Braided Groups, Braces, and the Yang-Baxter equation

Tatiana Gateva-Ivanova
IMI BAS & American University in Bulgaria

LA FIESTA de la YBE:
"Groups, Rings and the Yang-Baxter Equation"
Spa, Belgium, June 18 - 24, 2017
YBE and set-theoretic YBE

Let $V$ be a vector space over a field $k$, $R$ be a linear automorphism of $V \otimes V$. $R$ is a solution of YBE if

$$R^{12} R^{23} R^{12} = R^{23} R^{12} R^{23}$$

holds in $V \otimes V \otimes V$, $R^{12} = R \otimes \text{id}_V$, $R^{23} = \text{id}_V \otimes R$. 
YBE and set-theoretic YBE

Let \( V \) be a vector space over a field \( k \), \( R \) be a linear automorphism of \( V \otimes V \). \( R \) is a solution of YBE if

\[
R^{12} R^{23} R^{12} = R^{23} R^{12} R^{23}
\]

holds in \( V \otimes V \otimes V \), \( R^{12} = R \otimes id_V, R^{23} = id_V \otimes R \).

Let \( X \neq \emptyset \) be a set. A bijective map \( r : X \times X \rightarrow X \times X \) is a set-theoretic solution of YBE, if the braid relation

\[
r^{12} r^{23} r^{12} = r^{23} r^{12} r^{23}
\]

holds in \( X \times X \times X \), \( r^{12} = r \times id_X, r^{23} = id_X \times r \). In this case \((X, r)\) is called a braided set.
YBE and set-theoretic YBE

Let $V$ be a vector space over a field $k$, $R$ be a linear automorphism of $V \otimes V$. $R$ is a solution of YBE if

\[ R^{12}R^{23}R^{12} = R^{23}R^{12}R^{23} \]

holds in $V \otimes V \otimes V$, $R^{12} = R \otimes id_V, R^{23} = id_V \otimes R$.

Let $X \neq \emptyset$ be a set. A bijective map $r : X \times X \rightarrow X \times X$ is a set-theoretic solution of YBE, if the braid relation

\[ r^{12}r^{23}r^{12} = r^{23}r^{12}r^{23} \]

holds in $X \times X \times X$, $r^{12} = r \times id_X, r^{23} = id_X \times r$. In this case $(X, r)$ is called a braided set.

A braided set $(X, r)$ with $r$ involutive is called a symmetric set.
YBE and set-theoretic YBE

Let $V$ be a vector space over a field $k$, $R$ be a linear automorphism of $V \otimes V$. $R$ is a solution of YBE if

$$ R^{12} R^{23} R^{12} = R^{23} R^{12} R^{23} $$

holds in $V \otimes V \otimes V$, $R^{12} = R \otimes id_V, R^{23} = id_V \otimes R$.

Let $X \neq \emptyset$ be a set. A bijective map $r : X \times X \rightarrow X \times X$ is a set-theoretic solution of YBE, if the braid relation

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

holds in $X \times X \times X$, $r^{12} = r \times id_X, r^{23} = id_X \times r$. In this case $(X, r)$ is called a braided set.

A braided set $(X, r)$ with $r$ involutive is called a symmetric set.

In this talk "a solution" means "a nondegenerate symmetric set".
**YBE and set-theoretic YBE**

Let $V$ be a vector space over a field $k$, $R$ be a linear automorphism of $V \otimes V$. $R$ is a solution of YBE if

$$R^{12} R^{23} R^{12} = R^{23} R^{12} R^{23}$$

holds in $V \otimes V \otimes V$, $R^{12} = R \otimes id_V, R^{23} = id_V \otimes R$.

Let $X \neq \emptyset$ be a set. A bijective map $r : X \times X \rightarrow X \times X$ is a set-theoretic solution of YBE, if the braid relation

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

holds in $X \times X \times X$, $r^{12} = r \times id_X, r^{23} = id_X \times r$. In this case $(X, r)$ is called a braided set.

A braided set $(X, r)$ with $r$ involutive is called a symmetric set.

In this talk "a solution" means "a nondegenerate symmetric set".

Each set-theoretic solution of YBE induces naturally a solution to the YBE and QYBE.
Set theoretic solutions extend to special linear solutions but also lead to

- a great deal of combinatorics - group action on $X$, cyclic conditions,
- matched pairs of groups, matched pairs of semigroups
- semigroups of I type with a structure of distributive lattice
- special graphs
- algebras with very nice algebraic and homological properties such as being:
  - Artin-Schelter regular algebras; Koszul; Noetherian domains with PBW $k$-bases;
  - with good computational properties - the theory of noncommutative Groebner bases is applicable.
(Gl, AIM 12') Theorem 1. Let $A = k \langle X \rangle / (\mathcal{R})$ be a quantum binomial algebra, $|X| = n$. FAEQ:

- (1) $A$ is an Artin-Schelter regular PBW algebra.
Theorem 1. Let $A = k\langle X \rangle / (\mathcal{R})$ be a quantum binomial algebra, $|X| = n$. FAEQ:

- (1) $A$ is an Artin-Schelter regular PBW algebra.
- (2) $A$ is a Yang-Baxter algebra, that is the set of relations $\mathcal{R}$ defines canonically a solution of the Yang-Baxter equation.
Theorem 1. Let $A = k\langle X \rangle / (\mathcal{R})$ be a quantum binomial algebra, $|X| = n$. FAEQ:

- (1) $A$ is an Artin-Schelter regular PBW algebra.
- (2) $A$ is a Yang-Baxter algebra, that is the set of relations $\mathcal{R}$ defines canonically a solution of the Yang-Baxter equation.
- (3) $A$ is a binomial skew polynomial ring (in the sense of GI, 96), w.r.t. an enumeration of $X$. 
(GI, AIM 12′) **Theorem 1.** Let \( A = k\langle X \rangle / (\mathcal{R}) \) be a quantum binomial algebra, \(|X| = n\). FAEQ:

- (1) \( A \) is an Artin-Schelter regular PBW algebra.
- (2) \( A \) is a Yang-Baxter algebra, that is the set of relations \( \mathcal{R} \) defines canonically a solution of the Yang-Baxter equation.
- (3) \( A \) is a binomial skew polynomial ring (in the sense of GI, 96), w.r.t. an enumeration of \( X \).
- (4) The Hilbert series of \( A \) is

\[
H_A(z) = \frac{1}{(1 - z)^n}.
\]
A connected graded algebra $A$ is called *Artin-Schelter regular* (or *AS regular*) if:

- (i) $A$ has *finite global dimension* $d$, that is, each graded $A$-module has a free resolution of length at most $d$. 
A connected graded algebra $A$ is called *Artin-Schelter regular* (or *AS regular*) if:

- (i) $A$ has *finite global dimension* $d$, that is, each graded $A$-module has a free resolution of length at most $d$.
- (ii) $A$ has *finite Gelfand-Kirillov dimension*
A connected graded algebra $A$ is called Artin-Schelter regular (or AS regular) if:

1. $A$ has finite global dimension $d$, that is, each graded $A$-module has a free resolution of length at most $d$.
2. $A$ has finite Gelfand-Kirillov dimension
3. $A$ is Gorenstein, that is, $\text{Ext}^i_A(\mathbf{k}, A) = 0$ for $i \neq d$ and $\text{Ext}^d_A(\mathbf{k}, A) \cong \mathbf{k}$. 
A connected graded algebra $A$ is called *Artin-Schelter regular* (or *AS regular*) if:

- (i) $A$ has *finite global dimension* $d$, that is, each graded $A$-module has a free resolution of length at most $d$.
- (ii) $A$ has *finite Gelfand-Kirillov dimension*
- (iii) $A$ is *Gorenstein*, that is, $\text{Ext}^i_A(k, A) = 0$ for $i \neq d$ and $\text{Ext}^d_A(k, A) \cong k$.

AS regular algebras were introduced and studied first in 90’s. Since then AS regular algebras and their geometry have intensively been studied. When $d \leq 3$ all regular algebras are classified. (Some of them are not Yang-Baxter algebras).
A connected graded algebra $A$ is called *Artin-Schelter regular* (or *AS regular*) if:

1. $A$ has *finite global dimension* $d$, that is, each graded $A$-module has a free resolution of length at most $d$.
2. $A$ has *finite Gelfand-Kirillov dimension*.
3. $A$ is *Gorenstein*, that is, $\text{Ext}_A^i(k, A) = 0$ for $i \neq d$ and $\text{Ext}_A^d(k, A) \cong k$.

AS regular algebras were introduced and studied first in the 90’s. Since then AS regular algebras and their geometry have intensively been studied. When $d \leq 3$ all regular algebras are classified. (Some of them are not Yang-Baxter algebras).

The problem of classification of regular algebras seems to be difficult and remains open even for regular algebras of global dimension 5.
Def. (Gl, AIM 12) A quadratic algebra $A = k\langle X \rangle / (\mathcal{R})$ with binomial relations $\mathcal{R}$ is said to be a Q.B.A. if:

1. the set $\mathcal{R}$ satisfies
   \begin{align*}
   \text{B1} \quad \forall f \in \mathcal{R} & \text{ has the shape } f = xy - c_{yxx'y'}, \ c_{xy} \in k^\times, \\
   & x, y, x', y' \in X; \text{ and} \\
   \text{B2} \quad \forall xy \in X^2 & \text{ occurs at most once in } \mathcal{R}.
   \end{align*}

2. the associated quadratic set $(X, r)$ is quantum binomial, that is nondegenerate, square-free, and involutive (we do not assume it is a braided set!!).

Def. $A$ is an Yang-Baxter algebra (in the sense of Manin), if the associated map $R = R(\mathcal{R}) : V \otimes V \rightarrow V \otimes V$ is a solution of the YBE, $V = \text{Span}_k X$.

Lemma. (Gl) Every $n$-generated quantum binomial algebra has exactly $\binom{n}{2}$ relations.

Remark. Each binomial skew-polynomial ring $A$ is a PBW Q.B.A. The converse is not true! Make difference between my Q.B.A. and G. Lafaille’s QBA= Skew Poly Alg.
Quantum binomial algebras 2 (Reminder)

Let $V = \text{Span}_k X$, Given a set $\mathcal{R} \subset \mathbf{k}\langle X \rangle$ of quantum binomial relations, that is

**B1** $\forall f \in \mathcal{R}$ has the shape $f = xy - c_{yx}y'x'$, $c_{xy} \in \mathbf{k}^\times$, $x, y, x', y' \in X$ and

**B2** Each monomial $xy$ of length 2 occurs at most once in $\mathcal{R}$.

The associated quadratic set $(X, r)$ is defined as

$$r(x, y) = (y', x'), \; r(y', x') = (x, y) \text{ iff } xy - c_{xy}y'x' \in \mathcal{R}.$$  

$$r(x, y) = (x, y) \text{ iff } xy \text{ does not occur in } \mathcal{R}.$$  

The (involutive) automorphism $R = R(\mathcal{R}) : V^\otimes 2 \longrightarrow V^\otimes 2$ associated with $\mathcal{R}$ is defined analogously:

$$R(x \otimes y) = c_{xy}y' \otimes x', \; R(y' \otimes x') = (c_{xy})^{-1}x \otimes y \text{ iff } xy - c_{xy}y'x' \in \mathcal{R}.$$  

$$R(x \otimes y) = x \otimes y \text{ iff } xy \text{ does not occur in } \mathcal{R}.$$  

$R$ is called nondegenerate if $r$ is nondegenerate.
Thm 1 implies

- A classification of all *AS regular PBW algebras with quantum binomial relations and global dimension n* is equivalent to
Thm 1 implies

- A classification of all *AS regular PBW algebras with quantum binomial relations and global dimension* $n$ *is equivalent to*
- A classification of the Yang-Baxter $n$-generated QBA;
Thm 1 implies

- A classification of all AS regular PBW algebras with quantum binomial relations and global dimension $n$ is equivalent to
- A classification of the Yang-Baxter $n$-generated QBA;
- and is closely related (but not equivalent!) to the classification of square-free set-theor. sol of YBE, $(X, r)$, on sets $X$ of order $n$. 
Thm 1 implies

- A classification of all AS regular PBW algebras with quantum binomial relations and global dimension $n$ is equivalent to
- A classification of the Yang-Baxter $n$-generated QBA;
- and is closely related (but not equivalent!) to the classification of square-free set-theor. sol of YBE, $(X, r)$, on sets $X$ of order $n$.
- Even under these strong restrictions on the shape of the relations, the problem remains highly nontrivial. For $n \leq 8$ the square-free solutions of YBE $(X, r)$ are known (found by a computer programme). Moreover, numerous constructions of families of solutions were found.
Thm 1 implies

- A classification of all AS regular PBW algebras with quantum binomial relations and global dimension $n$ is equivalent to
- A classification of the Yang-Baxter $n$-generated QBA;
- and is closely related (but not equivalent!) to the classification of square-free set-theor. sol of YBE, $(X, r)$, on sets $X$ of order $n$.
- Even under these strong restrictions on the shape of the relations, the problem remains highly nontrivial. For $n \leq 8$ the square-free solutions of YBE $(X, r)$ are known (found by a computer programme). Moreover, numerous constructions of families of solutions were found.
- Already known: the solutions split into three large classes:
  (i) The multipermutation solutions of level $N \geq 0$; (ii) The irretractable solutions - these are "rigid" and do not retract;
  (iii) Solutions for which the recursive process of retraction stops before reaching one element;
Examples QBA- (1) "good" and (2) "bad"

- \( X = \{x, y, z, t\} \)
- (1) \( A_1 = k\langle X \rangle / (R_1) \) \( A_1 \) is "a good" QBA:
  \[
  R_1 = \{xy - \alpha zt, ty - \beta zx, xz - \gamma yt, tz - \delta yx, xt - atx, yz - bzy\}
  \]
  where \( \alpha, \beta, \gamma, \delta, a, b \in k^\times \)

  FAEQ (i) \( a^4 = 1, b^2 = a^2 \), no restrictions on the remaining (nonzero) coefficients; (ii) \( A_1 \) is a skew-poly ring (in the sense of GI); (iii) \( A_1 \) is a PBW Artin-Schelter regular algebra, (iv) \( A_1 \) is a Yang-Baxter algebra.

- (2) \( A_2 = k\langle X \rangle / (R_2) \) is "a bad" QBA:
  \[
  R_2 = \{xy - zt, ty - zx, xz - yx, tz - yt, xt - tx, yz - zy\}.
  \]

  \( A_2 \) is not an YB- algebra; \( R_2 \) is not a Groebner basis w.r. t. any order of \( X \) (A necessary condition: \textit{Cyclic condition is violated !!!}); hence \( A_2 \) is not an AS-regular algebra!
A quadratic set \((X, r)\)

is a nonempty set \(X\) with a bijective map \(r : X \times X \to X \times X\). The formula \(r(x, y) = (xy, xy)\) defines a "left action" \(L : X \times X \to X\), and a "right action" \(R : X \times X \to X\), on \(X\) as:

\[
L_x(y) = xy, \quad R_y(x) = yx 
\]

for all \(x, y \in X\).

- \(r\) is nondegenerate, if \(R_x\) and \(L_x\) are bijective \(\forall x \in X\), i.e. \(L_x, R_x \in \text{Sym}(X)\);
- \(r\) is square-free if \(r(x, x) = (x, x)\), for all \(x \in X\);
- \((X, r)\) is a quantum binomial set if it is nondegenerate, involutive and square-free.
- \((X, r)\) is a braided set if \(r^{12} r^{23} r^{12} = r^{23} r^{12} r^{23}\);
- A braided set \((X, r)\) with \(r\) involutive is called a symmetric set.
Associated algebraic objects to \((X, r)\)

These are generated by \(X\) and with quadratic defining relations \(\mathcal{R} = \mathcal{R}(r)\):

\[
xy = zt \in \mathcal{R} \iff r(x, y) = (z, t).
\]

- The group \(G = G(X, r) = \text{gr}\langle X; \mathcal{R}(r) \rangle\);
- The permutation group (of left action) \(G = G(X, r)\) defined as the subgroup \(L(G(X, r))\) of \(\text{Sym}(X)\).
- The groups \(G = G(X, r)\) and \(G(X, r)\) are braided groups with involutive braiding operators canonically induced by \((X, r)\).
- The monoid \(S = S(X, r) = \langle X; \mathcal{R}(r) \rangle\);
- The \(k\)-algebra \(A = A(k, X, r) = k\langle X; \mathcal{R}(r) \rangle \simeq kS\) where \(k\) is a field.
The retraction of a symmetric set \((X, r)\).

Define an equivalence relation \(\sim\) on \(X\):

\[
x \sim y \iff \mathcal{L}_x = \mathcal{L}_y.
\]

NB. This implies \(\mathcal{R}_x = \mathcal{R}_y\).

Denote by \([x]\) the equivalence class of \(x \in X\), \([X] := X/\sim\).

The left and the right actions of \(X\) onto itself naturally induce left and right actions on the retraction \([X]\), via

\[
[a][x] := [a^x] \quad [x][a] := [a^x], \quad \forall \ a, x \in X.
\]

and a canonical map

\[
r_{[X]} : [X] \times [X] \longrightarrow [X] \times [X], \quad r_{[X]}([x], [y]) = ([x^y], [x^y]).
\]

Then \(([X], r_{[X]})\) is a solution.

\(\mu : X \longrightarrow [X], \ x \mapsto [x]\) from \(X\) to its retraction is a homomorphism of solutions (a braiding-preserving map).
The solution $\text{Ret}(X, r) = ([X], r_{[X]})$ is called the retraction of $(X, r)$.

For all integers $m \geq 1$, $\text{Ret}^m(X, r)$ is defined recursively as

$$\text{Ret}^m(X, r) = \text{Ret}(\text{Ret}^{m-1}(X, r))$$

$$\text{Ret}^0(X, r) = (X, r), \quad \text{Ret}^1(X, r) = \text{Ret}(X, r).$$

$(X, r)$ is a multipermutation solution of level $m$, if $m$ is the minimal number (if any), such that $\text{Ret}^m(X, r)$ is the trivial solution on a set of one element, we write $\text{mpl}(X, r) = m$.

$\text{mpl}(X, r) = 1$ iff $(X, r)$ is a permutation solution.

$\text{mpl}(X, r) = 0$ iff $X$ is a one element set.
Questions and Problems.

- Find structural invariants which determine the process of recursive retraction on Symmetric groups, Braces and solutions \((X, r)\).
- Study Symmetric groups and Braces with special conditions.
- What is the special impact of \(\text{mpl } X = m < \infty\) on the corresponding algebraic structures of \(X\)? Some of the theorems in this talk are also related to this question.
- Where is the borderline between the classes of multipermutation solutions and solutions which are not multipermutation?

A nice answer was given recently by B. C. V.: \((X, r)\) is a multipermutation solution iff its structure group \(G(X, r)\) admits a left ordering. We give different characterisations in Thms 2 through 6 below.
We propose a general strategy: to involve simultaneously Symmetric groups and Braces in the study of symmetric sets (involutive solutions of any type and cardinality); respectively, Braided Groups and Skew Braces for the study of braided sets.

- We proved the equivalence of the two structures: a symmetric group \((G, \sigma)\) (a group \(G\) with an involutive braiding operator \(\sigma\)) and a left brace \((G, +, \cdot)\).
- We found an important structural invariant of a symmetric group \(G\): The derived chain of ideals of \((G, \sigma)\), DCI.
- DCI gives a precise information about the recursive process of retraction of \(G\) and reflects some algebraic properties of \(G\):
  - Theorem. If a symmetric group \((G, r)\) of arbitrary cardinality has finite multipermutation level \(m\) then \(G\) is a solvable group of solvable length \(\leq m\).
- Each solution \((X, r)\) has two invariant series of symmetric groups: (i) its derived symmetric groups \((G_i, r_i)\); (ii) its derived permutation groups \((G_i, r_G)\). ⇒ explicit descriptions of the
A braided group is a pair \((G, \sigma)\), where \(G\) is a group and \(\sigma : G \times G \longrightarrow G \times G\), \(\sigma(a, u) = (a^u, a^u)\) is a braiding operator, i.e. a bijective map s.t.

\[
\begin{align*}
\text{ML0 : } & \quad a^1 = 1, \quad 1^u = u, \\
\text{ML1 : } & \quad ab^u = a(b^u), \\
\text{ML2 : } & \quad a(u.v) = (a^u)(a^v), \\
\text{MR0 : } & \quad 1^u = 1, \quad a^1 = a, \\
\text{MR1 : } & \quad a^{uv} = (a^u)^v, \\
\text{MR2 : } & \quad (a.b)^u = (a^b)^u(b^u),
\end{align*}
\]

\(\forall a, b, u, v, \in S.\)
[LYZ] A braided group is a pair \((G, \sigma)\), where \(G\) is a group and \(\sigma : G \times G \rightarrow G \times G\), \(\sigma(a, u) = (a^u, a^u)\) is a braiding operator, i.e. a bijective map s.t.

\[
\begin{align*}
\text{ML0 : } & \quad a1 = 1, \quad 1^u = u, \quad \text{MR0 : } \quad 1^u = 1, \quad a^1 = a, \\
\text{ML1 : } & \quad ab^u = a(b^u), \quad \text{MR1 : } \quad a^{uv} = (a^u)^v, \\
\text{ML2 : } & \quad a^{(u,v)} = (a^u)(a^v), \quad \text{MR2 : } \quad (a.b)^u = (a^b)(b^u),
\end{align*}
\]

\(\forall a, b, u, v, \in S\).

\[
\begin{align*}
\text{and the the compatibility condition M3 holds in G:}
\end{align*}
\]

\[
\begin{align*}
\text{M3 : } & \quad uv = (u^v)(u^v), \quad \forall u, v \in G.
\end{align*}
\]
A braided group is a pair \((G, \sigma)\), where \(G\) is a group and \(\sigma : G \times G \to G \times G\), \(\sigma(a, u) = (a^u, a^u)\) is a braiding operator, i.e. a bijective map s.t.

\begin{align*}
\text{ML0} : & \quad a1 = 1, \ 1u = u, \\
\text{ML1} : & \quad abu = a(bu), \\
\text{ML2} : & \quad a(uv) = (a_u)(a^u v),
\end{align*}

\begin{align*}
\text{MR0} : & \quad 1^u = 1, \ a^1 = a, \\
\text{MR1} : & \quad a^{uv} = (a^u)^v, \\
\text{MR2} : & \quad (a.b)^u = (a^u b)(b^u),
\end{align*}

\(\forall a, b, u, v, \in S\).

and the compatibility condition \(\text{M3}\) holds in \(G\):

\[
\text{M3} : \quad uv = (u^v)(u^v), \quad \forall u, v \in G.
\]

If the map \(\sigma\) is involutive \((\sigma^2 = id_{G \times G})\) then \((G, \sigma)\) is called a symmetric group (in the sense of Takeuchi).
Facts on braided groups and symmetric groups. [LYZ]

- (1) If \((G, \sigma)\) is a symmetric group (resp. braided group), then \(\sigma\) satisfies the braid relations and is nondegenerate.
- So \((G, \sigma)\) is a solution to YBE.
- (2) Let \((X, r)\) be a nondegenerate (involutive) solution of YBE, \(G = G(X, r)\) the associated YB-group. Then there is unique braiding operator \(r_G : G \times G \to G \times G\), s.t. the restriction of \(r_G\) on \(X \times X\) is exactly the map \(r\).
- \((G, r_G)\) is a symmetric group.
Theorem 2. (GI 15’) The following two structures on a group \((G, .)\) are equivalent.

- (1) The pair \((G, \sigma)\) is a symmetric group, i.e. a braided group with an involutive braiding operator \(\sigma\).
Theorem 2. (GI 15’) The following two structures on a group \((G, .)\) are equivalent.

- (1) The pair \((G, \sigma)\) is a symmetric group, i.e. a braided group with an involutive braiding operator \(\sigma\).
- (2) \((G, +, .)\) is a left brace.
**Theorem 2.** (GI 15’) The following two structures on a group \((G, .)\) are equivalent.

- (1) The pair \((G, \sigma)\) is a *symmetric group*, i.e. a braided group with an involutive braiding operator \(\sigma\).
- (2) \((G, +, .)\) is a left brace.
- In this case

\[
a + a b := ab
\]
Theorem 2. (GI 15’) The following two structures on a group \((G, .)\) are equivalent.

- (1) The pair \((G, \sigma)\) is a symmetric group, i.e. a braided group with an involutive braiding operator \(\sigma\).
- (2) \((G, +, .)\) is a left brace.
- In this case
  \[
a + ^{a}b := ab
  \]
- Moreover, \((G, \sigma)\) is a solution of YBE.
Theorem 2. (GI 15’) The following two structures on a group \((G, .)\) are equivalent.

1. The pair \((G, \sigma)\) is a symmetric group, i.e. a braided group with an involutive braiding operator \(\sigma\).
2. \((G, +, .)\) is a left brace.

In this case

\[
a + {}^a b := ab
\]

Moreover, \((G, \sigma)\) is a solution of YBE.

Recent Results of Guarnieri-Smoktunowicz-Vendramin, ’17: Let \((G, \circ)\) be a group. The following two structures on \(G\) are equivalent: (i) The pair \((G, \sigma)\) is a braided group, with a braiding operator \(\sigma\); (ii) \((G, \cdot, \circ)\) is a skew brace. Moreover, \((G, \sigma)\) is a nondegenerate braided set.

Comments on the results:

- Characterize general solutions (braided sets) \((X, r)\) in terms of an induced matched pair of monoids \((S, S), S = S(X, r)\) ((X,r) is not necessarily nondegenerate, and has arbitrary cardinality)

- Construct solutions \((S, r_S)\) from the matched pair.

- Study extensions of solutions in terms of matched pairs of their associated semigroups.

- Use our matched pairs characterization to study regular YB-extensions \(Z = X \cup Y\).
The recursive process of retraction. The socle of a symmetric group $G = (G, r)$

- Let $\Gamma$ be the kernel of the left action of $G$ upon itself
  $$\Gamma = \{ a \in G \mid a^u = u, \forall u \in G \} = \{ a \in G \mid u^a = u, \forall u \in G \} = \Gamma_r.$$

- $\Gamma$ is a normal subgroup of $G$.
- $\Gamma$ is invariant w.r.t. the left (and the right) action of $G$ upon itself. (Hence $\Gamma$ is $r$-invariant).
- $\Gamma$ is abelian.
- $\Gamma$ will be called the socle of the symmetric group $(G, r)$. (This is by analogy with a socle of a left brace, (CJO, R)) $\Gamma$ is often denoted by $\text{Soc}(G)$.

**Definition.** A normal subgroup $H$ of $G$ is called an ideal of $G$ if it is (left) $G$-invariant (thus also right $G$-invariant).

- The socle $\text{Soc} G$ is an ideal of $G$. 
The quotient braided group $\tilde{G} = G/\Gamma$

- The matched pair structure $r : G \times G \to G \times G$ induces a map $r_{\tilde{G}} : \tilde{G} \times \tilde{G} \to \tilde{G} \times \tilde{G}$, which makes $\tilde{G}$ a braided group [Takeuchi, 2003].

- In fact, $(\tilde{G}, r_{\tilde{G}})$ is a symmetric group, called the quotient symmetric group of $(G, r)$ (since $r_{\tilde{G}}$ is involutive).
The quotient symmetric group \((\tilde{G}, r_{\tilde{G}})\) and the retraction \(\text{Ret}(G, r)\)

- Consider \((G, r)\) as a symmetric set, with retraction \(\text{Ret}(G, r) = ([G], r_{[G]})\). Then
- The map \(\varphi : (\tilde{G}, r_{\tilde{G}}) \to ([G], r_{[G]}), \tilde{a} \mapsto [a]\),

  is an isomorphism of symmetric sets.
- So \(\text{Ret}(G, r) = ([G], r_{[G]})\) is a symmetric group and \(\varphi\) is an isomorphism of symmetric groups.
The quotient symmetric group $(\tilde{G}, r_{\tilde{G}})$ and the retraction $\text{Ret}(G, r)$

- Consider $(G, r)$ as a symmetric set, with retraction $\text{Ret}(G, r) = ([G], r_{[G]})$. Then
- The map
  \[
  \varphi : (\tilde{G}, r_{\tilde{G}}) \longrightarrow ([G], r_{[G]}), \quad \tilde{a} \mapsto [a],
  \]
is an isomorphism of symmetric sets.
- So $\text{Ret}(G, r) = ([G], r_{[G]})$ is a symmetric group and $\varphi$ is an isomorphism of symmetric groups.
The quotient symmetric group \((\tilde{G}, r_{\tilde{G}})\) and *the retraction* \(\text{Ret}(G, r)\)

- Consider \((G, r)\) as a symmetric set, with retraction \(\text{Ret}(G, r) = ([G], r_{[G]})\). Then
- The map

\[
\phi : (\tilde{G}, r_{\tilde{G}}) \longrightarrow ([G], r_{[G]}), \quad \tilde{a} \mapsto [a],
\]

is an isomorphism of symmetric sets.
- So \(\text{Ret}(G, r) = ([G], r_{[G]})\) is a symmetric group and \(\phi\) is an isomorphism of symmetric groups.
The quotient symmetric group \((\tilde{G}, r_{\tilde{G}})\) and the retraction \(\text{Ret}(G, r)\)

- Consider \((G, r)\) as a symmetric set, with retraction \(\text{Ret}(G, r) = ([G], r_{[G]})\). Then
- The map

\[ \varphi : (\tilde{G}, r_{\tilde{G}}) \longrightarrow ([G], r_{[G]}), \quad \tilde{a} \mapsto [a], \]

is an isomorphism of symmetric sets.
- So \(\text{Ret}(G, r) = ([G], r_{[G]})\) is a symmetric group and \(\varphi\) is an isomorphism of symmetric groups.
- We identify the retraction \(\text{Ret}(G, r) = ([G], r_{[G]})\) and the quotient sym. group \((\tilde{G}, r_{\tilde{G}})\), where \(\tilde{G} = G/\Gamma\).
The case \((G, r_G)\), when \(G = G(X, r)\) is the YB group of a solution

- **Proposition 1.** Let \((X, r)\) be a nondegenerate symmetric set.
- There is an isomorphism of symmetric groups
  
  \[ \text{Ret}(G, r_G) = ([G], r_{[G]}) \simeq G(X, r). \]
- If the solution \((X, r)\) is finite then the retraction \(\text{Ret}(G, r_G) \simeq (G, r_G)\) is a finite symmetric group.
Isomorphism Theorems for Symmetric Groups

- **First Isomorphism Theorem for Symmetric Groups**
  - Let $f : (G, r) \rightarrow (\tilde{G}, r_{\tilde{G}})$ be an epimorphism of symmetric groups. Then
  - the kernel $K = \ker f$ is an ideal of $(G, r)$, and $\exists$ a natural isomorphism of symmetric groups $G/K \simeq \tilde{G}$.

- **Third Isomorphism Theorem for Symmetric groups**
  - $(G, r)$ -a symmetric group, $K$ -an ideal of $G$, $\tilde{G} = G/K$, let $f : G \rightarrow \tilde{G}$ be the canonical epimorphism of symmetric groups ($\ker f = K$).
  - There is a bijective correspondence
    \[
    \{ \text{ideals } H \text{ of } G \text{ containing } K \} \longleftrightarrow \{ \text{ideals } \tilde{H} \text{ of } \tilde{G} \},
    \]
    given by
    \[
    H \mapsto f(H) \simeq H/K, \quad f^{-1}(H) \leftrightarrow \tilde{H}.
    \]
Isomorphism Theorems for Symmetric Groups

- **First Isomorphism Theorem for Symmetric Groups**
  - Let $f : (G, r) \longrightarrow (\tilde{G}, r_{\tilde{G}})$ be an epimorphism of symmetric groups. Then
  - the kernel $K = \ker f$ is an ideal of $(G, r)$, and $\exists$ a natural isomorphism of symmetric groups $G / K \simeq \tilde{G}$.

- **Third Isomorphism Theorem for Symmetric groups**
  - $(G, r)$ - a symmetric group, $K$ - an ideal of $G$, $\tilde{G} = G / K$, let $f : G \longrightarrow \tilde{G}$ be the canonical epimorphism of symmetric groups ($\ker f = K$).
  - There is a bijective correspondence
    \[
    \{ \text{ideals } H \text{ of } G \text{ containing } K \} \longleftrightarrow \{ \text{ideals } \tilde{H} \text{ of } \tilde{G} \},
    \]
    given by
    \[
    H \mapsto f(H) \simeq H / K, \quad f^{-1}(H) \mapsto \tilde{H}.
    \]
Isomorphism Theorems for Symmetric Groups

- **First Isomorphism Theorem for Symmetric Groups**
  - Let $f : (G, r) \longrightarrow (\tilde{G}, r_{\tilde{G}})$ be an epimorphism of symmetric groups. Then
  - the kernel $K = \ker f$ is an ideal of $(G, r)$, and $\exists$ a natural isomorphism of symmetric groups $G/K \simeq \tilde{G}$.

- **Third Isomorphism Theorem for Symmetric groups**
  - $(G, r)$ - a symmetric group, $K$ - an ideal of $G$, $\tilde{G} = G/K$, let $f : G \longrightarrow \tilde{G}$ be the canonical epimorphism of symmetric groups ($\ker f = K$).
  - There is a bijective correspondence
    \[
    \{ \text{ideals } H \text{ of } G \text{ containing } K \} \longleftrightarrow \{ \text{ideals } \tilde{H} \text{ of } \tilde{G} \},
    \]
    given by
    \[
    H \mapsto f(H) \simeq H/K, \quad f^{-1}(H) \leftrightarrow \tilde{H}.
    \]
Isomorphism Theorems for Symmetric Groups

- **First Isomorphism Theorem for Symmetric Groups**
  - Let \( f : (G, r) \longrightarrow (\tilde{G}, r_{\tilde{G}}) \) be an epimorphism of symmetric groups. Then
  - the kernel \( K = \ker f \) is an ideal of \( (G, r) \), and \( \exists \) a natural isomorphism of symmetric groups \( G/K \cong \tilde{G} \).

- **Third Isomorphism Theorem for Symmetric groups**
  - \((G, r)\) -a symmetric group, \( K \) -an ideal of \( G \), \( \tilde{G} = G/K \), let \( f : G \longrightarrow \tilde{G} \) be the canonical epimorphism of symmetric groups (\( \ker f = K \)).
  - There is a bijective correspondence
    \[
    \{ \text{ideals } H \text{ of } G \text{ containing } K \} \longleftrightarrow \{ \text{ideals } \tilde{H} \text{ of } \tilde{G} \},
    \]
    given by
    \[
    H \mapsto f(H) \cong H/K, \quad f^{-1}(H) \leftarrow \tilde{H}.
    \]
Isomorphism Theorems for Symmetric Groups

- **First Isomorphism Theorem for Symmetric Groups**
  Let \( f : (G, r) \rightarrow (\tilde{G}, r_{\tilde{G}}) \) be an epimorphism of symmetric groups. Then
  - the kernel \( K = \ker f \) is an ideal of \((G, r)\), and \( \exists \) a natural isomorphism of symmetric groups \( G/K \cong \tilde{G} \).

- **Third Isomorphism Theorem for Symmetric groups**
  - \((G, r)\) -a symmetric group, \( K \)-an ideal of \( G \), \( \tilde{G} = G/K \), let \( f : G \rightarrow \tilde{G} \) be the canonical epimorphism of symmetric groups (\( \ker f = K \)).
  - There is a bijective correspondence
    \[
    \{ \text{ideals } H \text{ of } G \text{ containing } K \} \leftrightarrow \{ \text{ideals } \tilde{H} \text{ of } \tilde{G} \},
    \]
    given by
    \[
    H \mapsto f(H) \cong H/K, \quad f^{-1}(H) \leftrightarrow \tilde{H}.
    \]
Isomorphism Theorems for Symmetric Groups

- **First Isomorphism Theorem for Symmetric Groups**

Let $f : (G, r) \rightarrow (\tilde{G}, r_{\tilde{G}})$ be an epimorphism of symmetric groups. Then

the kernel $K = \ker f$ is an ideal of $(G, r)$, and $\exists$ a natural isomorphism of symmetric groups $G / K \cong \tilde{G}$.

- **Third Isomorphism Theorem for Symmetric groups**

$(G, r)$ -a symmetric group, $K$ -an ideal of $G$, $\tilde{G} = G / K$, let $f : G \rightarrow \tilde{G}$ be the canonical epimorphism of symmetric groups ($\ker f = K$).

There is a bijective correspondence

\[
\{ \text{ideals } H \text{ of } G \text{ containing } K \} \leftrightarrow \{ \text{ideals } \tilde{H} \text{ of } \tilde{G} \},
\]

given by

\[
H \mapsto f(H) \cong H / K, \quad f^{-1}(H) \leftrightarrow \tilde{H}.
\]
First Isomorphism Theorem for Symmetric Groups

Let \( f : (G, r) \rightarrow (\tilde{G}, r\tilde{G}) \) be an epimorphism of symmetric groups. Then

- the kernel \( K = \ker f \) is an ideal of \((G, r)\), and \( \exists \) a natural isomorphism of symmetric groups \( G/K \cong \tilde{G} \).

Third Isomorphism Theorem for Symmetric groups

- \((G, r)\) - a symmetric group, \( K \) - an ideal of \( G \), \( \tilde{G} = G/K \), let \( f : G \rightarrow \tilde{G} \) be the canonical epimorphism of symmetric groups (\( \ker f = K \)).

There is a bijective correspondence

\[ \{ \text{ideals } H \text{ of } G \text{ containing } K \} \leftrightarrow \{ \text{ideals } \tilde{H} \text{ of } \tilde{G} \}, \]

given by

\[ H \mapsto f(H) \cong H/K, \quad f^{-1}(H) \leftrightarrow \tilde{H}. \]

- \( \forall \) ideal \( H \supset K \) of \( G \) one has

\[ (G/K)/(H/K) \cong G/H, \quad gK.(H/K) \mapsto gH. \]
(Gl, 16') *The derived chain of ideals of a sym. gp. \((G, r)\).*

- \((G^j, r^j) := \text{Ret}^j(G, r) \simeq G^{j-1}/\Gamma_j, j \geq 1,\) where 
  \[\Gamma_j = \text{Soc}(G^{j-1});\ G^0 = \text{Ret}^0(G, r) = G, \ \Gamma_1 = \Gamma.\ \phi_{j+1}, \ j \geq 0,\] is the canonical epimorphism of symmetric groups, 
  \[\ker \phi_j = \Gamma_{j+1}:\]

\[
\text{Ret}^j(G, r) = G^j \xrightarrow{\phi_{j+1}} G^j/\Gamma_{j+1} \simeq G^{j+1} = \text{Ret}^{j+1}(G, r).
\]

- This implies a sequence of epimorphisms of symmetric gps (some possibly coincide):

\[
G \xrightarrow{\phi_1} G^1 = G/\Gamma \xrightarrow{\phi_2} G^2 = G^1/\Gamma_2 \xrightarrow{\phi_3} G^3 = G^2/\Gamma_3 \xrightarrow{\phi_4} \ldots.
\]

- **Def.** *The derived chain of ideals of the symmetric group \((G, r)\) (the derived series of \(G\)) is the nondecr. chain of ideals*

\[
\{1\} = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_j \subset \cdots,
\]

where \(K_0 := \{1\},\) and \(\forall j \geq 1, \ K_j\) is the pull-back of \(\Gamma_j\) in \(G\).
Proposition 2. (Gl 16’) Let \((G, r)\) be a sym. group.

- \(\forall j \geq 1\) there are isomorphisms \(K_j/K_{j-1} \cong \Gamma_j,\)
  \(G/K_j \cong G^{j-1}/\Gamma_j = \text{Ret}^j(G, r)\)
- and canonical epimorphisms of symmetric groups
  \(\mu_j : G/K_{j-1} \longrightarrow G/K_j, \ker \mu_j \cong K_j/K_{j-1}.\)
- \(K_j/K_{j-1} = \text{Soc}(G/K_{j-1}), j \geq 1,\) are abelian symmetric groups
  \((K_j/K_{j-1} = 1 \text{ is possible}).\)
- The following diagram is commutative (on the board!!):
- The derived chain of \(G\) stabilizes iff
  \(\text{Ret}^{j+1}(G, r) = \text{Ret}^j(G, r)\) (eq. \(K_{j+1} = K_j\)) for some \(j \geq 0.\)
- Let \(m\) be the minimal integer (if any) such that \(K_{m+1} = K_m.\)
  Then \(\text{Ret}^m(G, r) = \text{Ret}^{m+1}(G, r)\) and the recursive
  retraction halts in \(m\) steps. Either
- (a) \(K_m = G.\) Then \(m \geq 1,\) and \((G, r)\) is a multipermutation
  solution with \(\text{mpl}(G, r) = m;\) or
- (b) \(K_m \subsetneq G \) \((m = 0 \text{ is possible}).\) Then \(\text{Ret}^m(G, r)\) is a
  symmetric group of order \(\geq 2\) which can not be retracted.
Theorem 3. (GI 16') Let \( (G, r) \) be a nontrivial symmetric group, \( (G, +, \cdot) \) its associated left brace, and let \( \{1\} = K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots \) be its D.C.I.

- (1) FAEQ:
  - (i) \( (G, r) \) has a finite multipermutation level \( \text{mpl} G = m \geq 1 \).
  - (ii) The derived chain of ideals of \( G \) has the shape
    \[
    \{1\} = K_0 \nsubseteq K_1 \nsubseteq K_2 \nsubseteq \cdots \nsubseteq K_{m-1} \nsubseteq K_m = G.
    \]
  - (iii) \( K_{m-1} \nsubseteq K_m = G \).
- (2) In this case \( G \) is a solvable group of solvable length
  \[
  \text{sl} G \leq m.
  \]
Remark. The converse is not true.

It is known that if \((X, r)\) is a finite solution then the associated YB group \(G = G(X, r)\) is solvable. Take \((X, r)\) irretractable, say Vendr. example of order 8. Consider the symmetric group \((G, r_G)\). Thm 3 states mpl \(X = m\) iff mpl \(G = m\), but \(X\) is not multipermutation solution, and so is \(G\).
Theorem 4. (GI 15’) Let \((X, r)\) be a symmetric set, of order \(|X| \geq 2\), let \(G = (G, r_G), (\mathcal{G}, r_\mathcal{G})\), the ass. symmetric groups.

1. \((G, r_G)\) has finite multipermutation level iff \((X, r)\) is a multipermutation solution.
2. In this case one has

\[
0 \leq \text{mpl}(\mathcal{G}, r_\mathcal{G}) = m - 1 \leq \text{mpl}(X, r) \leq \text{mpl}(G, r_G) = m < \infty.
\]

3. Suppose furthermore that \((X, r)\) is a square-free solution. Then

\[
\text{mpl} X = m < \infty \iff \text{mpl} G = m < \infty.
\]
Derived symmetric groups and derived permutation groups of a solution.

- We set \( \text{Ret}^0(X, r) = (X, r) \), \( \text{Ret}^j(X, r) = \text{Ret}(\text{Ret}^{j-1}(X, r)) \) is the \( j \)-th retraction of \((X, r)\), \( j \geq 1 \).
- \( x^{(j)} \) denotes the image of \( x \) in \( \text{Ret}^j(X, r) \) \((x^{(0)} = x)\).
- \( G_j := G(\text{Ret}^j(X, r)) \), \( G_0 = G(X, r) = G \); \( G_j := G(\text{Ret}^j(X, r)) \), \( G_0 = G(X, r) = G \).
- \( \mathcal{L}^j : G_j \rightarrow G_j \) is the epimorphism extending the assignment \( x^{(j)} \mapsto \mathcal{L}_{x^{(j)}} \in \text{Sym}(\text{Ret}^j(X, r)), \ x \in X \), \( \mathcal{L}^0 = \mathcal{L} : G(X, r) \rightarrow G(X, r) \), extends \( x \mapsto \mathcal{L}_x, \ x \in X \).
- \( \mathcal{K}_j \) is the pull-back of \( \ker \mathcal{L}^j \) in \( G \), in particular \( \mathcal{K}_0 = \ker \mathcal{L} \).
- \( \nu_j : G_j \rightarrow G_{j+1} \) is the epimorphism extending the assignment \( x^{(j)} \mapsto x^{(j+1)} \). \( N_j \) is the pull-back of \( \ker \nu_j \) in \( G \), \( N_0 = \ker \nu_0 \).
- \( \varphi_j : G_j \rightarrow G_{j+1} \) is the epimorphism extending the assignments \( \mathcal{L}_{x^{(j)}} \mapsto \mathcal{L}_{x^{(j+1)}}, \ x \in X \).
Theorem 5. (Gl 16’) Notation as above, $\mathcal{K}_j$ is the pull-back of ker $\mathcal{L}_j$ in $G$

- There are isomorphisms of symmetric groups:
  
  $$\text{Ret}^2(G, r_G) \cong \text{Ret}(\mathcal{G}, r_\mathcal{G}) \cong \mathcal{G}(\text{Ret}(X, r)), \text{Soc}(\mathcal{G}) \cong \mathcal{K}_1 / \mathcal{K}_0.$$ 

- More generally,
  
  $$\text{Ret}^{j+1}(G, r_G) \cong \mathcal{G}(\text{Ret}^j(X, r)) = \mathcal{G}_j, \quad \text{Soc}(\mathcal{G}_j) \cong \mathcal{K}_{j+1} / \mathcal{K}_j.$$
Theorem 6. Every solution $(X, r)$ has two series of derived symmetric groups:

$$(G_j, r_{G_j}) = G(\text{Ret}^j(X, r)), j \geq 0, \text{ the derived symmetric groups of } (X, r)$$

$$(G_j, r_{G_j}) = G(\text{Ret}^j(X, r)), j \geq 0, \text{ the derived permutation groups of } (X, r).$$

One has

$$(G_j, r_{G_j}) \simeq \text{Ret}(G_j, r_{G_j}), \quad \text{Ret}(G_j, r_{G_j}) \simeq (G_{j+1}, r_{G_{j+1}}),$$

$$\text{Ret}^{j+1}(G, r_{G}) \simeq (G_j, r_{G_j}).$$

So each of the derived series is an invariant of the solution and reflects the process of retraction.

Remark. Each derived symmetric group and each derived permutation group encodes various combinatorial properties of the solution $(X, r)$ and may have strong impact on it.

In general, each of the derived series may have repeating members.
Epilogue. I. Suppose \((X, r)\) is a solution, \(|X| \geq 2\), \((G, r_G)\), \((G, r_G)\) are the associated symmetric groups, 
\((G_j, r_{G_j}) = G(\text{Ret}^j(X, r)), G_j = G(\text{Ret}^j(X, r)), j \geq 0\), are the derived symmetric groups, resp. the derived permutation groups, and \(m \geq 1\) is an integer. Then

\[
[mpl G < \infty] \iff [mpl X < \infty] \iff [mpl G < \infty].
\]

In this case

\[
0 \leq mpl G = m - 1 \leq mpl X \leq mpl G = m < \infty.
\]

Moreover, if \((X, r)\) is finite then

\[
[2 \leq mpl X < \infty] \iff \\
[\exists j \geq 0, \text{ s. t. } (G_j, +, \cdot) \text{ is a two-sided brace, } G_j \neq \{1\}]\].
II. Suppose \((X, r)\) is a square-free solution. FAEQ:

1. \(\text{mpl } X = m\);
2. \(\text{mpl } G = m\);
3. \((G_{m-2}, r_{G_{m-2}})\) satisfies \text{lri} and is not abelian; (In particular, \(\text{mpl } X = 2\) iff \((G, r_G)\) satisfies \text{lri} and is not abelian);
4. the DCI for \(G\) has the shape 
   \[
   \{1\} = K_0 \subsetneq K_1 \subsetneq K_2 \subsetneq \cdots \subsetneq K_{m-1} \subsetneq K_m = G;
   \]
5. The left brace \((G, +, \cdot)\) is right nilpotent of nilpotency class \(m + 1\).
6. If in addition \((X, r)\) is finite, then 
   \[
   [2 \leq \text{mpl } X < \infty] \iff [\exists j \geq 0, \text{ s.t. } (G_j, r_{G_j}) \text{ satisfies lri}, G_j \neq \{1\}].
   \]
(Gi, Majid) **Theorem A.**

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

\[
(\cdot)\mathord{\cdot} : X \times X \to X, \quad \mathord{\cdot}(\cdot) : X \times X \to X
\]

defined via \(r\) can be extended in a unique way to a left and a right action

\[
(\cdot)\mathord{\cdot} : S \times S \to S, \quad \mathord{\cdot}(\cdot) : S \times S \to S,
\]

which make \(S\) a strong graded \(\textbf{M3}\)-monoid with associated bijective map \(r_S\).
Theorem B.

Let $S$ be an $M3$-monoid with assoc. map $r_S$. Suppose $S$ is with 2-cancellation and one of the following holds:

- $S$ has a generating set invariant under the left and the right actions of the M.P. and the restriction $r_X : X \times X \rightarrow X \times X$ is a bijection;
- $(S, r_S)$ is graded, and the restriction $r_X : X \times X \rightarrow X \times X$ on deg. 1 is a bijection;
- $S$ is a monoid (not necessarily graded) with left cancellation.

Then

- $r_S$ is a solution of the YBE on $S$. Moreover,
- $r_S$ is bijective (so $(S, r_S)$ is a braided monoid) iff $(S, S)$ is a strong matched pair.
(Gl-Majid, JA 08’) **Theorem C.**

Let \((X, r)\) be a braided set, \(S = S(X, r)\), and let \((S, r_S)\) be the induced **M3**-monoid by **Theorem A**. Then

- \((S, r_S)\) is a braided monoid.
- \((S, r_S)\) is non-degenerate iff \((X, r)\) is non-degenerate.
- \((S, r_S)\) is involutive iff \((X, r)\) is involutive.