Abelian fixed point free endomorphisms and the Yang-Baxter equation

Alan Koch, Laura Stordy and Paul J. Truman

ABSTRACT. We obtain a simple family of solutions to the set-theoretic Yang-Baxter equation, one which depends only on considering special endomorphisms of a finite group. We show how such an endomorphism gives rise to two non-degenerate solutions to the Yang-Baxter equation, solutions which are inverse to each other. We give concrete examples using dihedral, alternating, symmetric, and metacyclic groups.

CONTENTS

1. Introduction

In the span of just a few years, Chen-Ning Yang [23], working in theoretical physics, and Rodney Baxter [2], working in statistical mechanics, independently developed an equation which is now commonly referred to as the *Yang-Baxter equation*. The Yang-Baxter equation has been found to have applications in many areas of mathematics and physics, including quantum groups [20], knots [13, 15], analysis of integrable systems [14], and quantum computing [7].

The Yang-Baxter equation describes a relationship between functions, namely

$$(R \otimes 1)(1 \otimes R)(R \otimes 1) = (1 \otimes R)(R \otimes 1)(1 \otimes R),$$

where $R \in \text{End}(V \otimes V)$ for some finite dimensional vector space V. Interesting solutions of this equation are difficult to find, so an easier problem was introduced by Drinfeld in [10]: that of finding *set-theoretic solutions*, where V is replaced by a finite set B, and tensor product replaced by the cross product. Given such a set-theoretic solution on B, one obtains a solution for a vector space with B as a basis.

Many interesting example of set-theoretic solutions start to appear when B carries some additional structure. For example, if $B = (B, \cdot)$ is an abelian group then Rump [21] showed how to construct solutions to the Yang-Baxter equation by giving B the structure of a *left brace*, where $(B, \cdot)$ is endowed with another binary operation $\circ$ such that $(B, \circ)$ is a group and a certain relation holds. The corresponding solutions to the equation were both *non-degenerate* (see section 2) and *involutive* (i.e., self-inverse).

Later, the concept of left brace was generalized by Guarnieri and Vendramin [12] to the case where $(B, \cdot)$ is nonabelian, obtaining a *(left) skew brace*. Skew braces correspond to non-degenerate solutions of the Yang-Baxter equations which are non-involutive, though one can easily compute the inverse to any solution [16].

Thus, identifying set-theoretic solutions to the Yang-Baxter equation reduces to finding skew braces. But skew braces may not be easy to find: they involve putting two (potentially) different group structures on B that interact with each other in a precise way. A breakthrough was obtained in 2016 by Bachiller [1], who observed a correspondence between skew braces and Hopf-Galois structures on Galois field extensions, a subject which had been studied for 30 years by numerous people–see, e.g., [18], [6], [8], [5]. The classification of Hopf-Galois structures on a Galois extension with Galois group G follows from a theorem of Greither and Pareigis, and amounts to finding regular subgroups N of $\text{Perm}(G)$, satisfying a certain stability condition. Given $N \leq \text{Perm}(G)$ as above, a skew brace can be constructed where one of the underlying groups is isomorphic to N, the other to G.

But Hopf-Galois theory still involves two groups interacting in a very precise way. In 2013, Childs [9] developed a technique using *fixed point free abelian endomorphisms* (definition 4.1 below) of a group G to construct a certain class of suitable regular subgroups, hence of Hopf-Galois structures.

In this work, we use Childs' theory to construct explicit solutions to the Yang-Baxter equation. If $\psi : G \to G$ is a fixed point free abelian endomorphism, then one can obtain a regular subgroup of $\text{Perm}(G)$. Here, we

construct the skew brace $\mathfrak{B}_\psi$ associated to ψ, and then we find a solution to the Yang-Baxter equation based on $\mathfrak{B}_\psi$. We then use the theory of opposite braces in [16] to develop a second solution, namely, the inverse to the first solution. In short, we prove the following.

Theorem (Theorem 5.1). Let G be a finite group.
  (1) Let $\psi : G \to G$ be a fixed point free abelian endomorphism. Let $R_\psi, R'_\psi : G \times G \to G \times G$ be given by

$$R_\psi(g,h) = \big(\psi(g^{-1})h\psi(g), \psi(hg^{-1})h^{-1}\psi(g)g\psi(g^{-1})h\psi(gh^{-1})\big)$$
$$R'_\psi(g,h) = \big(g\psi(g^{-1})h\psi(g)g^{-1}, \psi(h)g\psi(h^{-1})\big)$$

  Then:
    (a) Both R_ψ and R'_ψ are non-degenerate, set-theoretic solutions to the Yang-Baxter equation.
    (b) The functions R_ψ and R'_ψ are inverse to each other.
  (2) Two fixed point free abelian endomorphisms $\psi_1, \psi_2 : G \to G$ give *equivalent* solutions to the Yang-Baxter equation R_{ψ_1}, R_{ψ_2} if and only if $\psi_2 = \varphi\psi_1\varphi^{-1}$ for some $\varphi \in \mathrm{Aut}(G)$.

In section 3, we define precisely the concepts of *type* of solution and *equivalence* of solutions.

The significance of this result lies in its simplicity. Although the proof presented here uses the Greither-Pareigis correspondence for Hopf-Galois structures on separable field extensions and the theory of skew braces, the reader can generate pairs of solutions to the Yang-Baxter equation without a deep understanding of these concepts: one simply needs to be familiar with elementary group theory.

We start by describing, in greater detail, the Yang-Baxter equation. Then, we give an overview of Greither-Pareigis theory, which we then connect to skew braces which, in turn, give us set-theoretic solutions to the Yang-Baxter equation. Next, we discuss fixed-point free abelian endomorphisms on a finite group G and we explicitly construct a brace corresponding to such an endomorphism. We then prove the main result above (with some minor differences in notation) in Section 5. Finally, we provide examples in which G is dihedral, alternating, symmetric, or metacyclic.

Unless otherwise specified, we assume all groups (and braces) are finite.

2. The Yang-Baxter equation and its solutions

Let V be a finite dimensional vector space over some field K. A *solution* to the Yang-Baxter equation is a K-linear map $R : V \otimes V \to V \otimes V$ such

that

$$(R \otimes I)(I \otimes R)(R \otimes I) = (I \otimes R)(R \otimes I)(I \otimes R) : V \otimes V \otimes V \to V \otimes V \otimes V,$$

where $I : V \to V$ is the identity map. If we view $R \in M_{n^2}(K)$ where $\dim_K V = n$ then R is what is called an *R-matrix*. As a way to develop non-trivial examples of solutions, in [10], Drinfeld suggests considering set-theoretic solutions to the Yang-Baxter equation, that is, a set B and a function $R : B \times B \to B \times B$ such that

$$(R \times \mathrm{id})(\mathrm{id} \times R)(R \times \mathrm{id}) = (\mathrm{id} \times R)(R \times \mathrm{id})(\mathrm{id} \times R)$$

holds, where id is the identity map on B. If B is finite, we let V_B be the K-vector space with basis B; then a set theoretic solution on B gives a vector space solution on V_B.

A set-theoretic solution $R : B \times B \to B \times B$ is said to be *non-degenerate* if the functions $f_y, g_x : B \to B$ given by $R(x, y) = (f_y(x), g_x(y))$ are invertible. As above, we say R is *involutive* if $R^2 = \mathrm{id}$.

In the work being presented here, the set B will carry the structure of a (finite) group, say G, and the set-theoretic solutions will rely heavily on the group operation. Working with G will allow us to identify V_G naturally with $K[G]$, thereby naturally obtaining R-matrices on group algebras.

3. Regular subgroups, braces, and solutions to the YBE

In this section, we introduce many of the structures needed to prove Theorem 5.1. We start with the definition of regular G-stable subgroups of $\mathrm{Perm}(G)$, which give rise to skew braces, which in turn give rise to solutions to the Yang-Baxter equation.

Let G be a group, and denote by $\mathrm{Perm}(G)$ the group of all permutations of G. We say a subgroup N of $\mathrm{Perm}(G)$ is *regular* if the action of N on G is free and transitive, that is

   (1) for $\eta \in N, g \in G$ we have $\eta[g] = g$ if and only if $\eta = 1_N$; and
   (2) for $g, h \in G$ there exists an $\eta \in N$ such that $\eta[g] = h$.

If $N \le \mathrm{Perm}(G)$ is regular then $|N| = |G|$. Additionally, if $N \le \mathrm{Perm}(G)$ with $|N| = |G|$ and either of the above two conditions are satisfied, then N is a regular subgroup. Two fundamental examples of regular subgroups are the images of the left regular representation $\lambda : G \hookrightarrow \mathrm{Perm}(G)$ and the right regular representation $\rho : G \hookrightarrow \mathrm{Perm}(G)$.

In general, it is not necessarily the case that $N \cong G$. However, in the examples we will consider here these groups will in fact be isomorphic.

The subgroup $\lambda(G) \le \mathrm{Perm}(G)$ acts on $\mathrm{Perm}(G)$ by conjugation. We say $N \le \mathrm{Perm}(G)$ is *G-stable* if this action restricts to an action on N. In other

words, for all $\eta \in N, g \in G$ we have

$$^g\eta := \lambda(g)\eta\lambda(g^{-1}) \in N.$$

Certainly, $\lambda(G)$ is G-stable, and since $\lambda(G)$ and $\rho(G)$ commute in $\mathrm{Perm}(G)$ we see that $\rho(G)$ is G-stable as well.

Subgroups of $\mathrm{Perm}(G)$ which are regular and G-stable are essential in identifying Hopf-Galois structures on Galois extensions L/K in which we have $\mathrm{Gal}(L/K) \cong G$. This was first discovered by Greither and Pareigis in [11], but will not be needed here.

We will now introduce the notion of a skew (left) brace, and connect it to the regular, G-stable subgroups above.

A *skew left brace* is a triple $\mathfrak{B} = (B, \cdot, \circ)$ where $(B, \cdot)$ and $(B, \circ)$ are groups; and for all $a, b, c \in B$ the following condition holds:

$$a \circ (b \cdot c) = (a \circ b) \cdot a^{-1} \cdot (a \circ c),$$

where a^{-1} is the inverse to a in $(B, \cdot)$. We call this condition the *brace relation*.

For simplicity, we adopt the following conventions.

(1) We will refer to $\mathfrak{B}$ simply as a *brace*. The term "brace" was first used by Rump in [21] to describe a triple $(B, \cdot, \circ)$ satisfying the brace relation where $(B, \cdot)$ is abelian. The notion of brace was generalized 10 years later by Guarnieri and Vendramin [12].

(2) When no confusion will arise we will suppress the dot and write $ab = a \cdot b$.

(3) While $(B, \cdot)$ and $(B, \circ)$ share the same identity element, their inverses are different in general: we will denote the inverse to $a \in (B, \circ)$ by $\bar{a}$.

The reader should be made aware that there is no universal notation for braces at this point. Not only are the symbols for the two operations not standard, the order in which they appear in the triple is not standard as well.

Simple examples of braces include $(G, \cdot, \cdot)$, called the *trivial brace on G*, and $(G, \cdot, \cdot')$ where $(G, \cdot')$ is the opposite group to $(G, \cdot)$, giving the *almost trivial brace on G*.

As with regular, G-stable subgroups of $\mathrm{Perm}(G)$, we do not require that $(B, \cdot) \cong (B, \circ)$, however this paper will only deal with braces satisfying this property.

A regular, G-stable subgroup $N \leq \mathrm{Perm}(G)$ gives rise to a brace as follows. The map $\varkappa : N \to G$ given by $\varkappa(\eta) = \eta(1_G)$ is a bijection. Define

$\mathfrak{B}(N) = (N, \cdot, \circ)$, where $\cdot$ is the usual group operation on N, and

$$\eta \circ \pi = \varkappa^{-1}(\varkappa(\eta) *_G \varkappa(\pi)), \ \eta, \pi \in N.$$

It is well-known that every brace $(B, \cdot, \circ)$ arises from a regular, G-stable subgroup $N \leq \mathrm{Perm}(G)$ with $G \cong (B, \circ)$ [1, Prop. 6.1]. However, different regular G-stable subgroups can result in isomorphic braces. To describe this phenomenon more precisely we temporarily change our perspective by letting N be an abstract group of the same order as G. Then the embeddings $\alpha : N \hookrightarrow \mathrm{Perm}(G)$ such that $\alpha(N)$ is both regular and G-stable correspond bijectively with embeddings $\beta : G \hookrightarrow \mathrm{Hol}(N)$ such that the image $\beta(G)$ acts regularly on N. (Here $\mathrm{Hol}(N) = \rho(N) \rtimes \mathrm{Aut}(N)$ is the holomorph of N.) In [22, Proposition A.3], it is shown that two such embeddings $G \hookrightarrow \mathrm{Hol}(N)$ will give isomorphic braces if and only if their images are conjugate by some element in $\mathrm{Aut}(N)$.

Braces give set-theoretic solutions to the Yang-Baxter equation. Explicitly, for $\mathfrak{B} = (B, \cdot, \circ)$ a brace, define $R_{\mathfrak{B}} : B \times B \to B \times B$ by

$$R_{\mathfrak{B}} = (a^{-1}(a \circ b), \overline{a^{-1}(a \circ b)} \circ a \circ b) \tag{3.1}$$

Then $R_{\mathfrak{B}}$ is a non-degenerate, set-theoretic solution to the Yang-Baxter equation.

Definition 3.1. Let $\mathfrak{B} = (B, \cdot, \circ)$ be a brace. Then $R_{\mathfrak{B}}$ is said to be a solution of *type* (N, G) if N and G are abstract groups with $N \cong (B, \cdot)$ and $G \cong (B, \circ)$. If $N \cong G$ then we say $R_{\mathfrak{B}}$ is a solution of *type* G.

If $(B, \cdot)$ is abelian, then $R_{\mathfrak{B}}$ is involutive, i.e., $R_{\mathfrak{B}}$ is self-inverse. On the other hand, if $(B, \cdot)$ is non-abelian, two of the authors in [16, Th. 4.1] construct the inverse to $R_{\mathfrak{B}}$ through the use of opposite braces. The inverse to $R_{\mathfrak{B}}$, denoted $R'_{\mathfrak{B}}$, is simply

$$R'_{\mathfrak{B}} = ((a \circ b)a^{-1}, \overline{(a \circ b)a^{-1}} \circ a \circ b). \tag{3.2}$$

In this case, $R'_{\mathfrak{B}}$ is a solution of the same type as $R_{\mathfrak{B}}$. Notice that $R'_{\mathfrak{B}} = R_{\mathfrak{B}'}$, i.e., it is the solution obtained from 3.1 using the opposite brace to $\mathfrak{B}$.

It should be pointed out that braces can give additional set-theoretic solutions. For example, suppose $\phi : \mathfrak{B} \to \mathfrak{B}$ is a brace isomorphism, i.e., a bijective map which preserves both operations, and R is any solution to the Yang-Baxter equation with underlying set B. Then the function $R_\phi := R(\phi \times \phi) : B \times B \to B \times B$ is given by

$$R_\phi(a, b) = (\phi(a)^{-1}(\phi(a) \circ \phi(b)), \overline{\phi(a)^{-1}(\phi(a) \circ \phi(b))} \circ \phi(a) \circ \phi(b))$$

$$= (\phi(a^{-1}(a \circ b)), \phi(\overline{a^{-1}(a \circ b)} \circ a \circ b)),$$

so $R(\phi \times \phi) = (\phi \times \phi)R$ and the Yang-Baxter equation is clearly satisfied. However, if one is interested in set-theoretic solutions as a means to find vector space solutions, then R_ϕ and R can be thought of as being the same solution under a change of basis. Thus, if N_1 and N_2 are regular, G-stable subgroups which produce the same brace (up to isomorphism), we think of them as giving *equivalent* solutions to the Yang-Baxter equation.

4. Fixed-point free abelian endomorphisms and braces

The purpose of this section is to explicitly show how to obtain a brace from a fixed point free abelian endomorphism.

We start with a formal definition of what it means for an endomorphism to be fixed point free abelian. The term is self-explanatory. However, since these endomorphisms are central to this work, we wish to be explicit.

Definition 4.1. Let G be a group. An endomorphism $\psi : G \to G$ is said to be *fixed point free abelian* if both of the following hold:

   (1) If $\psi(g) = g$ then $g = 1_G$. (Fixed point free)
   (2) The image $\psi(G)$ is abelian. (Abelian)

Observe that if ψ is an abelian endomorphism, then $\psi(ghg^{-1}) = \psi(h)$ for all $g, h \in G$. That is, ψ is constant on conjugacy classes. We will use this fact extensively in section 6 when constructing these maps.

For a given group G, we will denote by $\mathrm{FPF}(G)$ the set of all fixed point free abelian endomorphisms of G. If $\psi_1, \psi_2 \in \mathrm{FPF}(G)$ their composition is typically not fixed point free, so $\mathrm{FPF}(G)$ should be viewed as simply a pointed set, with base point the trivial map ψ_0.

Example 4.2. Let G be any group. Certainly, the trivial homomorphism $\psi_0 : G \to G$, $\psi_0(g) = 1_G$ is fixed point free abelian.

Example 4.3. Let $G = D_4 = \langle r, s : r^4 = s^2 = rsrs = 1_G \rangle$ be the dihedral group of order 8. Define the endomorphism $\psi : G \to G$ on the generating set above by $\psi(r) = s$, $\psi(s) = 1_G$. Since $\psi(G) = \langle s \rangle$ this map is clearly abelian; it is also evidently fixed-point free, hence $\psi \in \mathrm{FPF}(G)$.

This example is well-known: see [9, p. 1264, (6)].

In [9], Childs constructs, from $\psi \in \mathrm{FPF}(G)$, a regular G-stable subgroup of $\mathrm{Perm}(G)$, namely $N = \{\lambda(g)\rho(\psi(g)) : g \in G\}$. Explicitly,

$$\eta_g[h] = gh\psi(g^{-1}) \text{ for all } g, h \in G.$$

The reader can check that N is regular, and that $^k\eta_g = \eta_{kgk^{-1}}$ for every $g, k \in G$.

Different fixed point free endomorphisms can yield the same group N. Indeed, ψ_1, $\psi_2 \in \text{FPF}(G)$ produce the same regular, G-stable subgroup of $\text{Perm}(G)$ if and only if there is a $\zeta \in \text{FPF}(G)$ with $\zeta(G) \leq Z(G)$ and such that

$$\psi_2(g) = \psi_1(g\zeta(g^{-1}))\zeta(g), \ g \in G.$$

In particular, $\psi \in \text{FPF}(G)$ gives the same regular, G-stable subgroup of $\text{Perm}(G)$ as ψ_0–namely, $\lambda(G) \leq \text{Perm}(G)$–if and only if $\psi(G) \leq Z(G)$. See [9, Th. 2] for details.

Thus, N gives rise to a brace $\mathfrak{B}_\psi = (N, \cdot, \circ)$ where the dot operation is the usual operation in N, which itself is inherited from G: since $\lambda(G)$ and $\rho(G)$ commute in $\text{Perm}(G)$ we have

$$\begin{aligned}
\eta_g \eta_h &= \lambda(g)\rho(\psi(g))\lambda(h)\rho(\psi(h)) \\
&= \lambda(g)\lambda(h)\rho(\psi(g))\rho(\psi(h)) \\
&= \lambda(gh)\rho(\psi(gh)) \\
&= \eta_{gh}.
\end{aligned}$$

We will now explicitly compute the circle operation, completing the description of $\mathfrak{B}_\psi$. Note that the bijection $\varkappa : N \to G$ is $\varkappa[\eta_g] = \eta_g[1_G] = g\psi(g^{-1})$. For $g, h \in G$ we have

$$\begin{aligned}
\eta_g \circ \eta_h &= \varkappa^{-1}(\varkappa(\eta_g) *_G \varkappa(\eta_h)) \\
&= \varkappa^{-1}\big(g\psi(g^{-1})h\psi(h^{-1})\big).
\end{aligned}$$

On the other hand, since ψ is constant on conjugacy classes,

$$\begin{aligned}
\varkappa\big(\eta_{g\psi(g^{-1})h\psi(g)}\big) &= g\psi(g^{-1})h\psi(g)\psi\big((g\psi(g^{-1})h\psi(g))^{-1}\big) \\
&= g\psi(g^{-1})h\psi(g)\psi(h^{-1}g^{-1}) \\
&= g\psi(g^{-1})h\psi(h^{-1}),
\end{aligned}$$

hence

$$\eta_g \circ \eta_h = \eta_{g\psi(g^{-1})h\psi(g)}.$$

At this point we remark that the map $g \mapsto \eta_g : G \to (N, \cdot)$ is in fact an isomorphism. This allows us to think of the underlying set of our brace as G, obtaining:

Proposition 4.4. *Let $\psi : G \to G$ be a fixed point free abelian endomorphism. Then $\mathfrak{B}_\psi = (G, \cdot, \circ)$ is a brace, where*

$$g \circ h = g\psi(g^{-1})h\psi(g), \ g, h \in G.$$

As mentioned earlier, the two groups in a brace need not be isomorphic, however for braces constructed from fixed point free abelian maps, it is necessary that they are.

Corollary 4.5. *Let* $\psi \in \mathrm{FPF}(G)$, *and let* $\mathfrak{B}_\psi = (G, \cdot, \circ)$ *be its corresponding brace. Then* $(G, \circ) \cong (G, \cdot)$.

Proof. Define $\phi : (G, \circ) \to (G, \cdot)$ by $\phi(g) = g\psi(g^{-1})$. We claim that ϕ is an isomorphism. Indeed, we have

$$\phi(g \circ h) = \phi(g\psi(g^{-1})h\psi(g))$$
$$= g\psi(g^{-1})h\psi(g)\psi(\psi(g^{-1})h^{-1}\psi(g)g^{-1})$$
$$= g\psi(g^{-1})h\psi(h^{-1})$$
$$= \phi(g)\phi(h)$$

so ϕ is a homomorphism. If $g \in \ker\phi$ then $\phi(g) = g\psi(g^{-1}) = 1_G$, from which it follows that $g = \psi(g)$. As ψ is fixed point free, this means $g = 1_G$. Thus, ϕ is injective, hence an isomorphism. $\square$

Direct calculation establishes the following, which will be needed in the sequel.

Corollary 4.6. *Let* $\psi \in \mathrm{FPF}(G)$. *Then for all* $g \in G$ *we have*

$$\bar{g} = \psi(g)g^{-1}\psi(g^{-1}).$$

From [17, §5], the group of automorphisms $\mathrm{Aut}(G)$ acts on $\mathrm{FPF}(G)$ via conjugation, i.e., $\varphi\psi\varphi^{-1} \in \mathrm{FPF}(G)$ whenever $\varphi \in \mathrm{Aut}(G)$, $\psi \in \mathrm{FPF}(G)$. Furthermore, the braces formed by ψ and $\varphi\psi\varphi^{-1}$ are isomorphic: in fact, any regular subgroup of $\mathrm{Perm}(G)$ which gives a brace isomorphic to the one determined by ψ is of this form.

Definition 4.7. We say the maps ψ_1, $\psi_2 \in \mathrm{FPF}(G)$ are *brace equivalent* if $\psi_2 = \varphi\psi_1\varphi^{-1}$ for some $\varphi \in \mathrm{Aut}(G)$.

Example 4.8. Let G be any group, and let $\psi_0 : G \to G$ be the trivial map as in example 4.2. Then

$$g \circ h = g\psi_0(g^{-1})h\psi_0(g) = gh$$

and $\mathfrak{B}_\psi = (G, \cdot, \cdot)$ is the trivial brace on G.

Notice that for any $\varphi \in \mathrm{Aut}(G)$ we have

$$\varphi^{-1}\psi_0\varphi(g) = \varphi^{-1}(1_G) = 1_G$$

so $\varphi^{-1}\psi_0\varphi = \psi_0$. Thus, no nontrivial $\psi \in \mathrm{FPF}(G)$ is equivalent to ψ_0.

Example 4.9. Let $G = D_4 = \langle r, s : r^4 = s^2 = rsrs = 1_G \rangle$ be the dihedral group of order 8, and let $\psi_1 \in \mathrm{FPF}(G)$ be $\psi_1(r) = \psi_1(s) = rs$ as in example 4.3. The circle operation in $\mathfrak{B}_{\psi_1}$ is given by

$$r^i \circ r^j = r^i(rs)^i r^j(rs)^i = r^{i+(-1)^i j}$$

$$r^i \circ r^j s = r^i(rs)^i r^j s(rs)^i = r^{-i+(-1)^i j} s$$

$$r^i s \circ r^j = r^i s(rs)^{i+1} r^j(rs)^{i+1} = r^{i+(-1)^i j} s$$

$$r^i s \circ r^j s = r^i s(rs)^{i+1} r^j s(rs)^{i+1} = r^{2-i+(-1)^i j}.$$

Example 4.10. Let $G = D_4$ as above, and let $\psi_2 : G \to G$ be the endomorphism given by $\psi_2(r) = r^2 s$, $\psi_2(s) = 1$. Since $\psi_2(G) = \langle r^2 s \rangle$ the map is abelian, and since $\psi(r^2 s) = 1_G \neq r^2 s$ we get $\psi_2 \in \mathrm{FPF}(G)$. The circle operation in $\mathfrak{B}_{\psi_2}$ is given by

$$r^i \circ r^j = r^i(r^2 s)^i r^j(r^2 s)^i = r^{i+(-1)^i j}$$

$$r^i \circ r^j s = r^i(r^2 s)^i r^j s(r^2 s)^i = r^{i+(-1)^i j} s$$

$$r^i s \circ r^j = r^i s(r^2 s)^i r^j(r^2 s)^i = r^{i-(-1)^i j} s$$

$$r^i s \circ r^j s = r^i s(r^2 s)^i r^j s(r^2 s)^i = r^{i-(-1)^i j}.$$

Now let $\varphi \in \mathrm{Aut}(G)$ be given by $\varphi(r) = r$, $\varphi(s) = r^3 s$. Then

$$\varphi^{-1}\psi_1\varphi(r) = \varphi^{-1}\psi_1(r) = \varphi^{-1}(rs) = r^2 s = \psi_2(r)$$

$$\varphi^{-1}\psi_1\varphi(s) = \varphi^{-1}\psi_1(r^3 s) = \varphi^{-1}(1_G) = 1_G = \psi_2(s),$$

so ψ_2 is equivalent to the ψ_1 found in example 4.9.

5. Proof of the main result

We are now well-positioned to prove our main theorem.

Theorem 5.1. *Let G be a finite group.*

(1) *Let $\psi \in \mathrm{FPF}(G)$. Let $R_\psi, R'_\psi : G \times G \to G \times G$ be given by*

$$R_\psi(g, h) = \left(\psi(g^{-1})h\psi(g), \psi(hg^{-1})h^{-1}\psi(g)g\psi(g^{-1})h\psi(gh^{-1})\right)$$

$$R'_\psi(g, h) = \left(g\psi(g^{-1})h\psi(g)g^{-1}, \psi(h)g\psi(h^{-1})\right).$$

Then:

(a) *Both R_ψ and R'_ψ are non-degenerate, set-theoretic solutions to the Yang-Baxter equation of type G.*

(b) *The functions R_ψ and R'_ψ are inverse to each other.*

(2) *The maps $\psi_1, \psi_2 \in \text{FPF}(G)$ give equivalent pairs of solutions to the Yang-Baxter equation R_{ψ_1}, R_{ψ_2} if and only if $\psi_2 = \varphi\psi_1\varphi^{-1}$ for some $\varphi \in \text{Aut}(G)$.*

Proof. Any $\psi \in \text{FPF}(G)$ gives rise to a regular, G-stable subgroup N_ψ of $\text{Perm}(G)$, which in turn corresponds to the brace $\mathfrak{B}_\psi = (G, \cdot, \circ)$ from before. The solution R_ψ can be readily computed from equation (3.1):

$$R_\psi(g,h) = \left(g^{-1}(g \circ h), \overline{g^{-1}(g \circ h)} \circ g \circ h\right)$$
$$= \left(g^{-1}g\psi(g^{-1})h\psi(g), \overline{g^{-1}g\psi(g^{-1})h\psi(g)} \circ g \circ h\right)$$
$$= \left(\psi(g^{-1})h\psi(g), (\psi(\psi(g^{-1})h\psi(g)))(\psi(g^{-1})h^{-1}\psi(g))\psi(\psi(g^{-1})h^{-1}\psi(g)) \circ g \circ h\right).$$

The first component now agrees with the statement of the theorem. For the second component,

$$(\psi(\psi(g^{-1})h\psi(g)))(\psi(g^{-1})h^{-1}\psi(g))\psi(\psi(g^{-1})h^{-1}\psi(g)) \circ g \circ h$$
$$= \psi(h)\psi(g^{-1})h^{-1}\psi(g)\psi(h^{-1}) \circ g\psi(g^{-1})h\psi(g)$$
$$= (\psi(hg^{-1})h^{-1}\psi(gh^{-1})\psi(\psi(gh^{-1})h\psi(hg^{-1}))g\psi(g^{-1})h\psi(g)\psi(\psi(hg^{-1})h^{-1}\psi(gh^{-1}))$$
$$= \psi(hg^{-1})h^{-1}\psi(gh^{-1})\psi(h)g\psi(g^{-1})h\psi(g)\psi(h^{-1})$$
$$= \psi(h\psi(h^{-1}))g\psi(g^{-1})h\psi(g\psi(h)),$$

as desired.

The solution R'_ψ can be computed using the theory of opposites as in [16]. Given a brace $\mathfrak{B} = (B, \cdot, \circ)$ with $(B, \cdot)$ nonabelian, one can construct an opposite brace $\mathfrak{B}' = (B, \cdot', \circ)$ where $a \cdot' b = b \cdot a$ for all $a, b \in B$. One then obtains a second solution to the YBE, namely

$$(g,h) \mapsto \left((g \circ h)g^{-1}, \overline{(g \circ h)g^{-1}} \circ g \circ h\right).$$

One can show that the expression above reduces to R'_ψ as in the statement of the theorem; that R'_ψ is the inverse to R_ψ can be found in [16, Th. 4.1].

Finally, to show (2), we use the fact that two regular, G-stable subgroups are brace equivalent if and only if their opposites are brace equivalent [17, Cor. 7.2]. □

Example 5.2. For any nonabelian group G, let $\psi : G \to G$ be the trivial map as in example 4.8. Then we get the trivial brace on G, and

$$R_\psi(g,h) = \left(\psi(g^{-1})h\psi(g), \psi(hg^{-1})h^{-1}\psi(g)g\psi(g^{-1})h\psi(gh^{-1})\right) = (h, h^{-1}gh)$$
$$R'_\psi(g,h) = \left(g\psi(g^{-1})h\psi(g)g^{-1}, \psi(h)g\psi(h^{-1})\right) = (ghg^{-1}, g).$$

Example 5.3. As in example 4.9, let G be the dihedral group of order 8, i.e., $G = D_4 = \langle r, s : r^4 = s^2 = rsrs = 1_G \rangle$, $\psi(r) = \psi(s) = rs$. Using theorem 5.1 we see, e.g., $R_\psi(rs, r^2) = (r^2, rs)$. More generally, the values for the solution R_ψ are given in the following table:

	1	r	r^2	r^3	s	rs	r^2s	r^3s
1	$(1,1)$	$(r,1)$	$(r^2,1)$	$(r^3,1)$	$(s,1)$	$(rs,1)$	$(r^2s,1)$	$(r^3s,1)$
r	$(1,r)$	(r^3,r^3)	(r^2,r)	(r,r^3)	(r^2s,r)	(rs,r^3)	(s,r)	(r^3s,r^3)
r^2	$(1,r^2)$	(r,r^2)	(r^2,r^2)	(r^3,r^2)	(s,r^2)	(rs,r^2)	(r^2s,r^2)	(r^3s,r^2)
r^3	$(1,r^3)$	(r^3,r)	(r^2,r^3)	(r,r)	(r^2s,r^3)	(rs,r)	(s,r^3)	(r^3s,r)
s	$(1,s)$	(r^3,s)	(r^2,s)	(r,s)	(r^2s,r^2s)	(rs,r^2s)	(s,r^2s)	(r^3s,r^2s)
rs	$(1,rs)$	(r,r^3s)	(r^2,rs)	(r^3,r^3s)	(s,r^3s)	(rs,rs)	(r^2s,r^3s)	(r^3s,rs)
r^2s	$(1,r^2s)$	(r^3,r^2s)	(r^2,r^2s)	(r,r^2s)	(r^2s,r^3s)	(rs,s)	(s,s)	(r^3s,s)
r^3s	$(1,r^3s)$	(r,rs)	(r^2,r^3s)	(r^3,rs)	(s,rs)	(rs,r^3s)	(r^2s,rs)	(r^3s,r^3s)

A table for R'_ψ can be similarly constructed using the formula as in Theorem 5.1; alternatively one could compute it by explicitly constructing the inverse to the table of values above.

6. Examples

We finish with examples, where we explicitly construct the solutions to the Yang-Baxter equation whose underlying sets are some well-known groups. We have tried to strike a balance between explicitness and simplicity of results.

Sometimes, the use of fixed point free abelian endomorphisms will find *all* solutions to the Yang-Baxter equation with underlying group G. We explore this topic in the examples below.

6.1. Abelian groups. The theory presented above gives useful results when G is nonabelian. In the case where G is abelian,

$$g \circ h = g\psi(g^{-1})h\psi(g) = gh$$

giving only the trivial brace. The only solution to the Yang-Baxter equation we construct is

$$R_\psi(a,b) = (b,a)$$

as $R'_\psi = R_\psi$ when G is abelian.

By [3], our construction will yield all possible solutions to the Yang-Baxter equation if and only if $\gcd(|G|, \phi(|G|)) = 1$, where ϕ is the Euler totient function. Such a group is necessarily cyclic.

6.2. The dihedral groups D_n. Generalizing the notation from example 4.9, write $G = D_n = \langle r, s : r^n = s^2 = rsrs = 1_G \rangle$. Classification of $\mathrm{FPF}(D_n)$ appears in [9, §5]. Here, we will give the Yang-Baxter solutions given by those maps.

Suppose first that n is odd. Then $\mathrm{FPF}(D_n)$ consists only of the trivial map. Indeed, if $\psi \in \mathrm{FPF}(D_n)$ is nontrivial then $\ker \psi = \langle r \rangle$. Additionally,

$\psi(s) = r^i s$ for some $0 \le i \le n - 1$. But then $\psi(r^i s) = r^i s$ is a fixed point, which is a contradiction.

Thus, the two solutions to the Yang-Baxter equation we obtain when n is odd are the two from example 5.2.

By the main theorem in [19], the number of regular, G-stable subgroups of D_n isomorphic to n for n odd is equal to the number of self-inverse elements in $\mathbb{Z}_n^\times$, from which it follows that our process obtains all such subgroups if and only if p is a power of an odd prime.

Now suppose that n is even, and write $n = 2m$. Each element of $\text{FPF}(D_n)$ which does not give the trivial regular subgroup $\lambda(G)$ is in at least one of the following four forms.

(1) $\alpha_i(r) = r^{2i}s$, $\alpha_i(s) = 1$, $0 \le i \le m - 1$;
(2) $\beta_i(r) = r^{2i+m}s$, $\beta_i(s) = r^m$, $0 \le i \le m - 1$;
(3) $\gamma_i(r) = r^{2i+1}s$, $\gamma_i(s) = r^{2i+1}s$, $0 \le i \le m - 1$;
(4) $\delta_i(r) = r^{2i+1+m}s$, $\delta_i(s) = r^{2i+1}s$, $0 \le i \le m - 1$.

For $0 \le i, j \le n - 1$, $\gcd(i, n) = 1$ let $\varphi_{i,j} : D_n \to D_n$ be given by $\varphi_{i,j}(r) = r^i$, $\varphi_{i,j}(s) = r^j s$. Then $\text{Aut}(D_n) = \{\varphi_{i,j}\}$. If we set $i = 1$ we have

$$\varphi_{1,j}^{-1}\alpha_0\varphi_{1,j}(r) = \varphi_{1,j}^{-1}\alpha_0(r) = \varphi_{1,j}^{-1}(s) = r^{-j}s$$
$$\varphi_{1,j}^{-1}\alpha_0\varphi_{1,j}(s) = \varphi_{1,j}^{-1}\alpha_0(r^j s) = \varphi_{1,j}^{-1}(s^j).$$

Hence, if j is even we get $\varphi_{1,j}^{-1}\alpha_0\varphi_{1,j} = \alpha_{j-2}$; on the other hand if j is odd we get $\varphi_{1,j}^{-1}\alpha_0\varphi_{1,j}(s) = r^{-j}s$ and so $\varphi_{1,j}^{-1}\alpha_0\varphi_{1,j} = \gamma_{(-j-1/2)}$. By allowing j to vary we see that $\{\alpha_i, \gamma_j\}$ are all equivalent.

Using $\varphi_{1,j}$ it can also be shown that $\{\beta_i, \delta_j\}$ are all brace equivalent in a very similar manner. Furthermore, in the case m is even the homomorphism $\zeta : D_n \to D_n$ given by $\zeta(r) = r^m$, $\zeta(s) = r^m$ is a fixed point free endomorphism whose image is the center of D_n. Additionally,

$$\alpha_0(r\zeta(r^{-1}))\zeta(r) = \alpha_0(r^{1+m})r^m = s^{1+m}r^m = r^m s = \beta_0(r)$$
$$\alpha_0(s\zeta(s^{-1}))\zeta(s) = \alpha_0(r^m s)r^m = s^m r^m = r^m = \beta_0(s),$$

so there is only one nontrivial class.

We have

$$R_{\alpha_0}(r^i s^j, r^k s^\ell) = (s^i r^k s^\ell, s^{k+i+\ell} r^{-k} s^i r^i s^{i+j} r^k s^{j+k+\ell})$$
$$R'_{\alpha_0}(r^i s^j, r^k s^\ell) = (r^i s^{i+k} r^k s^{i+\ell+j} r^i, s^k r^i s^{j+k})$$

and for m odd we have, since $r^m \in Z(D_n)$,

$$R_{\beta_0}(r^i s^j, r^k s^\ell) = (s^i r^k s^{i+\ell}, s^{i+k+\ell} r^{-k} s^i r^i s^{i+j} r^k s^{i+k+\ell})$$
$$R'_{\beta_0}(r^i s^j, r^k s^\ell) = (r^i s^{i+j} r^k s^{i+j+\ell} r^{-i}, s^k r^i s^{j+k}).$$

As mentioned above, in [19], Kohl enumerates all regular, G-stable subgroups of $\mathrm{Perm}(D_n)$ isomorphic to D_n. Since a regular, G-stable subgroup arising from $\psi \in \mathrm{FPF}(G)$ never gives the same brace as one arising from a regular, G-stable subgroup which does *not* come from such a ψ, this allows us to determine when we have found all the Yang-Baxter solutions of dihedral type. More precisely:

Proposition 6.1. *With the constructions above, we obtain every Yang-Baxter solution of dihedral type if and only if one of the following holds:*

(1) $n = p^k$ *for some prime p and positive integer k;*
(2) $n = 2p^k$ *for some odd prime p and positive integer k;*

Proof. The main result of [19] indicates that the number $\mathscr{R}(D_n)$ of regular, G-stable subgroups of D_n isomorphic to D_n is given by the following formula:

$$\mathscr{R}(D_n) = |\Upsilon_n| \cdot \begin{cases} 1 & v_2(n) = 0 \\ 2m + 1 & v_2(n) = 1 \\ m + 1 & v_2(n) = 2 \\ m + 2 & v_2(n) > 2 \end{cases},$$

where $v_2(n)$ is the 2-adic valuation of n, $n = 2m$ where appropriate, and Υ_n is the subgroup of self-inverse elements of $\mathbb{Z}_n^\times$. Note that Υ_n is nontrivial for $n > 3$, and $|\Upsilon_n| = 2$ if and only if $\mathbb{Z}_n^\times$ is cyclic, which holds if and only if $n = 1, 2, p^k$ or $2p^k$ for some odd prime p and $k \geq 1$.

On the other hand, in [9], Childs counts the number of regular, G-stable subgroups arising from fixed point free abelian endomorphisms on D_n. For our purposes, since the theory of opposites allow us to obtain *two* regular, G-stable subgroups from each ψ, we get that the number of subgroups $\mathscr{S}(D_n)$ we obtain is

$$\mathscr{S}(D_n) = \begin{cases} 2 & v_2(n) = 0 \\ 4m + 2 & v_2(n) = 1 \\ 8m + 2 & v_2(n) > 1 \end{cases}.$$

By comparing these, we see that if n is odd we will get every regular, G-stable subgroup (hence, every Yang-Baxter solution) if and only if $|\Upsilon_n| = 2$, i.e., n is a power of a prime. If $v_2(n) = 1$ we again require $|\Upsilon_n| = 2$; since $n \geq 3$ is even this means $n = 2p^k$ for some p. If $v_2(n) = 2$ then we would need $(m + 2)|\Upsilon_n| = 4m + 2$. Since $|\Upsilon_n|$ is necessarily a nontrivial power of 2 and $4m + 2 \equiv 2 \pmod 4$, we see that we cannot get all regular, G-stable subgroups in this manner. Similarly, if $v_2(n) > 2$ then we would need $(m + 2)|\Upsilon_n| = 8m + 2$ which cannot happen. $\qquad\square$

6.3. The alternating group A_4. It is well-known that $G = A_4$ can be expressed as a semidirect product $V \rtimes C_3$ where V is the (unique) Sylow 2-subgroup of A_4 and C_3 is generated by a 3-cycle, say x. Then

$$A_4 = \{vx^i : 0 \leq i \leq 2, v \in V\}.$$

Let $\psi \in \mathrm{FPF}(G)$ be nontrivial. Then, for some $v \in V$ we have either $\psi(v) = 1_G$ or $\psi(v)$ is an element of order 2, say $\psi(v) = w$. But v and w are conjugate in A_4, hence $\psi(w) = \psi(v) = w$, a contradiction. Thus, $\psi(v) = 1_G$ for all $v \in V$.

Since ψ is assumed to be nontrivial, $\psi(x)$ is an element of order 3 which is not conjugate to x. There are two conjugacy classes for the 3-cycles in A_4, and every 3-cycle is in a different class than its inverse. Thus, each conjugacy class has four elements; hence, there are four possibilities for $\psi(x)$. One such example is $\psi(x) = x^2$. The reader can verify that all four choices give valid fixed-point free abelian endomorphisms.

We omit the technical details above because each of the nontrivial elements of $\mathrm{FPF}(G)$ give the same brace. To see this, suppose $\psi_1(x) = y$ and $\psi_2(x) = z$. Necessarily, y and z are in the same conjugacy class, so there exists an inner automorphism of G carrying $\psi_1(x)$ to $\psi_2(x)$.

Including the trivial map, we have:

Proposition 6.2. *There are five fixed point free abelian maps on A_4 and two brace equivalence classes of fixed point free abelian maps.*

If we use $\psi(x) = x^2$ the solutions obtained are

$$R_\psi(v_1 x^i, v_2 x^j) = (x^i v_2 x^{j-i}, x^i v_2 x^{-i} v_1 x^{-i} v_2 x^{-i-j})$$
$$R'_\psi(x^i v_1, x^j v_2) = (v_1 x^{-i} v_2 x^{i-j} v_1, x^{-j} v_1 x^{i+j})$$

where $v_1, v_2 \in V$.

As $\mathrm{Perm}(A_4)$ has 10 regular, G-stable subgroups [6, Th. 7], we see that the solutions presented above are all of the solutions of type A_4.

The situation changes drastically for A_5, as we shall see.

6.4. The alternating groups $A_n, n \geq 5$. It is easy to compute the set $\mathrm{FPF}(A_n)$ for $n \geq 5$. In fact, we generalize, computing $\mathrm{FPF}(G)$ in the case G is a simple group. This is well known and can be shown by direct computation or by considering Hopf-Galois structures on Galois extensions with simple Galois group [4].

Proposition 6.3. *Suppose G is a nonabelian simple group. Then $\mathrm{FPF}(G)$ consists of only the trivial map.*

Proof. If $\psi : G \to G$ is any homomorphism, then $\ker \psi = \{1_G\}$ or $\ker \psi = G$ since $\ker \psi \lhd G$. If $\ker \psi = \{1_G\}$ then $\psi(G) = G$ and hence ψ cannot be abelian. Thus ψ is trivial. $\qquad \square$

Thus, the only solutions to the Yang-Baxter equation obtained via fixed-point-free abelian maps are the solutions found in example 5.2. Unlike in the abelian case, we do get multiple solutions. Trivially, this gives us all the Yang-Baxter equation solutions of type G for G a nonabelian simple group.

6.5. The symmetric groups $S_n, n \geq 5$. Let $\psi : S_n \to S_n$ be a homomorphism. In a manner similar to the previous section, $\ker \psi = \{1_G\}, A_n$, or S_n. If we assume ψ is nontrivial and fixed point free, then $\ker \psi = A_n$ and ψ is constant on odd permutations. Furthermore, $\psi(\sigma^2) = 1_G$, hence a nontrivial ψ sends odd permutations to some element of order 2, say τ. Finally, if τ is odd then $\psi(\tau) = \tau$ and we have a fixed point. In fact, we have:

Proposition 6.4. *Let*

$$A_n^{(2)} = \{\tau \in A_n : \tau^2 = 1_{A_n}\}.$$

Then there is a bijection between $A_n^{(2)}$ and $\mathrm{FPF}(S_n)$ given by $\tau \mapsto \psi_\tau$, where

$$\psi_\tau(\sigma) = \begin{cases} 1 & \sigma \in A_n \\ \tau & \sigma \notin A_n \end{cases}.$$

Furthermore, ψ_{τ_1} and ψ_{τ_2} are brace equivalent if and only if τ_1 and τ_2 have the same cycle structure.

Proof. From the discussion above it is clear that any $\psi \in \mathrm{FPF}(G)$ must be of this form, and it is routine to show that $\psi_\tau \in \mathrm{FPF}(G)$ for any $\tau \in A_n$ with $\tau^2 = 1_G$. Any $\tau_1, \tau_2 \in A_n$ with $\tau_1^2 = \tau_2^2 = 1_G$ are conjugate if and only if they have the same cycle structure. Now, if $\tau_2 = \xi\tau_1\xi^{-1}$, $\xi \in S_n$ then the map $C(\xi) : S_n \to S_n$ given by conjugation by ξ is an automorphism. If $\sigma \in S_n$ then

$$C(\xi)\psi_1 C(\xi)^{-1}(\sigma) = C(\xi)\psi_1(\xi^{-1}\sigma\xi) = C(\xi)(1_G) = 1_G = \psi_2(\sigma)$$

if σ is even; and

$$C(\xi)\psi_1 C(\xi)^{-1}(\sigma) = C(\xi)\psi_1(\xi^{-1}\sigma\xi) = C(\xi)\tau_1 = \xi\tau_1\xi^{-1} = \tau_2 = \psi_2(\sigma)$$

if $\sigma \in S_n$ is odd. Thus, if τ_1, τ_2 have the same cycle structure then the corresponding maps ψ_1 and ψ_2 are brace equivalent.

Conversely, for $n \neq 6$ every automorphism of S_n is inner, hence these account for all the brace equivalences. Finally, if $n = 6$ every element of order 2 has the same cycle type, so the result follows. $\qquad \square$

Corollary 6.5. *Let $\tau \in A_n$ have order at most two. Then*

$$R_\tau(\sigma, \pi) = \begin{cases} (\pi, \pi^{-1}\sigma\pi) & \sigma, \pi \in A_n \\ (\pi, \tau\pi^{-1}\sigma\pi\tau) & \sigma \in A_n, \ \pi \notin A_n \\ (\tau\pi\tau, \tau\pi^{-1}\tau\sigma\tau\pi\tau) & \sigma \notin A_n, \ \pi \in A_n \\ (\tau\pi\tau, \pi^{-1}\tau\sigma\tau\pi) & \sigma, \pi \notin A_n \end{cases}, \ and$$

$$R'_\tau(\sigma, \pi) = \begin{cases} (\sigma\pi\sigma^{-1}, \sigma) & \sigma, \pi \in A_n \\ (\sigma\pi\sigma^{-1}, \tau\sigma\tau) & \sigma \in A_n, \ \pi \notin A_n \\ (\sigma\tau\pi\tau\sigma^{-1}, \sigma) & \sigma \notin A_n, \ \pi \in A_n \\ (\sigma\tau\pi\tau\sigma^{-1}, \tau\sigma\tau) & \sigma, \pi \notin A_n \end{cases}$$

are solutions to the Yang-Baxter equation.

Here, we get all of the solutions of type S_n. This can be seen from [6, Th. 5], where the authors find two families of regular, G-stable subgroups of $\mathrm{Perm}(G)$, each parameterized by elements of order 2 in S_n.

6.6. The family of nonabelian metacyclic groups $M_{p,q}$. For our last set of examples we consider the simplest nonabelian metacyclic groups. Let p, q be primes with $p \equiv 1 \pmod q$, and define

$$M_{p,q} = \langle s, t : s^p = t^q = 1_G, \ tst^{-1} = s^d \rangle,$$

where d is chosen to have order q modulo p. (Note that the group is independent of the choice of d: changing its value merely changes the presentation.) By Sylow theory, the Sylow p-subgroup $\langle s \rangle$ is normal in $M_{p,q}$, however since $sts^{-1} \notin \langle t \rangle$ the Sylow q-subgroups are not normal in $M_{p,q}$. Thus, if ψ is any endomorphism of $M_{p,q}$, then $\ker \psi = \{1_G\}$, $\langle s \rangle$, or $M_{p,q}$. Thus for any ψ fixed point free and abelian, $\ker \psi = \langle s \rangle$ and hence $\psi(s) = 1_G$.

It therefore suffices to determine $\psi(t)$. Since the Sylow p-subgroup is normal, an element $s^i t^j$ will have order q if and only if $j \neq 0$. Let us write

$$\psi(t) = s^i t^j, \ 0 \le i \le p - 1, \ 1 \le j \le q - 1.$$

Then ψ respects the relations in the presentation of $M_{p,q}$, hence is an endomorphism. Since $\psi(M_{p,q}) = \langle s^i t^j \rangle \cong C_q$ the map is abelian. Suppose $\psi(s^k t^\ell) = s^k t^\ell$. Then

$$(s^i t^j)^\ell = s^k t^\ell.$$

For this to hold we require $j\ell \equiv \ell \pmod q$, so either $j = 1$ or $\ell = 0$. If $\ell = 0$ then $\psi(s^k) = s^k$, so $k = 0$ and we have the trivial element. If $j = 1$ then $\psi(s^i t) = s^i t$ and we have a fixed point. Thus:

Proposition 6.6. *If $\psi \in \mathrm{FPF}(M_{p,q})$ is nontrivial, then $\psi = \psi_{i,j}$, where*

$$\psi_{i,j}(s) = 1, \ \psi_{i,j}(t) = s^i t^j, \ 0 \le i \le p - 1, 2 \le j \le q - 1.$$

It follows from [17, Lemma 8.13] that ψ_{i_1,j_1} is brace equivalent to ψ_{i_2,j_2} if and only if $i_1 = i_2$. From this we obtain

Corollary 6.7. *The set $\{\psi_j := \psi_{0,j} : 2 \le j \le q - 1\}$ is a complete set of nontrivial brace classes of fixed point free abelian maps.*

The endomorphism ψ_j produces the following solutions to the Yang-Baxter equation:

$$R_{\psi_j}(s^k t^\ell, s^m t^n) = (t^{-j\ell} s^m t^{n+j\ell}, t^{j(n-\ell)}(s^m t^n)^{-1} t^{j\ell} s^k t^{\ell-j\ell} s^m t^{n+j(\ell-n)})$$

$$R'_{\psi_j}(s^k t^\ell, s^m t^n) = (s^k t^{\ell-j\ell} s^m t^{n+j\ell}(s^k t^\ell)^{-1}, t^{jn} s^k t^{\ell-jn}).$$

One can see that we get all solutions of metacyclic type by using the regular, G-stable classification from [5]; alternatively, see [17, §8], which explicitly shows this.

References

[1] BACHILLER, DAVID. Counterexample to a conjecture about braces. *J. Algebra* **453** (2016), 160–176. MR3465351, Zbl 1338.16022, arXiv:1507.02137, doi: 10.1016/j.jalgebra.2016.01.011. 1474, 1478

[2] BAXTER, RODNEY J. Partition function for the eight-vertex lattice model. *Ann. Phys.* **70** (1972), 193–228, doi: 10.1016/0003-4916(72)90335-1. 1473

[3] BYOTT, NIGEL P. Uniqueness of Hopf Galois structure for separable field extensions. *Comm. Algebra* **24** (1996), no. 10, 3217–3228. MR1402555, Zbl 0878.12001, doi: 10.1080/00927879608825743. 1484

[4] BYOTT, NIGEL P. Hopf–Galois structures on field extensions with simple Galois groups. *Bull. London Math. Soc.* **36** (2004), no. 1, 23–29. MR2011974, Zbl 1038.12002, doi: 10.1112/S0024609303002595. 1487

[5] BYOTT, NIGEL P. Hopf–Galois structures on Galois field extensions of degree *pq*. *J. Pure Appl. Algebra* **188** (2004), no. 1-3, 45–57. MR2030805, Zbl 1047.16022, doi: 10.1016/j.jpaa.2003.10.010. 1474, 1490

[6] CARNAHAN, SCOTT; CHILDS, LINDSAY. Counting Hopf Galois structures on non-abelian Galois field extensions.*J. Algebra*, **218** (1999), no. 1, 81–92. MR1704676, Zbl 0988.12003, doi: 10.1006/jabr.1999.7861. 1474, 1487, 1489

[7] CHEN, REBECCA S. Generalized Yang–Baxter equations and braiding quantum gates. *J. Knot Theory Ramifications* **21** (2012), no. 9, 1250087, 18 pp. MR2926570, Zbl 1247.81084, arXiv:1108.5215, doi: 10.1142/S0218216512500873. 1473

[8] CHILDS, LINDSAY N. Taming wild extensions: Hopf algebras and local Galois module theory. Mathematical Surveys and Monographs, 80. *American Mathematical Society, Providence, RI*, 2000. viii+215 pp. MR1767499, Zbl 0944.11038, doi: 10.1090/surv/080. 1474

[9] CHILDS, LINDSAY N. Fixed-point free endomorphisms and Hopf Galois structures. *Proc. Amer. Math. Soc.* **141** (2013), no. 4, 1255–1265. MR3008873, Zbl 1269.12003, doi: 10.1090/S0002-9939-2012-11418-2. 1474, 1479, 1480, 1484, 1486

[10] DRINFELD, VLADIMIR G. On some unsolved problems in quantum group theory. *Quantum groups* (Leningrad, 1990), 1–8, Lecture Notes in Math., 1510, *Springer, Berlin,* 1992. MR1183474, Zbl 0765.17014, doi: 10.1007/BFb0101175. 1474, 1476

[11] Greither, Cornelius; Pareigis, Bodo. Hopf Galois theory for separable field extensions. *J. Algebra* **106** (1987), no. 1, 239–258. MR878476, Zbl 0615.12026, doi: 10.1016/0021-8693(87)90029-9. 1477

[12] Guarnieri, L.; Vendramin, Leandro. Skew braces and the Yang–Baxter equation. *Math. Comp.* **86** (2017), no. 307, 2519–2534. MR3647970, Zbl 1371.16037, arXiv:1511.03171, doi: 10.1090/mcom/3161. 1474, 1477

[13] Jimbo, Michio. Introduction to the Yang–Baxter equation. *Braid group, knot theory and statistical mechanics*, 111-134, Adv. Ser. Math. Phys., 9, *World Sci. Publ., Teaneck, NJ*, 1989. MR1062425, Zbl 0697.35131, doi: 10.1142/9789812798350_0005. 1473

[14] Jimbo, Michio., (Ed). Yang–Baxter equation in integrable systems. Advanced Series in Mathematical Physics, 10. *World Scientific Publishing Co., Inc., Teaneck, NJ*, 1989. x+715 pp. ISBN: 981-02-0120-6; 981-02-0121-4. MR1061379, Zbl 0726.58005, doi: 10.1142/1021. 1473

[15] Jimbo, Michio. Introduction to the Yang–Baxter equation. *Braid group, knot theory and statistical mechanics, II*, 153–176, Adv. Ser. Math. Phys., 17, *World Sci. Publ., River Edge, NJ*, 1994. MR1338602, Zbl 0820.17012, doi: 10.1142/9789812798275_0006. 1473

[16] Koch, Alan; Truman, Paul J. Opposite skew left braces and applications. *J. Algebra* **546** (2020), 218–235. MR4033084, Zbl 07148874, arXiv:1908.02682, doi: 10.1016/j.jalgebra.2019.10.033. 1474, 1475, 1478, 1483

[17] Koch, Alan; Truman, Paul J. Skew left braces and isomorphism problems for Hopf–Galois structures on Galois extensions. (2020). arXiv:2005.05809. 1481, 1483, 1490

[18] Kohl, Timothy. Classification of the Hopf Galois structures on prime power radical extensions. *J. Algebra* **207** (1998), no. 2, 525–546. MR1644203, Zbl 0953.12003, doi: 10.1006/jabr.1998.7479. 1474

[19] Kohl, Timothy. Enumerating dihedral Hopf–Galois structures acting on dihedral extensions. *J. Algebra* **542** (2020), 93–115. MR4018326, Zbl 07128728, arXiv:1907.03844, doi: 10.1016/j.jalgebra.2019.08.040. 1485, 1486

[20] Lambe, Larry A.; Radford, David E. Introduction to the quantum Yang–Baxter equation and quantum groups: an algebraic approach. Mathematics and Its Applications, 423. *Kluwer Academic Publishers, Dordrecht*, 1997. xx+293 pp. ISBN: 0-7923-4721-8. MR1483071, Zbl 0888.16021, doi: 10.1007/978-1-4615-4109-7. 1473

[21] Rump, Wolfgang. Braces, radical rings, and the quantum Yang–Baxter equation. *J. Algebra* **307** (2007), no. 1, 153–170. MR2278047, Zbl 1115.16022, doi: 10.1016/j.jalgebra.2006.03.040. 1474, 1477

[22] Smoktunowicz, Agata; Vendramin, Leandro. On skew braces (with an appendix by N. Byott and L. Vendramin) *J. Comb. Algebra* **2** (2018), no. 1, 47–86. MR3763907, Zbl 1416.16037, arXiv:1705.06958, doi: 10.4171/JCA/2-1-3. 1478

[23] Yang, Chen N. Some exact results for the many-body problem in one dimension with repulsive delta-function interaction. *Phys. Rev. Lett.* **19** (1967), 1312–1315. MR261870, Zbl 0152.46301, doi: 10.1103/PhysRevLett.19.1312. 1473

(Alan Koch) Department of Mathematics, Agnes Scott College, 141 E. College Ave., Decatur, GA 30030, USA
akoch@agnesscott.edu

(Laura Stordy) School of Mathematics, Georgia Institute of Technology, 686 Cherry St NW, Atlanta, GA 30332, USA
lstordy3@gatech.edu

(Paul J. Truman) School of Computing and Mathematics, Keele University, Staffordshire, ST5 5BG, UK
p.j.truman@keele.ac.uk

This paper is available via `http://nyjm.albany.edu/j/2020/26-58.html`.