On the set-theoretical Yang-Baxter equation

Jiang-Hua Lu[*]
Department of Mathematics
University of Arizona

Min Yan,   Yong-Chang Zhu[†]
Department of Mathematics
Hong Kong University of Science and Technology

Abstract

We propose a general way of constructing set-theoretical solutions of the Yang-Baxter equation. We study the properties of the construction. We also show that our construction includes the earlier ones given by Weinstein-Xu and Etingof-Schedler-Soloviev.

Contents

1 Introduction

Let V be a vector space. Let $R : V \otimes V \to V \otimes V$ be an invertible linear transformation. The Yang-Baxter equation is the following equality

$$R_{12}R_{13}R_{23} = R_{23}R_{13}R_{12} \tag{1}$$

of linear transformations on $V \otimes V \otimes V$. Denote $\tau(w \otimes v) = v \otimes w : V \otimes V \to V \otimes V$ and $\sigma = \tau \circ R$. Then the Yang-Baxter equation is equivalent to the braid relation

$$\sigma_{12}\sigma_{23}\sigma_{12} = \sigma_{23}\sigma_{12}\sigma_{23}. \tag{2}$$

Because of this, a solution of the Yang-Baxter equation gives arise to a linear representation of the Braid group B_n on $V^{\otimes n}$ for every n.

In [D], Drinfel'd raised the question of finding set-theoretical solutions of the Yang-Baxter equation. Specifically, we consider a set S and an invertible map $R : S \times S \to S \times S$. We think of the Yang-Baxter equation (1) as an equality of maps from $S \times S \times S$ to $S \times S \times S$. As in the linear case, a solution of (1) on a set S gives arise to an action of B_n on the set S^n.

By studying Poisson group, Weinstein and Xu [WX] found a way of constructing set-theoretical solutions of the Yang-Baxter equation. Later on, Etingof, Schedler, and Soloviev [ESS] gave a complete classification of the non-degenerate set-theoretical solutions R of the Yang-Baxter equation satisfying $(\tau \circ R)^2 = id$ (where $\tau(w, v) = (v, w)$).

In this paper, we present the following construction of set-theoretical solutions of the Yang-Baxter equation.

Theorem 1 *Let G be a group. Let ξ and η be left and right actions of G on itself, denoted by $(u, v) \mapsto {}^{\xi(u)}v$ and $(u, v) \mapsto u^{\eta(v)}$, respectively. If the two actions satisfy the compatibility condition*

$$uv = ({}^{\xi(u)}v)(u^{\eta(v)}), \tag{3}$$

then

$$R(u, v) = (u^{\eta(v)}, \, {}^{\xi(u)}v)$$

is invertible and is a solution of the Yang-Baxter equation on the set G.

In Section 2, we give two conceptual reformulations of the conditions in the theorem. The second reformulation immediately indicates that our construction generalizes the one in [ESS]. In Section 3, we further show that the construction in [WX] is also a special case of our construction.

General set-theoretical solutions of the Yang-Baxter equation are related to our construction in the following way. Given a non-degenerate solution R of the Yang-Baxter

equation on a set S, we may consider triples (G, ξ, η) satisfying the conditions of Theorem 1 and maps $S \to G$ commuting with the solutions of the Yang-Baxter equation. We can construct a universal triple and the associated map in the sense that any other triple factors through the map by a homomorphism of the triples. The group in the universal triple is generated by S under the relation $uv = yx$ whenever $R(u, v) = (x, y)$. This group was first introduced in [ESS].

The conceptual reason behind the construction in Theorem 1 is the following. It is well-known that representations of quasi-triangular Hopf algebras give solutions of the Yang-Baxter equation. Therefore we establish a set-theoretical theory of Hopf algebras in [LYZ1]. Then we establish the corresponding theory of quasi-triangular structures in [LYZ2]. Just as in the usual theory of Hopf algebras, such set-theoretical quasi-triangular structures lead us to the set-theoretical solutions of the Yang-Baxter equation.

We would like to thank the referee for pointing out the reformulation of our construction in terms of bijective 1-cocycles, which simplified the presentation of the paper.

2 Braiding operators and bijective 1-cocycles

We start with the proof of Theorem 1.

Proof of Theorem 1: We verify the braid relation (2) for $\sigma(u, v) = \tau R(u, v) = \left({}^{\xi(u)}v, u^{\eta(v)}\right)$. Denote

$$\sigma_{12}\sigma_{23}\sigma_{12}(u, v, w) = (u_1, v_1, w_1), \qquad \sigma_{23}\sigma_{12}\sigma_{23}(u, v, w) = (u_2, v_2, w_2).$$

The compatibility condition (3) implies that $u_1 v_1 w_1 = u_2 v_2 w_2$. Thus it suffices to prove $u_1 = u_2$ and $w_1 = w_2$. By direct computation, we find $u_1 = {}^{\xi\left({}^{\xi(u)}v\right)\xi\left(u^{\eta(v)}\right)}w$ and $u_2 = {}^{\xi(u)\xi(v)}w$. Then we have

$$ {}^{\xi\left({}^{\xi(u)}v\right)\xi\left(u^{\eta(v)}\right)}w = {}^{\xi\left({}^{\xi(u)}v\ u^{\eta(v)}\right)}w \overset{(3)}{=} {}^{\xi(uv)}w = {}^{\xi(u)\xi(v)}w, $$

where the first and the third equalities are due to the fact that ξ is a left action. The equality $w_1 = w_2$ can be proved in similar way.

To see R is invertible, let $(x, y) = R(u, v)$, i.e., $x = u^{\eta(v)}$ and $y = {}^{\xi(u)}v$. Then

$$ \left({}^{\xi(x)}(v^{-1})\right) u = \left({}^{\xi(x)}(v^{-1})\right) \left(x^{\eta(v^{-1})}\right) \overset{(3)}{=} xv^{-1} \overset{(3)}{=} y^{-1}u, $$

which implies $v^{-1} = {}^{\xi(x^{-1})}(y^{-1})$. Similarly, we have $u^{-1} = (x^{-1})^{\eta(y^{-1})}$. Thus we conclude that $R(x^{-1}, y^{-1}) = (u^{-1}, v^{-1})$. In other words, if we denote $\imath(u, v) = (u^{-1}, v^{-1})$, then $(\imath R)^2 = id$. In particular, this implies that R is invertible.

$\square$

3

Next we give two alternative descriptions of our construction.

Definition Let G be a group with multiplication m. A *braiding operator* on G is a bijective map $\sigma : G \times G \to G \times G$ satisfying

1. For any $u, v, w \in G$,

$$\sigma(uv, w) = (id \times m)\sigma_{12}\sigma_{23}(u, v, w), \tag{4}$$
$$\sigma(u, vw) = (m \times id)\sigma_{23}\sigma_{12}(u, v, w); \tag{5}$$

2. For any $u \in G$,
$$\sigma(e, u) = (u, e), \qquad \sigma(u, e) = (e, u); \tag{6}$$

3. For any $u, v \in G$,
$$m\sigma(u, v) = uv. \tag{7}$$

Let G be any group. Then $\sigma(u, v) = (v, v^{-1}uv)$ is a braiding operator, called the *conjugate braiding*. The corresponding solution $R(u, v) = (v^{-1}uv, v)$ of the set-theoretical Yang-Baxter equation is the *conjugate solution*. The conjugate solution appeared at the end of [D], and was attributed to Venkov.

Definition Let G and A be groups. Let G act on the left of A as automorphisms, denoted as $(u, a) \mapsto u \cdot a$. A *bijective 1-cocycle* of G with coefficient in A is a bijection $\pi : G \to A$ such that
$$\pi(uv) = \pi(u)(u \cdot \pi(v)), \quad \text{for any } u, v \in G. \tag{8}$$

The definition is consistent with the one in [EG] and differ from the one in [ESS] by inverse. We also remark that if $(u, a) \mapsto u \cdot a$ is only assumed to be an action, then the bijection and the 1-cocycle condition (8) imply the action must be automorphisms of A.

Theorem 2 *Over any group G, the following data are equivalent*

1. *(ξ, η): compatible left and right actions of G on itself;*

2. *σ: braiding operator;*

3. *(A, π): a group acted upon by G as automorphisms and a bijective 1-cocycle of G with coefficient in the group.*

Proof of $(\xi, \eta) \Leftrightarrow \sigma$:

The equivalence between (ξ, η) and σ is simply given by $\sigma(u, v) = \left(^{\xi(u)}v, u^{\eta(v)}\right)$.

First we assume ξ and η are compatible and verify that σ is a braiding operator. Denote

$$\sigma(uv, w) = (u_1, v_1), \qquad (id \times m)\sigma_{12}\sigma_{23}(u, v, w) = (u_2, v_2).$$

A direct computation gives $u_1 = \ ^{\xi(uv)}w$ and $u_2 = \ ^{\xi(u)\xi(v)}w$, which are equal because ξ is a left action. Moreover, the compatibility condition (3) implies that $u_1 v_1 = uvw = u_2 v_2$. Therefore we also have $v_1 = v_2$, and the equality (4) is verified. The equality (5) can be verified in a similar way.

Since ξ is an action, we have $^{\xi(e)}v = v$. Taking $u = e$ in (3), we have $v = \left(^{\xi(e)}v\right)\left(e^{\eta(v)}\right) = v(e^{\eta(v)})$, which implies $e^{\eta(v)} = e$. This proves the first equality in (6). The second equality can be proved similarly.

Finally, the equality (7) is exactly the compatibility condition (3). This completes the proof that σ is a braiding operator.

Conversely, we assume σ is a braiding operator. Then by comparing the first coordinates of (4), we see that $^{\xi(uv)}w = \ ^{\xi(u)\xi(v)}w$. Moreover, the first equality in (6) implies $^{\xi(e)}u = u$. This proves ξ is a left action. Similarly, η is a right action. The compatibility condition (3) then follows directly from (7).

$\square$

Proof of $(\xi, \eta) \Leftrightarrow (A, \pi)$:

Given compatible actions ξ and η, we take $A = G$ with the following product

$$u \star v = u\left(^{\xi(u^{-1})}v\right). \tag{9}$$

By replacing v in the formula with $^{\xi(u)}v$, we find that $uv = u \star\ ^{\xi(u)}v$, which means exactly that $\pi = id : G \to A$ is a bijective 1-cocycle. It remains to show (9) is indeed a group structure, and ξ acts as automorphisms of A.

Clearly, e is a left unit, and $^{\xi(u)}(u^{-1})$ is a right inverse of u with regard to $\star$. By the compatibility condition, we have

$$u \star v = u\left(^{\xi(u^{-1})}v\right) = v\left((u^{-1})^{\eta(v)}\right)^{-1}. \tag{10}$$

Then it is also easy to see that e is also a right unit, and $(u^{\eta(u^{-1})})^{-1}$ is a left inverse of u.

To prove the associativity of $\star$ and ξ acts as automorphisms, we first use compatibility condition (3) to get

$$
\begin{aligned}
\left(^{\xi(u)}(vx)\right)\left(u^{\eta(vx)}\right) &= uvx \\
&= \left(^{\xi(u)}v\right)\left(u^{\eta(v)}\right)x \\
&= \left(^{\xi(u)}v\right)\left(^{\xi(u^{\eta(v)})}x\right)\left((u^{\eta(v)})^{\eta(x)}\right).
\end{aligned}
\tag{11}
$$

Since η is a right action, the right factors on both sides are the same. Thus by canceling the factor and taking $x = {}^{\xi(v^{-1})}w$, we conclude

$$
\begin{aligned}
{}^{\xi(u)}(v \star w) &= {}^{\xi(u)}(vx) \overset{(11)}{=} {}^{\xi(u)}v\, {}^{\xi(u^{\eta(v)})}x \overset{(a)}{=} {}^{\xi(u)}v\, {}^{\xi(u^{\eta(v)}\, v^{-1})}w \\
&\overset{(3)}{=} {}^{\xi(u)}v\, {}^{\xi((\xi(u)}v)^{-1}u)}w \overset{(a)}{=} {}^{\xi(u)}v \star {}^{\xi(u)}w,
\end{aligned}
\tag{12}
$$

where we use (a) to denote the use of the fact that ξ is a left action. Moreover,

$$
\begin{aligned}
u \star (v \star w) &= u\left({}^{\xi(u^{-1})}(v \star w)\right) \overset{(12)}{=} u\left({}^{\xi(u^{-1})}v\right)\left({}^{\xi((\xi(u^{-1})}v)^{-1}u^{-1})}w\right) \\
&= (u \star v)\left({}^{\xi((u\star v)^{-1})}w\right) = (u \star v) \star w.
\end{aligned}
$$

Conversely, we use π to identify A with G, and denote by $\star$ the pullback of the product of A to G. Moreover, we take ξ to be the pullback of the action of G on A. Then the 1-cocycle condition means that (9) holds. Finally, we define η according to the compatibility condition, so that (10) also holds.

It remains to show η is indeed a right action. Since ξ is a left action, we have $e \star e = e({}^{\xi(e^{-1})}e) = e$. This implies that e is also a unit with respect to $\star$. Then by taking $u = e$ in (10), we find $v^{\eta(e)} = v$. On the other hand, by the compatibility condition, we still have the equality (11). Moreover, since ξ acts as automorphisms of $(G, \star)$, we have

$$
{}^{\xi(u)}(vx) = {}^{\xi(u)}(v \star w) = {}^{\xi(u)}v \star {}^{\xi(u)}w = {}^{\xi(u)}v\, {}^{\xi(u^{\eta(v)})}x,
$$

where we used part of the computations in (12) in the last equality. Then we conclude from the equality (11) that

$$
u^{\eta(vx)} = (u^{\eta(v)})^{\eta(x)}.
$$

This completes the proof that η is a right action.

$\square$

Corollary 1 *Any braiding operator is invertible and satisfies the braid relation* (2).

$\square$

We finish the section with two useful properties of braiding operators.

Proposition 2 *Let σ be a braiding operator on a group G. Then $\sigma^2 = \mathrm{id}$ if and only if the star product* (9) *is commutative.*

Proof: We have $\sigma^{-1}(u, v) = \left(((v^{-1})^{\eta(u^{-1})})^{-1}, ({}^{\xi(v^{-1})}(u^{-1}))^{-1}\right)$ from the proof of the invertibility of R in Theorem 1. Therefore $\sigma^2 = \mathrm{id}$ is equivalent to $({}^{\xi(u)}v)((v^{-1})^{\eta(u^{-1})}) = e$. On the other hand, we have $u \star v = u({}^{\xi(u^{-1})}v)$ and $v \star u = u((v^{-1})^{\eta(u)})^{-1}$ from (10). Therefore $\star$ is commutative if and only if $({}^{\xi(u^{-1})}v)((v^{-1})^{\eta(u)}) = e$. This condition is clearly equivalent to the condition for $\sigma^2 = \mathrm{id}$.

$\square$

Proposition 3 *Let σ be a braiding operator on a group G. If $\sigma(u,v) = (y,x)$, then*

$$\sigma(x^{-1}, y^{-1}) = (v^{-1}, u^{-1}), \quad \sigma(u^{-1}, y) = (v, x^{-1}), \quad \sigma(x, v^{-1}) = (y^{-1}, u).$$

Proof: The equality $\sigma(x^{-1}, y^{-1}) = (v^{-1}, u^{-1})$ can be found in the proof of the invertibility of R in Theorem 1. To prove $\sigma(u^{-1}, y) = (v, x^{-1})$, we note that $^{\xi(u^{-1})}y = v$ implies $\sigma(u^{-1}, y) = (v, z)$ for some z. Then from the compatibility condition (7) we have $u^{-1}y = vz$. On the other hand, by applying the compatibility condition to $\sigma(u, v) = (y, x)$, we have $uv = yx$. Thus we conclude that $z = x^{-1}$. The proof of the equality $\sigma(x, v^{-1}) = (y^{-1}, u)$ is similar.

$\square$

3   Comparison with known solutions

Besides the conjugate solution, there have been two general methods for constructing set-theoretical solutions of the Yang-Baxter equation, given by Weinstein and Xu [WX], and Etingof, Schedler, and Soloviev [ESS]. The reformulation in terms of bijective 1-cocycles indicates that our construction generalizes the one in [ESS]. In this section, we will compare our construction with the conjugate solution and the solution in [WX].

Denote the conjugate braiding operator on $(G, \star)$ by

$$\sigma^\star(u, v) = (v \,, \, v^{\star -1} \star u \star v),$$

where

$$v^{\star -1} = \, ^{\xi(v)}(v^{-1}) = (v^{\eta(v^{-1})})^{-1}$$

is the inverse with respect to the new group structure.

Theorem 3 *Let σ be a braiding operator on a group G. Let $\sigma^\star$ be the conjugate braiding operator induced by σ. Then the transformation*

$$T_n(u_1, u_2, \cdots, u_{n-1}, u_n) = \left(u_1 \,, \, ^{\xi(u_1)}u_2 \,, \, \cdots \,, \, ^{\xi(u_1 \cdots u_{n-2})}u_{n-1} \,, \, ^{\xi(u_1 \cdots u_{n-1})}u_n \right)$$

is an equivalence between the two actions of the braid group B_n on G^n induced by σ and $\sigma^\star$.

In Proposition 1.7 of [ESS], Etingof, Schedler, and Soloviev showed that the action of the braid group B_n on G^n induced by their solution is equivalent to the usual action via the symmetric group S_n. Note that the action via the symmetric group S_n is induced by the conjugate solution in an abelian group structure. Thus the theorem generalizes the result in [ESS].

We emphasize that the conjugation is with regard to a *different* group structure on G. Moreover, although the braid group actions are equivalent, the underlying solutions of the Yang-Baxter equation are not necessarily equivalent.

Proof of Theorem 3: It is quite easy to see that T_n is invertible. We mainly need to show that T_n intertwines the two actions.

First we consider the beginning case $n = 2$. The equality $T_2\sigma = \sigma^\star T_2$ means

$$\xi^{(\xi^{(u)}v)}(u^{\eta(v)}) = \left({}^{\xi^{(u)}}v\right)^{-1} \star u \star \left({}^{\xi^{(u)}}v\right). \tag{13}$$

We have

$$u \star \left({}^{\xi^{(u)}}v\right) = u \star {}^{\xi^{(u^{-1})}}\left({}^{\xi^{(u)}}v\right) = uv. \tag{14}$$

If we substitute u and v by ${}^{\xi^{(u)}}v$ and $u^{\eta(v)}$ in (14), then we have

$$\xi^{(u)}v \star \left({}^{\xi^{(\xi^{(u)}v)}}(u^{\eta(v)})\right) = \left({}^{\xi^{(u)}}v\right)(u^{\eta(v)}) = uv. \tag{15}$$

Comparing (14) and (15), we have $u \star \left({}^{\xi^{(u)}}v\right) = {}^{\xi^{(u)}}v \star \left({}^{\xi^{(\xi^{(u)}v)}}(u^{\eta(v)})\right)$, which proves (13).

In general, let $\sigma_{i,i+1}$ and $\sigma^\star_{i,i+1}$ be the actions of the braid group B_n on G^n induced from σ and $\sigma^\star$. Then we need to show

$$T_n\sigma_{i,i+1} = \sigma^\star_{i,i+1}T_n, \qquad i = 1, 2, \cdots, n-1. \tag{16}$$

By induction, we assume (16) holds for $n-1$. Denote

$$U_n(u_1, u_2, \cdots, u_{n-1}, u_n) = (u_1, {}^{\xi^{(u_1)}}u_2, \cdots, {}^{\xi^{(u_1)}}u_{n-1}, {}^{\xi^{(u_1)}}u_n).$$

Since ξ is a left action, we have

$$T_n = U_n(\mathrm{id} \times T_{n-1}). \tag{17}$$

Since ξ is automorphisms of $(G, \star)$, we have

$$\xi^{(w)}(v^{\star-1} \star u \star v) = \left({}^{\xi^{(w)}}v\right)^{\star-1} \star {}^{\xi^{(w)}}u \star {}^{\xi^{(w)}}v.$$

It is easy to see that this implies

$$U_n\sigma^\star_{i,i+1} = \sigma^\star_{i,i+1}U_n \tag{18}$$

for $i \geq 2$. Combining (17), (18), and the inductive hypothesis, we conclude that (16) holds for $i \geq 2$. Finally, the equality $T_n\sigma_{1,2} = \sigma^\star_{1,2}T_n$ is the same as $T_2\sigma = \sigma^\star T_2$, which has already been proved.

$\square$

Now we turn to the solution given by Weinstein and Xu in [WX].

For two subgroups G_+ and G_- of G, we say that $G = G_+ G_-$ is a *unique factorization* if for any $g \in G$, there are unique $g_+ \in G_+$ and $g_- \in G_-$ such that $g = g_+ g_-$. We will denote $(g_+)^{-1} \in G_+$ and $(g_-)^{-1} \in G_-$ simply by g_+^{-1} and g_-^{-1}. The unique factorization induces a left action of the product group $G_+ \times G_-$ on G by

$$(g_+, g_-) \cdot a = g_- a g_-^{-1}.$$

Moreover, it is easy to verify that

$$\pi(g_+, g_-) = g_+ g_-^{-1}$$

is a bijective 1-cocycle of $G_+ \times G_-$ with coefficient in G. From these data, we may construct a set-theoretical solution of the braid relation over $G_+ \times G_-$. Then we may use the bijection π to translate the solution to get a solution over G. A detailed computation shows that this solution is

$$\sigma(g, h) = \left(h_-^{-1} g h_- , \, (h_-^{-1} g h_-)_+^{-1} h (h_-^{-1} g h_-)_+ \right).$$

This solution appeared in Theorem 9.2 of [WX], under the assumption that G is a factorizable Poisson Lie group (we also note that g_- is defined in [WX] by the equality $g = g_+ g_-^{-1}$, so that in their formula, the negative elements differ from ours by inverse).

4 A universal construction

Let a bijective map $\sigma : S \times S \to S \times S$ be a solution of the braid relation (2) on a set S. Denote

$$\sigma(u, v) = (y, x). \tag{19}$$

We call σ *non-degenerate* if

(i) For any fixed u, the map $v \mapsto y : S \to S$ is bijective;

(ii) For any fixed v, the map $u \mapsto x : S \to S$ is bijective.

A non-degenerate solution has the following property.

Lemma 4 *Suppose $\sigma : S \times S \to S \times S$ is non-degenerate. Then*

1. *For any (u, y), there is unique (v, x) such that (19) holds;*

2. *For any (v, x), there is unique (u, y) such that (19) holds.*

Proof of Lemma 4: Suppose u, y are given. Then we fix u and find the unique v corresponding to y via (i). Once v is found, we may fix v and further find the unique x corresponding to u via (ii). This proves the first statement. The second statement can be proved similarly.

$\square$

The best way to understand and utilize the conclusion of Lemma 4 is through the graphical interpretation. It is well known that a solution (19) of the braid relation fits into the braiding scheme in Figure 1 (which we will call a σ-*square*).
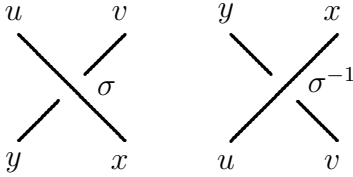
Figure 1: σ-square and σ^{-1}-square

The bijectivity of σ means that any row determines the whole σ-square. The conclusion of Lemma 4 means that any column determines the whole σ-square. Moreover, the braid relation means that, if we start with the same triple (u, v, w), then the two chains of three σ-squares in Figure 2 will give the same results (z, y, x) at the bottoms (note that the two braids are topologically equivalent).
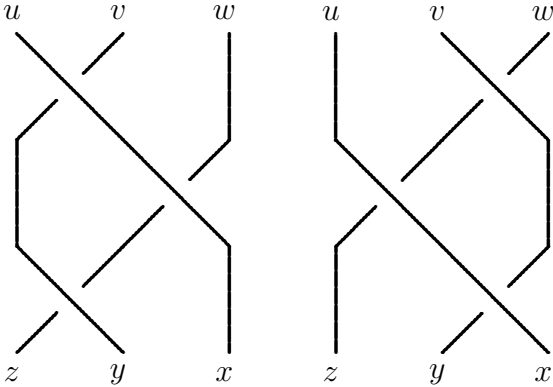
Figure 2: braid relation

The purpose of this section is to construct a universal group $G = G(S, \sigma)$ with a braiding operator σ^G from a set S and a non-degenerate set-theoretical solution σ of the braid relation on S.

As in [ESS], we take the group G to be generated by the set S, subject to the relation

$$uv = yx, \qquad \text{whenever } \sigma(u, v) = (y, x),$$

10

which is necessary by the compatibility condition on σ. Then we need to extend σ to a braiding operator σ^G on G. To construct σ^G, we need to know in detail how G is constructed. Let S' be another copy of S, with $x' \in S'$ denoting the element corresponding to $x \in S$. Let $\bar{S}$ be the disjoint union of S and S'. Let

$$U(S) = \coprod_{i=0}^{\infty} \bar{S}^i = \{e\} \coprod \bar{S} \coprod \bar{S} \times \bar{S} \coprod \bar{S} \times \bar{S} \times \bar{S} \coprod \cdots$$

be the free monoid generated by $\bar{S}$. Let $\sim$ be the equivalence relation on $U(S)$ generated by $guu'h \sim gh$, $gu'uh \sim gh$, and $guvh \sim gyxh$ whenever $\sigma(u,v) = (y,x)$, where $g, h \in U(S)$ and $u, v, x, y \in S$. Then $G = U(S)/\sim$.

We start the construction of σ^G by extending σ to $\bar{S}$. Note that $x' \in S'$ will become x^{-1} in G. Therefore by Proposition 3, the extension $\bar{\sigma} : \bar{S} \times \bar{S} \to \bar{S} \times \bar{S}$ should be given as follows: If $\sigma(u,v) = (y,x)$, then

$$\bar{\sigma}(u,v) = (y,x), \quad \bar{\sigma}(x',y') = (v',u'), \quad \bar{\sigma}(u',y) = (v,x'), \quad \bar{\sigma}(x,v') = (y',u).$$

By the discussion after the proof of Lemma 4, our assumption implies that $\bar{\sigma}$ is well-defined.

The definition of $\bar{\sigma}$ has the graphical interpretation that the σ-square in Figure 1 induces the $\bar{\sigma}$-squares in Figure 3.
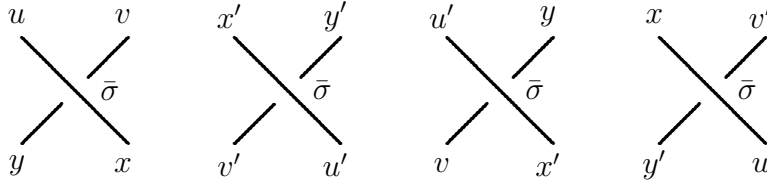

Figure 3: definition of $\bar{\sigma}$

Proposition 5 $\bar{\sigma}$ *satisfies the braid relation.*

Proof: $\bar{S} \times \bar{S} \times \bar{S}$ is a disjoint union of eight subsets of the form $S_1 \times S_2 \times S_3$, where each S_i is either S or S'. We will show that $\bar{\sigma}$ satisfies the braid relation on $S \times S \times S$, $S \times S \times S'$, and $S \times S' \times S$. The other cases can be similarly proved.

(1) Braid relation on $S \times S \times S$

This follows from the fact that σ satisfies the braid relation.

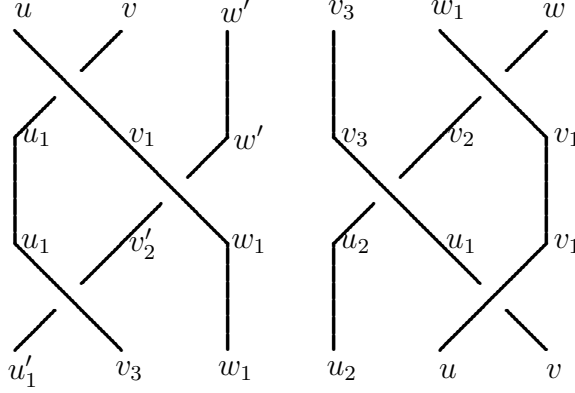(2) Braid relation on $S \times S \times S'$

11

Figure 4: $\bar{\sigma}_{12}\bar{\sigma}_{23}\bar{\sigma}_{12}$ on $S \times S \times S'$

For $(u, v, w') \in S \times S \times S'$, the triple $\bar{\sigma}_{12}\bar{\sigma}_{23}\bar{\sigma}_{12}(u, v, w')$ is computed as in the left graph in Figure 4. According to Figure 3, the left graph is equivalent to the right graph.

By Lemma 4, we see that u, v, w in the right graph in Figure 4 successively determine the other elements $u_1, v_1, w_1, v_2, v_3, u_2$ in the graph.

On the other hand, the triple $\bar{\sigma}_{23}\bar{\sigma}_{12}\bar{\sigma}_{23}(u, v, w')$ is computed as in the left graph in Figure 5. According to Figure 3, the left graph is equivalent to the middle graph. Furthermore, by the braid relation (see Figure 2) and the bijectivity of σ, the middle graph gives rise to the right graph.
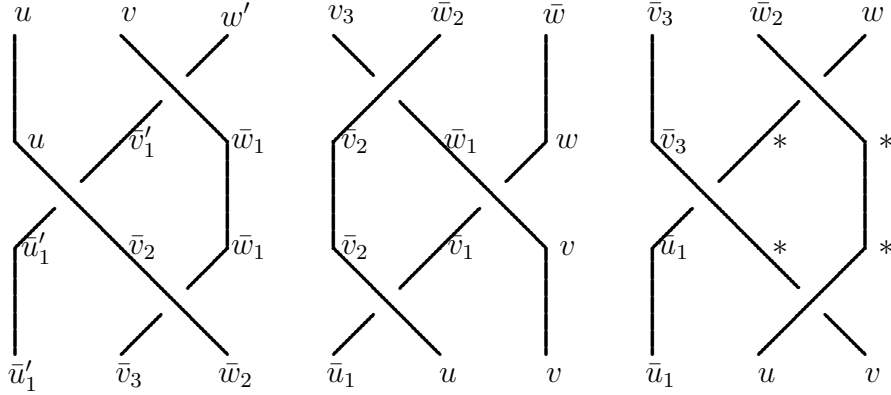
Figure 5: $\bar{\sigma}_{23}\bar{\sigma}_{12}\bar{\sigma}_{23}$ on $S \times S \times S'$

Note that the right graphs in Figures 4 and 5 have the same structures and the same u, v, w. As we have argued before, the other elements in the graphs must be the same. Thus we conclude that

$$\bar{\sigma}_{12}\bar{\sigma}_{23}\bar{\sigma}_{12}(u, v, w') = (u'_2, v_3, w_1) = (\bar{u}'_1, \bar{v}_3, \bar{w}_2) = \bar{\sigma}_{23}\bar{\sigma}_{12}\bar{\sigma}_{23}(u, v, w').$$

12

(3) Braid relation on $S \times S' \times S$

For $(u, v', w) \in S \times S' \times S$, the triples $\bar{\sigma}_{12}\bar{\sigma}_{23}\bar{\sigma}_{12}(u, v', w)$ and $\bar{\sigma}_{23}\bar{\sigma}_{12}\bar{\sigma}_{23}(u, v', w)$ are computed as in the graphs in Figure 6. According to Figure 3, the graphs are equivalent to six basic σ squares, four of which fit into a braid relation (see Figure 7).
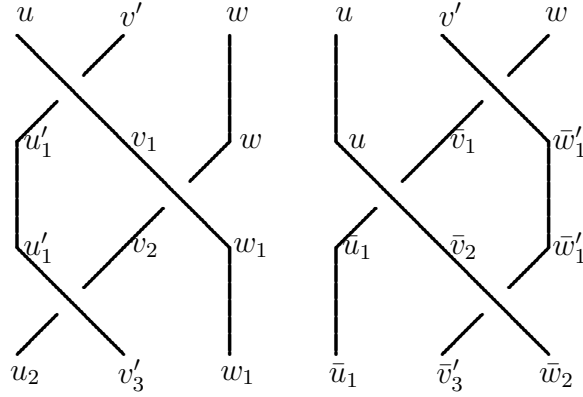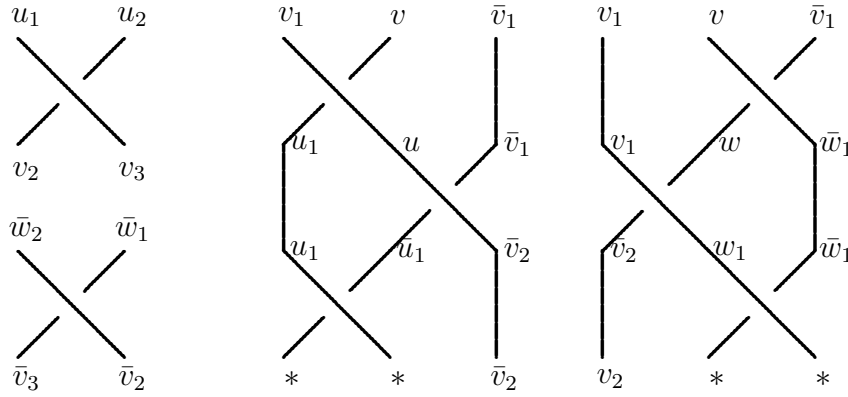

Figure 6: braid relation on $S \times S' \times S$

Figure 7: interpreting braid relation on $S \times S' \times S$

Since the end results of the braid relation in Figure 7 must be the same, we conclude that the result is of the form $(v_2, z, \bar{v}_2)$. Thus we get two σ-squares in Figure 8.

Comparing these σ-squares in Figure 8 with the σ-squares in Figure 7, we have

$$u_2 = \bar{u}_1, \qquad v_3 = z = \bar{v}_3, \qquad w_1 = \bar{w}_2$$

from the bijectivity of σ. This further implies

$$\bar{\sigma}_{12}\bar{\sigma}_{23}\bar{\sigma}_{12}(u, v', w) = (u_2, v'_3, w_1) = (\bar{u}_1, \bar{v}'_3, \bar{w}_2) = \bar{\sigma}_{23}\bar{\sigma}_{12}\bar{\sigma}_{23}(u, v', w).$$
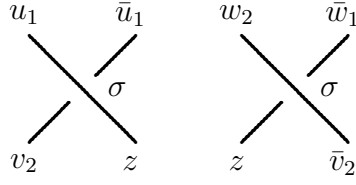
13

Figure 8: two σ-squares from $S \times S' \times S$

$\square$

Next we extend $\bar{\sigma}$ to σ^U over $U(S)$. The extension can be better understood through the graphical meaning of the braid relation.

The idea for the definition of σ^U comes from (4) and (5). Note that the product of $u, v \in \bar{S}$ in $U(S)$ is simply the pair $(u, v) \in \bar{S}^2$. Therefore if σ^U satisfies (4) and (5), then we should have

$$\sigma^U((u, v), w) = \bar{\sigma}_{12}\bar{\sigma}_{23}(u, v, w), \qquad \sigma^U(u, (v, w)) = \bar{\sigma}_{23}\bar{\sigma}_{12}(u, v, w),$$

where the triples on the right sides are considered as in $\bar{S} \times \bar{S}^2$ and $\bar{S}^2 \times \bar{S}$ because $(1 \times m)(u, v, w) = (u, (v, w))$ and $(m \times 1)(u, v, w) = ((u, v), w)$ in $U(S)$. Figure 9 provides the graphical interpretation of the definitions.
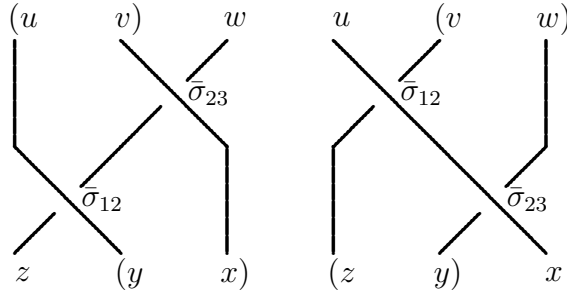

Figure 9: σ^U on $\bar{S} \times \bar{S}^2$ and $\bar{S}^2 \times \bar{S}$

This leads to the natural generalization that defines $\sigma^U((u_1, \cdots, u_m), (v_1, \cdots, v_n))$. For example, the graph in Figure 10 suggests us to define

$$\sigma^U((u_1, u_2, u_3), (v_1, v_2)) = \bar{\sigma}_{23}\bar{\sigma}_{12}\bar{\sigma}_{34}\bar{\sigma}_{23}\bar{\sigma}_{45}\bar{\sigma}_{34}((u_1, u_2, u_3), (v_1, v_2)).$$

In general, we define $\sigma^U : U(S) \times U(S) \to U(S) \times U(S)$ by
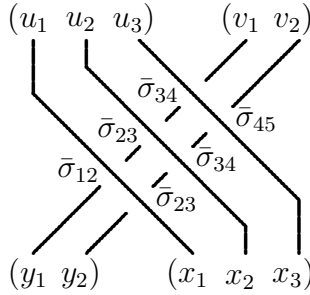
1. $\sigma^U(e, u) = (u, e)$, $\sigma^U(u, e) = (e, u)$;

14

Figure 10: σ^U on $\bar{S}^3 \times \bar{S}^2$

2. on $\bar{S}^m \times \bar{S}^n$, $m, n \geq 1$,

$$\begin{aligned}
\sigma^U &= (\bar{\sigma}_{n,n+1} \cdots \bar{\sigma}_{23}\bar{\sigma}_{12})(\bar{\sigma}_{n+1,n+2} \cdots \bar{\sigma}_{34}\bar{\sigma}_{23}) \\
&\cdots\cdots (\bar{\sigma}_{n+m-1,n+m} \cdots \bar{\sigma}_{m+1,m+2}\bar{\sigma}_{m,m+1}),
\end{aligned}$$

and the image is considered to be in $\bar{S}^n \times \bar{S}^m$.

It is easy to see (from the graphical interpretation, for example) that the definition above is equivalent to the requirement that the first two conditions for σ^U to be a braiding operator on $U(S)$ (conditions (4), (5), and (6)) are satisfied. Moreover, σ^U still satisfies the braid relation. This can be seen graphically by "thickening" each of the three threads in Figure 2 into parallel threads. The result is a pair of graphs that are related by a sequence of the usual braid relations (i.e., Figure 2) with some additional vertical lines (i.e., identity maps) added on both sides. For example, the graphs in Figure 11 shows that σ^U satisfies the braid relation over $\bar{S}^3 \times \bar{S}^2 \times \bar{S}^2$.
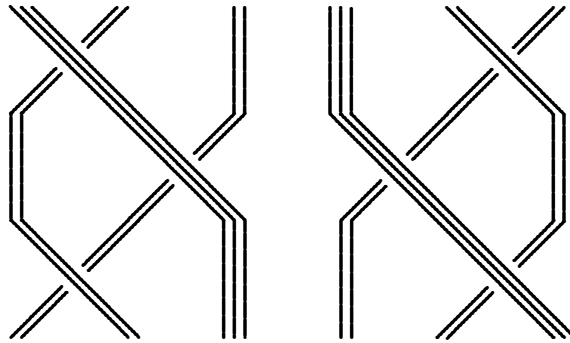

Figure 11: braid relation for σ^U on $\bar{S}^3 \times \bar{S}^2 \times \bar{S}^2$

It remains to reduce the operator σ^U over $U(S)$ to an operator σ^G over G. We first consider the reduction with respect to the relations $guu'h \sim gh$ and $gu'uh \sim gh$ in $U(S)$.

15

Note that in case $\sigma(u, v) = (y, x)$, it is easy to show $\sigma^U((u, u'), y) = (y, (x, x'))$ by the graph in Figure 12.
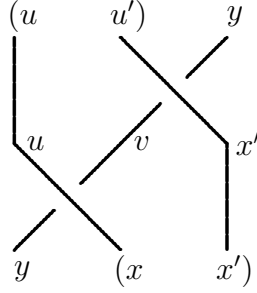

Figure 12: a special case of σ^U consistent with $uu' \sim e$

Now for $g, h, k \in U(S)$, we embed several copies (number $=$ length of k) of the graph in Figure 12 (with various y) into the graph for the definition of $\sigma^U(gh, k)$. The result, as shown in Figure 13 (the region bounded by the dotted square is where the embedding happens), is the graph for the definition of $\sigma^U(guu'h, k)$.
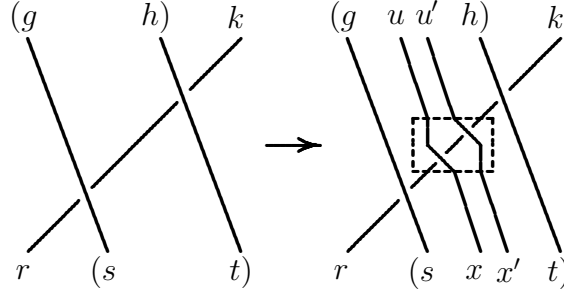

Figure 13: a general case of σ^U consistent with $uu' \sim e$

It is easy to see from the graphs in Figure 13 that $\sigma^U(guu'h, k)$ is obtained from $\sigma^U(gh, k)$ by inserting some xx' in an appropriate place. Similarly, $\sigma^U(g, huu'k)$, $\sigma^U(guu'h, k)$, and $\sigma^U(g, hu'uk)$ are obtained from $\sigma^U(g, hk)$ and/or $\sigma^U(gh, k)$ by inserting some xx' and/or $x'x$ in some appropriate place. This implies that σ^U is consistent with the relations $guu'h \sim gh$ and $gu'uh \sim gh$.

Next, we consider the reduction with respect to the relation $guvh \sim gyxh$ whenever $\sigma(u, v) = (y, x)$. Again we first consider the simplest case. Suppose $u, v, w \in S$, $\sigma(u, v) = (y, x)$, and
$$\sigma^U((u, v), w) = (r_1, s_1, t_1), \qquad \sigma^U((y, x), w) = (r_2, s_2, t_2).$$

16

By the braid relation, the two graphs in Figure 14 should have the same outcome at the bottoms. In particular, we conclude that $r_1 = r_2$ and $\sigma(s_1, t_1) = (s_2, t_2)$. Moreover, the argument above also applies to the case that some of u, v, w are assumed to be in S', because of Proposition 5. As in the proof of the consistency with the relations $guu'h \sim gh$ and $gu'uh \sim gh$, we may embed Figure 14 (and its generalization over $\bar{S}$) into the graphs for the definitions of $\sigma^U(guvh, k)$ and $\sigma^U(gyxh, k)$ and find that $\sigma^U(gyxh, k)$ is obtained from $\sigma^U(guvh, k)$ by applying σ at an appropriate adjacent pair of coordinates. The similar statements can be proved regarding $\sigma^U(g, huvk)$ and $\sigma^U(g, hyxk)$. This implies that σ^U is consistent with the relation $guvh \sim gyxh$.
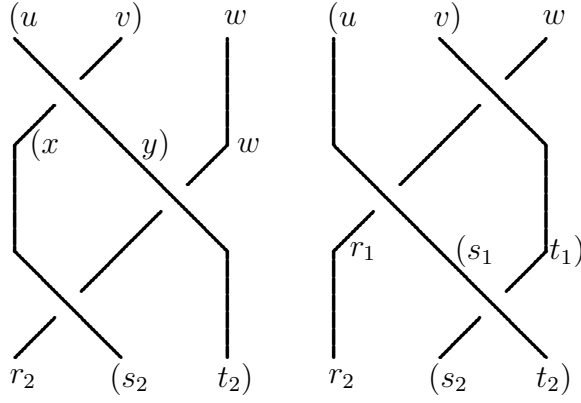

Figure 14: a special case of σ^U consistent with $uv \sim yx$

Thus we have shown that σ^U can be reduced to an operator σ^G on G. Since σ^U satisfies the conditions (4), (5), and (6), σ^G satisfies the same conditions. To conclude σ^G is a braiding operator, it remains to explain that σ^G satisfies the compatibility condition (7). But this is quite obvious because by the definition, $(g, h) \in U(S) \times U(S)$ and $\sigma^U(g, h)$ differ by the successive applications of σ on some adjacent pairs of coordinates in the words (i.e., ignore the parenthesis). Such applications of σ are considered as identity in G. Therefore we conclude that $gh \in G$ is equal to the multiplication of the two coordinates in $\sigma^G(g, h) \in G \times G$.

Now we are ready to state the main result of this section.

Theorem 4 *Let a bijective map $\sigma : S \times S \to S \times S$ be a non-degenerate solution of the braid relation. Let $G(S, \sigma)$ be the group generated by S and subject to the relation $uv \sim yx$ whenever $\sigma(u, v) = (y, x)$. Let $i : S \to G(S, \sigma)$ be the canonical map. Then*

1. *There is a unique braiding operator σ^G on $G(S, \sigma)$ such that $\sigma^G(i \times i) = (i \times i)\sigma$;*

17

2. *The group $G(S,\sigma)$ and the braiding operator σ^G have the following universal prop-*
   erty: If σ' is a braiding operator on a group G', and $f : S \to G'$ is a braiding-
   preserving map, then there is a unique braiding-preserving group homomorphism
   $\phi : G \to G'$ such that $f = \phi i$.

We have shown the existence of σ^G by constructing it. The uniqueness follows from the conditions (4), (5), and (6), as we have explained when we defined σ^U. The universal property is also tautological from the construction.

In the special case $\sigma^2 = id$ studied in [ESS], it is not difficult to use the graphical interpretation to show that $(\sigma^G)^2 = id$. By Proposition 2, the star product (9) on the universal group $G(S,\sigma)$ is commutative. Then it is easy to show that $(G(S,\sigma),\star)$ is in fact free abelian with S as a basis. In particular, i is an embedding, and we recover the classification theorem in [ESS].

In general, a set-theoretical solution of the Yang-Baxter equation is embedded in a group with a braiding operator if and only if the canonical map $i : S \to G(S,\sigma)$ into the universal construction is an embedding. However, we feel that the canonical map is probably not always an embedding.

We end the paper with a remark on the universal group $G(S,\sigma)$.

Proposition 6 *If S is a finite set, then $G(S,\sigma)$ has a finitely generated abelian normal subgroup of finite index.*

Proof: Let $P(i(\bar{S}))$ be the permutation group of $i(\bar{S}) = i(S) \cup i(S)^{-1}$, the image of S and the inverses in $G(S,\sigma)$. Since σ^U exchanges $\bar{S}^i \times \bar{S}$ and $\bar{S} \times \bar{S}^i$, the actions ξ and η (associated to σ^G) induce a homomorphism and an anti-homomorphism of groups

$$\xi_{\bar{S}}, \eta_{\bar{S}} : \quad G(S,\sigma) \to P(i(\bar{S})).$$

Since $P(i(\bar{S}))$ is finite, $A = \ker \xi_{\bar{S}} \cap \ker \eta_{\bar{S}}$ is a normal subgroups of finite index. We claim that A is abelian.

Suppose $g \in \ker \eta_{\bar{S}}$. Then $i(u)^{\eta(g)} = i(u)$ for any $u \in \bar{S}$. By the compatibility condition (3), we also have $i(u)g = (^{\xi(i(u))}g)(i(u)^{\eta(g)}) = (^{\xi(i(u))}g)i(u)$. Therefore we conclude

$$^{\xi(i(u))}g = i(u)gi(u)^{-1}. \tag{20}$$

Suppose we have shown $h^{\eta(g)} = h$ for all elements $h \in G(S,\sigma)$ of length $\leq n-1$ (with regard to the generating set $\bar{S}$). Then we write an element of length $\leq n$ as $h\,i(u)$, where h has length $\leq n-1$ and $u \in \bar{S}$. By condition (4), we have

$$(h\,i(u))^{\eta(g)} = h^{\eta(^{\xi(i(u))}g)}i(u)^{\eta(g)} = h^{\eta(i(u)gi(u)^{-1})}i(u), \tag{21}$$

where we use $g \in \ker \eta_{\bar{S}}$ and (20) in the last equality. From the definition of σ^U, we see that $h^{\eta(i(u))}$ still has length $\leq n-1$. Thus by the inductive assumption, we have

$$h^{\eta(i(u)gi(u)^{-1})} = \left((h^{\eta(i(u))})^{\eta(g)}\right)^{\eta(i(u)^{-1})} = \left(h^{\eta(i(u))}\right)^{\eta(i(u)^{-1})} = h. \tag{22}$$

Combining (21) and (22) together, we conclude that $\eta(g)$ fixes $hi(u)$.

Thus we have shown that any $g \in \ker \eta_{\bar{S}}$ actually fixes the whole group $G(S, \sigma)$ under η. Similarly, any $g \in \ker \xi_{\bar{S}}$ fixes the whole group $G(S, \sigma)$ under ξ. Therefore if $g, h \in A$, then we have

$$\sigma^G(g, h) = (^{\xi(g)}h, g^{\eta(h)}) = (h, g).$$

By the compatibility condition (3), this further implies $gh = hg$. This proves that A is abelian.

Finally, A is finitely generated because a subgroup A of a finitely generated group $G(S, \sigma)$ of finite index is always finitely generated. This fact can be proved, for example, by considering the pullback to the finitely generated free group with a homomorphism onto $G(S, \sigma)$.

$\square$

The subgroup A constructed in the last proposition contains all the "trivial" actions of $G(S, \sigma)$, so that it does not essentially contribute to the construction of our solution. In the special case $\sigma^2 = id$, we already know $(G(S, \sigma), \star)$ is a free abelian group of rank $|S|$. Then the triviality of A acting on $G(S, \sigma)$ implies that the original product and the new star product coincide on A. Therefore A is also a subgroup of $(G(S, \sigma), \star)$ of finite index, and A itself must be a free abelian group of rank $|S|$.

This leaves the interesting question of the rank of A in general. We suspect the rank is also $|S|$. But we do not know how to show it.

References

[D] Drinfel'd, V., On some unsolved problems in quantum group theory, *Lecture Notes in Mathematics* **1510** (1992), 1-8.

[EG] Etingof, P., Gelaki, S., A method of construction of finite dimensional triangular semisimple Hopf algebras, *Math. Res. Lett.* **5** (1998), 551 - 561.

[ESS] Etingof, P., Schedler, T. and Soloviev, A., Set-theoretical solutions to the quantum Yang-Baxter equation, *to appear in Duke Math. J.*

[LYZ1] Lu, J.-H., Yan, M., and Zhu, Y.-C., On Hopf algebras with positive bases. *Preprint*, 1998.

[LYZ2] Lu, J.-H., Yan, M., and Zhu, Y.-C., Quasi-triangular structures on Hopf algebras with positive bases. *Preprint*, 1999.

[WX] Weinstein, A. and Xu, P., Classical solutions of the quantum Yang-Baxter equation, *Comm. Math. Phys.* **148** (1992), 309 - 343.