$. A *braided monoid* is an **M3**-monoid S where r_S is bijective and obeys the YBE.

Similarly a strong **M3**-monoid is one where (S, S) is a strong matched pair and this clearly happens precisely when r_S is invertible.

Proposition 3.5. *If an* **M3**-*monoid S has left cancellation then r_S obeys the YBE. Hence a strong* **M3**-*monoid with left cancellation is necessarily a braided monoid.*

Proof. Clearly **l1,r1** on the set of S hold in view of **ML1,MR1,M3**. Next we consider the identities

$${}^{u}(vw) =^{\mathbf{M3}} {}^{u}({}^{v}w v^{w}) =^{\mathbf{ML2,ML1}} {}^{uv}w.{}^{(u^{{}^{v}w})}(v^{w})$$

$${}^{u}v.{}^{u^{v}}w =^{\mathbf{M3,ML1}} {}^{{}^{u}v u^{v}}w.({}^{u}v)^{({}^{u^{v}}w)} =^{\mathbf{M3}} {}^{uv}w.({}^{u}v)^{({}^{u^{v}}w)}.$$

The two left hand sides are equal by **ML2** and hence if we can cancel on the left, the second factors on the right are equal, which is **lr3** on the set S. We then apply Lemma 2.5 to the set S. □

This covers the group case where r_S does automatically obey the YBE and have an inverse. Also note that it is perfectly equivalent to think of an **M3**-monoid as a pair (S, r_S) where S is a monoid and r_S is a set map such that ${}^{u}v$ and u^{v} defined by r_S via the formula above makes (S, S) a matched pair and such that the product of S is r_S-commutative in the sense $\mu r_S(u, v) = uv$, where μ is the product in S.

There is also a 'surface transport' description of the YBE. Here, it was already observed in [22] that the subdivision property in Figure 1(b) implies a notion of surface transport defined by the matched pair. Fitting in with this now is a pictorial description of the generalised Yang-Baxter equation shown in part (c) of the figure, which holds in any category for a collection of such maps $r_{T,S}$; we require three objects (in our case monoids) S, T, U and such 'exchange' maps which we represent as $\Rightarrow$ as above. The Yang-Baxter equation then has the interpretation that if we 'surface transport' elements along the edges U, T, S shown as 'input' around the top and front of the cube to the output using $\Rightarrow$, and keeping the plane of the surface with respect to which the notation in Figure 1(a) is interpreted with normal outward, we get the same answer as the going around the bottom and back of the cube with normal pointing inwards. In other words the net 'surface-holonomy' with normal always outwards right round the cube should be the identity operation. In this way the YBE has the interpretation of zero 'higher curvature'. This works in any category (but not a point of view that we have seen before), but in our case fits in with the subdivision property to imply a genuine surface-transport gauge theory. We note that it appears to be somewhat different from ideas of 2-group gauge theory currently being proposed in the physics literature. Theorem 3.22 will use this to give a matched pair point of view on when an **M3**-monoid is braided.

Assume (X,r) is a braided set. We shall mostly be interested in $S = S(X,r) = \langle X|\Re(r)\rangle$ the associated Yang-Baxter monoid. Clearly, S is graded by length:

$$S = \bigcup_{n\geq 0} S^n; \quad S^0 = 1, \quad S^1 = X, \quad S^n = \{u \in S; |u| = n\}$$

and

$$S^n.S^m \subseteq S^{n+m}.$$

In the sequel whenever we speak of a graded monoid S we shall mean that it is generated by $S^1 = X$ and graded by length. An **M3** or braided monoid (S, r_S) is *graded* if (S,S) is a graded matched pair. For a graded **M3**-monoid (S, r_S), we define the *restriction* $r = r_X$ of r_S on $X \times X$, where X is the degree 1 generating set. The left and the right actions respect the grading of S, and condition **M3** implies

$$r(x,y) = ({}^xy, x^y), \quad r : X\times X \to X\times X.$$

as required for consistency with our notations in Section 2.

3.2. **Matched pair construction of the braided monoid** (S, r_S) **from** (X,r)**.** Here, to each braided set (X,r) we will associate a matched pair (S,S) ($S = S(X,r)$) with left and right actions uniquely determined by r, which defines a unique 'braided monoid' (S, r_S) associated to (X,r). This is not a surprise given the analogous results for the group $G(X,r)$ [17] but our approach is necessarily different. In fact we first construct the matched pair or monoids (Theorem 3.6) which is a self-contained result and then consider r_S (Theorem 3.14). The reader should be aware that due to the possible lack of cancellation in S (we want the statements to be as general as possible) the proofs of our results for monoids are difficult and necessarily involve different computations and combinatorial arguments. Surely, the results can not be extracted from the already known results from the group case. Nevertheless, the monoid case is the one naturally arising in this context. Both the monoid $S(X,r)$ and the quadratic algebra $\mathcal{A} = \mathcal{A}(k,X,r)$ over a field k, see 2.1 are of particular interest. It is known for example that in some special cases of finite solutions (X,r), S, and A have remarkable algebraic and homological properties, see [10, 8, 9].

We shall extend the left and right actions ${}^x\bullet$ and $\bullet^x$ on X defined via r , see (1.1), to a left action

$${}^{(\,)}\bullet : S\times S \longrightarrow S$$

and a right action

$$\bullet^{(\,)} : S\times S \longrightarrow S.$$

By construction, these actions agree with the grading of S, i.e. $|{}^au| = |u| = |u^a|$, for all $a, u \in S$.

Theorem 3.6. *Let* (X,r) *be a braided set and* $S = S(X,r)$ *the associated monoid. Then the left and the right actions*

$${}^{(\,)}\bullet : X\times X \longrightarrow X, \text{ and } \bullet^{(\,)} : X\times X \longrightarrow X$$

defined via r *can be extended in a unique way to a left and a right action*

$${}^{(\,)}\bullet : S\times S \longrightarrow S, \text{ and } \bullet^{(\,)} : S\times S \longrightarrow S.$$

which make S a strong graded **M3***-monoid. The associated bijective map r_S restricts to r.*

Proof. The proof of the theorem will be made in several steps and we will need several intermediate results under the hypothesis of the theorem.

We will define first left and right actions of S on the free monoid $\langle X\rangle$.

$$^{(\ )}\bullet : S\times\langle X\rangle \longrightarrow \langle X\rangle, \text{ and } \bullet^{(\ )} : \langle X\rangle\times S \longrightarrow \langle X\rangle$$

We set

$$^{u}1 := 1,\ 1^{u} := 1 \text{ for all } u\in S.$$

Clearly, the free monoid $\langle X\rangle$ is graded by length

$$\langle X\rangle = \bigcup_{n\geq 0} X^n, \text{ where } X^0 = 1, X^1 = X, X^n = \{u\in\langle X\rangle; |u| = n\}$$

and

$$X^n.X^m \subseteq X^{n+m}.$$

Step 1. We define the *"actions"*

$$^{(\ )}\bullet : X\times\langle X\rangle \longrightarrow \langle X\rangle, \text{ and } \bullet^{(\ )} : \langle X\rangle\times X \longrightarrow \langle X\rangle \tag{3.2}$$

recursively as follows. For $n=1$ we have $X^1 = X$, and the actions

$$^{(\ )}\bullet : X\times X^1 \longrightarrow X^1, \text{ and } \bullet^{(\ )}\ X^1\times X \longrightarrow X^1$$

are well defined via r, see (1.1).

Assuming that the "actions" $X\times X^n \longrightarrow X^n$, and $X^n\times X \longrightarrow X^n$, are defined for n, we will define them for $n+1$. Let $u\in X^{n+1}$. Then $u = y.a = b.z$, where $y,z\in X, a,b\in X^n$. We set

$$^{x}u = {}^{x}(y.a) := ({}^{x}y)({}^{x^{y}}a), \tag{3.3}$$

$$u^{x} = (bz)^{x} := (b^{{}^{z}x})(z^{x}). \tag{3.4}$$

This way we have defined the "actions" $X\times X^n \longrightarrow X^n$, and $X^n\times X \longrightarrow X^n$, for all $n\geq 1$. The next lemma shows now that these definitions are consistent with the multiplication in $\langle X\rangle$, therefore these are well-defined "actions" (3.2) as required to complete step 1.

Lemma 3.7.

a) **ML2** *holds for X "acting" (on the left) on $\langle X\rangle$, that is:*

$$^{x}(ab) = ({}^{x}a).({}^{x^{a}}b) \text{ for all } x\in X, a,b\in\langle X\rangle,\ \ |a|,|b|\geq 1.$$

b) **MR2** *holds for X "acting" (on the right) on $\langle X\rangle$, that is:*

$$(ab)^{x} = (a^{{}^{b}x})b^{x} \text{ for all } x\in X,\ a,b\in\langle X\rangle,\ \ |a|,|b|\geq 1.$$

Note that these are equalities of monomials in the free monoid $\langle X\rangle$.

Proof. We prove (a) by induction on the length $|a| = n$. Definition 3.3 gives the base for the induction. Assume the statement part a) is true for all $a,b\in\langle X\rangle$, with $|a| \leq n$. Let $|a| = n+1$. Then $a = ya_1$, with $y \in X, |a_1| = n$. Consider the equalities:

$$\begin{aligned} {}^x(ab) &= {}^x(y(a_1b)) = ({}^xy).({}^{x^y}(a_1.b)) \text{ : by (3.3)} \\ &= ({}^xy).(({}^{x^y}a_1).({}^{((x^y)^{a_1})}b) \text{ : by the inductive assumption} \\ &= ({}^x(ya_1)).({}^{x^{ya_1}}b) \text{ : by (3.3)} \\ &= {}^xa.({}^{x^a}b). \end{aligned}$$

This verifies (a). The proof of (b) is analogous. □

Step 2. Extend the "actions" (3.2) to a left and a right actions ${}^{(\ )}\bullet : S \times \langle X\rangle \longrightarrow \langle X\rangle$, and $\bullet^{(\ )} : \langle X\rangle \times S \longrightarrow \langle X\rangle$ of S onto $\langle X\rangle$.

Note here that conditions **l1** (respectively **r1**) on X imply that there is a well defined left action $S \times X \longrightarrow X$, and a right action $X \times S \longrightarrow X$ given by the equalities:

$${}^{(x_1 \dots x_k)}y : {}^{x_1}(\dots({}^{x_{k-1}}({}^{x_k}y))..)$$

and

$$y^{(x_1 \dots x_k)} := (\dots((y^{x_1})^{x_2})\dots)^{x_k}.$$

Clearly ${}^{(ab)}x = {}^a({}^bx)$, and $x^{(ab)} = (x^a)^b$, for all $x \in X, a, b \in S$.

Proposition 3.8. *The actions ${}^x\bullet$, and $\bullet^x$ on $\langle X\rangle$ extend to ${}^a\bullet$, and $\bullet^a$ for arbitrary monomials $a \in S$. That is to left and right actions $S \times \langle X\rangle \longrightarrow \langle X\rangle$, and $\langle X\rangle \times S \longrightarrow \langle X\rangle$ obeying*

$$\textbf{ML1} \textit{ for } {}^S\langle X\rangle : \quad {}^{ab}u = {}^a({}^bu), \quad \textbf{MR1} \textit{ for } \langle X\rangle^S : \quad u^{ab} = (u^a)^b$$

for all $a, b \in S$, $u \in \langle X\rangle$.

Proof. We have to show that the following equalities hold for all $x, y \in X, u \in \langle X\rangle$

$$\textbf{L1} \text{ for } {}^S\langle X\rangle : \quad {}^x({}^yu) = {}^{{}^xy}({}^{x^y}u) \tag{3.5}$$

$$\textbf{R1} \text{ for } \langle X\rangle^S : \quad (u^x)^y = (u^{{}^xy})^{x^y}. \tag{3.6}$$

We denote these conditions in upper case to distinguish them from **l1,r1** on X itself. We prove (3.5) by induction on $|u| = n$. Clearly, when $|u| = 1$, (3.5) is simply condition **l1** on X. Assume (3.5) is true for all $u \in X^n$. Let $u \in X^{n+1}$. We can write $u = tv$, with $t \in X$, $v \in X^n$. Then

$${}^x({}^yu) = {}^x({}^y(tv)) =^{Lemma\ 3.7a)} {}^x(({}^yt).({}^{y^t}v)) =^{Lemma\ 3.7a)} ({}^x({}^yt))({}^{x^{{}^yt}}({}^{y^t}v)) \tag{3.7}$$

$$=^{\text{inductive ass.}} ({}^x({}^yt))({}^{((x^{{}^yt}).(y^t))}v) =^{Lemma\ 3.7b)} ({}^{xy}t)({}^{(xy)^t}v). \tag{3.8}$$

We have shown

$${}^x({}^yu) = ({}^{xy}t)({}^{(xy)^t}v) = w. \tag{3.9}$$

Similarly, as in (3.7), (3.8) we obtain:

$${}^{{}^xy}({}^{x^y}u) = {}^{{}^xy}({}^{x^y}tv)({}^{{}^xy}({}^{x^y}t))({}^{({}^xy.x^y)^t}v) = w_1. \tag{3.10}$$

We use conditions **L1** and **R2** on ${}^SX$ to simplify the right-hand side monomial w_1 in this equality:

$$w_1 = ({}^{{}^xy}({}^{x^y}t))({}^{({}^xy.x^y)^t}v) =^{\mathbf{L1},\mathbf{R2}} ({}^{xy}t)({}^{(xy)^t}v) = w. \tag{3.11}$$

Now (3.9), (3.10), (3.11) imply

$$ {}^{x_y}({}^{x^y}u) = w = {}^{x}({}^{y}u) $$

We have shown that (3.5) holds for all $u \in \langle X\rangle$, and all $x, y \in X$. Therefore the equality

$$ {}^{(x_1 \dots x_k)}u : {}^{x_1}(\dots({}^{x_{k-1}}({}^{x_k}u))..) $$

gives a well defined left action $S \times \langle X\rangle \longrightarrow \langle X\rangle$, which satisfies **ML1**.

The proof of (3.6) is analogous. So the right action $\langle X\rangle \times S \longrightarrow \langle X\rangle$ is also well defined, and satisfies **MR1**. □

Proposition 3.9.

$$ \textbf{ML2 for } {}^S\langle X\rangle : \quad {}^a(uv) = ({}^au).({}^{(a^u)}v), \qquad \textbf{MR2 for } \langle X\rangle^S : \quad (vu)^a = (v^{{}^ua}).(u^a), $$

for all $a \in S, u, v \in \langle X\rangle$.

Proof. We prove first the following equalities:

$$ (3.12) \quad {}^a(yv) = ({}^ay)({}^{a^y}v), \qquad (vy)^a = (v^{{}^ya})(y^a), \text{for all } a \in S, y \in X, v \in \langle X\rangle. $$

The proofs of the two identities in (3.12) are analogous. In both cases one uses induction on $|a|$. We shall prove the left-hand side equality. By the definition of the left action one has ${}^yxv = ({}^yx)({}^{y^x}v)$. This gives the base for the induction. Assume (3.12) holds for all a, with $|a| \le n$. Let $a_1 \in S$, $|a_1| = n+1$, $y \in X$, $v \in \langle X\rangle$. Clearly, $a_1 = ax$, where $x \in X$, $a \in S, |a| = n$. Consider the equalities

$$ {}^{ax}(yv) =^{\mathbf{ML1}} {}^a({}^x(yv)) =^{(3.3)} {}^a[({}^xy)({}^{x^y}v)] =^{\text{inductive ass.}} [{}^a({}^xy)][{}^{(a^{{}^xy})}({}^{x^y}v)] $$

$$ =^{\mathbf{ML1}} [{}^{(ax)}y][{}^{((a^{{}^xy}).(x^y))}v] =^{(3.4)} [{}^{(ax)}y][{}^{(ax)^y}v]. $$

We have verified the left-hand side of (3.12).

Now we verify Proposition 3.9) using again induction on $|a|$. **Step 1.** Base for the induction. The equality ${}^x(uv) = ({}^xu).({}^{x^u}v)$, for all $x \in X$, $u, v \in \langle X\rangle$, is verified by Lemma 3.7. **Step 2.** Assume the statement holds for all monomials $a \in S$, with $|a| \le n$. Let $a_1 = ax \in S$, where $|a| = n$, $x \in X$. The following equalities hold in $\langle X\rangle$:

$$ {}^{ax}(uv) =^{\mathbf{ML1}} {}^a({}^x(uv)) = {}^a({}^xu).({}^{x^u}v) =^{\text{inductive ass.}} [{}^a({}^xu)][{}^{(a^{{}^xu})}({}^{x^u}v)] $$

$$ =^{\mathbf{ML1}} [{}^{ax}u][{}^{((a^{{}^xu})(x^u))}v] =^{(3.12)} [{}^{ax}u][{}^{(ax)^u}v]. $$

This verifies the left-hand half for the stated proposition. Analogous argument proves the right-hand half. □

We will show next that the left and right actions of S on $\langle X\rangle$ defined and studied above induce naturally left and right actions ${}^{(\,)}\bullet : S \times S \longrightarrow S$, and $\bullet^{(\,)} : S \times S \longrightarrow S$. We need to verify that the actions agree with the relations in S. We start with the following lemma, which gives an analogue of **L2**, but for S acting on monomials of length 2.

Lemma 3.10. *The following equalities hold in* X^2.

$$ {}^a(yz) = {}^a({}^yz.y^z), \qquad (yz)^a = ({}^yz.y^z)^a, \qquad \textit{for all } a \in S; y, z \in X. $$

Proof. As usual we use induction on the length $|a| = n$.

Step 1. $|a| = 1$, so $a = x \in X$. Then by **l2** on X we have

$$^{x}(yz) = {}^{x}({}^{y}z.y^{z}), \quad \text{for all } x, y, z \in X.$$

Step 2. Assume the statement of the lemma holds for all $y, z \in X$, and all $a \in S$, with $|a| = n$. Let $a_1 \in S, |a_1| = n + 1$, so $a_1 = ax, x \in X, a \in S, |a| = n$. Now

(3.13)

$$^{(ax)}(yz) =^{\mathbf{ML1}} {}^{a}[{}^{x}(yz)] = {}^{a}[({}^{x}y)({}^{x^{y}}z)] =^{\text{induct. ass.}} {}^{a}[({}^{({}^{x}y)}({}^{x^{y}}z)).({}^{x}y)^{({}^{x^{y}}z)}] = {}^{a}(uv),$$

where for convenience we denote

$$u = {}^{({}^{x}y)}({}^{x^{y}}z) =^{\mathbf{l1}} {}^{x}({}^{y}z), \quad v = ({}^{x}y)^{({}^{x^{y}}z)} =^{\mathbf{lr3}}= {}^{x^{{}^{y}z}}(y^{z}).$$

So

$$uv = ({}^{x}({}^{y}z))({}^{x^{{}^{y}z}}(y^{z})) =^{Lemma\ 3.10} {}^{x}({}^{y}z.y^{z}). \tag{3.14}$$

is an equality in X^2. It follows from (3.13) and (3.14) that

$$^{(ax)}(yz) = {}^{a}(uv) =^{(3.14)} {}^{a}({}^{x}({}^{y}z.y^{z})) =^{\mathbf{ML1}} {}^{ax}({}^{y}z.y^{z}).$$

This proves the first equality stated in the lemma. Analogous argument verifies the second. □

The following statement shows that the left action agrees with all replacements coming from the defining relations of S, and therefore agrees with equalities of words in S

Proposition 3.11. *The left and right actions* $^{(\,)}\bullet : S\times S \longrightarrow S$, *and* $\bullet^{(\,)} : S\times S \longrightarrow S$ *are well defined. They make* (S, S) *a graded matched pair of monoids.*

Proof. We need to verify the following equalities in S:

$$^{a}(u.yz.v) = {}^{a}(u.({}^{y}z.y^{z}).v). \tag{3.15}$$

It easily follows from (3.15) that

$$w_1 = w_2 \text{ is an equality in } S \implies {}^{a}w_1 = {}^{a}w_2 \text{ is an equality in } S.$$

Indeed, $w_1 = w_2$ is an equality in S if and only if w_2 can be obtained from w_1 after a finite number of replacements coming from the relations $\Re(r)$. Note that each relation in $\Re(r)$ has the shape $yz = {}^{y}z.y^{z}$, where $y, z \in X$.

We prove now (3.15). Let $a, u, v \in S, y, z \in X$. Then

$$^{a}(u.yz.v) = [{}^{a}u].[{}^{a^{u}}(yz)].[{}^{a^{u(yz)}}v] =^{Lemma\ 3.10} [{}^{a}u].[{}^{a^{u}}({}^{y}z.y^{z})].[{}^{a^{u(yz)}}v]$$

$$= {}^{a}[u.({}^{y}z.y^{z})].[{}^{a^{u(yz)}}v] =^{(3.16)} {}^{a}[u.({}^{y}z.y^{z})].[{}^{(a^{(u({}^{y}z.y^{z}))})}v] =^{\mathbf{ML2}} {}^{a}[u.({}^{y}z.y^{z}).v].$$

We used above the following equality implied by condition **M3**:

$$a^{u(yz)} = ((a^{u})^{y})^{z}) = ((a^{u})^{{}^{y}z})^{y^{z}}. \tag{3.16}$$

□

Proposition 3.12. *S in Proposition 3.11 is an **M3**- monoid (i.e. for every* $u, v \in S$, *the equality* $uv = {}^{u}v.u^{v}$ *holds in S.)*

Proof. Using induction on $|w|$ we first show that there is an equality in S

$$xw = {}^{x}w.x^{w} \text{ for all } w \in S, x \in X. \tag{3.17}$$

When $|w| = 1$, one has $r(xw) = {}^{x}w.x^{w}$, therefore (3.17) either belongs to the set of defining relations $\Re(r)$ (1.3) for S, or is an equality in X^2. Assume (3.17) is true for all w with $|w| \leq n$. Let $v \in S, |v| = n+1$, $x \in X$. Present $v = yw$, where $y \in X, w \in S, |w|n$. The following equalities follow from the associativity of the multiplication in S, the inductive assumption, and **ML2**.

$$x.v = x.(yw) = (xy)w = ({}^{x}y.x^{y})w = ({}^{x}y)(x^{y}.w)({}^{x}y)[({}^{x^{y}}w)(x^{y})^{w}]$$
$$=^{\mathbf{MR1}} [({}^{x}y)({}^{x^{y}})w][x^{(yw)}] =^{\mathbf{ML2}} \ [{}^{x}(yw)].[x^{(yw)}].$$

This proves (3.17) for all x, w, $x \in X, w \in S$.

Next we use induction on $|u|$ to prove the statement of the proposition.

Assume

$$uv = {}^{u}v.u^{v} \quad \text{for all} \quad u, v \in S, \quad \text{with} \quad |u| \leq n.$$

Let $u_1 = ux$, where $u \in S, |u| = n$, $x \in X$. Then the associative law in S, the inductive assumption, **ML1**, and **MR2** imply the following equalities

$$(ux)v = u(xv) =^{(3.17)} u({}^{x}v.x^{v}) = [u.{}^{x}v].x^{v}$$
$$= [{}^{u}({}^{x}v)].[u^{({}^{x}v)}).(x^{v})] =^{\mathbf{ML1},\mathbf{MR2}} \ [{}^{(ux)}v].[(ux)^{v}]$$

□

We have shown that the left and the right actions constructed above make (S, S) a graded matched pair of monoids with condition **M3**. Moreover the matched pair axioms imply that these actions are uniquely determined by r. So we define the associated braided monoid (S, r_S), with $r_S(u, v) = ({}^{u}v, u^{v})$, which is also uniquely determined by r.

It remains to show that (S, S) is a strong matched pair. By Theorem 3.14.1 (S, r_S) is a braided set, in particular r_S is a bijective map, therefore by Proposition 3.21.2 (S, S) is a strong matched pair. This completes the proof of Theorem 3.6 □

In the case when (S, r_S) is a graded **M3**-monoid generated by X, $(X = S^1)$, by definition, the set X is invariant under the left and the right actions. The next proposition will be used in this case, but later on we will also need it more generally and therefore we prove it now in this greater generality. Thus, suppose (S, r_S) is an **M3**-monoid (not necessarily graded). Suppose S is generated by a set X which is invariant under the left and the right actions of the matched pair. We define the restriction $r = r_X$ of r_S to $X \times X$, so $r(x, y) = ({}^{x}y, x^{y})$ as usual. Then (X, r) is a set with a quadratic map and condition **M3** implies that the set of defining relations $\Re(S)$ of S satisfy

$$\Re(S) \supseteq \Re(r),$$

where in general there might be a strict inequality ($\Re(r)$ are the quadratic relations coming from r, see (1.3)).

The monoid S can be presented as $S = \langle X; \Re(S)\rangle$ and, it is, in general, homomorphic image of the monoid $S(X, r) = \langle X; \Re(r)\rangle$. Clearly, S is graded *iff* $\Re(S)$ consists of homogeneous relations. All relations in S are results of replacements coming from the set of defining relations $\Re(S)$. In particular, a relation of the shape $x_{i_1} \cdots x_{i_m} = 1$ can hold in S *iff* the set $\Re(S)$ explicitly contains relations of the form $u = 1$ where $u \in \langle X \rangle$ has length $|u| \leq m$. Every monomial $u \in S$ can be presented as a product

$$u = x_{i_1} \cdots x_{i_m} \tag{3.18}$$

of elements of X, (since X is a generating set) but in general, there might be presentations of u as words of different length. However we can always consider a presentation (3.18) in which the length $m = m(u)$ is minimal. Clearly, for each $u \in S$ the minimal length $m(u)$ is uniquely determined. Furthermore, $m(u.v) \leq m(u) + m(v)$. Clearly, every sub-word a of a "minimal" presentation of w is also a presentation of minimal length for a, i.e. if $w =^{inS} w_1 w_2,\ w_1, w_2 \in \langle X \rangle$ is a presentation of minimal length, then $m(w) = m(w_1) + m(w_2)$. In particular, if $w = xu, x \in X, u \in S$ is a presentation of w of minimal length then $m(u) = m(w) - 1$.

Proposition 3.13. *Let (S, r_S) be an* **M3***-monoid with associated map r_S. Suppose S is generated by a set X which is invariant under the left and the right actions of the matched pair. Let $r : X \times X \to X \times X$ be the restriction of r_S on $X \times X$. Suppose condition* **lr3** *holds on the quadratic set (X, r). Then*

$$\mathbf{LR3}: \qquad ({}^{a}w)^{({}^{a^{w}}b)} = {}^{(a^{{}^{w}b})}(w^{b}), \qquad \text{for all } a, b, w \in S.$$

Proof. Using induction on $m(b) = n$ we prove first

$$({}^{z}t)^{({}^{z^{t}}b)} = {}^{(z^{{}^{t}b})}(t^{b}), \quad \text{for all } b \in S, t, z \in X. \tag{3.19}$$

Clearly, when $m(b) = 1$, condition (3.19) is simply **lr3** on (X, r), which gives the base for induction. Assume (3.19) is true for all $b \in S, m(b) \leq n$, and all $t, z \in X$. Let $b \in S, m(b) = n+1$, so $b = xu$, $x \in X, u \in S, m(u) = n$. Consider the equalities:

$$\begin{aligned} {}^{(z^{{}^{t}(xu)})}[t^{xu}] &= {}^{(z^{({}^{t}x)})^{({}^{t^{x}}u)}}[(t^{x})^{u}] =^{\text{inductive ass.}} [{}^{(z^{{}^{t}x})}(t^{x})]^{[(z^{{}^{t}x})^{t^{x}}]u} \\ &=^{\mathbf{lr3},\mathbf{ML2}} [({}^{z}t)^{{}^{z^{t}}x}]^{{}^{(z^{(tx)})}u} = ({}^{z}t)^{[({}^{z^{t}}x).({}^{(z^{t})^{x}}u)]} = ({}^{z}t)^{({}^{z^{t}}(xu))} \end{aligned}$$

This proves (3.19).

Analogous argument with induction on $m(a) = n$ verifies

$$({}^{a}t)^{({}^{a^{t}}b)} = {}^{(a^{{}^{t}b})}(t^{b}), \quad \text{for all } a, b \in S, t \in X. \tag{3.20}$$

Note that (3.19) gives the base for the induction.

Finally we prove **LR3** as stated. We use induction on $m(w) = n$. In the case $m(w) = 1$, **LR3** is exactly condition (3.20). This is the base for the induction. Assume **LR3** holds for all $a, b, w \in S$, where $m(w) \leq n$. Let $w \in S, m(w) = n + 1$, then $w = xv$, $x \in X$, $m(v) = n$. We have to show

$${}^{({}^{a^{(xv)}}b)}[(xv)^{b}] = [{}^{a}(xv)]^{({}^{a^{(xv)}}b)} \tag{3.21}$$

We compute

$$\begin{aligned} W_1 \quad \equiv \quad & {}^{({}^{a^{(xv)}}b)}[(xv)^{b}] =^{\mathbf{MR2}} {}^{({}^{a^{(xv)}}b)}[(x^{{}^{v}b}).(v^{b})] =^{\mathbf{ML1}} {}^{a^{x({}^{v}b)}}[(x^{{}^{v}b}).(v^{b})] \\ & =^{\mathbf{ML2}} [{}^{a^{x({}^{v}b)}}(x^{{}^{v}b})].[{}^{(a^{x({}^{v}b)})^{(x^{{}^{v}b})}}(v^{b})] =^{\mathbf{MR1}} [{}^{a^{x({}^{v}b)}}(x^{{}^{v}b})].[{}^{(a^{(x.{}^{v}b)})}(v^{b})] \\ & =^{\text{inductive ass.}} [({}^{a}x)^{({}^{a^{x}}({}^{v}b))}].[{}^{((a^{x})^{{}^{v}b})}(v^{b})] \\ W_2 \quad \equiv \quad & [{}^{a}(xv)]^{{}^{(a^{(xv)})}b} = [({}^{a}x).({}^{a^{x}}v)]^{{}^{((a^{x})^{v})}b} = [({}^{a}x)^{{}^{({}^{a^{x}}v)((a^{x})^{v})}b}].[({}^{a^{x}}v)^{{}^{((a^{x})^{v})}b}] \\ & =^{\mathbf{ML1}} [({}^{a}x)^{({}^{a^{x}}({}^{v}b))}].[({}^{a^{x}}v)^{{}^{((a^{x})^{v})}b}] =^{\text{inductive ass.}} [({}^{a}x)^{({}^{a^{x}}({}^{v}b))}].[{}^{((a^{x})^{{}^{v}b})}(v^{b})]. \end{aligned}$$

We have shown $W_1 = W_2$ which proves (3.21). Hence **LR3** is proven on S. □

We have completed all the necessary parts for the construction of a solution r_S of the YBE on S.

Theorem 3.14. *Let (X, r) be a braided set and (S, r_S) the induced graded* **M3**-*monoid with associated map r_S by Theorem 3.6. Then*

1. *(S, r_S) is a graded braided monoid.*
2. *(S, r_S) is non-degenerate iff (X, r) is non-degenerate.*
3. *(S, r_S) is involutive iff (X, r) is involutive.*

Proof. We have already in Theorem 3.6 extended the left and the right actions on X induced by r to a left and a right actions of S onto itself which make S a graded a graded **M3**-monoid with associated map r_S. To show that r_S obeys the YBE we use Lemma 2.5 applied to the set S. We already have **l1,r1** on S from **ML1,MR1,M3** by the same argument as in the proof of Proposition 3.5. (S, r_S) satisfies the hypothesis of Proposition 3.13, therefore we also have **lr3** on S as required.

For bijectivity of r_S we consider (X, r^{-1}) (that r is bijective is our convention throughout the paper) and consruct a matched pair (T, S) (where $T = S$) using our previous results applied to (X, r^{-1}). Thus, we define $\triangleright, \triangleleft$ by $r^{-1}(x, y) = (x \triangleright y, x \triangleleft y)$. One may then prove inductively with respect to the grading that these obey (3.1) and hence provide the inverse of r_S. Thus, suppose these equations for all a, u of given degrees and also for x of degree 1 in the role of a. Then

$$\begin{aligned} {}^{xa}u \triangleright (xa)^u &= {}^{x}({}^{a}u) \triangleright (x^{{}^{a}u} a^u) = {}^{x}({}^{a}u) \triangleright x^{({}^{a}u)} . ({}^{x}({}^{a}u) \triangleleft x^{({}^{a}u)}) \triangleright a^u = x.({}^{a}u \triangleright a^u) = xa \\ {}^{xa}u \triangleleft (xa)^u &= ({}^{x}({}^{a}u) \triangleleft x^{({}^{a}u)}) \triangleleft a^u = {}^{a}u \triangleleft a^u = u \end{aligned}$$

using that both sets of actions form matched pairs and the assumptions. Similarly for the other cases. At the lowest level (3.1) holds as r^{-1} is inverse to r. We have shown that (S, r_S) is a braided monoid.

Next we observe one direction of part (2). By definition the solution r_S respects the grading by length of S, hence clearly, the non-degeneracy of r_S implies that r is non-degenerate. For the converse we will need some additional statements. We recall a standard notation.

Notation 3.15. For $1 \leq i$, the replacements $r_i, 1 \leq i \leq m-1$ are defined as

$$r_i(y_1 y_2 \cdots y_m) = y_1 \cdots y_{i-1} r(y_i y_{i+1}) y_{i+2} \cdots y_m$$

$$= y_1 \cdots y_{i-1} [{}^{y_i} y_{i+1} y_i^{y_{i+1}}] y_{i+2} \cdots y_m,$$

for all $m > i$, and $y_1, \cdots, y_m \in X$.

Note that, clearly, each replacement r_i agrees with the defining relations of S, so for all $u \in \langle X \rangle$, and all $i < |u|$ the equality $r_i(u) = u$ holds in S.

Lemma 3.16. *For any $a \in S, u \in \langle X \rangle$, and any sequence $r_{i_1} \cdots r_{i_s}$, with $1 \leq i_j < |u|$, for $1 \leq j \leq s$, the following is an equality of words in $\langle X \rangle$*

$${}^{a}(r_{i_1} \circ \cdots \circ r_{i_s}(u)) = r_{i_1} \circ \cdots \circ r_{i_s}({}^{a}u)$$

Proof. We show first that ${}^a r_i(u) = r_i({}^a u)$, for all $a \in S$, $u \in \langle X, \rangle, 1 \leq i < |u|$. For our convenience we present u as $u = vxyw$, where $|v| = i-1, x, y \in X$. The following are equalities in $\langle X \rangle$:

$$\begin{aligned} r_i({}^a u) \quad = \quad & r_i({}^a vxyw) =^{\mathbf{ML2}} r_i({}^a v.({}^{a^v} x.{}^{a^{vx}} y).{}^{a^{vxy}} w) \\ & = ({}^a v).[r({}^{a^v} x.{}^{a^{vx}} y)].({}^{a^{vxy}} w) = ({}^a v).[{}^{{}^{a^v} x ({}^{(a^v)^x} y)}.({}^{a^v} x)^{{}^{a^{vx}} y}].{}^{a^{vxy}} w \\ & =^{\mathbf{ML1}} ({}^a v).({}^{(a^v.x)} y).({}^{a^v} x)^{({}^{(a^v)^x} y)}].{}^{a^{vxy}} w \\ & =^{\mathbf{ML1,\ LR3}} ({}^a v).[({}^{a^v}({}^x y)).{}^{(a^v)^{x^y}}(x^y)].{}^{a^{vxy}} w \\ & =^{\mathbf{ML2}} {}^a v.[{}^{a^v}({}^x y.x^y)].{}^{a^{vxy}} w =^{\mathbf{M3}} {}^a v.[{}^{a^v}({}^x y.x^y)].{}^{a^{v({}^x y.x^y)}} w \\ & =^{\mathbf{ML2}} {}^a(v.({}^x y.x^y).w) = {}^a r_i(v.xy.w) = {}^a r_i(u) \end{aligned}$$

The statement of the lemma then follows easily and we leave it to the reader. □

Proposition 3.17. *Suppose (X, r) is non-degenerate, then for any $a, b, u, v \in S$*

(1) ${}^a u = {}^a v$ *in $S \Longrightarrow u = v$ in S*
(2) $a^u = b^u$ *in $S \Longrightarrow a = b$ in S*
(3) *(S, r_S) is a non-degenerate solution.*

Proof. We will show first (1). From the definition of the left action of S on $\langle X \rangle$ and the non-degeneracy of r we deduce

(3.22) ${}^a(y_1 y_2 \cdots y_m) = {}^a(z_1 z_2 \cdots z_m)$ in $\langle X \rangle \Longrightarrow y_1 y_2 \cdots y_m = z_1 z_2 \cdots z_m$ in $\langle X \rangle$.

Suppose ${}^a u = {}^a v$ holds in S, where $a, u, v \in S$. Clearly then the monomial ${}^a v$, considered as an element of $\langle X \rangle$ is obtained from ${}^a u$, by applying finite sequence of replacements which come from the defining relations. So there exist $r_{i_1}, r_{i_2}, \cdots, r_{i_s}$, such that there is an equality in $\langle X \rangle$:

$$r_{i_1} \circ \cdots \circ r_{i_s}({}^a u) = {}^a v.$$

It follows from Lemma 3.16 that

$${}^a(r_{i_1} \circ \cdots \circ r_{i_s}(u)) = r_{i_1} \circ \cdots \circ r_{i_s}({}^a u) = {}^a v \quad \text{in } \langle X \rangle.$$

Hence, by (3.22), the equality

$$r_{i_1} \circ \cdots \circ r_{i_s}(u) = v$$

holds in $\langle X \rangle$. Then, clearly, $u = v \in S$. This verifies the left non-degeneracy of r_S, (1). The proof of right non-degeneracy (2) is analogous. (1) and (2) imply (3). □

This completes the part (2) of Theorem 3.14. Now we will prove part (3). Clearly, the involutiveness of (S, r_S) implies (X, r) involutive. The following lemma gives the opposite implication.

Lemma 3.18. *Under the hypothesis of the theorem, assume (X, r) is an involutive solution. Then (S, r_S) is involutive.*

Proof. We have to show that equalities in S :

$$({3.23}) \qquad {}^{{}^u v}(u^v) = u, \quad ({}^u v)^{u^v} = v, \quad \text{for all} \quad u, v \in S.$$

We show first the two equations

$$({3.24}) \qquad {}^{{}^{xy} z}(xy^z) = xy \quad \text{for all} \quad x, y, z \in X,$$

$$({3.25}) \qquad ({}^{xy} z)^{(xy^z)} = z \quad \text{for all} \quad x, y, z \in X.$$

Indeed,

$$\begin{aligned}{}^{{}^{xy}z}(xy^z) \quad &=^{\mathbf{MR2}} \quad {}^{{}^{xy}z}(x^{{}^{y}z}.y^z) =^{\mathbf{MR1,\ ML2}} [{}^{{}^{x}({}^{y}z)}(x^{{}^{y}z})].{}^{({}^{x}({}^{y}z))^{(x^{{}^{y}z})}}(y^z)\\ &=^{r \text{ involutive}} x.{}^{{}^{y}z}(y^z) =^{r \text{ involutive}} xy.\end{aligned}$$

This proves (3.24). For the second equality, we have

$$\begin{aligned}({}^{xy}z)^{(xy^z)} \quad &=^{\mathbf{ML1,\ MR2}} \quad [{}^{x}({}^{y}z)]^{(x^{{}^{y}z}.y^z)}\\ &=^{\mathbf{ML1}} \qquad [[{}^{x}({}^{y}z)]^{(x^{{}^{y}z})}]^{y^z} =^{r \text{ involutive}} ({}^{y}z)^{y^z} = z,\end{aligned}$$

hence (3.25) also holds. We give a sketch of the proof of ${}^{{}^{u}v}(u^v) = u$, for all $u, v \in S$, and leave the details for the reader. One uses double induction on $|u| = m$ and $|v| = n$. **Step 1.** By induction on $|v| = n$, one proves the equality ${}^{{}^{z}v}(z^v) = z, z \in X, v \in S$. To do this one uses a tecnique similar to the one in the proof of (3.25). **Step 2.** Assuming ${}^{{}^{u}v}(u^v) = u$, for all $u, v \in S, |u| \leq m$, one uses argument similar to the proof of (3.24) to show that ${}^{{}^{xu}v}(xu^v) = xu$, for all $x \in X, |u| = m, u, v, \in S$. This proves the first equality in (3.23). The second is proven by analogous arguments. □

The proof of Theorem 3.14 is complete now. □

3.3. **M3-monoids and braided monoids** (S, r_S)**.** In this section we will study general **M3**-monoids S with associated map r_S. We recall that *a braided group*, [26], is a pair (G, σ), where G is a group and $\sigma : G \times G \to G \times G$ is a map such that the left and the right actions induced by σ make (G, G) a matched pair of groups with condition **M3**. Note that in the case of matched pair of groups the notions of an **M3**-group (G, r_G) and a braided group are equivallent; it is shown in [17], Theorem 1 that a braided group (G, σ) forms a non-degenerate braided set. The proof follows straightforwardly from the definition of a braided group and the cancellative law in G. Analogous argument can not be applied in the general case of **M3**-monoid (S, r_S). We show that an **M3**-monoid (S, r_S) is braided in cases when some natural additional conditions on S are imposed.

In various cases, when necessary, we shall impose the condition of 2-cancellativity.

Definition 3.19. We say that a monoid S is *2-cancellative* with respect to a generating set X when it has cancellation on monomials of length 2 in the generators in the sense:

$$xy = xz \Longrightarrow y = z; \quad xz = yz \Longrightarrow x = y, \quad \text{for all} \quad x, y, z \in X.$$

Clearly for a graded **M3**-monoid (S, r_S), the 2-cancellativity of S implies that r is 2-cancellative. Recall that in the particular case when $S = S(X, r)$, S is 2-cancellative *iff* r is 2-cancellative, see Definition 2.10 and Proposition 2.11. Furthermore, by Corollary 2.13 every nondegenerate involutive quadratic set (X, r) is 2-cancellative, so the condition of 2-cancellativeness is a natural restriction.

Lemma 3.20. *Let S be an* **M3***-monoid with associated map r_S. Suppose S is 2-cancellative with respect to a generating set X which is invariant under the left and the right actions of the matched pair. Let $r : X \times X \to X \times X$ be the restriction of r_S on $X \times X$. Then (X, r) is a set-theoretic solution of the Yang-Baxter equation. Furthermore, if the map r is a bijection then (X, r) is a braided set.*

Proof. We have to show that (X,r) satisfies the relations **lr3**. The following equalities hold in S :

$$^{x}(yz) =^{\mathbf{ML2}}\ {}^{x}y.{}^{x^y}z =^{\mathbf{M3}}\ {}^{^xy}({}^{x^y}z)).({}^{x}y)^{^{x^y}z}$$

and

$$^{x}(yz) =^{\mathbf{M3}}\ {}^{x}({}^{y}z.y^{z}) =^{\mathbf{ML2}}\ {}^{x}({}^{y}z).{}^{x^{^yz}}(y^{z}).$$

Comparing the right hand sides of these equalities we obtain

$$ {}^{^xy}({}^{x^y}z).({}^{x}y)^{^{x^y}z} = {}^{x}({}^{y}z).{}^{x^{(^yz)}}(y^{z}). \tag{3.26}$$

By **ML1, M3** one has ${}^{^xy}({}^{x^y}z) = {}^{x}({}^{y}z)$, which together with (3.26) and the 2-cancellativity yields

$$({}^{x}y)^{^{x^y}z} = {}^{x^{^yz}}(y^{z}).$$

This verifies **lr3** on (X,r). Clearly, the conditions **ML1, MR1** give **l1, r1** on (X,r), hence (X,r) is a solution. □

Proposition 3.21. *Let S be an **M3**-monoid with associated map r_S. Suppose one of the following conditions is satisfied:*

(i) S has a generating set X invariant under the left and the right actions of the matched pair, the restriction r of r_S on $X\times X$ is bijective, and **lr3** *holds on the quadratic set (X,r);*

(ii) S has a generating set X invariant under the left and the right actions of the matched pair, S is 2-cancellative with respect to it, and the restriction r of r_S on $X\times X$ is bijective;

(iii) (S,r_S) is graded, S is 2-cancellative, and the restriction $r: X\times X \to X\times X$ on degree 1 is a bijection;

(iv) S is a monoid (not necessarily graded) with left cancellation.

Then (S,r_S) is a set-theoretic solution of the YBE.

Proof. As in the proof of Proposition 3.5 we only need to have **lr3** on the set of S, which condition we denote in upper case as **LR3** to avoid confusion with the condition on X.

If (i) holds then (S,r_S) satisfies the hypothesis of Proposition 3.13, so condition **LR3** holds and (S,r_S) is a solution.

If (ii) holds then by Lemma 3.20 **lr3** holds on the quadratic set (X,r), so condition (i) is satisfied therefore (S,r_S) is a solution.

Condition (iii) implies that X is invariant under the left and the right actions of the matched pair, therefore the assumptions of (ii) are satisfied, and (S,r_S) is a solution.

Case (iv) is already covered in Proposition 3.5 and included for completeness. □

At this level the conceptual basis for why (S,S) with cancellation (or rather with **LR3**) has a solution of the YBE on it is then provided by the following. Note that the monoids S are somewhat analogous to the 'FRT bialgebras' $A(R)$ in the theory of quantum groups and just as there one has[22] that $A(R)\bowtie A(R)\to A(R)$, similarly we have a monoid homorphism $S\bowtie S\to S$ given by $u.a\mapsto ua$ (i.e. by the product in S). In fact this is the exact content of the **M3** condition and is analogous to the parallel observation in the group case [26]. Likewise, just as one has iterated $\bowtie$s for $A(R)$, we have:

Theorem 3.22. *Let S be an* **M3***-monoid with respect to a matched pair structure (S,S) and associated map r_S. Then the following are equivalent*

(1) *r_S obeys the YBE.*
(2) *$(S, S \bowtie S)$ form a matched pair with actions extending those of (S, S).*
(3) *$(S \bowtie S, S)$ forms a matched pair with actions extending those of (S, S).*

In this case the respective actions are

$$ {}^{u.a}v = {}^{ua}v, \quad (u.a)^v = u^{{}^a v}.a^v; \quad v^{u.a} = v^{ua}, \quad {}^v(u.a) = {}^v u.{}^{v^u}a $$

for all $u.a \in S \bowtie S,\ v \in S,$ and $S \bowtie (S \bowtie S) = (S \bowtie S) \bowtie S$.

Proof. We verify the first matched pair, the second is analogous. The left action here is to view a general element $u.a \in S \bowtie S$ as built from $u, a \in S$ where we multiply them and use the given action of S on S (we use the dot to emphasis the product in $S \bowtie S$): We have

$$ {}^a({}^u v) = {}^{au}v \overset{\mathbf{M3}}{=} {}^{{}^a u a^u}v = {}^{{}^a u.a^u}v $$

so the relations in $S \bowtie S$ are represented, and this requirement determines the action uniquely. We similarly have a unique extension of the actions in (S, S) to an action of $S \bowtie S$, as stated. We then check that these form a matched pair:

$$ {}^{u.a}(wv) = {}^{ua}(wv) = {}^{ua}w\,({}^{(ua)^w}v) = {}^{u.a}w\,({}^{u^{{}^a w}a^w}v) = {}^{ua}w\,({}^{u^{{}^a w}.a^w}v) = {}^{u.a}w\,({}^{(u.a)^w}v) $$

since the action of S on $S \bowtie S$ has the same structural form as the action of S on a product in S. For the other action in the matched pair,

$$ \begin{aligned} ((u.a)(v.b))^w &= (u^a v.a^v b)^w = (u^a v)^{({}^{a^v b}w)}.(a^v b)^w = u^{{}^{{}^a v a^v b}w}({}^a v)^{({}^{a^v b}w)}.a^{v\,{}^b w}b^w \\ &= u^{{}^{avb}w}({}^a v.a^v)^{{}^b w}b^w = u^{{}^{avb}w}.(a.v)^{{}^b w}.b^w \\ ((u.a)^{{}^{(v.b)}w})(v.b)^w &= (u.a)^{{}^{vb}w}(v^{{}^b w}.b^w) = u^{{}^{avb}w}.a^{{}^{vb}w}.v^{{}^b w}.b^w \end{aligned} $$

where $(a.v)^w$ is by definition the action of w on $({}^a v.a^v)$. To have equality of these expressions we require $(a.v)^w = a^{{}^v w}.v^w$ for all w. Using the unique factorisation in $S \bowtie S$, we need

$$ ({}^a v.a^v)^w \equiv ({}^a v)^{(a^{{}^v w})}.a^{vw} = a^{{}^v w}.v^w \equiv {}^{(a^{{}^v w})}(v^w).(a^{({}^v w\, v^w)}) \equiv {}^{(a^{{}^v w})}(v^w).a^{vw} $$

which holds if we assume **LR3** in S. Conversely, this condition is also necessary due to the unique factorisation in $S \bowtie S$. As remarked above, given **M3**, the condition **LR3** is equivalent to r_S obeying the YBE. The other matched pair is similar and requires the same assumption. That the two matched pairs give the same product on $S \times S \times S$ is a matter of direct computation of the products in the two cases, one readily verifies that they give the same on reducing all expressions to $S \times S \times S$ in the obvious way. □

Now, the operation $r_S : S \times S \to S \times S$ expresses reordering of two factors: the value in $S \times S$ read on the left and bottom is transported to the value read on the top and right by $\Rightarrow$ in Figure 1(a) (here $S = T$), an equality $a.u = {}^a u.a^u$ in $S \bowtie S$. Similarly working within the above triple factorisation and calling the three copies of S as S, T, U to keep them distinct, the 'input' of the Yang-Batxer cube in Figure 1(b) is a reverse-ordered expression in $S \bowtie T \bowtie U$. Each $\Rightarrow$ is a reordering and the 'output' of the cube is the canonically ordered expression. Since at each stage the same elements in the triple product are involved, we have the same result going around the front or around the back of the cube, i.e. the Yang-Baxter equation for r_S holds. This is a geometric reason for r_S to obey the YBE and provides a different point of view than that in Section 2.

We are also now in position to provide a full characterisation of the exponentiation problem for r_S under some minimal cancellation assumption. This provides is a "monoidal" analogue of a theorem for the group $G(X,r)$, see [17], see also [26]. Note that we do not know, in general, under which conditions on (X,r) the monoid $S(X,r)$ is embedded in $G(X,r)$ so one can not deduce our result from the group case.

Theorem 3.23. *Let (X,r) be a 2-cancellative quadratic set, and let $S=S(X,r)$ be the associated monoid, graded by length. Then (S,r_S) is a graded braided monoid reducing to (X,r) on degree one iff (X,r) is a braided set.*

Proof. If (X,r) is a braided set, then by Theorem 3.6 S is a graded **M3**-monoid with actions extending uniquely the canonical left and right actions associated with r, next by Theorem 3.14 (S,r_S) is a braided monoid. (In this direction we do not need 2-cancellativeness of r). Conversely, assume that (S,r_S) is a graded braided monoid reducing to (X,r) on degree one, then, clearly, the hypothesis of Lemma 3.20 is satisfied, so (X,r) is a braided set. □

We close the section with an open question.

Open Question 3.24. *1) Let (X,r) be an involutive nondegenerate solution of YBE, $S=S(X,r)$ the associated YB-monoid. Is it true that S is cancellative?*

2) Is it true that if (X,r) is a 2-cancellative braided set, the associated monoid $S=S(X,r)$ is cancellative?

In the case when (X,r) is a finite square-free solution, the answer is affirmative, see [8]. In this case the monoid $S(X,r)$ is embedded in $G=G(X,r)$ and the elements of G are of the shape $u^{-1}v$, where $u,v\in S$. Proposition 2.11 shows that for arbitrary 2-cancellative solution S satisfies cancellative law on monomials of length 3.

4. Matched pair approach to extensions of solutions

In this section we study extensions of solutions and their relations with matched pairs of monoids. The notions of *a union* of solutions, extensions and one-sided extensions were introduced in [2], but only for nondegenerate involutive solutions (X,r_X), (Y,r_Y). We introduce what we call *regular extensions* (Z,r) of arbitrary solutions (X,r_X), (Y,r_Y), and provide necessary and sufficient conditions (in terms of left and right actions) for a regular extension (Z,r) to satisfy YBE. Moreover, regular extensions obeying the YBE have a very natural interpretation in terms of matched pairs. They correspond to certain types of strong matched pairings between the associated monoids.

4.1. Regular extensions and YB-extensions.

In this section we introduce the notion of regular extensions and provide first results on when a regular extension obeys the YBE, see Theorem 4.9. We also introduce notations to be used throughout the section.

Definition 4.1. Let (X,r_X) and (Y,r_Y) be disjoint quadratic sets (i.e. with bijective maps $r_X: X\times X\longrightarrow X\times X$, $r_Y: Y\times Y\longrightarrow Y\times Y$). Let (Z,r) be a set with a bijection $r: Z\times Z\longrightarrow Z\times Z$. We say that (Z,r) is *a (general) extension of* $(X,r_X),(Y,r_Y)$, if $Z=X\bigcup Y$ as sets, and r extends the maps r_X and r_Y, i.e.

$r_{|X^2} = r_X$, and $r_{|Y^2} = r_Y$. Clearly in this case X, Y are r-invariant subsets of Z. (Z, r) is *a YB-extension of* (X, r_X), (Y, r_Y) if r obeys YBE.

Remark 4.2. In the assumption of the above definition, suppose (Z, r) is a non-degenerate extension of $(X, r_X), (Y, r_Y)$. Then the equalities $r(x, y) = ({}^x y, x^y)$, $r(y, x) = ({}^y x, y^x)$, and the non-degeneracy of r, r_X, r_Y imply that

$${}^y x, x^y \in X, \text{ and } {}^x y, y^x \in Y, \text{ for all } x \in X, y \in Y.$$

Therefore, r induces bijective maps

$$\rho : Y \times X \longrightarrow X \times Y, \text{ and } \sigma : X \times Y \longrightarrow Y \times X, \tag{4.1}$$

and left and right "actions"

$${}^{(\,)}\bullet : Y \times X \longrightarrow X, \quad \bullet^{(\,)} : Y \times X \longrightarrow Y, \text{ projected from } \rho \tag{4.2}$$

$$\triangleright : X \times Y \longrightarrow Y, \quad \triangleleft : X \times Y \longrightarrow X, \text{ projected from } \sigma. \tag{4.3}$$

Clearly, the 4-tuple of maps (r_X, r_Y, ρ, σ) uniquely determine the extension r. The map r is also uniquely determined by r_X, r_Y, and the maps (4.2), (4.3).

However, if we do not assume (Z, r) non-degenerate, there is no guarantee that r induces maps as (4.1), neither actions (4.2), (4.3).

Remark 4.3. Clearly, (X, r) with $r = \mathrm{id}_{X\times X}$ is a solution, which is degenerate whenever X is a set with more than one element, since ${}^x y = x$ for all $x, y \in X$.

Given two disjoint solutions (X, r_X), and (Y, r_Y), let $Z = X \bigcup Y$. The following two examples yield the "easiest" extensions we can get:

1. [2] Define $r : Z \times Z \longrightarrow Z \times Z$ as $r(x_1, x_2) := r_X(x_1, x_2)$, $x_1, x_2 \in X$, $r(y_1, y_2) := r_Y(y_1, y_2)$, for all $y_1, y_2 \in Y$ and
$$r(y, x) := (x, y); \; r(x, y) := (y, x), \text{ for all } x \in X, y \in Y.$$
Then r is a solution, it is called *the trivial extension.*
2. Define $r : Z \times Z \longrightarrow Z \times Z$ as $r(x_1, x_2) := r_X(x_1, x_2)$, for all $x_1, x_2 \in X$, $r(y_1, y_2) := r_Y(y_1, y_2)$, for all $y_1, y_2 \in Y$ and
$$r(y, x) := (y, x); \; r(x, y) := (x, y), \text{ for all } x \in X, y \in Y.$$
Then, r is an extension, r is bijective, but does not induce maps (4.1), nor actions (4.2), (4.3). Moreover, r obeys YBE if and only if $r_X = \mathrm{id}_{X\times X}$, and $r_Y = \mathrm{id}_{Y\times Y}$.

   As a very particular example of an YB- extension (Z, r) of two non-degenerate solutions, which does not induces maps (4.1), one can consider the extreme case when $X = \{x\}, Y = \{y\}$ are one element sets, with the trivial solutions $r_X = \mathrm{id}_{X\times X}, r_Y = \mathrm{id}_{Y\times Y}$.

If we want to assure the existence of maps (4.1), (we need them if we want to apply the theory of strong matched pairs), but not assuming necessarily the bijection r to be non-degenerate, we should consider only *regular* extensions (Z, r), which are defined below.

Definition 4.4. In notation as above, a (general) extension (Z, r) of $(X, r_X), (Y, r_Y)$ is *a regular extension* if r is bijective, and the restrictions $r_{|Y\times X}$ and $r_{|X\times Y}$ have the shape

$$r_{|Y\times X} : Y \times X \longrightarrow X \times Y, \quad r_{|X\times Y} = (r_{|Y\times X})^{-1} : X \times Y \longrightarrow Y \times X.$$

We call

$$ {}^{Y}\bullet : Y \times X \longrightarrow X, \quad \bullet^{X} : Y \times X \longrightarrow Y $$

$$ \triangleright : X \times Y \longrightarrow Y, \quad \triangleleft : X \times Y \longrightarrow X $$

projected from $r_{|Y\times X}$ and $r_{|X\times Y}$ the associated ground action and accompanying action respectively.

It follows from the definition that each regular extension (Z, r) satisfies

$$ (r \circ r)_{|Y\times X} = \mathrm{id}_{|Y\times X}, \quad (r \circ r)_{|X\times Y} = \mathrm{id}_{|X\times Y}, $$

but r is not necessarily involutive on $X \times X$, neither on $Y \times Y$.

Definition 4.5. With respect to solutions (X, r_X), (Y, r_Y), a pair of maps

$$ {}^{Y}\bullet : Y \times X \longrightarrow X, \quad \bullet^{X} : Y \times X \longrightarrow Y $$

is called *regular* if the map $r_{|Y\times X}(\alpha, x) =_{\mathrm{def}} ({}^{\alpha}x, \alpha^{x})$ is invertible.

There is clearly a 1-1 correspondence between regular extensions (Z, r) and regular pairs of actions $({}^{Y}\bullet, \bullet^{X})$. Moreover, regularity of a pair of actions is clearly equivalent to the existence of the accompanying actions such that

$$ {}^{\alpha}x\triangleright\alpha^{x} = \alpha, \quad {}^{\alpha}x\triangleleft\alpha^{x} = x, \quad {}^{x\triangleright\alpha}(x\triangleleft\alpha) = x, \quad (x\triangleright\alpha)^{x\triangleleft\alpha} = \alpha. \tag{4.4} $$

Sometimes for simplicity we shall write ${}^{x}\alpha$ instead of $x\triangleright\alpha$, or x^{α}, instead of $x\triangleleft\alpha$.

Henceforth we shall assume that (X, r_X), (Y, r_Y) are arbitrary disjoint braided sets (r_X, r_Y are bijective maps obeying YBE), not necessarily involutive, nondegenerate, or finite. Any additional restriction on the solutions will be mentioned explicitly. We shall consider only regular extensions (Z, r) of (X, r_X), (Y, r_Y), with corresponding regular ground actions as in Definition 4.5.

Furthermore, assuming the actions in Definition 4.5 are given, we also deduce automatically a left action of Y on X^2 and a right action of X on Y^2 defined as

$$ {}^{\alpha}xy := {}^{\alpha}x.{}^{\alpha^{x}}y, \qquad (\alpha\beta)^{x} := \alpha^{{}^{\beta}x}\beta^{x}, \quad \text{for all} \quad x, y \in X, \alpha, \beta \in Y. $$

For convenience we shall use notation x, y, z, for the elements of X, α, β, γ for the elements of Y. Then the following lemma is straightforward:

Lemma 4.6. *In notation as above, let (Z, r) be a regular extension of (X, r_X), (Y, r_Y). Then*

(1) *The set of defining relations $\Re(r)$ of $U = S(Z, r)$ is:*

$$ \Re(r) = \{\alpha x = {}^{\alpha}x\alpha^{x} \mid x \in X, \alpha \in Y\} \bigcup \{x\alpha = (x\triangleright\alpha)(x\triangleleft\alpha) \mid x \in X, \alpha \in Y\} \bigcup \Re(r_X) \bigcup \Re(r_Y). $$

(2) *r is 2-cancellative* iff *r_X, and r_Y are 2-cancellative;*
(3) *r is involutive* iff *r_X, and r_Y are involutive;*
(4) *r is square-free* iff *r_X, and r_Y are square-free.*

Notation 4.7. In order to study regular extensions further it will be helpful to have a 'local' notation for some of our conditions, in which the specific elements for which the condition is being imposed will be explicitly indicated, indicated in lexicographical order of first appearance. Thus for example **l1(x,y,z)** means the condition exactly as written in Lemma 2.5 for the specific elements x, y, z. Similarly **r2(x,y,z)** means for the elements x, y, z exactly as appearing as in Definition 2.8.

Then for example the 'local' version of Lemma 2.9 proved in the same way as at the end of the proof there, is the result

$$r^{12}r^{23}r^{12}(x,y,z) = r^{23}r^{12}r^{23}(x,y,z) \Longleftrightarrow \mathbf{r1(x,y,z)}, \mathbf{l2(x,y,z)} \Longleftrightarrow \mathbf{l1(x,y,z)}, \mathbf{r2(x,y,z)}$$

for any fixed triple (x,y,z). In the present section we consider triples in the set Z^3 so for example

$$\mathbf{l1}(\alpha,\mathbf{x},\mathbf{y}): \quad {}^{\alpha}({}^{x}y) = {}^{{}^{\alpha}x}({}^{\alpha^x}y)$$

where $\alpha, x, y \in Z$. Finally, we use this notation to specify the restrictions of any of our conditions to subsets of interest. For example

$$\mathbf{l1}(\mathbf{Y},\mathbf{X},\mathbf{X}) := \{\mathbf{l1}(\alpha,\mathbf{x},\mathbf{y}) \quad \textit{for all } \alpha \in Y,\ x,y \in X\}.$$

Finally, in view of the following key lemma, we concentrate on the particular examples

$$\begin{array}{lll}
\mathbf{ml1} := \mathbf{l1}(\mathbf{Y},\mathbf{Y},\mathbf{X}): & {}^{\alpha}({}^{\beta}x) = {}^{\alpha\beta}({}^{\alpha^\beta}x) & \textit{for all } x \in X, \alpha,\beta \in Y \\
\mathbf{mr1} := \mathbf{r1}(\mathbf{Y},\mathbf{X},\mathbf{X}): & (\alpha^x)^y = (\alpha^{{}^{x}y})^{x^y} & \textit{for all } x,y \in X, \alpha \in Y \\
\mathbf{ml2} := \mathbf{l2}(\mathbf{Y},\mathbf{X},\mathbf{X}): & {}^{\alpha}(r_X(xy)) = r_X({}^{\alpha}(xy)) & \textit{for all } x,y \in X, \alpha \in Y \\
\mathbf{mr2} := \mathbf{r2}(\mathbf{Y},\mathbf{Y},\mathbf{X}): & (r_Y(\alpha\beta))^x = r_Y((\alpha\beta)^x) & \textit{for all } x \in X, \alpha,\beta \in Y.
\end{array}$$

Lemma 4.8. *Let (Z,r) be a regular extension of the quadratic sets $(X,r_X),(Y,r_Y)$.*

A. *The following are equivalent:*

(1) **r1(Y,X,X)**, **l2(Y,X,X)**
(2) **r1(X,Y,X)**, **l2(X,Y,X)**
(3) **r1(X,X,Y)**, **l2(X,X,Y)**.

B. *The following are equivalent:*

(1) **l1(Y,Y,X)**, **r2(Y,Y,X)**
(2) **l1(Y,X,Y)**, **r2(Y,X,Y)**
(3) **l1(X,Y,Y)**, **r2(X,Y,Y)**.

Proof. These are all restrictions of the YBE to different parts of Z^3. As explained above, the 'local' YBE at (α,x,y), say, is equivalent to $\mathbf{r1}(\alpha,x,y)$, $\mathbf{l2}(\alpha,x,y)$ which for all $x,y \in X, \alpha \in Y$ is condition $\mathbf{A}(1)$. That the three parts of $\mathbf{A}$ are in fact equivalent uses in an essential way that, by definition, a regular extension is involutive on $X \times Y$ and $Y \times X$. Thus, for example, we look more carefully at the 'local' YBE diagram,

$$\begin{array}{ccc}
\alpha x y & \xrightarrow{r^{23}} & \alpha({}^{x}y x^{y}) \\
{\scriptstyle r^{12}}\downarrow & & \downarrow{\scriptstyle r^{12}} \\
({}^{\alpha}x\alpha^{x})y & & [{}^{\alpha}({}^{x}y)\alpha^{{}^{x}y}]x^{y} \\
{\scriptstyle r^{23}}\downarrow & & \downarrow{\scriptstyle r^{23}} \\
{}^{\alpha}x[{}^{\alpha^x}y(\alpha^x)^y] & & [{}^{\alpha}({}^{x}y)][{}^{\alpha^{{}^{x}y}}(x^y)][(\alpha^{{}^{x}y})^{x^y}] = w_1 \\
{\scriptstyle r^{12}}\downarrow & & \\
[{}^{{}^{\alpha}x}({}^{\alpha^x}y)][({}^{\alpha}x)^{{}^{\alpha^x}y}][(\alpha^x)^y] = w_2 & &
\end{array} \tag{4.5}$$

for which $w_1 = w_2$ is the condition $r_{12}r_{23}r_{12}(\alpha,x,y) = r_{23}r_{12}r_{23}(\alpha,x,y)$. However, all arrows are bijections so inverting the first r_{12} on the left and the last r_{23} on the right we have that $w_1 = w_2$ is equivalent to an instance of the equation $r_{23}^{-1}r_{12}r_{23} =$

$r_{12}r_{23}r_{12}^{-1}$ applied to some element of $X \times Y \times X$. But the inverted instances of r are of mixed type and hence involutive as explained, i.e. $r_{12}^{-1} = r_{12}$ acting the other way, $r_{23}^{-1} = r_{23}$ acting the other way here. Hence if condition A(1) holds then so does A(2). Similarly for all the other parts of the lemma. □

Theorem 4.9. *Let (X, r_X), (Y, r_Y) be disjoint solutions, with a regular pair of ground actions ${}^Y\bullet, \bullet^X$, and let (Z, r) be the corresponding regular extension. Then (Z, r) obeys YBE* if and only if **ml1,mr1,ml2,mr2**.

Proof. By hypothesis r is an extension of r_X and r_Y, therefore the 'local' YBE already holds on all $(x, y, z) \in X^3$ and $(\alpha, \beta, \gamma) \in Y^3$. All the other cases are covered in Lemma 4.8 as explained in the proof of that. Part A there covers the cases where exactly one element is from Y and these hold by the lemma *iff* **mr1**,**ml2**. Part B covers the cases where exactly two elements are from Y and these hold *iff* **ml1**,**mr2**. □

Corollary 4.10. *If (X, r) is a braided set, it has a canonical 'double braided set' $(X \sqcup X, r_D)$ where*

$$r_D(x, y) = r(x, y), \quad r_D(\bar{x}, \bar{y}) = r(\bar{x}, \bar{y}), \quad r_D(\bar{x}, y) = r(\bar{x}, y), \quad r_D(x, \bar{y}) = r^{-1}(\bar{y}, x)$$

for all $x, y \in X$. Here the bar denotes that the element is viewed in the second copy of X and the result of r is correspondingly interpreted.

Proof. Here $X = Y$ and $r_X = r_Y$. The ground actions are also those of X, hence all the conditions **ml1,mr1,ml2,mr2** reduce to **l1,r1,l2,r2** in X. □

Remark 4.11. Condition **ml1** implies that the assignment $\alpha \longrightarrow {}^{\alpha}\bullet$ extends to a left action of the associated YB-monoid $S(Y, r_Y)$ and YB-group $G(Y, r_Y)$ on X. **mr1** assures that the assignment $x \longrightarrow \bullet^x$ extends to a right action of the associated YB-monoid or YB-group (X, r_X) on Y. Hence **ml1,mr1** are degree 1 versions of axioms **ML1, MR1** of a matched pair. Meanwhile, **ml2** as a restriction of the invariance condition **l2** to parts of Z asserts that for every $\alpha \in Y$ the two maps r_X and the left action ${}^{\alpha}\bullet$ (extended on X^2 as usual) commute on X^2 so

$$({}^{\alpha}\bullet) \circ r_X = r_X \circ ({}^{\alpha}\bullet) : X^2 \longrightarrow X^2$$

i.e. that the action ${}^{\alpha}\bullet$ is compatible with the product of the YB-monoid or YB-group of (X, r_X). Similarly, **mr2** asserts that for every $x \in X$ there is an equality of maps in Y^2:

$$(\bullet^x) \circ r_Y = r_Y \circ (\bullet^x) : Y^2 \longrightarrow Y^2$$

or compatibility of $\bullet^x$ with the product of the YB-monoid or group of (Y, r_Y). In this way **ml2**, **mr2** can be viewed as the degree one analogue of the conditions **ML2, MR2** of a matched pair. This will be developed further in the next section.

Remark 4.12. Just as **l2** contains **l1** and **r2** contains **r1** in Lemma 2.9, the local version of the proof there, applied to parts of Z, includes the assertions

$$\mathbf{ml2} \quad \Rightarrow \quad \mathbf{ml1a} := \mathbf{l1(Y, X, X)} : \quad {}^{\alpha}({}^{x}y) = {}^{{}^{\alpha}x}({}^{\alpha^x}y), \quad \textit{for all } x, y \in X, \alpha \in Y$$

$$\mathbf{mr2} \quad \Rightarrow \quad \mathbf{m1ra} := \mathbf{r1(Y, Y, X)} : \quad (\alpha^{\beta})^x = (\alpha^{{}^{\beta}x})^{\beta^x}, \quad \textit{for all } x \in X, \alpha, \beta \in Y.$$

We now show that the under minor assumption of 3-cancellation these weaker conditions together are still sufficient.

Theorem 4.13. *Suppose (X, r_X), and (Y, r_Y) are 2-cancellative and U has cancellation on monomials of length 3. Then (Z, r) obeys YBE* iff **ml1, mr1**,**ml1a**,**mr1a**.

Proof. Under the hypothesis of the theorem, and Lemma 4.6, we know that (Z, r) is 2-cancellative and hence by Lemma 2.15 applied to (Z, r) we know that it obeys YBE iff **l1,r1** hold for Z. The mixed parts of these are **ml1,mr1**,**ml1a**,**mr1a**. The parts of **l1,r1** wholly for elements of X already hold as (X, r_X) is a braided set, and similarly for the parts wholly for elements of Y. The next lemma then completes the proof. □

By looking in detail at the proof of Lemma 2.15 applied to (Z, r), one can see that the proof there is again 'local' i.e. applies pointwise and hence to restricted versions of **l1,r1,l2,r2**. In this way one can establish using the methods above:

Lemma 4.14. *Under the hypothesis of Theorem 4.13:*

$$\mathbf{mr1}, \mathbf{ml1a} \Longleftrightarrow \mathbf{ml2}; \qquad \mathbf{ml1}, \mathbf{mr1a} \Longleftrightarrow \mathbf{mr2}.$$

Hence under the hypotheses of the theorem one can also say that (Z, r) is a braided set *iff* **ml2**,**mr2**. Finally, we look at the simplest types of regular extensions.

4.2. **Construction of matched pair extensions.** In this section we study the regular extensions (Z, r) of braided sets (X, r_X) and (Y, r_Y) in terms of their YB-monoids $S = S(X, r_X)$, $T = S(Y, r_Y)$ respectively. We let $U = S(Z, r)$ denote the monoid associated to (Z, r). Typically u, v, w will denote elements of S or in $\langle X \rangle$ but if there is ambiguity we shall indicate exactly which monoid is considered, similarly, a, b, c will denote elements of T or $\langle Y \rangle$. Our main Theorem 4.15 answers the question: under what conditions do the ground actions corresponding to the regular extension extend to a matched pair (S, T). The difference with Theorem 4.9 for (Z, r) to obey the YBE is that instead of **ml2,mr2** we require:

$$\begin{array}{lll} \mathbf{ml2w}: & \text{for all } x, y \in X,\ \alpha \in Y & \exists k,\ {}^{\alpha}(r_X(xy)) = r_X^k({}^{\alpha}(xy)) \\ \mathbf{mr2w}: & \text{for all } x \in X,\ \alpha, \beta \in Y & \exists k,\ (r_Y(\alpha\beta))^x = r_Y^k((\alpha\beta)^x). \end{array}$$

These equalities are in X^2 in the first case and in Y^2 in the second. We recall that two words $xy, x'y' \in \langle X \rangle$ of length two are equal in $S = S(X, r_X)$ *iff*

$$xy = r_X^k(x'y') \quad \text{in } \langle X \rangle \quad \text{for some integer } k$$

(this follows from standard Groebner basis results for monoids of this type). So **ml2w** is a weaker version of **ml2** in which equality is only required modulo the relations of S. Similarly for **mr2w**.

Theorem 4.15. *Let (X, r_X), (Y, r_Y) be disjoint solutions, with associated monoids S, and T. Let ${}^{Y}\bullet, \bullet^{X}$ be a regular pair of ground actions. Then (S, T) is a graded strong matched pair with actions extending respectively ${}^{Y}\bullet$ and $\bullet^{X}$*, if and only if **ml1, mr1,ml2w,mr2w**.

Proof. Assume (S, T) is a graded strong matched pair. Then since the matching actions are graded, conditions **ML1**, and **MR1**, restricted on X, Y give straightforwardly the identities **ml1, mr1** . Since the left action of T on S is graded and agrees with the relations on S, we conclude that $xy = zt$ in S implies ${}^{a}(xy) = {}^{a}(zt)$ in S, for all a in T. Clearly $xy = r(xy)$ in S for all $x, y \in S$. Hence **ml2w** comes straightforwardly from the following equalities in S^2

$$ {}^{\alpha}(r(xy)) = {}^{\alpha}(xy) = r({}^{\alpha}(xy)) \tag{4.6}$$

for all $x, y \in X, \alpha \in Y$. Similarly we deduce **mr2w**. It follows then that **ml1, mr1**, **ml2w**, **mr2w** are necessary conditions.

Next we show that these conditions are also sufficient. Hence we now assume that the conditions **ml1, mr1**, **ml2w**, **mr2w** are satisfied. We follow a strategy similar to the one in Section 3 to extend the actions on the generating sets to actions of a strong matched pair (S, T). Under the assumptions of the theorem we shall prove several statements. The procedure is parallel to the one in Section 3 and we omit those proofs that are essentially the same.

Thus, as a first approximation we extend the ground actions ${}^Y\bullet$ and $\bullet^X$, to a left action of T onto $\langle X\rangle$, ${}^T\bullet : T \times \langle X\rangle \longrightarrow \langle X\rangle$, and a right action of S onto $\langle Y\rangle$, $\bullet^S : \langle Y\rangle \times S \longrightarrow \langle Y\rangle$. Note that **ml1** implies straightforwardly a left action of T on X, and **mr1** implies a right action of S on Y defined the usual way. Clearly ${}^{(ab)}x = {}^a({}^bx)$, and $\alpha^{(uv)} = (\alpha^u)^v$, for all $x \in X, \alpha \in Y, u, v \in S, a, b \in T$.

Step 1. We define recursively a left "action"

$$
{}^Y\bullet : Y \times \langle X\rangle \longrightarrow \langle X\rangle \tag{4.7}
$$

via ${}^\alpha xu := {}^\alpha x {}^{\alpha^x}u$ (assuming that the actions ${}^\alpha v$ are defined for all $\alpha \in Y$, and all $v \in X^n$, with $n = |v|$. Analogously we define a right action

$$
\bullet^X : \langle Y\rangle \times X \longrightarrow \langle Y\rangle \tag{4.8}
$$

via $a\beta^x := a^{{}^\beta x}\beta^x$.

To be sure that these actions are well defined we need the following lemma. It is verified by an argument similar to the proof of Lemma 3.7. We consider equalities of monomials in the free monoids $\langle X\rangle$, and $\langle Y\rangle$.

Lemma 4.16. *The following conditions hold: a)* **ML2** *holds for Y "acting" (on the left) on $\langle X\rangle$, that is:*

$$
{}^\alpha(uv) = ({}^\alpha u).({}^{\alpha^u}v) \ \textit{for all} \ \alpha \in Y, u, v \in \langle X\rangle, \ \ |u|, |v| \geq 1.
$$

b) **MR2** *holds for X "acting" (on the right) on $\langle Y\rangle$, that is:*

$$
(ab)^x = (a^{{}^bx})b^x \ \textit{for all} \ x \in X, \ a, b \in \langle Y\rangle, \ \ |a|, |b| \geq 1.
$$

So the left and the right "actions" (4.7), (4.8) are well defined.

Step 2. We extend the "actions" (4.7), (4.8) to a left action of T onto $\langle X\rangle$, and a right action of S onto $\langle Y\rangle$.

Lemma 4.17. *The actions ${}^\alpha\bullet$, on $\langle X\rangle$ and $\bullet^x$ on $\langle Y\rangle$ extend to ${}^a\bullet$, and $\bullet^u$ for arbitrary monomials $a \in T, u \in S$, that is to left and right actions ${}^T\bullet : T \times \langle X\rangle \longrightarrow \langle X\rangle$ and $\bullet^S : \langle Y\rangle \times S \longrightarrow \langle Y\rangle$ obeying*

$$
{}^{ab}u = {}^a({}^bu) \ \textit{is an equality in} \ \langle X\rangle, \ \textit{for all} \ u \in \langle X\rangle, a, b \in T
$$

$$
a^{uv} = (a^u)^v \ \textit{is an equality in} \ \langle Y\rangle, \ \textit{for all} \ a \in \langle Y\rangle, u, v \in S.
$$

Proof. It will be enough to show that the following equalities hold:

$$
{}^\alpha({}^\beta u) = {}^{{}^\alpha\beta}({}^{\alpha^\beta}u) \text{ for all } \alpha, \beta \in Y, u \in \langle X\rangle. \tag{4.9}
$$

$$
(a^x)^y = (a^{{}^xy})^{x^y} \text{ for all } x, y \in X, a \in \langle Y\rangle. \tag{4.10}
$$

(4.9) is proven by induction on $|u| = n$. By hypothesis (4.9) holds for $|u| = 1$, which gives the base for induction. Assume (4.9) is true for all $u \in X^n$. Let $u \in X^{n+1}$. Then $u = tv$, with $t \in X$, $v \in X^n$. Consider the equalities:

$$^{\alpha}(^{\beta}u) = {}^{\alpha}(^{\beta}tv) = {}^{\alpha}((^{\beta}t).(^{\beta^t}v)) = (^{\alpha}(^{\beta}t))(^{\alpha^{\beta t}}(^{\beta^t}v))$$

where the second and last are by Lemma 4.16a), and

$$=^{\text{inductive ass.}} (^{\alpha}(^{\beta}t))(^{((\alpha^{\beta t}).(\beta^t))}v) = (^{\alpha}(^{\beta}t))(^{(\alpha\beta)^t}v)$$

using Lemma 4.16b) for the last equality. We have shown

$$^{\alpha}(^{\beta}u) = (^{\alpha\beta}t)(^{(\alpha\beta)^t}v) = w_1. \tag{4.11}$$

Similarly, we obtain:

$$^{^{\alpha}\beta}(^{\alpha^{\beta}}u) = (^{^{\alpha}\beta}(^{\alpha^{\beta}}t))(^{(^{\alpha}\beta.\alpha^{\beta})^t}v) = w_2. \tag{4.12}$$

Now

$$^{^{\alpha}\beta}(^{\alpha^{\beta}}t) =^{\mathbf{ml1}} {}^{\alpha\beta}t, \quad (^{\alpha}\beta.\alpha^{\beta})^t =^{\mathbf{mr2w}} (\alpha\beta)^t.$$

Therefore, the last two equalities and (4.11)-(4.12) imply $^{^{\alpha}\beta}(^{\alpha^{\beta}}u) = {}^{\alpha}(^{\beta}u)$. This verifies (4.9).

Now the equality

$$^{(\alpha_1\ldots\alpha_k)}u := {}^{\alpha_1}(\ldots(^{\alpha_{k-1}}(^{\alpha_k}u))..)$$

gives a well defined left action $T \times \langle X \rangle \longrightarrow \langle X \rangle$, which implies the first part of the lemma.

The proof of (4.10) is analogous. So the right action $\langle Y \rangle \times S \longrightarrow \langle Y \rangle$ is also well defined, and this implies the second part of the lemma. □

The following lemma is analogous to Proposition 3.9 and is proven by similar argument.

Lemma 4.18.

$$^{a}(uv) = (^{a}u).(^{(a^u)}v), \textit{ is an equality in } \langle X \rangle \textit{ for all } a \in T, u, v \in \langle X \rangle.$$

$$(ab)^u = (a^{^{b}u}).(b^u) \textit{ is an equality in } \langle Y \rangle \textit{ for all } a, b \in \langle Y \rangle, u \in S.$$

So far we have extended the actions ^{Y}X, and Y^X to actions $^{T}\langle X \rangle$ and $\langle Y \rangle^S$.

Step 3. We will show next that these actions respect the relations in S, T, and therefore they induce naturally left and right actions $^{(\,)}\bullet : T \times S \longrightarrow S$, and $\bullet^{(\,)} : T \times S \longrightarrow T$. We need analogues of Lemma 3.10, and Proposition 3.11. For these analogues we use slightly different arguments.

Lemma 4.19. *Condition* **ml2w** *is equivalent to the following*

$$xy = zt \textit{ in } S^2 \Longrightarrow {}^{\alpha}(xy) = {}^{\alpha}(zt) \textit{ in } S^2 \textit{ for all } x, y, z, t \in X, \alpha \in Y.$$

Proof. Since clearly $r(xy) = xy$ in S, so if we assume the stated condition in the lemma, $^{\alpha}(r(xy)) = {}^{\alpha}xy$ in S, which together with the evident equality $^{\alpha}xy = r(^{\alpha}xy)$ in S, imply $^{\alpha}(r(xy)) = r(^{\alpha}xy)$. Conversely, assume **ml2w** holds, and let $xy = zt$ in S^2. Remind that all equalities in S^2 come straightforwardly from the defining relations $\Re(r)$, therefore there exists positive integers k, l and a monomial $tu \in X^2$ such that $xy = r^l(tu)$, $zt = r^k(tu)$, (We do not assume r is necessarily of finite order.) Suppose now $\alpha \in Y$. The following equalities hold in S:

$$^{\alpha}(zt) = {}^{\alpha}(r^k(tu)) =^{\mathbf{ml2w}} r(^{\alpha}(r^{k-1}(tu))) = \cdots = r^k(^{\alpha}(tu)) = {}^{\alpha}(tu),$$

Similarly, ${}^{\alpha}(xy) = {}^{\alpha}(tu)$ hence **ml2w** implies the condition stated in the lemma. □

Lemma 4.20.
(i) $xy = zt$ *in* $S^2 \Longrightarrow {}^{a}(xy) = {}^{a}(zt)$ *in* S^2, *for all* $x, y, z, t \in X, a \in T$.
(ii) $\alpha\beta = \gamma\delta$ *in* $T^2 \Longrightarrow (\alpha\beta)^u = (\gamma\delta)^u$ *in* T^2, *for all* $\alpha, \beta, \gamma, \delta \in Y, u \in S$.

Proof. We shall prove (i), the proof of (ii) is analogous. We use induction on $|a|$ with Lemma 4.19 as base for the induction. Assume (i) is true for all a, with $|a| = n$. Consider:

$$\begin{aligned} {}^{a\beta}(xy) &= {}^{a}({}^{\beta}(xy)) && : \text{by } \mathbf{ML1} \\ &= {}^{a}({}^{\beta}(zt)) && : \text{by } \textit{Lemma } 4.19, \text{ and the inductive assumption} \\ &= {}^{a\beta}(zt) && : \text{by } \mathbf{ML1}. \end{aligned}$$

□

Corollary 4.21. *The actions* ${}^{(\,)}\bullet : T \times S \longrightarrow S$, *and* $\bullet^{(\,)} : T \times S \longrightarrow T$ *are well defined.*

Proof. It will be enough to verify:

$$xy = zt \text{ is an equality in } S^2 \Longrightarrow {}^{a}uxyv = {}^{a}uztv \text{ is an equality in } S$$

for all $x, y, z, t \in X, u, v \in S, a \in T$.

By Lemma 4.18 the following are equalities in $\langle X \rangle$:

$$(4.13) \qquad {}^{a}uxyv = ({}^{a}u)({}^{a^{u}}xy)({}^{a^{uxy}}v), \quad {}^{a}uztv = ({}^{a}u)({}^{a^{u}}zt)({}^{a^{uzt}}v).$$

Now the equality $xy = zt$ in S implies ${}^{a^{u}}xy = {}^{a^{u}}zt$ in S (by Lemma 4.17), and $a^{(uxy)} = a^{(uzt)}$ in $\langle Y \rangle$ (by **MR1**), so replacing these in (4.13) we obtain ${}^{a}uxyv = {}^{a}uztv$ holds in S. It follows then that for any $w_1, w_2 \in S$, and any $a \in T$, one has

$$w_1 = w_2 \text{ holds in } S \Longrightarrow {}^{a}w_1 = {}^{a}w_2 \text{ holds in } S.$$

Hence the left action of T on S is well defined. Similar argument verifies that the right action of S on T is also well defined. □

It follows from Lemmas 4.17, 4.18 that the actions obey **ML1, MR1, ML2, MR2**. (Clearly, an equality of words $u = v$ in $\langle X \rangle$ implies $u = v$ as elements of S, and an equality of words $a = b$ in $\langle Y \rangle$ implies $a = b$ as elements of T). We have proved Theorem 4.15. □

Proposition 4.22. *Suppose* (X, r_X), *and* (Y, r_Y) *are 2-cancellative and* U *has cancellation on monomials of length 3. Then* S, T *is a matched pair* iff **ml1, mr1** *hold for all* $x, y \in X, \alpha, \beta \in Y$. .

Proof. Under the hypothesis of the propositon, we first prove that

$$(4.14) \qquad \mathbf{ml1} \Longleftrightarrow \mathbf{mr2w}; \qquad \mathbf{mr1} \Longleftrightarrow \mathbf{ml2w}.$$

Thus, let $x, y \in X$, $\alpha \in Y$. We consider again the diagram (4.5). As we know each two monomials in the diagram are equal as elements of $U = S(Z, r)$. Hence $w_1 = w_2$ in U, which as before we can write as

$$(4.15) \qquad w_1 = [{}^{\alpha}(r_X(xy))][(\alpha^{{}^{x}y})^{x^{y}}] = [r_X({}^{\alpha}(xy))][(\alpha^{x})^{y}] = w_2$$

as an equality in U^3. By assumption U has cancellation on monomials of length 3, so (4.15) yields the second of (4.14). Analogous argument for a diagram starting with $\alpha\beta x$ gives the first of (4.14). We then use Theorem 4.15. □

Proposition 4.23. *Suppose* (X, r_X)*, and* (Y, r_Y) *are 2-cancellative,* S, T *is a matched pair and* $U = S \bowtie T$*. Then* (Z, r) *is a solution* iff **ml1a, mr1a**.

In this case S, T *is a strong matched pair.*

Proof. By Theorem 4.9 (Z, r) obeys YBE *if and only if* **ml1,mr1,ml2,mr2**. By hypothesis S, T is a matched pair, so **ml1, mr1** hold. It will be enough then to prove that under our assumptions one has:

$$\textbf{ml1a} \Longleftrightarrow \textbf{ml2}; \quad \textbf{mr1a} \Longleftrightarrow \textbf{mr2},$$

for all $x, y \in X, \alpha, \beta \in Y$.

We will show **ml1a** $\Longleftrightarrow$ **ml2**. Let $x, y \in X, \alpha \in Y$. Look again at the monomials w_1, w_2 in the the diagram (4.5). We know that

$$w_1 = [{}^{\alpha}({}^{x}y)][{}^{\alpha^{{}^{x}y}}(x^y)][(\alpha^{{}^{x}y})^{x^y}] = [{}^{{}^{\alpha}x}(\alpha^{x}y)][({}^{\alpha}x)^{\alpha^{x}y}][(\alpha^x)^y] = w_2 \tag{4.16}$$

is an equality in U^3. By assumption $U = S \bowtie T$, hence (4.16) implies the following equality in S^2 :

$$[{}^{\alpha}({}^{x}y)][{}^{\alpha^{{}^{x}y}}(x^y)] = [{}^{{}^{\alpha}x}(\alpha^{x}y)][({}^{\alpha}x)^{\alpha^{x}y}], \tag{4.17}$$

furthermore

$$[{}^{\alpha}({}^{x}y)][{}^{\alpha^{{}^{x}y}}(x^y)] = {}^{\alpha}(r_X(xy)), \quad [{}^{{}^{\alpha}x}(\alpha^{x}y)][({}^{\alpha}x)^{\alpha^{x}y}] = r_X({}^{\alpha}(xy)), \tag{4.18}$$

see for example (2.4). Then the 2-cancellativeness of r_X, (4.17), and (4.18) give the desired implications. Analogous argument proves **mr1a** $\Longleftrightarrow$ **mr2**. □

It is possible to prove further results along these lines [12]. For example, one can show under the same hypotheses as the above proposition, if the left and right ground actions are nondegenerate then U has cancellation on monomials of length 3.

4.3. **Matched pair characterisation of regular YB-extensions.** It is clear comparing Theorem 4.9 and Theorem 4.15 that regular extensions of (X, r_X) and (Y, r_Y) obey the YBE require that the associated monoids $S = S(X, r_Y)$ and $T = S(Y, r_Y)$ form a matched pair but that the latter is a weaker assertion. In this section we give a further matched pair requirement that then gives an exact characterisation of when a regular extension obeys the YBE, see Theorem 4.28. We use the conventions above for S, T and as above we let $U = S(Z, r)$.

First of all, let (Z, r) be an YB-extension of (X, r_X), (Y, r_Y). Then (U, r_U) is a braided monoid, induced from (Z, r), see Theorem 3.14. As we have seen in Section 3, the "ground" left and right actions ${}^{(\,)}\bullet : Z \times Z \longrightarrow Z$, $\bullet^{(\,)} : Z \times Z \longrightarrow Z$ induced by r extend uniquely to left and right actions

$${}^{(\,)}\bullet : U \times U \longrightarrow U, \ \bullet^{(\,)} : U \times U \longrightarrow U,$$

which respect the grading and make (U, U) a graded strong matched pair, with condition **M3**, see Theorem 3.6. (Note that its proof in this direction does not need the assumption that r is 2-cancellative). It is not difficult to see that these induce left and right actions:

$${}^{T}\bullet : T \times S \longrightarrow S, \ \text{ and } \ \bullet^{S} : T \times S \longrightarrow T, \tag{4.19}$$

and accompanying actions

$$\triangleright : S \times T \longrightarrow T, \ \text{ and } \ S \longleftarrow S \times T : \triangleleft \tag{4.20}$$

which make (S,T) a graded strong matched pair. Hence the following lemma is true.

Lemma 4.24. *Let (X,r_X), (Y,r_Y) be disjoint solutions, with YB-monoids, respectively S and T. Let (Z,r) be a regular YB- extension of (X,r_X), (Y,r_Y), with a YB-monoid U. Then (S,T), is a graded strong matched pair with actions (4.19) and (4.20) induced from the braided monoid (U,r_U).*

We will show first that in the case when (Z,r) is an YB- extension its associated group $G(Z,r)$ is a double crossed product of $G(X,r_X)$ and $G(Y,r_Y)$.

Proposition 4.25. *Let (X,r_X), (Y,r_Y) be disjoint solutions, with YB- groups $G_X=G(X,r_X)$, and $G_Y=G(Y,r_Y)$. Let (Z,r) be a regular YB- extension of (X,r_X), (Y,r_Y), with a YB-group $G_Z=G(Z,r)$. Then*

1. *G_X,G_Y is a matched pair of groups with actions induced from the braided group (G_Z,r).*
2. *G_Z is isomorphic to the double crossed product $G_X\bowtie G_Y$.*

Proof. (1) is straightforward. To prove (2) we first show that $G_Z=G_X.G_Y$ as set, i.e. that every element $w\in G_Z$ can be presented as $w=ua, u\in G_X, a\in G_Y$. Indeed, G_Z is generated by $Z=X\bigcup Y$, so every element $w\in G_Z, w\neq 1$ has the shape

$$w=u_1a_1u_2a_2\cdots u_{s+1}a_{s+1}, \tag{4.21}$$

where $u_i\in G_X, a_i\in G_Y, i=1,...s$, $u_1=1$, or $a_s=1$, is possible, but if $s\geq 0$, one has $u_i\neq 1$, for $2\leq i\leq s+1$, and $a_j\neq 1$, for $1\leq j\leq s$. We have to "normalize" w. For the purpose we use induction on the number $n(w)=s$ of sub-words a_i of w which occur in a "wrong" place, and have to be "moved" to the right. There is nothing to prove if $s=0$. This is the base for the induction. Suppose every w with $n(w)\leq s-1$ can be reduced to a presentation $w=ua$, with $u\in G_X$, $a\in G_Y$. Let $w\in G_Z$ has a presentation (4.21) with $n(w)=s, s\geq 1$. We reduce w using condition **M3**.

(4.22)
$$w=u_1a_1u_2a_2\cdots u_sa_su_{s+1}a_{s+1}=^{\mathbf{M3}} u_1a_1u_2a_2\cdots u_s({}^{a_s}u_{s+1})({a_s}^{u_{s+1}}).a_{s+1}=w_1$$

Now (4.22) gives a new presentation w_1 of w, $w=w_1$ as elements of G_Z, but $n(w_1)=s-1$, so by the inductive assumption w_1 can be reduced to the shape $w_1=ua$, with $u\in G_X$, $a\in G_Y$. Hence every element of G_Z can be presented in the required normal form.

Moreover, it is easy to see that for each $w\in G_Z$ the presentation $w=ua$, with $u\in G_X, a\in G_Y$ is unique. Indeed, if we assume,

$$ua=vb, u,v\in G_X, a,b\in G_Y$$

then

$$v^{-1}u=ba^{-1}\in G_X\bigcap G_Y.$$

By hypothesis X and Y are disjoint sets, so $G_X\bigcap G_Y=1$, which in view of the previous equality implies $v=u, b=a$. This proves part (2). □

We will show analogous result about monoids. In this case we do not assume cacellation holds in U.

Lemma 4.26. *Let (Z,r) be a YB-extension in the setting above. Each element $w\in U$ can be presented uniquely as $w=ua, u\in S, a\in T$.*

Proof. We will make first some general remarks. Let $W_0 \in \langle Z \rangle$. Clearly W_0 is a product of elemets of $Z = X \bigcup Y$. Suppose $|W_0| = N$. By hypothesis (Z, r) is a solution, therefore the *braid group* B_N acts on Z^N. Note that the orbit of W_0 under this action consists exactly of all words $W \in \langle Z \rangle$, with the property $W_0 = W$ as elements of U. Indeed, $W_1 = W_2$ in U *iff* there are finite sequences of replacements $\rho_i, 1 \leq i \leq p, \sigma_j, 1 \leq j \leq q$, coming from the relations $\Re(r)$, and such that the following is an equality of words in the free monoid $\langle Z \rangle$:

$$\rho_p \circ \cdots \rho_1(W_1) = \sigma_q \circ \cdots \circ \sigma_1(W_2). \tag{4.23}$$

But each such a replacement is exactly r^{ii+1}, for an appropriate $i, 1 \leq i \leq N-1$. ($r^{ii+1} = \mathrm{id}_{Z^{i-1}} \times r \times \mathrm{id}_{Z^{N-i-1}}$). Now consider $\deg_X$ (respectively $\deg_Y$) which count the number of symbols from X, (respectively, from Y) that occur in an element of $\langle Z \rangle$. Since each relation in $\Re(r)$ has the shape $yz = {}^y z.y^z$, where $y, z \in Z$ it is immediate that each replacement in (4.23) leaves the degrees unchanged. Hence both $\deg_X$ and $\deg_Y$ are defined on U itself and in particular are independent of the choice of representative W_0, say, of our given element w. We let $K = \deg_X(w)$ and $L = \deg_Y(w)$.

Since U is an **M3** monoid we can clearly use similar replacements as in the proof of Proposition 4.25 to put w in a normal form $w = ua$ with corresponding presentatation in normal form $W_0 = U_0A_0$, where $U_0 \in X^K$, $A_0 \in Y^L$. The following sub-lemma shows that any element of B_N that sends W_0 to something again of this form has the same action as an element of $B_K \times B_L$. Hence any other presentation in normal form has the shape $\rho_1(U_0)\rho_2(A_0)$ where $\rho_1 \in B_K$ and $\rho_2 \in L$. But by the remarks above applied to X (respectively Y) we see that $U_0 = \rho_1(U_0)$ when viewed in S and $A_0 = \rho_2(A_0)$ when viewed in T. □

Lemma 4.27. *Let $N = K + L \geq 2$ be positive integers and consider the action of the braid group B_N on Z^N induced by a regular YB-extension (Z, r) of (X, r_X), (Y, r_Y). The action of any braid group element sending $X^K \times Y^L \to X^K \times X^L$ can be presented as the action of an element of $B_K \times B_L$.*

Proof. A regular extension means that the restrictions $r_{X,X} = r_X$, $r_{Y,Y} = r_Y$, $r_{Y,X}$ and $r_{X,Y} = r^{-1}_{Y,X}$ obey the mixed braided relations where strands are labelled by X or Y (i.e. there is a braided category for which objects are arbitrary products of X, Y and the braiding is given by the various restrictions of r). We present an element of $b \in B_N$ as a series of elementary crossings and we represent it as a map $X^K \times Y^L \to X^K \times Y^L$ defined as the corresponding composition of $r_{X,X}, r_{Y,Y}, r_{X,Y}, r_{Y,X}$ or their inverses according to the orientation and labelling of strands as at each crossing. A standard crossing say with a left strand passing down and over a right strand is represented by one of the r, while a reversed crossing where the left strand passes down and under is represented by one of the r^{-1}. The most important fact for us is that in this representation an $X - Y$ crossing is represented by the same map for either orientation of crossing. With these preliminaries, the proof of the lemma proceeds by induction on the total number M of $X - X$ or $Y - Y$ crossings in a presentation of b.

Case $M = 0$. This means that the only crossings are of $X - Y$ or $Y - X$ type. We are going to do an induction in the even number P of such crossings to prove that the representation of such a braid is the identity. If $P = 0$ we have the identity braid and are done. By the remarks above the representation does not depend on whether the crossings are 'under' or 'over'. Our notation in Figure 2 therefore does

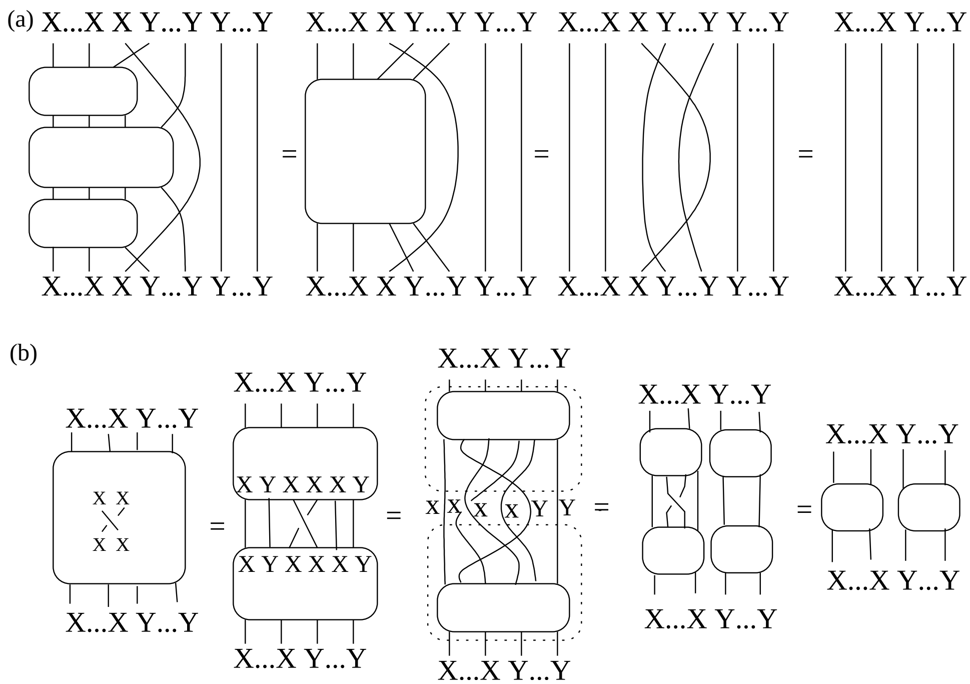

Figure 2. Diagrams in proof of Lemma 4.27 needed for $U = S \bowtie T$, (a) case $M = 0$ and (b) case $M \geq 1$.

not distinguish these. Moreover, if a strand crosses another and then immediately crosses back as the braid presentation is read from top down, the representation is the same as if the two crossings were replaced by identity maps. This is then a presentation of a braid of the same type but with $P-2$ crossings, and we assume the result is true for all such braid presentations as induction hypothesis. Therefore it suffices to prove the result for braid presentations with $M = 0$ and no 'double crosses' in which a strand is crossed and then crossed back. In this case consider the right-most X strand in $X^K \times Y^L$. It cannot cross to the left as this would need an $X - X$ crossing but it can cross to the right. However there are only a finite number of Y' to the right so it cannot keep crossing to the right. At some point the X strand must cross over some Y strand in maximal position L' to the right followed at some point later by crossing back to the left. By the same argument of no double-crossings, it must then keep crossing Y's to the left until it eventually crosses back over all the Y strands. This is depicted in Figure 2(a) where the boxes depict unkown braid of $X - Y$ and $Y - X$ type. Since operations in disjoint strands commute we can group all these boxes as one large box which is then a presentation of a braid on $X^{K-1} \times Y^{L'}$ and less than P crossings. Hence by our induction hypothesis the representation of this unknown braid is trivial. Hence our original braid has the same representation as one of the form shown in the middle in Figure 2(a) which is then trivial for reasons as above. An informal explanation of the idea behind the above argument is that r is involutive for $X - Y$ and $Y - X$

crossings and since only these are involved, the representation is "effectively" as for a representation of the symmetric group S_N, which would be trivial here.

Case $M \geq 1$. Mark an $X-X$ or $Y-Y$ crossing according to what is available, for example we illustrate the former case. We divide the braid presentation into two boxes, those that came before and those that came after the marked crossing. In each case we use only $X-Y$ and $Y-X$ crossings to move all the Y strands to the right after the first box, and before the second box. This is shown in Figure 2(b). In each case the composites shown dashed are braid presentations in our standard form on $X^K \times Y^L$ but with smaller total number of $X-X$ and $Y-Y$ crossings. By our induction hypothesis, these composites have the same representation as the product of some braid on X^K and some braid on Y^L. This is the middle equality in Figure 2(b). Hence the original braid has representation in the same required form. Analogous arguments apply if the marked crossing is a $Y-Y$ one. $\square$

We have done most of the work in these lemmas for one direction of the following theorem.

Theorem 4.28. *Let (X, r_X), (Y, r_Y) be disjoint solutions, with associated monoids S, and T. Let ${}^Y\bullet, \bullet^X$ be a regular pair of ground actions, (Z, r) the corresponding regular extension and U its associated monoid. Then (Z, r) obeys YBE* if and only if *the following condition hold:*

1. *$U = S \bowtie T$, where (S, T) is a strong matched pair, with actions extending the ground actions; and*
2. *(S, U) and (U, T) are matched pairs with canonical actions induced from the actions of S, T.*

In this case $G_Z = G_X \bowtie G_Y$.

Proof. Assume first that (Z, r) is a YB-regular extension of (X, r_X), (Y, r_Y). By Lemma 4.24 (S, T), is a graded strong matched pair with actions (4.19) and (4.20) induced from the braided monoid (U, r_U). The last lemma shows that $U = S \bowtie T$, which is part (1). For (2) we use again the fact that the "ground" left and right actions extend uniquely to left and right actions which make (U, U) a graded strong matched pair, see Theorem 3.6. These actions immediately restrict to actions

$$^{(\,)}\bullet : U \times S \longrightarrow U, \quad \bullet^{(\,)} : U \times S \longrightarrow S,$$

which make (S, U) a graded matched pair. Similarly, (U, T) is a matched pair with actions restricted from those of from (U, U).

Conversely, assume conditions (1), (2) are satisfied. We will show that (Z, r) obeys YBE. By Theorem 4.9 it will be enough to prove conditions **mr1, ml2, ml1, mr2**. By assumption (S, U) is a matched pair, so the action of S respects the relations of U. Using **MR2** from the matched pair axioms we have in particular that

$$(^{\alpha}y)^{(\alpha^{y}x)}.(\alpha^{y})^{x} = (^{\alpha}y.\alpha^{y})^{x} = (\alpha y)^{x} = \alpha^{^{y}x}.y^{x} = {}^{\alpha^{(^{y}x)}}(y^{x}).(\alpha^{^{y}x})^{y^{x}} \tag{4.24}$$

in U for all $x, y \in X, \alpha \in Y$ (this can also be written as **mr2w** with Z in the role of Y for construction of the matched pair (S, U)). By assumption part (1) holds, so U decomposes into ST and each element $w \in U$ has unique presentation as $w = ua, u \in S, a \in T$. Hence equality of the two factors of (4.24) holds separately, which we identify as $\mathbf{lr3}(\alpha, \mathbf{y}, \mathbf{x})$ and $\mathbf{r1}(\alpha, \mathbf{y}, \mathbf{x})$. Also, since U acts on S, its relations are respected which means ${}^{\alpha}(^{y}x) = {}^{^{\alpha}y}(^{\alpha^{y}}x)$ or $\mathbf{l1}(\alpha, \mathbf{y}, \mathbf{x})$. We group this with $\mathbf{lr3}(\alpha,\mathbf{y},\mathbf{x})$ as $\mathbf{l2}(\alpha,\mathbf{y},\mathbf{x})$, as in the local version of the proof of Lemma 2.9 applied in a part of Z^2. Since these remarks hold for all $x, y \in X$ and $\alpha \in Y$, we have proven **mr1, ml2** as required. The other two follow similarly from a matched pair (U, T). □

We have found explicit minimal conditions on the ground actions (4.4) which are necessary and sufficient to have extensions with nice properties. Now we give a global description of the nature of extensions of this type. Theorem 3.23 tells us that r_Z obeys the YBE when constructed in this form of a matched pair extension (U, U), and we shall see that essentially this form is forced on us for any extension with nice properties.

Definition 4.29. A regular extension of **M3**-monoids S, T is an **M3**-monoid U such that $U = S \bowtie T$ where (S, T) is a strong matched pair and the actions of (U, U) extend the actions of $(S, S), (T, T), (S, T), (T, S)$. We denote the last of these by $\triangleright, \triangleleft$.

Remark 4.30. If the actions in the initial matched pairs extend, then

$$ {}^{v}(u.a) = {}^{v}u(v^{u}\triangleright a), \quad {}^{b}(u.a) = {}^{b}u.{}^{b^{u}}a \tag{4.25}$$

are the only possible definitions for the actions of S, T. Hence the extended actions necessarily take the form

$$ {}^{(v.b)}(u.a) = {}^{v}({}^{b}u).(v^{{}^{b}u}\triangleright {}^{b^{u}}a), \quad (v.b)^{(u.a)} = (v^{{}^{b}u}\triangleleft {}^{b^{u}}a).(b^{u})^{a}. \tag{4.26}$$

Equivalently, the associated map r_U in terms of the associated maps for each matched pair takes the form

$$ r_U = {r_{T,S}^{23}}^{-1} \circ r_T^{34} \circ r_S^{12} \circ r_{T,S}^{23} : S\times T\times S\times T \to S\times T\times S\times T, \tag{4.27}$$

where the numerical indices denote the positions in which the map is applied.

Theorem 4.31. *Let $U = S \bowtie T$ for (S, T) a strong matched pair of* **M3**-*monoids. The following are equivalent:*

(1) U is a regular extension of **M3**-*monoids.*
(2) $(U, T), (S, U)$ are matched pairs extending the given actions.
(3) **ml2,mr2** *defined analogously to Notation 4.7 but for S, T, hold.*

Proof. The conditions in part (3) are the monoid versions of **ml1, mr2** in the notation used previously, except that we apply them now to the sets of the monoids S, T in the role of X, Y. Let us also decompose **ml2=l2(T,S,S)** into pieces **ml1a=l1(T,S,S)** and **lr3a** analogously to Section 2, and similarly for **mr2= r2(T,T,S)**. Explicitly the conditions of part (3) therefore read:

$$ \mathbf{ml1a}: \quad {}^{{}^{a}u}({}^{a^{u}}v) = {}^{a}({}^{u}v), \quad \mathbf{lr3a}: \quad ({}^{a}u)^{({}^{a^{u}}v)} = {}^{(a^{{}^{u}v})}(u^{v}) $$

$$ \mathbf{mr1a}: \quad (a^{b})^{u} = (a^{{}^{b}u})^{b^{u}}, \quad \mathbf{lr3b}: \quad ({}^{a}b)^{({}^{a^{b}}u)} = {}^{(a^{{}^{b}u})}(b^{u}) $$

for all $u, v \in S$ and $a, b \in T$. The **ml1a, mr1a** are the same conditions as previously but applied here to S, T in the role of X, Y. We first show that these four are equivalent to part (2).

Under the hypothesis of the theorem we have matched pairs $(S, S), (T, S), (S, T), (T, S)$ and we define left actions of T, S on U by the necessary formula (4.25). That these are separately well-defined actions of S, T follows from

$$ {}^{b}({}^{c}(ua) = {}^{b}({}^{c}u.{}^{c^{u}}a) = {}^{b}({}^{c}u).{}^{b^{{}^{c}u}c^{u}}a = {}^{bc}u.{}^{(bc)^{u}}a = {}^{bc}(u.a) $$

and a similar computation for $\triangleright$, using only that the initial matched pair data. Similarly for the right actions of S, T on $(u.a)$.

In particular for the (U, T) matched pair we look at the above left action of T on U and a right action of U on T given necessarily by $b^{u.a} = (b^u)^a$. Since the cross-relations of $U = S \bowtie T$ are $au = {}^a u.a^u$, the latter is an action exactly when **mr1a** holds. In this case

$$(bc)^{u.a} = ((bc)^u)^a = (b^{{}^c u} c^u)^a = (b^{{}^c u})^{(c^u)a}.(c^u)^a = b^{({}^c u.{}^{c^u} a)}(c^u)^a = b^{{}^c(u.a)} c^{u.a}$$

again from just the initial matched pair data and the definitions. So the matched pair condition on this side holds automatically. For the condition on the other side

$$\begin{aligned} {}^c((u.a)(v.b)) &= {}^c(u.{}^a v.a^v.b) = {}^c(u.{}^a v)^{c^{(u.{}^a v)}}(a^v.b) = {}^c u.{}^{(c^u.a)}v.{}^{(c^{(u.{}^a v)})}(a^v).{}^{(c^{(u.{}^a v)})^{a^v}} b \\ {}^c(u.a).{}^{c^{u.a}}(v.b) &= ({}^c u.{}^{c^u} a).({}^{c^{u.a}} v.{}^{(c^{u.a})^v} b) = {}^c u.{}^{(({}^{c^u} a)(c^u)^a)} v.({}^{c^u} a)^{({}^{c^{u.a}} v)}.{}^{(c^{u.{}^a v})^{a^v}} b \end{aligned}$$

using only the definitions. The second factors agree by the **M3** property in T. The outer factors agree, and the third factors agree if **lr3b** holds. This is also necessary for agreement if one sets $u = b = 1$ and uses unique factorisation in $U = S \bowtie T$ (i.e. an equality means equality of each factor in normal form). Similarly, we have the actions for a matched pair (S, U) precisely when **ml1a** holds and they form a matched pair precisely when **lr3a** holds. Hence (2) $\Leftrightarrow$ (3).

Clearly (1) implies (2) by restricting the actions in the (U, U) matched pair. We now show the converse, i.e. that the (S, U) and (U, T) matched pairs automatically extend to a (U, U) one with actions of the form (4.26). Note that if our actions do form a matched pair, then

$$\begin{aligned} (vb)(ua) &= v.{}^b u.b^u.a = {}^v({}^b u)(v^{{}^b u})({}^{b^u} a)(b^u)^a = {}^v({}^b u).(v^{{}^b u} \triangleright {}^{b^u} a).(v^{{}^b u} \triangleleft {}^{b^u} a).(b^v)^a \\ &= {}^{(vb)}(ua)(vb)^{(ua)}. \end{aligned}$$

i.e. **M3** necessarily holds for (U, U).

In order to proceed, we first prove an equivalent version of part (2); we can equally well construct matched pairs $(U, S), (T, U)$ in the same way. To do this, we use Lemma 4.8 applied now to the sets S, T. The conditions **mr1=r1(T,S,S)** which is part of the (S, T) matched pair hypothesis and **l2(T,S,S)** together are equivalent to **r1(S,S,T), l2(S,S,T)**. Similarly **ml1=l1(T,T,S)** and **r2(T,T,S)** together are equivalent by the lemma to **r2(S,T,T), l1(S,T,T)**. Note that we do not actually need r_S, r_T to be invertible in the proof of the lemma and we do not have this here, otherwise the proof is the same (alternatively one can understand **L2** as a covariance property of $r_{T,S}$ and this holds if an only if its inverse is covariant; one can eventually deduce the required result from this). We write **mr1a'=r1(S,S,T)** and **ml1', lr3a'** for the two parts of **l2(S,S,T)**. Explicitly:

$$\textbf{mr1a}': \quad u^v \triangleleft a = (u \triangleleft (v \triangleright a)) \triangleleft (v \triangleright a), \quad \textbf{lr3a}': \quad {}^u v \triangleleft (u^v \triangleright a) = (u \triangleleft (v \triangleright a)) \triangleright (v \triangleleft a).$$

Here **ml1'** is part of the (T, S) matched pair data that S acts on T from the left. Meanwhile **mr1a'** says that $U = T \bowtie S$ acts on S from the right as an extension of the given actions. That S acts on U from the matched pair hypothesis and one of the matching conditons requires precisely the **lr3a'** condition. The details are strictly analogous to our proof above so we omit them. In the same way, that the relevant actions extend to matched pairs (T, U) uses **ml1a'=l1(S,T,T)** and the two parts **mr1'** and **lr3b'** of **l2(S,T,T)**. The middle one is part of the (T, S)

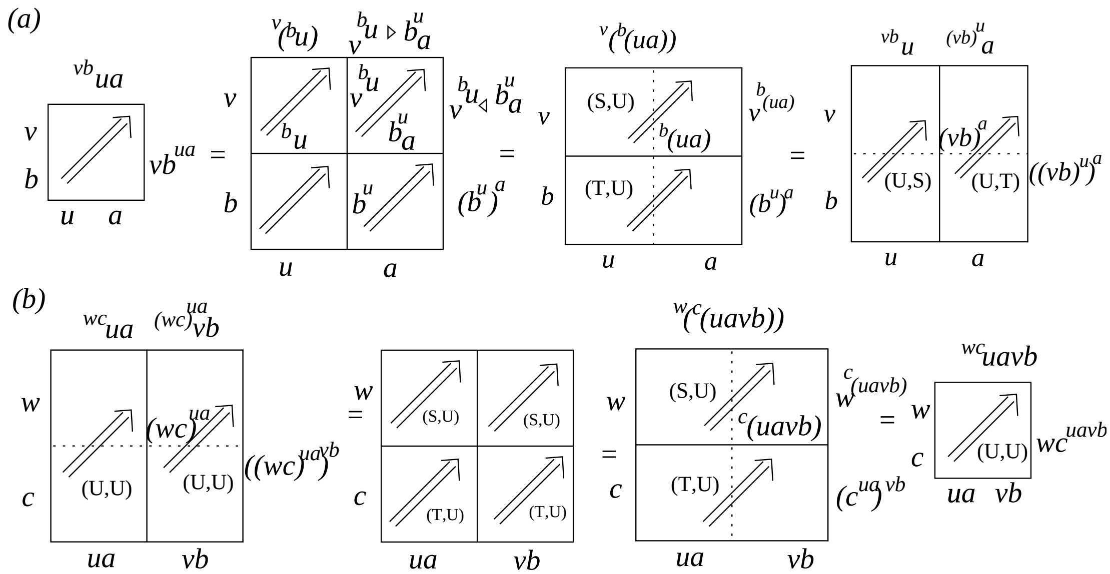

FIGURE 3. Proof that extension forms a matched pair. (a) definition of extended actions, (b) proof of vertical subdivision property.

matched pair data and the the other two read explicitly

$$\mathbf{ml1a'}:\quad u\triangleright {}^a b = {}^{u\triangleright a}((u\triangleleft a)\triangleright b),\qquad \mathbf{lr3b'}:\quad (u\triangleright a)\triangleleft((u\triangleleft a)\triangleright b) = (u\triangleleft {}^a b)\triangleright a^b.$$

In principle one can now proceed to use these variant conditions as well as the original conditions (3) to verify the matched pair structure for (U,U). We have given them explicitly in case the reader wishes to verify any parts of this (for example that that $v\in S, b\in T$ acting on U as above indeed form a representation of $S\bowtie T$ is a reasonable computation). Here we provide a diagrammatic proof using the subdivision form of the matched pair axioms explained in Figure 1(a) and the results already proven. In our case the proposed action of $S\bowtie T$ on itself is given in terms of its composite square in Figure 3(a). By definition it consists of composing the four actions in our initial data according to the same 'transport' rules, namely that the action takes place as the element is taken through the box (to the top or to the right). That this composite could also be viewed as a vertical composite of two horizontal rectangular boxes or a horizontal composite of two vertical boxes, is nothing other than a restatement of the definitions. In the first case the (U,U) actions are represented as the (S,U) actions placed above the (T,U) actions. In the second case it is represented as the (U,S) actions placed to the left of the (U,T) actions.

We can now prove the subdivision property as follows. The horizontal one is shown in Figure 3(b). On the left is the horizontal composition of two instances of the (U,U) actions. We wish to show that this can be merged into a single (U,U) box as on the right. To do this we break the boxes on the dotted line to give four boxes. The lower two are two horizontally composed instances of the (T,U) actions and since this is a matched pair by the variant of part (2) it composes to a single horizontal box. Similarly, the two upper boxes are horizontally composed (S,U)

actions and hence by part (2) they compose to a single horizontal box. This is shown in the middle of Figure 3(b). Finally, the placement of one horizontal box vertically over the other is nothing other than one definition of the (U,U) actions as explained above.

The vertical subdivision property is entirely analogous. We break two vertically composed (U,U) boxes into four boxes. The two on the left are vertically composed instances of (U,S) boxs, the two on the right are vertically composed instances of (U,T) boxes. Since we have proven above that these are matched pairs as part (2) and its variant, we can merge these boxes and recognise a single (U,U) box as a single (U,S) box followed horizontally by a single (U,T) box, which is our alternate definition of the (U,U) box as explained above. □

Corollary 4.32. *Let $U = S \bowtie T$ be a regular extension of* **M3**-*monoids.*

(1) U is strong iff *S,T are.*

(2) U is braided iff *S,T are braided.*

Proof. Part (1) is clear as r_U is invertible precisely when both r_S, r_T are. For part (2) we recall that **mr1=r1(T,S,S), l2(T,S,S)** have the interpretation explained in the proof of Lemma 4.8 of the YBE restricted to $T \times S \times S$, the difference is that we now work on the sets S,T with the restrictions of r_U but the diagram involved is analogous. Similarly for **ml1, r2(T,T,S)**. By Lemma 4.8 we deduce that the YBE holds for all mixed triples (those involving elements of both S,T) using the restrictions $r_S, r_T, r_{S,T}, r_{T,S}$. We have seen in the theorem that that these are precisely the conditions for a regular extension of **M3**-monoids. Hence, given this, the YBE holds for all combinations precisely when it holds for r_S and r_T separately. □

Corollary 4.33. *If (S, r_S) is a braided monoid then it has a canonical 'quantum double' braided monoid $(S \bowtie S, r_{S\bowtie S})$.*

Proof. The conditions in part (3) of the theorem hold because all the actions involved are based on the actions of (S,S) and (S,r_S) is assumed to be a braided monoid. In more explicit terms **ml1a, mr1a** for S,T hold automatically as the actions are given by the actions of S on itself, which is a strong matched pair (S,S) by assumption, while conditions **lr3a, lr3b** hold as part of the assumption that r_S obeys YBE. We then use the theorem and the preceding corollary. □

We remark that this is exactly analogous to the construction of a quasitriangular structure or 'doubled braiding' on $A(R) \bowtie A(R)$ as a version of Drinfeld's quantum double, see [22]. In the case of S given by a braided set (X,r), it corresponds to the braided set $(X \sqcup X, r_D)$ in Corollary 4.10.

Proposition 4.34. *Suppose that S,T are cancellative* **M3**-*monoids forming a strong matched pair. Then $U = S \bowtie T$ is a regular extension* iff **ml1a, mr1a** *hold for S,T. In this case U is cancellative.*

Proof. Since (S,T) are a matched pair we can argue that

$$\begin{aligned} {}^a(uv) &= {}^a({}^uv.u^v) = {}^a({}^uv).^{(a^{{}^uv})}(u^v) \\ &= {}^au.^{a^u}v = {}^{{}^au}({}^{a^u}v).({}^au)^{({}^{a^u}v)} \end{aligned}$$

using the **M3** property for the first and last equalities. So if we assume the **ml1a** condition stated and left cancellation in S we will have **lr3a** above. Similarly for

lr3b using **mr1a** and right cancellation in T. If we assume cancellation on both sides then suppose $(u.a)(v.b) = (u'.a').(v.b)$ in U. Using the cross-relations in $U = S \bowtie T$ and the unique factorisation there, this means

$$u.{}^a v = u'.{}^a v, \quad a^v.b = a'^v.b$$

From the second and right cancellation in T we have $a'^v = a^v$. Using (3.1) we deduce

$$u \triangleright a = (u{}^a v) \triangleright a^v = (u'{}^{a'} v) \triangleright a^v = u' \triangleright ({}^{a'} v \triangleright a'^v) = u' \triangleright a'$$

$$(u \triangleleft a)v = u \triangleleft ({}^a v \triangleright a^v).({}^a v \triangleleft a^v) = (u{}^a v) \triangleleft a^v = (u'{}^{a'} v) \triangleleft a^v = (u'{}^{a'} v) \triangleleft a'^v = (u' \triangleleft a').v$$

hence if we have right cancellation in S we deduce that $u' \triangleleft a' = u \triangleleft a$. It follows from (3.1) that $u' = u, a' = a$. From the other side, $(u.a)(v.b) = (u.a).(v'.b')$ means

$$u.{}^a v = u.{}^a v', \quad a^v.b = a^{v'}.b'$$

so by left cancellation in S we have ${}^a v = {}^a v'$. This and the remainder of the proof is analogous to the proof on the other side already given. □

5. Application to symmetric sets and strong twisted unions

In this section we apply the matched pair approach developed in the paper to construct extensions in some important special cases such as nondegenerate involutive solutions (or as they are often called *symmetric sets*) (X, r), strong twisted unions of solutions, see Definition 5.1, finite square-free solutions, etc. Note that every finite non-degenerate involutive square-free solution (Z, r) is an extension of some nonempty disjoint square-free involutive solutions (X, r_X), and (Y, r_Y), [24]. Furthermore, in this case the monoid $S(Z, r)$ and the YB-algebra $\mathcal{A}(k, Z, r)$ (over arbitrary field k) have remarkable algebraic and homological properties, see [10, 5, 8, 9, 14]. In [12] our matched pair approach is applied to various special cases of extensions of solutions, in particular to strong twisted union of solutions, finite symmetric sets, finite square-free involutive solutions, etc.

Definition 5.1. We call a regular extension (Z, r) a *strong twisted union* of the quadratic sets (X, r_X) and (Y, r_Y) if

(1) The assignment $\alpha \longrightarrow {}^\alpha \bullet$ extends to a left action of the associated group $G(Y, r_Y)$ (and the associated monoid $S(Y, r_Y)$) on X, and the assignment $x \longrightarrow \bullet^x$ extends to a right action of the associated group of $G(X, r_X)$ (and the associated monoid $S(X, r_X)$) on Y;
(2) The regular pair of ground actions satisfy

$$\textbf{stu}: \qquad {}^{\alpha^y} x = {}^\alpha x; \qquad \alpha^{{}^\beta x} = \alpha^x, \quad \text{for all} \quad x, y \in X, \alpha, \beta \in Y$$

Remark 5.2. In [2], Definition 3.3. the notion of *a generalized twisted union* (Z, r) of the solutions (X, r_X) and (Y, r_Y), is introduced in the class of symmetric sets. More precisely, a symmetric set (Z, r) is a generalized twisted union of the disjoint symmetric sets (X, r_X), and (Y, r_Y) if it is an extension, and for every $x \in X, \alpha \in Y$ the ground action ${}^{\alpha^x}\bullet : Y \times X \longrightarrow X$ does not depend on x, and the ground action $\bullet^{{}^\alpha x} : Y \times X \longrightarrow Y$ does not depend on α.

Note that in contrast with a generalized twisted union, a strong twisted union (Z, r) of (X, r_X) and (Y, r_Y) does not necessarily obey YBE and is not limited to symmetric sets. It is easy to see that a strong twisted union (Z, r) of symmetric sets which obeys YBE, is a generalized twisted union. Furthermore, it will be shown in

[12] that a generalized twisted union (Z, r) of two involutive square-free solutions is a strong twisted union.

Remark 5.3. Let (X, r) be a quadratic set. A permutation $\tau \in \mathrm{Sym}(X)$ is called *an automorphism of* (X, r) (or shortly an *r-automorphism*) if $(\tau\times\tau)\circ r = r\circ(\tau\times\tau)$. The group of r-automorphisms of (X, r) will be denoted by $\mathrm{Aut}(X, r)$. In [12] it will be shown that a strong twisted union (Z, r) of solutions (X, r_X) and (Y, r_Y) obeys the YBE *if and only if* the assignment $\alpha \longrightarrow {}^{\alpha}\bullet$ extends to a a group homomorphism

$$G(Y, r_Y) \longrightarrow Aut(X, r)$$

and the assignment $x \longrightarrow \bullet^{x}$ extends to a a group homomorphism

$$G(X, r_X) \longrightarrow Aut(Y, r).$$

Here we limit ourselves to some first results connecting with those of Section 2.

Proposition 5.4. *Let (Z, r) be a strong twisted union of the 2-cancellative disjoint solutions, (X, r_X) and (Y, r_Y). Suppose* **lri** *holds for (Z, r) and $U = S(Z, r)$ has cancellation on monomials of length 3. Then (Z, r) obeys YBE* iff

$$\textbf{csla}: \quad {}^{{}^{y}\alpha}({}^{y}x) = {}^{{}^{\alpha}y}({}^{\alpha}x) \qquad \textbf{csra}: \quad (\alpha^{\beta})^{x^{\beta}} = (\alpha^{x})^{\beta^{x}},$$

for all $x, y \in X, \alpha, \beta \in Y$.

Proof. Note first that the hypothesis of Theorem 4.13 is satisfied, so (Z, r) obeys YBE *iff* **ml1, mr1**,**ml1a**,**mr1a**, where we use our original notions for $Z = X \sqcup Y$. As a strong twisted union (Z, r) satisfies **ml1, mr1**. Now we interprete condition **ml1a**:

$$ {}^{\alpha}({}^{y}x) = {}^{{}^{\alpha}y}({}^{\alpha^{y}}x) =^{\textbf{stu}} {}^{{}^{\alpha}y}({}^{\alpha}x), \tag{5.1}$$

Apply **stu** again to yield

$${}^{\alpha}({}^{y}x) = {}^{{}^{y}\alpha}({}^{y}x),$$

which together with (5.1) gives **ml1a** $\Longleftrightarrow$ **csla**. One similarly finds **mr1a** $\Longleftrightarrow$ **csra** under our hypotheses. □

Remark 5.5. Under the hypothesis of Proposition 5.4 suppose (X, r_X) and (Y, r_Y) are symmetric sets. Then

(1) (Z, r) is nondegenerate, involutive and the cyclic conditions hold.
(2) (Z, r) is a solution of YBE *iff* (Z, r) is a cycle set, i.e. conditions **csl, csr** hold. In this case (Z, r) is a symmetric set.

This follows immediately from Proposition 2.24 on noting that the involutiveness of (X, r_X) and (Y, r_Y) imply (Z, r) involutive while **lri** holds by assumption.

Proposition 5.6. *Let (Z, r) be a regular extension of two trivial solutions (X, r_X), (Y, r_Y). Suppose the monoid $U = S(Z, r)$ is with cancellation on monomials of length 3. Then (Z, r) obeys YBE* iff *it is a strong twisted union of $(X, r_X), (Y, r_Y)$.*

Proof. More generally, under the hypothesis of Theorem 4.13, suppose (Z, r) is a regular extension of the involutive solutions $(X, r_X), (Y, r_Y)$. Suppose furthermore that (X, r_X) is a trivial solution, i.e. $r_X(xy) = yx$ for all $x, y \in X$. This gives ${}^{x}y = y$, for all $x, y \in X$, thus an easy computation shows

$$\textbf{ml1a} \Longleftrightarrow {}^{\alpha^{x}}y = {}^{\alpha}y, \qquad \textbf{mr1} \Longleftrightarrow (\alpha^{x})^{y} = (\alpha^{y})^{x} \tag{5.2}$$

for all $x, y \in X, \alpha \in Y$. Analogously, in the case when (Y, r_Y) is a trivial solution one has

$$\textbf{mr1a} \Longleftrightarrow \alpha^{{}^{\beta}x} = \alpha^x \qquad \textbf{ml1} \Longleftrightarrow {}^{\alpha}({}^{\beta}x) = {}^{\beta}({}^{\alpha}x). \tag{5.3}$$

Assume now both $(X, r_X), (Y, r_Y)$ are trivial solutions. Clearly the hypothesis of Theorem 4.13 is satisfied so (5.2), (5.3) are in force. This yields

$$\textbf{ml1a}, \textbf{mr1a} \Longleftrightarrow \textbf{stu},$$

and

$$\textbf{ml1}, \textbf{mr1} \Longleftrightarrow \text{part (1) of Definition 5.1},$$

which completes the proof. □

Given a quadratic set (X, r_X), the set of *r_X-fixed pairs* is $\{x, y \in X \mid r_X(xy) = xy\}$. We have seen in section 2 that in the case of involutive nondegenerate solutions there is a close relation between the set of r_X-fixed pairs and 2-cancellativeness, see Lemma 2.12 and Corollary 2.13. We will show now that for involutive nondegenerate solutions (X, r_X), and (Y, r_Y), the conditions **ml2, mr2** can be interpreted in terms of the r_X and r_Y-fixed pairs. This is especially useful in the case of square free solutions, where the set of r_X-fixed pairs is exactly the diagonal, $diag X \times X$.

Lemma 5.7. *In the notation of Theorem 4.15, suppose (X, r_X) and (Y, r_Y) are involutive solutions, and S, T is a matched pair of monoids. Let (Z, r) be the associated regular extension. Then*

(*i*) $\textbf{ml2} \Longleftrightarrow [r_X(xy) = xy \Longrightarrow r_X({}^{\alpha}xy) = {}^{\alpha}xy,$ *for all* $x, y \in X, \alpha \in Y]$.

(*ii*) $\textbf{mr2} \Longleftrightarrow [r_Y(\alpha\beta) = \alpha\beta \Longrightarrow r_Y((\alpha\beta)^x) = (\alpha\beta)^x,$ *for all* $x \in X, \alpha, \beta \in Y]$.

Proof. It is clear that when r_X is involutive condition **ml2w** implies that for every $x, y \in X, \alpha \in Y$ one of the following is an equality of words, either

$$ {}^{\alpha}(r_X(xy)) = r_X({}^{\alpha}(xy)) \quad \text{holds in } X^2; \tag{5.4}$$

or

$$ {}^{\alpha}(r_X(xy)) = {}^{\alpha}(xy) \quad \text{holds in } X^2. \tag{5.5}$$

Assume now (5.5) holds. Then the equalities

$${}^{\alpha}(r_X(xy)) = {}^{\alpha}({}^{x}y.x^{y}) = {}^{\alpha}({}^{x}y).{}^{\alpha^{({}^{x}y)}}(x^{y})$$

and (5.5) imply

$${}^{\alpha}(xy) = {}^{\alpha}x.{}^{\alpha^{x}}y) = {}^{\alpha}({}^{x}y).{}^{\alpha^{({}^{x}y)}}(x^{y}) \quad \text{in } X^2.$$

Therefore

$${}^{\alpha}x = {}^{\alpha}({}^{x}y),$$

which by the nondegeneracy implies $x = {}^{x}y$. This by Lemma 2.12, is equivalent to $r(x, y) = (x, y)$, i.e. (x, y) is an r_X fixed pair. Clearly for a r_X-fixed pair (x, y) (5.4) holds *iff* $r_X({}^{\alpha}(xy)) = {}^{\alpha}(xy)$. This proves (i). Analogous argument proves (ii). □

Proposition 5.8. *Let $(X, r_X), (Y, r_Y)$ be non-degenerate involutive disjoint solutions with YB-monoids $S = S(X, r_X)$, $T = S(Y, r_Y)$. Suppose (S, T) is a strong matched pair, and let (Z, r), be the associated regular extension. Then*

(1) *r obeys YBE* iff

$$^{x}y = x \Longrightarrow {}^{\alpha}x({}^{\alpha^x}y) = {}^{\alpha}x, \qquad \alpha^{\beta} = \beta \Longrightarrow (\alpha^{{}^{\beta}x})^{\beta^x} = \beta^x, \quad \text{for all } x, y \in X, \alpha, \beta \in Y.$$

(2) *Suppose that both* $(X, r_X), (Y, r_Y)$ *are square free. Then r obeys YBE* iff *the following "mixed" weak cyclic conditions hold:*

$$^{\alpha^x}x = {}^{\alpha}x, \ \ \textit{and} \ \ \alpha^{{}^{\alpha}x} = \alpha^x, \ \ \textit{for all} \ x \in X, \alpha \in Y.$$

In this case (Z, r) *is also square-free and satisfies* **lri**.

Proof. We give sketch of the proof. To verify (1) one uses Lemma 2.12 again and interpretes the implications in Lemma 5.7 in terms of the left and the right actions.

Assume now (X, r_X) and (Y, r_Y) are square-free. Then, (x, y) is an r_X fixed point iff $y = x$, similarly, $(\alpha\beta)$ is an r_Y fixed point iff $\alpha = \beta$, (see Lemma 2.43).

Next we replace $y = x$, $\alpha = \beta$ in (1) and obtain the implications in (2). □

We now give various examples of extensions (Z, r) of a fixed pair of solutions $(X, r_X), (Y, r_Y)$. All solutions are involutive, non-degenerate, square-free, with **lri**. In this case $\mathcal{R}_z = \mathcal{L}_z^{-1}$ for all $z \in Z$. We find the extensions applying effectively Theorem 4.15 and our theory about the behaviour of finite square-free solutions (rather than by computer).

Example 5.9. Let $X = \{x_1, x_2, x_3, x_4; y_1, y_2, y_3, y_4; z_1, z_2, z_3, z_4\}$ Let ρ, σ, τ be the following cycles of length 4 in $Sym(X)$

$$\rho = (x_1, x_2, x_3, x_4), \quad \sigma = (y_1, y_2, y_3, y_4), \quad \tau = (z_1, z_2, z_3, z_4)$$

Define the involutive map $r_X : X^2 \longrightarrow X^2$ as:

$$\begin{array}{llll}
r_X(x_iy_j) = \sigma(y_j)\rho^{-1}(x_i), & r_X(x_iz_j) = \tau(z_j)\rho^{-1}(x_i), & & r_X(y_ix_j) = \rho(x_j)\sigma^{-1}(y_i), \\
r_X(y_iz_j) = \tau^{-1}(z_j)\rho^{-1}(y_i), & r_X(z_ix_j) = \rho(x_j)\tau^{-1}(z_i), & & r_X(z_iy_j) = \rho(y_j)\tau(z_i) \\
r_X(x_1x_2) = x_4x_3, & r_X(x_1x_4) = x_2x_3, & r_X(x_3x_2) = x_4x_1, & r_X(x_3x_4) = x_2x_1, \\
r_X(y_1y_2) = y_4y_3, & r_X(y_1y_4) = y_2y_3, & r_X(y_3y_2) = y_4y_1, & r_X(y_3y_4) = y_2y_1, \\
r_X(z_1z_2) = z_4z_3, & r_X(z_1z_4) = z_2z_3, & r_X(z_3z_2) = z_4z_1, & r_X(z_3z_4) = z_2z_1, \\
r_X(x_1x_3) = x_3x_1, & r_X(x_2x_4) = x_4x_2, & r_X(y_1y_3) = y_3y_1, & r_X(y_2y_4) = y_4y_2, \\
 & r_X(z_1z_3) = z_3z_1, & r_X(z_2z_4) = z_4z_2. &
\end{array}$$

For the left action on X we have:

$$\begin{array}{ll}
\mathcal{L}_{x_1} = \mathcal{L}_{x_3} = \sigma \circ \tau \circ (x_2x_4) & \mathcal{L}_{x_2} = \mathcal{L}_{x_4} = \sigma \circ \tau \circ (x_1x_3); \\
\mathcal{L}_{y_1} = \mathcal{L}_{y_3} = \rho \circ \tau^{-1} \circ (y_2y_4) & \mathcal{L}_{y_2} = \mathcal{L}_{y_4} = \rho \circ \tau^{-1} \circ (y_1y_3) \\
\mathcal{L}_{z_1} = \mathcal{L}_{z_3} = \rho \circ \sigma \circ (z_2z_4) & \mathcal{L}_{z_2} = \mathcal{L}_{z_4} = \rho \circ \sigma \circ (z_1z_3).
\end{array}$$

The second solution (Y, r_Y) is simpler. Let $Y = \{\alpha_1, \alpha_2, \alpha_3; \beta_1, \beta_2, \beta_3\}$. Take the cycles $f = (\alpha_1, \alpha_2, \alpha_3), g = (\beta_1, \beta_2, \beta_3)$ in $Sym(Y)$ and define $r_Y : Y^2 \longrightarrow Y^2$ as

$$\begin{array}{ll}
r_Y(\alpha_i\beta_j) = g(\beta_j)f^{-1}(\alpha_i), & r_Y(\beta_j\alpha_i) = f(\alpha_i)g^{-1}(\beta_j) \\
r_Y(\alpha_i\alpha_j) = \alpha_j\alpha_i, & r_Y(\beta_i\beta_j) = \beta_j\beta_i,
\end{array}$$

for all $i, j, 1 \leq i, j \leq 3$. The left actions on Y are: $\mathcal{L}_{\beta_i} = f, \mathcal{L}_{\alpha_i} = g$, for all $1 \leq i \leq 3$.

These initial data are shown in Figure 4. The definition of the graph is given after the examples. We omit most of the labels on the arrows in order not to clutter the diagram. We present several examples of YB extension (Z, r) of X, Y with $Z = X \sqcup Y$.

Note that all (Z, r) are square free, as extensions of square-free solutions, therefore we can apply the combinatorics developed in [8]. In particular **cc** is in force for (Z, r). Clearly, $\mathbf{x} = \{x_1, x_2, x_3, x_4\}$ and $\mathbf{y} = \{y_1, y_2, y_3, y_4\}, \mathbf{z} = \{z_1, z_2, z_3, z_4\}$ are

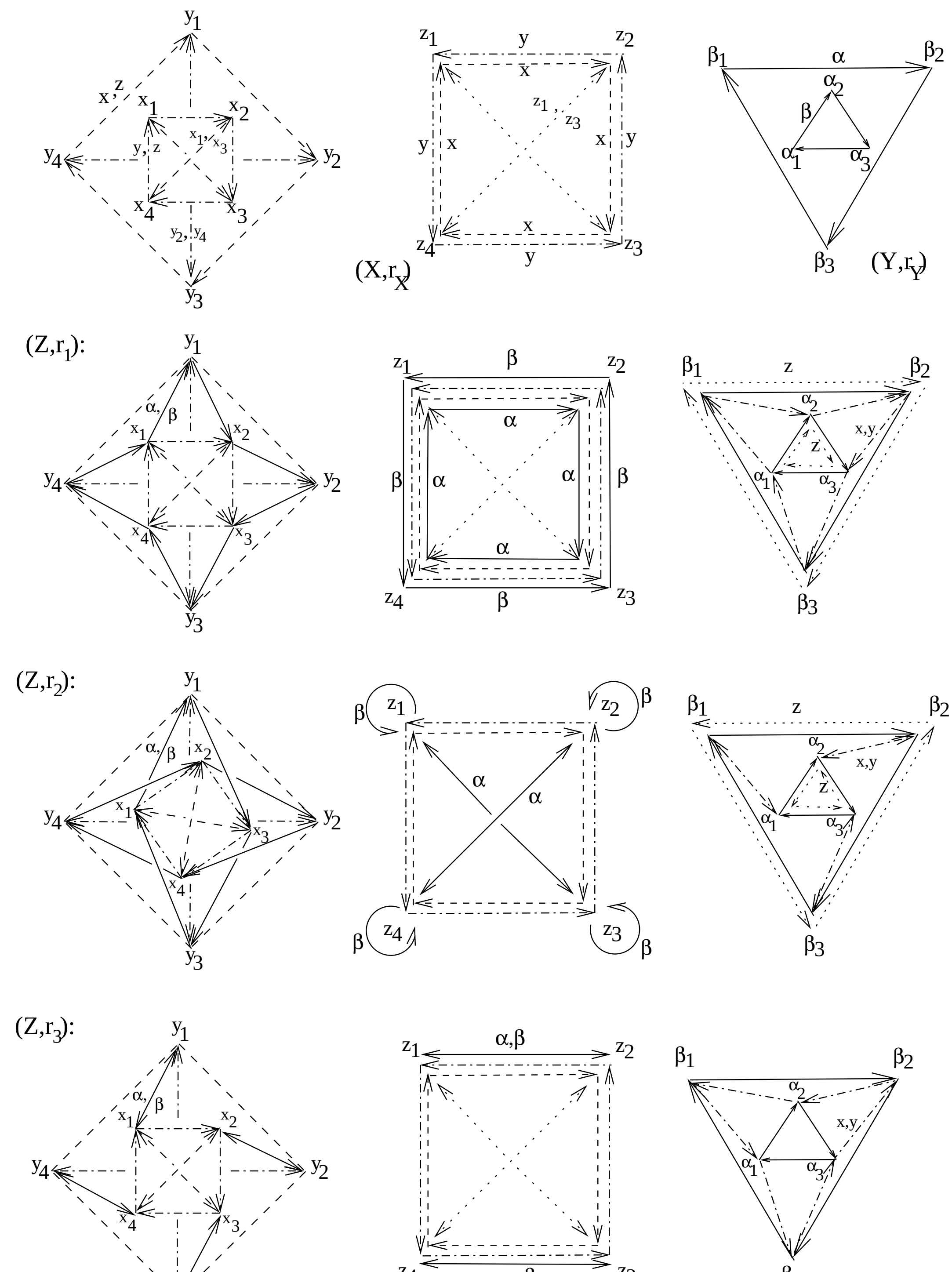

FIGURE 4. Example 5.9 of extensions (Z, r)

the orbits of X under the action of $G(X, r_X)$, and $\alpha = \{\alpha_1, \alpha_2, \alpha_3\}, \beta = \{\beta_1, \beta_2, \beta_3\}$ are the orbits of Y, under the action of $G(Y, r_Y)$,. Each orbit in X is r_X invariant subsets, so we have to bear in mind also "mini-extensions" of pairs like $(\mathbf{x}, Y)$, $(\mathbf{y}, Y)$, $(\mathbf{z}, Y)$, $(\mathbf{x} \sqcup \mathbf{y}, Y)$ etc. One can show that with this initial data, it is impossible to have extension (Z, r) in which some x_i, y_j, z_k belong to the same orbit.

We are interested in cases when the left action of Y onto X provides "links" between the two orbits $\mathbf{x}, \mathbf{y}$. So we need extensions for the pairs $\mathbf{x} \sqcup \mathbf{y}, Y$ and for $\mathbf{z}, Y$, which are compatible. We shall write $r(\alpha\mathbf{x}) = \mathbf{y}\beta$,(respectively $r(\alpha\mathbf{x}) = \mathbf{y}\alpha$ to indicate that

$$r(\alpha_i x_p) = y_q\beta_j \text{ (resp. } r(\alpha_i x_p) = y_q\alpha_j \text{ for some } 1 \leq i, j \leq 3, 1 \leq p, q \leq 4. \tag{5.6}$$

More detailed study shows what kind of pairs $(p, q), 1 \leq p, q \leq 4$ are admissible with the structure of (X, r_X). For this particular Y every pair $(i, j), 1 \leq i, j \leq 3$ is admissible. Note that no restriction on compatibility between the two pairs (i, j) and (p, q) are necessary. There are two types of extensions which connect $\mathbf{x}, \mathbf{y}$, in one orbit, these are **A:** $r(\alpha\mathbf{x}) = \mathbf{y}\beta$; and **B:** $r(\alpha\mathbf{x}) = \mathbf{y}\alpha$. The admissible actions of Y on $\mathbf{z}$ depend only on the general type **A**, or **B**, and do not depend on the particular pairs of indices p, q, α, β, occurring in (5.6). Furthermore, for simplicity we consider the case $\mathcal{L}_{\beta|\mathbf{x}\sqcup\mathbf{y}} = \mathcal{L}_{\alpha|\mathbf{x}\sqcup\mathbf{y}}$, for all α and β. We shall discuss only case **A**. Clearly, under these assumptions Y does not act as automorphisms on X iff $\mathcal{L}_{\alpha|\mathbf{z}} \neq \mathcal{L}_{\beta|\mathbf{z}}$. We start with a list of the left actions of Y onto $\mathbf{x} \sqcup \mathbf{y}$, satisfying **A** and producing solutions r. Assume

$$\mathcal{L}_{\beta|\mathbf{x}\sqcup\mathbf{y}} = \mathcal{L}_{\alpha|\mathbf{x}\sqcup\mathbf{y}}.$$

Three subcases are possible.

A1. The set $\mathbf{x}\sqcup\mathbf{y}$ becomes a cycle of length 8. Denote $\theta = (x_1y_1x_2y_2x_3y_3x_4y_4) \in Sym(\mathbf{x} \sqcup \mathbf{y})$. The admissible actions in this subcase are:
(5.7)

$$\textbf{(i)} \quad \mathcal{L}_{\alpha|\mathbf{x}\sqcup\mathbf{y}} = \theta; \quad \textbf{(ii)} \quad \mathcal{L}_{\alpha|\mathbf{x}\sqcup\mathbf{y}} = \theta^3; \quad \textbf{(iii)} \quad \mathcal{L}_{\alpha|\mathbf{x}\sqcup\mathbf{y}} = \theta^5; \quad \textbf{(iv)} \quad \mathcal{L}_{\alpha|\mathbf{x}\sqcup\mathbf{y}} = \theta^7.$$

A2. $(\mathbf{x}\sqcup\mathbf{y})$ splits into two disjoint cycles of length 4. Only two cases are admissible.
(5.8)

$$\textbf{(i)}\mathcal{L}_{\alpha|\mathbf{x}\sqcup\mathbf{y}} = (x_1y_1x_3y_3)(x_2y_2x_4y_4) = \vartheta; \quad \textbf{(ii)}\mathcal{L}_{\alpha|\mathbf{x}\sqcup\mathbf{y}} = (y_3x_3y_1x_1)(y_4x_4y_2x_2) = \vartheta^{-1}.$$

A3. X_0 splits into four disjoint cycles of length 2. There are three admissible actions.

$$\mathcal{L}_{\alpha|\mathbf{x}\sqcup\mathbf{y}} = (x_1\sigma^i(y_1))(x_2\sigma^i(y_2))(x_3\sigma^i(y_3))(x_4\sigma^i(y_4)),\ 1 \leq i \leq 3. \tag{5.9}$$

To determine the left actions of Y on X completely, we need to know admissible actions $\mathcal{L}_{\alpha|\mathbf{z}}$ and $\mathcal{L}_{\beta|\mathbf{z}}$. One can verify that $\mathcal{L}_{\alpha|\mathbf{z}}$ determines uniquely $\mathcal{L}_{\beta|\mathbf{z}}$. In four cases $\mathcal{L}_\alpha \neq \mathcal{L}_\beta$, see $(\mathbf{a}), (\mathbf{b}), (\mathbf{g}), (\mathbf{h})$, each of which produces solutions (Z, r) with $G(Z, r)$ acting on Z not as automorphisms. We give now the list of admissible actions of Y on z, which agree with the initial data, and the assumption **A**. (Note that in case B, the list of admissible actions of Y on z, is different.)
(5.10)

(a)	$\mathcal{L}_{\alpha\|\mathbf{z}} = \tau, \mathcal{L}_{\beta\|\mathbf{z}} = \tau^{-1};$	**(b)**	$\mathcal{L}_{\alpha\|\mathbf{z}} = \tau^{-1}, \mathcal{L}_{\beta\|\mathbf{z}} = \tau;$
(c)	$\mathcal{L}_{\alpha\|\mathbf{z}} = \mathcal{L}_{\beta\|\mathbf{z}} = (z_1z_2)(z_3z_4);$	**(d)**	$\mathcal{L}_{\alpha\|\mathbf{z}} = \mathcal{L}_{\beta\|\mathbf{z}} = (z_1z_4)(z_2z_3);$
(e)	$\mathcal{L}_{\alpha\|\mathbf{z}} = \mathcal{L}_{\beta\|\mathbf{z}} = (z_1z_3);$	**(f)**	$\mathcal{L}_{\alpha\|\mathbf{z}} = \mathcal{L}_{\beta\|\mathbf{z}} = (z_2z_4);$
(g)	$\mathcal{L}_{\alpha\|\mathbf{z}} = (z_1z_3)(z_2z_4); \mathcal{L}_{\beta\|\mathbf{z}} = \mathrm{id}_{\mathbf{z}};$	**(h)**	$\mathcal{L}_{\alpha\|\mathbf{z}} = id_{\mathbf{z}}; \mathcal{L}_{\beta\|\mathbf{z}} = (z_1z_3)(z_2z_4).$

We now have a list of admissible actions of Y on X that are compatible with r obeying the YBE; it remains to present similarly admissible actions of X on Y. We give next two types of actions of $\mathbf{x}\sqcup\mathbf{y}$ upon Y which are admissible with the list of actions already specified above. (This is not a complete list of admissible choices). Each of the actions below glues Y in one orbit:

$$\mathcal{L}_{x_j|Y} = \mathcal{L}_{y_j|Y} = \pi^q, \quad \text{where}, \quad \pi = (\alpha_1\beta_1\alpha_2\beta_2\alpha_3\beta_3), \quad q = 1, 3, 5, \tag{5.11}$$

and

$$\mathcal{L}_{x_j|Y} = \mathcal{L}_{y_j|Y} = (\alpha_1 g^k(\beta_1)) \circ (\alpha_2 g^k(\beta_2)) \circ (\alpha_3 g^k(\beta_3)), \quad 0 \leq k \leq 2. \tag{5.12}$$

As a final step we determine the admissible actions of $\mathbf{z}$ on Y. The choice is limited:

$$\mathcal{L}_{z_j|Y} = (f\circ g)^k, \quad 0 \leq k \leq 2. \tag{5.13}$$

Note that to make a list of what we call *admissible actions* is enough to verify conditions **ml1, ml1a**. We leave as an exercise to the reader to check that any 4tiple of actions

$$\mathcal{L}_{\alpha|\mathbf{x}\sqcup\mathbf{y}} \circ \mathcal{L}_{\alpha|\mathbf{z}}, \quad \mathcal{L}_{\beta|\mathbf{x}\sqcup\mathbf{y}} \circ \mathcal{L}_{\beta|\mathbf{z}}, \quad \mathcal{L}_{x|Y} = \mathcal{L}_{y|Y}, \quad \mathcal{L}_{z|Y}$$

chosen from the lists (5.7)–(5.9), (5.10), (5.11)–(5.12), and (5.13), respectively, satisfies **ml1, ml1a**, and therefore defines a solution (Z,r). Note that different triples can produce isomorphic extensions.

In all cases the left action of the group $G(Z,r)$ splits Z into three orbits, i.e. 3 invariant subsets, namely $O_1 = \mathbf{x}\sqcup\mathbf{y}, O_2 = \mathbf{z}, O_3 = Y$. We now give three concrete extensions, with graphs presented in Figure 4.

1) (Z, r_1) is determined by the actions

$$\mathcal{L}_{\alpha_i|X} = (x_1y_1x_2y_2x_3y_3x_4y_4)\circ\tau, \quad \mathcal{L}_{\beta_i|X} = (x_1y_1x_2y_2x_3y_3x_4y_4)\circ\tau^{-1},$$
$$\mathcal{L}_{x_j|Y} = \mathcal{L}_{y_j|Y} = (\alpha_1\beta_1\alpha_2\beta_2\alpha_3\beta_3),\ \mathcal{L}_{z_j|Y} = f\circ g \quad ,$$

for all $1 \leq i \leq 3, 1 \leq j \leq 4$.

2) (Z, r_2) is determined by the actions

$$\mathcal{L}_{\alpha_i|X} = (x_1y_1x_3y_3)\circ(x_2y_2x_4y_4)\circ(z_1z_3)(z_2z_4), \quad \mathcal{L}_{\beta_i|X} = (x_1y_1x_3y_3)\circ(x_2y_2x_4y_4)\circ\mathrm{id}_{\mathbf{z}},$$
$$\mathcal{L}_{x_j|Y} = \mathcal{L}_{y_j|Y} = (\alpha_1\beta_1)\circ(\alpha_2\beta_2)\circ(\alpha_3\beta_3), \quad \mathcal{L}_{z_j|Y} = (f\circ g)^2,$$

for all $1 \leq i \leq 3, 1 \leq j \leq 4$.

3) (Z, r_3) is determined by the actions

$$\mathcal{L}_{\alpha_i|X} = \mathcal{L}_{\beta_i|X} = (x_1y_1)(x_2y_2)(x_3y_3)(x_4y_4)(z_1z_2)(z_3z_4),$$
$$\mathcal{L}_{x_j|Y} = \mathcal{L}_{y_j|Y} = (\beta_3\alpha_3\beta_2\alpha_2\beta_1\alpha_1), \quad \mathcal{L}_{z_j|Y} = \mathrm{id}_Y,$$

for all $1 \leq i \leq 3, 1 \leq j \leq 4$.

We make some comments on the solutions and their graphs. For arbitrary solution (X,r) with **lri**, we define the graph $\Gamma = \Gamma(X,r)$ as follows. It is an oriented graph, which reflects the left action of $G(X,r)$ on X. The set of vertices of Γ is exactly X. There is a labelled arrow $x\stackrel{z}{\longrightarrow}y$, if $x,y,z \in X, x \neq y$ and ${}^zx = y$. Clearly $x\stackrel{z}{\longleftrightarrow}y$ indicates that ${}^zx = y$ and ${}^zy = x$. (One can make such graph for arbitrary solutions but then it should be indicated which action is considered). The graphs $\Gamma(X,r_X), \Gamma(Y,r_Y)$, and $\Gamma(Z,r)$ for the above three extensions are presented in Figure 4. To avoid clutter we typically omit self-loops unless needed for clarity or contrast (for example $\Gamma(Z,r_2)$ shows these explicitly to indicate ${}^{\beta}z_i = z_i$). Also for the same reason, we use the line type to indicate when the same type of element acts, rather than labelling every arrow.

Moreover, these extensions are non-isomorphic. This can be read directly from the choice of the actions, but also from the graphs $\Gamma(Y, r_i)$. Note that two solutions are isomorphic if and only if their oriented graphs are isomorphic.

In the cases **1)**, and **2)** $G(Y, r_Y)$ does not act as automorphisms on X. For (Z, r_1) this follows from the

$$^{\alpha_k}(x_i z_j) = {}^{\alpha_k}x_i{}^{\alpha_k{}^{x_i}}z_j = {}^{\alpha_k}x_i{}^{\beta_{k-1}}z_j = y_j z_{j-1} \neq {}^{\alpha_k}x_i{}^{\alpha_k}z_j = y_j z_{j+1}.$$

In the second case it is also easy to verify that $^{\alpha_k}(x_i z_j) \neq {}^{\alpha_k}x_i{}^{\alpha_k}z_j$. In all cases the group $G(X, r_x)$ acts as automorphisms on Y. In case **3)** $G(Z, r_3)$ acts as automorphisms on Z.

Acknowledgments. The first author thanks The Abdus Salam International Centre for Theoretical Physics, where she worked on the paper in the summers of 2004 and 2005. It is her pleasant duty to thank Professor Le Dung Trang and the Mathematics group of ICTP for the inspiring and creative atmosphere during her visits. Thanks also to QMUL for partial support during her two visits there.

References

[1] V. G. Drinfeld, *On some unsolved problems in quantum group theory*, Quantum Groups (P. P. Kulish, ed.), Lecture Notes in Mathematics, vol. 1510, Springer Verlag, 1992, pp. 1–8.
[2] P. Etingof, T. Schedler, A. Soloviev *Set-theoretical solutions to the quantum Yang-Baxter equation*, Duke Math. J. **100** (1999) 169–209.
[3] 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.
[4] T. Gateva-Ivanova, *Noetherian properties of skew polynomial rings with binomial relations*, Trans.Amer.Math.Soc. **343** (1994), 203–219.
[5] T. Gateva-Ivanova, *Skew polynomial rings with binomial relations*, J. Algebra **185** (1996) 710–753.
[6] T. Gateva-Ivanova, *Regularity of the skew polynomial rings with binomial relations*, preprint (1996).
[7] T. Gateva-Ivanova, *Set-theoretic solutions of the Yang-Baxter equation*, Math. and Education in Math. **29** (2000) 107–117.
[8] T. Gateva-Ivanova, *A combinatorial approach to the set-theoretic solutions of the Yang-Baxter equation*, J. Math. Phys. **45** (2004) 3828–3858.
[9] T. Gateva-Ivanova, *Quantum binomial algebras, Artin-Schelter regular rings, and solutions of the Yang-Baxter equations*, Serdica Math. J. 30 (2004), 431–470.
[10] T. Gateva-Ivanova and M. Van den Bergh, *Semigroups of I-type*, J. Algebra **206** (1998) 97–112.
[11] T. Gateva-Ivanova, E.Jespers, and J. Okninski *Quadratic algebras of skew polynomial type and the inderlying semigroups*, J.Algebra **270** (2003) 635–659.
[12] T. Gateva-Ivanova, S. Majid, *Computations in the algebraic structures related to set-theoretic solutions of the Yang-Baxter equation*, preprint 2006.
[13] J. Hietarinta, *Permutation-type solution to the Yang-Baxter and other n-simplex equations*, J.Phys. A **30** (1997) 4757–4771.
[14] E. Jespers and J. Okninski, *Binomial Semigroups*, J. Algebra **202** (1998) 250–275. .
[15] G.I. Kac and V.G. Paljutkin *Finite ring groups*, Trans. Amer. Math. Soc. **15** (1966) 251294.
[16] G. Laffaille, *Quantum binomial algebras*, Colloquium on Homology and Representation Theory (Spanish) (Vaquerías, 1998). Bol. Acad. Nac. Cienc. (Córdoba) **65** (2000), 177–182.
[17] J. Lu, M. Yan, Y. Zhu *On the set-theoretical Yang-Baxter equation*, Duke Math. J. **104** (2000) 1-18.
[18] K. Mackenzie. Double Lie algebroids and second-order geometry, I. *Adv. Math.* **94** (1992) 180–239.
[19] S. Majid. Matched pairs of Lie groups associated to solutions of the Yang-Baxter equations. *Pac. J. Math.*, **141** (1990) 311–332.

[20] S. Majid. Physics for algebraists: Non-commutative and non-cocommutative Hopf algebras by a bicrossproduct construction. *J. Algebra* **130** (1990) 17–64.

[21] S. Majid. More examples of bicrossproduct and double cross product Hopf algebras. *Isr. J. Math* **72** (1990) 133–148.

[22] S. Majid, *Foundations of the Quantum Groups*, Cambridge University Press, 1995.

[23] N.Yu. Reshetikhin, L.A. Takhtadzhyan, L.D. Faddeev *Quantization of Lie groups and Lie algebras* (in Russian) , Algebra i Analiz **1** (1989), pp. 178–206; English translation in Leningrad Math.J. **1** (1990), pp. 193–225.

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

[25] M. Takeuchi *Matched pairs of groups and bismash products of Hopf algebras*, Commun. Alg., **9** (1981) 841.

[26] M. Takeuchi *Survey on matched pairs of groups. An elementary approach to the ESS-LYZ theory*, Banach Center Publ. **61** (2003) 305–331.

[27] A. Weinstein and P. Xu *Classical solutions of the quantum Yang-Baxter equation*, Comm. Math. Phys. **148** (1992), pp. 309–343.

TGI: Institute of Mathematics and Informatics, Bulgarian Academy of Sciences, Sofia 1113, Bulgaria, S.M: Queen Mary, University of London, School of Mathematics, Mile End Rd, London E1 4NS, UK

E-mail address: tatianagateva@yahoo.com, tatyana@aubg.bg, s.majid@qmul.ac.uk