



Deposited via The University of Leeds.

White Rose Research Online URL for this paper:

<https://eprints.whiterose.ac.uk/id/eprint/240470/>

Version: Accepted Version

Article:

Colazzo, I., Okniński, J. and Van Antwerpen, A. (Accepted: 2026) Bijective solutions to the Pentagon Equation. *Selecta Mathematica*. ISSN: 1022-1824 (In Press)

This is an author produced version of an article accepted for publication in *Selecta Mathematica* made available via the University of Leeds Research Outputs Policy under the terms of the Creative Commons Attribution License (CC-BY), which permits unrestricted use, distribution and reproduction in any medium, provided the original work is properly cited.

Reuse

This article is distributed under the terms of the Creative Commons Attribution (CC BY) licence. This licence allows you to distribute, remix, tweak, and build upon the work, even commercially, as long as you credit the authors for the original work. More information and the full terms of the licence here:

<https://creativecommons.org/licenses/>

Takedown

If you consider content in White Rose Research Online to be in breach of UK law, please notify us by emailing eprints@whiterose.ac.uk including the URL of the record and the reason for the withdrawal request.

BIJECTIVE SOLUTIONS TO THE PENTAGON EQUATION

I. COLAZZO, J. OKNIŃSKI, AND A. VAN ANTWERPEN

ABSTRACT. A complete classification of all finite bijective set-theoretic solutions (S, s) to the Pentagon Equation is obtained. First, it is shown that every such solution determines a semigroup structure on the set S that is the direct product $E \times G$ of a semigroup of left zeros E and a group G . Next, we prove that this leads to a decomposition of the set S as a Cartesian product $X \times A \times G$, for some sets X, A and to the discovery of a hidden group structure on A . Then an unexpected structure of a matched product of groups A, G is found such that the solution (S, s) can be explicitly described as a lift of a solution determined on the set $A \times G$ by this matched product of groups. Conversely, every matched product of groups leads to a family of solutions arising in this way. Moreover, a simple criterion for the isomorphism of two solutions is obtained. These results significantly extend those of Colazzo, Jespers, and Kubat, in their treatment of the involutive case. Furthermore, connections to solutions to the Yang–Baxter Equation and to the theory of skew braces are uncovered. The latter motivate a further investigation of the relationship between solutions to the Yang–Baxter Equation and the Pentagon Equation at the set-theoretical level.

1. INTRODUCTION

A linear map $v : V \otimes V \rightarrow V \otimes V$ on the tensor square of a vector space V is a solution to the *Pentagon Equation* if, on $V \otimes V \otimes V$, one has

$$v_{23}v_{13}v_{12} = v_{12}v_{23},$$

where each v_{ij} is the map applying v to the (i, j) -component and acting as the identity on the remaining one. If S is a nonempty set and $s : S \times S \rightarrow S \times S$ is a map, then the pair (S, s) is said to be a set-theoretic solution to the Pentagon Equation if the equality

$$s_{23}s_{13}s_{12} = s_{12}s_{23}$$

holds on $S \times S \times S$, with the same notation agreement as above. Namely, if $\tau : S \times S \rightarrow S \times S$, $\tau(x, y) = (y, x)$ is the flip map then $s_{12} = s \times \text{id}$, $s_{13} = (\tau \times \text{id})(\text{id} \times s)(\tau \times \text{id})$ and $s_{23} = \text{id} \times s$. Clearly, every set-theoretic solution (S, s) to the Pentagon Equation extends linearly to a unique solution (V, v) on the vector space V with basis S .

The Pentagon Equation has appeared in several areas of mathematics, especially in the theory of quantum groups and Hopf algebras, as well as in various contexts of mathematical physics. In particular, these include: operators on Hilbert spaces with applications to duality results on compact groups [BS93; BS98], three dimensional integrable systems and the so called tetrahedron equation [Mai94], conformal

2020 *Mathematics Subject Classification*. Primary: 81R12, 20M99, Secondary: 16T25, 20E22, 81R50 .

Key words and phrases. Pentagon equation, Set-theoretic solution, Matched product of groups, Semigroup.

field theory [MS89], the Heisenberg double and classification problems for Hopf algebras [Mil04], Cuntz algebras [Kaw10]. The Pentagon Equation also appears in low-dimensional topology in the construction of link invariants in the work of Kashaev [Kas94]. In [KR07], the set-theoretic version of the Pentagon Equation was applied to the so called symmetrically factorizable Lie groups, while in [Kas11] it was considered in the context of the discrete Liouville equation. Moreover, non-trivial relations between the Pentagon Equation and another important equation of mathematical physics, the Yang–Baxter Equation, were indicated and investigated by several authors. In particular, in [Kas96] it is shown that the Pentagon Equation plays the same role for the Heisenberg double as the Quantum Yang–Baxter Equation does for the Drinfeld double. The context of Hopf algebras and of the relations between the Yang–Baxter and Pentagon Equations were studied also in [VV94]. Solutions to the Pentagon Equation also have appeared with different names. For example, a unitary operator on the tensor square of a Hilbert space is said to be multiplicative if it is a solution to the Pentagon Equation [BS93; Wor96]; while in [Str98], for a fixed braided monoidal category A , a map $V : A \otimes A \rightarrow A \otimes A$ is said to be a fusion operator if it satisfies the Pentagon Equation. Recently, set-theoretic solutions to the Pentagon Equation received a lot of attention. They have been approached via new methods, including methods of semigroup theory, with an effort to describe and classify certain special classes of such solutions, see [CMM20; CMS20; CJK20; Cas26; JL05; MPS24]. In particular, Colazzo, Jespers and Kubat [CJK20] completely classified involutive set-theoretic solutions (S, s) (meaning that $s^2 = \text{id}$) to the Pentagon Equation, while Castelli [Cas26] more recently obtained a description of some other special classes of bijective set-theoretic solutions.

In this paper we deal with arbitrary finite bijective set-theoretic solutions (S, s) to the Pentagon Equation and we provide a complete classification of all such solutions. In particular, our results provide far-reaching extensions of those obtained in [CJK20] and [Cas26].

Surprisingly, matched products of groups play a crucial role in our main results. These are also known as Zappa–Szép products or bicrossed products of groups, and they arise as exact factorizations of groups, $G = AB$ with A, B subgroups of G and $A \cap B = \{1\}$. For a survey, with an emphasis on their role in the theory of the Yang–Baxter Equation, we refer to the paper of Takeuchi [Tak03].

Our main theorem can be formulated as follows (see Section 4 for the definition of a matched pair of groups).

Theorem 1.1. *Let (S, s) be a finite bijective set-theoretic solution to the Pentagon Equation. Then there exists a matched pair of groups (A, G, σ, δ) , a set X and maps $\varphi_a \in \text{Sym}(X)$, for all $a \in A$, such that S , as a set, is the Cartesian product $X \times A \times G$ and s is of the following form*

$$(\star) \quad s((\alpha, a, x), (\beta, b, y)) = ((\alpha, a, xy), (\varphi_{b(\delta_x(a))^{-1}}\varphi_b(\beta), b(\delta_x(a))^{-1}, \sigma_{\delta_x(a)}(y)))$$

for $\alpha, \beta \in X, a, b \in A$ and $x, y \in G$. Moreover, for any matched pair of groups (A, G, σ, δ) , a set X and maps $\varphi_a \in \text{Sym}(X)$, defined for all $a \in A$, the map s defined on $S = X \times A \times G$ in (\star) is a bijective set-theoretic solution to the Pentagon Equation.

There is also a natural notion of a homomorphism of set-theoretic solutions to the Pentagon Equation (see Definition 2.2) and the proof of Theorem 1.1 yields a transparent criterion for when two set-theoretic solutions are isomorphic. In fact,

up to isomorphism the family of permutations $\{\varphi_a\}$ is not essential, i.e. every finite bijective solution is isomorphic to one of the form (\star) with $\varphi_a = \text{id}_X$ for all $a \in A$. In particular, up to isomorphism we may assume $\varphi_a = \text{id}_X$ for all $a \in A$, and then (\star) becomes

$$s((\alpha, a, x), (\beta, b, y)) = ((\alpha, a, xy), (\beta, b(\delta_x(a))^{-1}, \sigma_{\delta_x(a)}(y))).$$

In addition, isomorphism classes of finite bijective solutions to the Pentagon Equation are in a bijection with pairs consisting of a positive integer and an isomorphism class of matched pairs of groups (see Corollary 6.6). It is worth stressing that Theorem 1.1 seems quite surprising, since the analogous problem on (describing all) bijective set-theoretic solutions to the Yang–Baxter Equation has proved to be extremely difficult and remains wide open, see [Ven24] and references therein.

By convention, if (S, s) is a set-theoretic solution to the Pentagon Equation, we write $s(x, y) = (x \cdot y, \theta_x(y))$, for a map $S \times S \rightarrow S$, $(x, y) \mapsto x \cdot y$ and certain maps $\theta_x: S \rightarrow S$, for $x \in S$. It is well known that (S, \cdot) is a semigroup, [KS98].

The proof of our main theorem proceeds in several steps. The first step is crucial: we show that as a semigroup S is a direct product $S = E \times G$ of a left zero semigroup E (meaning that $ef = e$ for every $e, f \in E$) and a group G ; see Theorem 2.4. Next in Theorem 2.9 we prove that each map θ_x for $x \in S$, is a permutation of S . This allows us to exploit group-theoretic tools, which turn out to be central in the formulation and proof of our main results.

In Section 3, we introduce a notion of retract $\text{Ret}(S, s)$ (see Proposition 3.4) defined via a congruence on the semigroup (S, \cdot) . This retract again carries the structure of a set-theoretic solution to the Pentagon Equation, which we denote by $\text{Ret}(S, s) = (\bar{S}, \bar{s})$. Then using the bijectivity of s we discover a dual bijective set-theoretic solution $(S, \tau s^{-1} \tau)$ that defines another semigroup structure (S, \circ) on the set S . This yields a decomposition into a Cartesian product $S = X \times A \times G$ such that the underlying set of the retract \bar{S} can be identified with $A \times G$ and the set of idempotents E of S can be identified with $X \times A$. Later, we show that the retract operator is idempotent, in other words $\text{Ret}(\text{Ret}(S, s)) = \text{Ret}(S, s)$, for any finite bijective set-theoretic solution to the Pentagon Equation (S, s) . We emphasize that our notion of retract differs from the retraction for set-theoretic solutions to the Yang–Baxter Equation introduced in [ESS99]. In the Yang–Baxter setting, retraction is often iterated and serves as a measure of the complexity of the solution, whereas in the present setting the retract is a key structural ingredient and, in the finite bijective case, it allows one to reconstruct (S, s) from $\text{Ret}(S, s)$. In Section 4 we focus on irretractable solutions $(S, s) = \text{Ret}(S, s) = (\bar{S}, \bar{s})$, so $S = A \times G$. Here we show that for an irretractable solution the dual solution $(S, \tau s^{-1} \tau)$ endows A with a group structure and surprisingly switches the roles of A and G . This unravels a hidden symmetry in the retract solution (\bar{S}, \bar{s}) and leads to the construction of a matched product of groups A and G in Theorem 5.4. Conversely, every matched product of groups leads, in a natural way, to an irretractable solution to the Pentagon Equation, and it turns out to be responsible for the formula describing the set-theoretic solution (\bar{S}, \bar{s}) , see Theorem 4.1. Finally, we show that the original set-theoretic solution (S, s) is a natural extension (lift) of its retract, so that the formula (\star) follows, see Theorem 6.4.

Although every matched pair of groups leads in a natural way to a set-theoretic solution to the Pentagon Equation, in Section 7 we provide certain concrete constructions that may be used to illustrate the main ideas and strategy used in

the paper. In particular, in the finite case the description of all involutive set-theoretic solutions, obtained earlier in [CJK20], via a different approach, follows easily from Theorem 1.1. Matched pairs of groups also appear naturally in the theory of set-theoretic solutions to the Yang–Baxter Equation, see [GM08; Tak03; LYZ00]. Moreover, braces and skew braces introduced by Rump in [Rum07] and by Guarnieri–Vendramin in [GV17] in the context of set-theoretic solutions to the Yang–Baxter Equation, canonically determine a matched pair of groups (see [SV18, Lemma 5.9]). In the last section we show explicitly how skew braces also define irretractable set-theoretic solutions to the Pentagon Equation. Thus, our results open a new connection (at the set-theoretic level) between solutions to the Pentagon Equation and solutions to the Yang–Baxter Equation. Skew braces can also be described in terms of regular subgroups of holomorphs [GV17]. This provides a computationally efficient way of defining matched pairs of groups and creates also a bridge with Hopf-Galois structures [Byo96]. For more details we refer to Section 7. We conclude by relating set-theoretic solutions to the Pentagon Equation to Hopf algebras with positive bases. In particular, we recall that any finite set-theoretic solution to the Pentagon Equation gives rise to a Hopf algebra with a positive basis [CJ26], and we explain why Hopf-algebraic classification results do not directly recover the set-theoretic classification we obtained in Theorem 1.1.

2. SET-THEORETIC BIJECTIVE SOLUTIONS TO THE PENTAGON EQUATION

In this section we prove key results on the semigroup structures arising from finite set-theoretic bijective solutions to the Pentagon Equation.

Definition 2.1. A pair (S, s) , where S is a set and $s: S \times S \rightarrow S \times S$ is said to be a *set-theoretic solution to the Pentagon Equation* if the equality

$$(2.1) \quad s_{23}s_{13}s_{12} = s_{12}s_{23}$$

holds in $S \times S \times S$.

From now on, by a *solution to the PE* we always mean a set-theoretic solution to the Pentagon Equation.

Definition 2.2. Let (S, s) and (T, t) be solutions to the PE. We say that a map $f: S \rightarrow T$ is a *homomorphism of solutions* if the diagram

$$\begin{array}{ccc} S \times S & \xrightarrow{f \times f} & T \times T \\ s \downarrow & & \downarrow t \\ S \times S & \xrightarrow{f \times f} & T \times T \end{array}$$

commutes. The solutions (S, s) , (T, t) are *isomorphic* if there exists a bijective homomorphism of solutions $f: S \rightarrow T$.

By convention, if (S, s) is a solution to the PE, we write $s(x, y) = (x \cdot y, \theta_x(y))$, for a map $S \times S \rightarrow S$, $(x, y) \mapsto x \cdot y$, and maps $\theta_x: S \rightarrow S$ for $x, y \in S$.

The following lemma appears in [KS98].

Lemma 2.3. *Let S be a set and $s: S \times S \rightarrow S \times S$ be a map. Then (S, s) is a solution to the PE if and only if*

$$(2.2) \quad x \cdot (y \cdot z) = (x \cdot y) \cdot z,$$

$$(2.3) \quad \theta_x(y) \cdot \theta_{x \cdot y}(z) = \theta_x(y \cdot z),$$

$$(2.4) \quad \theta_{\theta_x(y)}\theta_{x \cdot y}(z) = \theta_y(z),$$

for all $x, y, z \in S$. Moreover, s is bijective if and only if for every $x, y \in S$ there exists a unique pair $(u, v) \in S \times S$ such that $u \cdot v = x$ and $\theta_u(v) = y$.

Proof. It is straightforward. \square

In particular, every solution (S, s) carries a natural semigroup structure on S and we will often simply write xy in place of $x \cdot y$. If (S, \cdot) is a group, then it is easy to check that $s(x, y) = (xy, y)$ is a bijective solution to the PE. Moreover, Kashaev and Sergeev [KS98] proved that this is the only bijective solution when S is equipped with a group structure via \cdot .

The first crucial step towards our classification will be to describe the structure of the semigroup S . Namely, we will prove that if (S, s) is a finite bijective solution to the PE then S is a left group, i.e. S is isomorphic to $E \times G$ where E is a set, G is a group, and the multiplication on S is defined by

$$(e, g)(f, h) = (e, gh)$$

for every $(e, g), (f, h) \in E \times G$. We refer the reader to [CP61] for the necessary background on semigroups.

For any semigroup S we denote with $E(S)$ the set of idempotent elements of S .

Theorem 2.4. *Let (S, s) be a finite bijective solution to the PE. Then S is a left group.*

Proof. By [CJK20, Proposition 2.2], if (S, s) is a solution to the PE of finite order, then S is a simple semigroup. This implies, in particular, that if (S, s) is bijective and S is finite, S is a completely simple semigroup (cf [CP61, page 76]).

By Rees' theorem it follows that we may identify S with a completely simple matrix semigroup $\mathcal{M}(G, I, \Lambda; P)$ with G a finite group whenever (S, s) is a finite bijective solution to the PE. We recall that, if G is a group, I and Λ are non-empty sets, and P is a matrix indexed by I and Λ with entries $p_{\lambda, i} \in G$ then the *Rees matrix semigroup* $S = \mathcal{M}(G, I, \Lambda; P)$ is the set $I \times G \times \Lambda$ with multiplication given by

$$(i, g, \lambda)(j, h, \mu) = (i, gp_{\lambda, j}h, \mu).$$

In particular, the set of idempotent elements of S is given by

$$E(S) = \{(i, p_{\lambda i}^{-1}, \lambda) : i \in I, \lambda \in \Lambda\}.$$

If $e = (i, p_{\lambda i}^{-1}, \lambda) \in E(S)$, then the right ideal generated by e is

$$eS = \{(i, g, \mu) : g \in G, \mu \in \Lambda\}$$

and the left ideal generated by e is

$$Se = \{(j, g, \lambda) : j \in I, g \in G\}.$$

Let $m = |I|$ and $n = |\Lambda|$. Then $|eS| = |G||\Lambda| = n|G|$ and $|Se| = |I||G| = m|G|$. Now notice that for every $x = (i, g, \mu) \in eS$, there exist exactly m elements $y \in Se$

such that $xy = e$, i.e. $y \in \{(j, p_{\mu,j}^{-1}g^{-1}p_{\lambda,i}^{-1}, \lambda) : j \in I\}$. Therefore, we get $nm|G|$ different pairs $(x, y) \in S \times S$ such that $xy = e$. Next, we use property (2.3) with $xy = e$, and then $y = ye$ and $x = ex$. So, in particular

$$\theta_x(y) = \theta_x(ye) = \theta_x(y)\theta_{xy}(e) = \theta_x(y)\theta_e(e),$$

and $\theta_x(y)\mathcal{L}\theta_e(e)$, where as usual \mathcal{L} denotes the Green's relation. It follows that $|\{\theta_x(y) : xy = e\}| \leq |S\theta_e(e)| = m|G|$. However, $|\{(x, y) : xy = e\}| = mn|G|$. Since s is bijective, considering the set

$$s^{-1}(\{(xy, \theta_x(y)) : xy = e\}),$$

we get that $mn|G| \leq m|G|$. Hence $n = 1$ and the statement follows. \square

The second crucial step is to describe important properties of the maps θ_x , for $x \in S$. In particular, we will prove that all of them are bijective. We begin with some preparatory lemmas.

Lemma 2.5. *Let (S, s) be a finite bijective solution to the PE and set $E = E(S)$. Then $\theta_x(E) \subseteq E$ for all $x \in S$. In particular, s restricts to a finite bijective solution on E (since $E(S)$ is closed under multiplication).*

Moreover, if $E(S) = S$ (equivalently S is a left zero semigroup), then for each $x \in S$ the map θ_x is bijective and is either the identity or a fixed-point free permutation.

Proof. By Theorem 2.4, S is a left group, so every element in $E(S)$ is a right identity, i.e. $xe = x$ for all $x \in S$ and $e \in E(S)$. Let $x \in S$ and $e \in E(S)$. From (2.3) it follows that

$$\theta_x(e) = \theta_x(e^2) = \theta_x(e)\theta_{xe}(e) = \theta_x(e)\theta_x(e),$$

i.e. $\theta_x(e) \in E(S)$.

For the second statement see [CJK20, Lemma 2.4]. \square

Lemma 2.6. *Let (S, s) be a finite bijective solution to the PE and let $e \in E(S)$. If $x \in eS$, then $\theta_y(x) \in \theta_y(e)S$.*

Proof. By Lemma 2.5, $\theta_y(e) \in E(S)$. Let $e \in E(S)$, $x \in eS$ and $y \in S$. By (2.3) and from $x = ex$ we get

$$\theta_y(x) = \theta_y(ex) = \theta_y(e)\theta_{ye}(x) = \theta_y(e)\theta_y(x),$$

hence $\theta_y(x) \in \theta_y(e)S$. \square

For a map $\theta : S \rightarrow S$ let \sim_θ be the relation $\{(a, b) \in S \times S \mid \theta(a) = \theta(b)\}$.

Lemma 2.7. *Let (S, s) be a finite bijective solution to the PE. Then the following statements hold:*

- (1) $\sim_{\theta_x} = \sim_{\theta_y}$, for any $x, y \in S$.
- (2) $|\theta_x(S)| = |\theta_y(S)|$, for any $x, y \in S$.
- (3) The relation $\sim = \sim_{\theta_x}$, for any x , is a left congruence on S .

Proof. Let us prove (1). Let $x, y \in S$. By equation (2.4),

$$(2.5) \quad \sim_{\theta_{xy}} \subseteq \sim_{\theta_y}.$$

Moreover, since S is a left group, there exists v such that $y = vxy$. It follows that

$\sim_{\theta_y} = \sim_{\theta_{vxy}} \stackrel{(2.5)}{\subseteq} \sim_{\theta_{xy}} \stackrel{(2.5)}{\subseteq} \sim_{\theta_x}$. Therefore, $\sim_{\theta_{xy}} = \sim_{\theta_y}$. Finally, let $x' \in S$. Since S is left simple, there exists z such that $x' = zx$. Then $\sim_{\theta_{x'}} = \sim_{\theta_{zx}} = \sim_{\theta_x}$.

We prove (2). Since \sim_{θ_x} is an equivalence relation, by (1) and the fact that S is finite it follows that $|\theta_x(S)| = |\theta_{x'}(S)|$, for any $x, x' \in S$.

We now prove (3). By (1), $\sim_{\theta_x} = \sim_{\theta_y}$, for every $x, y \in S$. We denote this relation simply with \sim . Let $a \sim b$ and $y \in S$. Then $\theta_{xy}(a) = \theta_{xy}(b)$ for any $x \in S$. It follows that $\theta_x(ya) \stackrel{(2.3)}{=} \theta_x(y)\theta_{xy}(a) = \theta_x(y)\theta_{xy}(b) \stackrel{(2.3)}{=} \theta_x(yb)$. Therefore \sim is a left congruence. \square

Lemma 2.8. *Let (S, s) be a finite bijective solution to the PE. Let $e \in E(S)$. Then, there exists a subgroup H_e of $G_e = eS$, such that for any $a, b \in G_e$,*

$$a \sim b \iff aH_e = bH_e.$$

Proof. Define

$$H_e = \{a \in G_e \mid a \sim e\}.$$

We claim that H_e is a subgroup of G_e . Clearly $e \in H_e$. If $a, b \in H_e$, then for any $x \in S$ we have

$$(2.6) \quad \theta_x(a) = \theta_x(e)$$

$$(2.7) \quad \theta_x(b) = \theta_x(e).$$

Then

$$(2.8) \quad \theta_x(ab) \stackrel{(2.3)}{=} \theta_x(a)\theta_{xa}(b) \stackrel{(2.6)(2.7)}{=} \theta_x(e)\theta_{xa}(e) = \theta_x(e)$$

where the last equality holds since, by Lemma 2.5, $\theta_x(e), \theta_{xa}(e) \in E(S)$ and any idempotent element in S is a right identity.

Now, let $a \in H_e$ and denote by \bar{a} the unique element in G_e such that $a\bar{a} = e = \bar{a}a$. It follows that, for any $x \in S$

$$\theta_x(e) = \theta_x(\bar{a}a) = \theta_x(\bar{a})\theta_{x\bar{a}}(a) = \theta_x(\bar{a})\theta_{x\bar{a}}(e) = \theta_x(\bar{a}),$$

where the last equality holds because $\theta_{x\bar{a}}(e) \in E(S)$ and so it is a right identity. It follows that $\bar{a} \in H_e$, so H_e is a subgroup of G_e . The assertion follows from Lemma 2.7. \square

We are now ready to derive a key structural result that will clearly indicate that group theoretical methods must naturally appear when dealing with finite bijective solutions to the PE.

Theorem 2.9. *If (S, s) is a finite bijective solution to the PE, then θ_x is bijective for every $x \in S$.*

Proof. Since (S, s) is a finite bijective solution to the PE, by Theorem 2.4 S is a left group, i.e., $S = E \times G$, where $E = E(S)$ and G is a group. We write $G_e = eG$ for $e \in E$. By Lemma 2.7(1), if $x, y \in S$ then $\theta_{\theta_x(y)}$, θ_{xy} and θ_y determine the same congruence \sim . Moreover, by (2.4) we have the inclusion of images $\theta_y(S) \subseteq \theta_{\theta_x(y)}(S)$. By Lemma 2.7(2), since S is finite, we get $\theta_y(S) = \theta_{\theta_x(y)}(S)$ and also $|\theta_y(S)| = |\theta_{xy}(S)|$. Applying Equation (2.4) yields that the restriction of $\theta_{\theta_x(y)}$ to $\theta_{xy}(S)$ is bijective.

On the other hand, the relation $\sim = \sim_{\theta_x}$, for every $x \in S$, is a left congruence on S by Lemma 2.7(3). And by Lemma 2.8, for any $e \in E$ we can define a group $H_e = \{a \in G_e \mid a \sim e\}$ such that $a, b \in G_e$ and $a \sim b$ if and only if $aH_e = bH_e$. Moreover

$fH_e = H_f$ for every $e, f \in E$. Now, since $\theta_{\theta_x(y)}$ is bijective when restricted to $\theta_{xy}(S)$, we get that for every $e \in E(S)$

$$(2.9) \quad |\theta_{xy}(S) \cap H_e| \leq 1.$$

But using Lemma 2.5 we have $\theta_{xy}(f)S = G_{\theta_{xy}(f)}$ and $e = \theta_{xy}(f) \in \theta_{xy}(G_f)$ is the identity of the group $G_{\theta_{xy}(f)}$. Therefore $\theta_{xy}(S) \cap H_e = \{\theta_{xy}(f)\}$. We know also that every $\theta_{e'}, e' \in E(S)$, permutes the set $E(S)$ (by Lemma 2.5) and $\theta_{e'}$ maps every G_f into some $G_{f'}$. Suppose that $\theta_z, z \in S$, are not bijections. Then it follows that (every) H_e must be a nontrivial subgroup in G_e . Therefore, (2.9) implies that every nonidentity element h of the group $H_{\theta_{xy}(f)}$ is not in the image of θ_{xy} , for all $x, y \in S$. So $h \notin \bigcup_{z \in S} \theta_z(S)$. However, bijectivity of the solution s implies that $S = \bigcup_{z \in S} \theta_z(S)$. This contradiction proves that every θ_y must be bijective. \square

Our final results in this section highlight the role of the maps θ_e determined by the idempotents e of the semigroup S .

Proposition 2.10. *Let (S, s) be a finite bijective solution to the PE. Then, for every $x \in S$ there exists an $e \in E(S)$ such that $\theta_x = \theta_e$. Moreover, the set $\theta_E = \{\theta_e \mid e \in E(S)\}$ is a group with identity $\theta_{\theta_e(e)}$ independent of the choice of $e \in E(S)$.*

Proof. We start by proving the latter claim. Let $e \in E(S)$. Then, by relation (2.4)

$$\theta_{\theta_e(e)}\theta_e = \theta_{\theta_e(e)}\theta_{ee} = \theta_e.$$

By Theorem 2.9, θ_e is bijective, which shows that $\theta_{\theta_e(e)} = \text{id}_S$. Let $e, f \in E(S)$. Then, by Lemma 2.5, $E(S)$ is closed under θ_e , thus there is a $f_2 \in E(S)$ with $\theta_e(f_2) = f$. Hence, as $ef_2 = e$, we get

$$\theta_f\theta_e = \theta_{\theta_e(f_2)}\theta_{ef_2} \stackrel{(2.4)}{=} \theta_{f_2},$$

which shows that the set θ_E is a submonoid of $\text{Sym}(S)$. As the latter is finite, θ_E is a subgroup.

Let $x \in S$ and let $e \in E(S)$. Then by (2.4)

$$\theta_{\theta_x(e)}\theta_{xe} = \theta_e,$$

which is equivalent to

$$\theta_x = \theta_{\theta_x(e)}^{-1}\theta_e.$$

As $\theta_x(e) \in E(S)$, the latter can be rewritten as θ_f for some $f \in E(S)$. \square

From now on we fix $e_0 \in E(S)$ and denote $1 = \theta_{e_0}(e_0)$.

Proposition 2.11. *Let (S, s) be a finite bijective solution to the PE. Denote $G = G_1 = 1S$. Then for any $g \in G$, we have $\theta_g = \text{id}_S$.*

Proof. By Proposition 2.10, $\theta_1 = \text{id}_S$. Then

$$\theta_g\theta_g = \theta_{\theta_1(g)}\theta_{1g} \stackrel{(2.4)}{=} \theta_g,$$

which shows that $\theta_g = \text{id}_S$, by Theorem 2.9. \square

3. THE RETRACT OF A BIJECTIVE SOLUTION

Since we assume that the solution (S, s) is bijective, the inverse map $s^{-1} : S \times S \rightarrow S \times S$ can be exploited. As shown below, this leads to a dual solution of the PE and the corresponding dual semigroup structure (S, \circ) . In this section we combine the structure of the left groups (S, \cdot) and (S, \circ) . In particular, we show that the set of idempotent elements $e \in (S, \cdot)$ with $\theta_e = \text{id}_S$ coincides with the intersection of the corresponding subsemigroups of idempotents. This allows us to define the retract of a bijective solution to the PE. In particular, it identifies this intersection into a single element and produces an irretractable solution, i.e. a solution with exactly one idempotent $e \in E(S, \cdot)$ such that $\theta_e = \text{id}_S$. While the retract of (S, s) has a substantially simpler structure than (S, s) , Theorem 6.4 shows that nevertheless it retains enough information to completely recover (S, s) as a natural extension. This is in sharp contrast with the Yang–Baxter setting, where the situation is more intricate and the retraction introduced in [ESS99] can be applied to a solution multiple times, yielding the multipermutation level as an invariant measure of the complexity of the solution. Even though the retraction and the multipermutation level of a solution to the Yang–Baxter Equation have been widely studied and used, see for instance [BCV18; CJO10; Gat18; GC12], they do not provide a mechanism for reconstructing the original solution.

Let (S, s) be a bijective solution to the PE. Then we denote

$$s^{-1}(x, y) = (\psi_y(x), y \circ x).$$

Then, as s is a solution to the PE, we have that

$$s_{12}^{-1} s_{13}^{-1} s_{23}^{-1} = s_{23}^{-1} s_{12}^{-1},$$

(in other words, s^{-1} satisfies the so called Reversed Pentagon Equation). As in Lemma 2.3, this translates into the following equalities.

$$(3.1) \quad z \circ (y \circ x) = (z \circ y) \circ x,$$

$$(3.2) \quad \psi_z(y) \circ \psi_{z \circ y}(x) = \psi_z(y \circ x),$$

$$(3.3) \quad \psi_{\psi_z(y)} \psi_{z \circ y} = \psi_y,$$

which shows that $t(x, y) = (x \circ y, \psi_x(y))$ is a bijective solution to PE. Hence, one obtains the following proposition on the structure of (S, \circ) .

Proposition 3.1. *Let (S, s) be a finite bijective solution to the PE. Then (S, \circ) is a left group.*

Furthermore, we note consequences that follow from the equalities

$$s \circ s^{-1} = \text{id}_{S \times S} = s^{-1} \circ s.$$

Namely, for all $x, y \in S$ we have

$$(3.4) \quad \psi_y(x)(y \circ x) = x,$$

$$(3.5) \quad \theta_{\psi_y(x)}(y \circ x) = y,$$

$$(3.6) \quad \psi_{\theta_x(y)}(xy) = x,$$

$$(3.7) \quad \theta_x(y) \circ (xy) = y.$$

Define

$$\theta : S \rightarrow \text{Sym}(S), x \mapsto \theta_x, \quad \text{and} \quad \psi : S \rightarrow \text{Sym}(S), x \mapsto \psi_x.$$

Hence, it follows easily that θ , respectively ψ , is a homomorphism from (S, \circ) , respectively (S, \cdot) , to $\text{Sym}(S)$. Denote

$$\ker \theta = \{s \in S \mid \theta_s = \text{id}_S\},$$

and similarly

$$\ker \psi = \{s \in S \mid \psi_s = \text{id}_S\}.$$

Lemma 3.2. *Let (S, s) be a finite bijective solution to the PE. Denoting $E = E(S, \cdot)$ and $F = E(S, \circ)$, we get*

$$\ker \theta \cap E = \{\theta_e(e) \mid e \in E\} = \ker \psi \cap F = \{\psi_f(f) \mid f \in F\}.$$

Proof. We present the proof that the first three sets are equal; then the last equality is true by symmetry. As noted before, $\theta_{\theta_e(e)} = \text{id}_S$ for all $e \in E$. Moreover, if $e \in \ker \theta \cap E$, then $\theta_e(e) = e$, which shows the first equality.

Let $e \in \ker \theta \cap E$. Then, by relation (3.7)

$$e \circ e = \theta_e(e) \circ (ee) = e,$$

which shows that e is an idempotent in (S, \circ) . Hence, $e \in F$.

Let $x \in S$. Then by (3.4) we find that

$$\psi_e(x)(e \circ x) = x.$$

Moreover, rewriting relation (3.5), one finds, as $e \in E$, that

$$e \circ x = \theta_{\psi_e(x)}^{-1}(e) \in E$$

by Lemma 2.5. Combining this information, since $e \circ x = \theta_{\psi_e(x)}^{-1}(e)$ is a right identity, we get that

$$x = \psi_e(x)(e \circ x) = \psi_e(x),$$

which shows that $\psi_e = \text{id}_S$. Thus, $\ker \theta \cap E \subseteq \ker \psi \cap F$, the reverse equality is analogous. \square

The previous allows us to fully determine $F = E(S, \circ)$ and by symmetry $E = E(S, \cdot)$. Recall that $1 = \theta_{e_0}(e_0)$, as fixed before Proposition 2.11.

Proposition 3.3. *Let (S, s) be a finite bijective solution to the PE. Then, one has that $F = (\ker \theta \cap E)G_1$. In particular, F is a subsemigroup of (S, \cdot) .*

Proof. Let $e \in \ker \theta \cap E$ and $g \in G_1$. Then, by relation (3.7),

$$eg \circ eg = \theta_e(eg) \circ (eeg) = eg,$$

which shows that $eg \in F$. Hence, $(\ker \theta \cap E)G_1 \subseteq F$. In particular, as $1 = \theta_{\bar{e}}(\bar{e}) \in \ker \theta \cap E$ by Proposition 2.10, one obtains that $G_1 = 1G_1 \subseteq F$. Vice versa, one notes that for any $f_1, f_2 \in F$ one has, by rewriting relation (3.6), that

$$f_1 f_2 = \psi_{\theta_{f_1}(f_2)}^{-1}(f_1),$$

where the latter is in F by Lemma 2.5. This shows that F is a subsemigroup of (S, \cdot) .

Let $f \in F$. Then there exist $e \in E$ and $g \in G_1$ such that $f = eg$. It remains to show that $e \in \ker \theta$. As $G_1 \subseteq F$ and F is a subsemigroup of (S, \cdot) , it follows that $e = (eg)(g^{-1}) \in E \cap F$, where g^{-1} denotes the inverse of g in G_1 . Let $y \in S$. Considering relation (3.5), one finds that

$$\theta_e(y \circ \psi_y^{-1}(e)) = y.$$

As $e \in F$, one has, by applying Lemma 2.5 on the solution t (introduced above Proposition 3.1), that $\psi_y^{-1}(e) \in F$. Thus, the above equality can be reduced to

$$\theta_e(y) = y.$$

Hence, $e \in \ker \theta$, showing that $\theta_e = \text{id}_S$ and proving the result. \square

Proposition 3.4. *Let (S, s) be a finite bijective solution to the PE. For any elements $e, f \in E = E(S, \cdot)$ and $g, h \in G_1$, define the following equivalence relation on S : $eg \approx fh$, if $\theta_e = \theta_f$ and $g = h$. Denote $\bar{S} = S/\approx$. Then s induces a bijective solution (\bar{S}, \bar{s}) , which we call the retract of (S, s) .*

Proof. Clearly, \approx is a congruence on the semigroup (S, \cdot) . Let $eg \approx fh$ such that $e, f \in E$ and $g, h \in G_1$. Then $\theta_e = \theta_f$ and $g = h$. Let $q \in S$. First, we claim that θ_q is independent of the choice of the representing element in the congruence class of q . Indeed, using relation (2.4) twice, we find that

$$\theta_{eg} = \theta_{\theta_e^{-1}(g)}\theta_g = \theta_{\theta_f^{-1}(g)}\theta_g = \theta_{fg},$$

which shows the claim. Secondly, using relation (2.3) and that $e \in E$, one gets that

$$\theta_q(eg) = \theta_q(e)\theta_q(g).$$

Similarly,

$$\theta_q(fg) = \theta_q(f)\theta_q(g).$$

From relation (2.4) we get that

$$\theta_{\theta_q(e)} = \theta_{\theta_q(e)}\theta_{qe}\theta_{qe}^{-1} = \theta_e\theta_q^{-1} = \theta_f\theta_q^{-1} = \theta_{\theta_q(f)}.$$

This means that $\theta_q(e) \approx \theta_q(f)$. So $\theta_q(eg) = \theta_q(e)\theta_q(g) \approx \theta_q(f)\theta_q(g) = \theta_q(fg)$. Thus, indeed, θ_{eg} and θ_{fg} induce the same map on \bar{S} .

It now follows easily that \bar{S} carries an induced semigroup structure and satisfies relations (2.2), (2.3) and (2.4) for the maps induced by θ_q for all $q \in S$, proving the result. \square

Let (S, s) be a finite bijective solution to the PE and (\bar{S}, \bar{s}) its retract. We denote by

$$\pi : S \rightarrow \bar{S}, x \rightarrow \bar{x}$$

the homomorphism from (S, \cdot) to \bar{S} with respect to the induced semigroup structure. Moreover we denote with $\bar{\theta}$ the induced θ -map for the retract. In other words

$$\bar{s}(\bar{x}, \bar{y}) = (\bar{xy}, \bar{\theta}_{\bar{x}}(\bar{y}))$$

for $x, y \in S$.

Note that from the definition of the retract it easily follows that if $e \in E(S)$ and $x \in S$ are such that $e \approx x$ then $x \in E(S)$. In particular, $\pi(E(S)) = E(\bar{S})$ and we denote it by \bar{E} .

We will say that a solution (S, s) is *irretractable* if $\bar{S} = S$.

Proposition 3.5. *Let (S, s) be a finite bijective solution to the PE and (\bar{S}, \bar{s}) its retract. Then, $|\ker \theta \cap \bar{E}| = 1$. In particular, (\bar{S}, \bar{s}) is irretractable.*

Proof. Let $x \in \overline{E}$ with $\overline{\theta}_x = \text{id}_{\overline{S}}$. Then there exists an $e \in E$ such that $\pi(e) = x$. Denote $f = \theta_e(e) \in \ker \theta$. As $\overline{\theta_e(f)} = \overline{\theta_e(f)} = \overline{f}$, it follows that $\theta_f = \theta_{\theta_e(f)}$, so that $\theta_e(f) \in \ker \theta$. However,

$$\theta_{\theta_e(f)}\theta_e = \theta_f = \text{id}_S,$$

which implies, using that $\theta_e(f) \in \ker \theta$ that $\theta_e = \theta_{\theta_e(f)}^{-1} = \text{id}_S$. This shows that $e \in \ker \theta$. Hence, both assertions follow by the remarks made before. \square

4. FROM MATCHED PAIRS OF GROUPS TO IRRETRACTABLE SOLUTIONS

Recall that a quadruple (G, A, σ, δ) is a *matched pair of groups* if A and G are groups and there are a left action $\sigma : A \rightarrow \text{Sym}(G)$ and a right action $\delta : G \rightarrow \text{Sym}(A)$ such that

$$(4.1) \quad \sigma_a(xy) = \sigma_a(x)\sigma_{\delta_x(a)}(y)$$

$$(4.2) \quad \delta_x(ab) = \delta_{\sigma_b(x)}(a)\delta_x(b)$$

for all $x, y \in G$ and $a, b \in A$. If the quadruple (G, A, σ, δ) forms a matched pair of groups, then $G \times A$ is a group with multiplication

$$(x, a)(y, b) = (x\sigma_a(y), \delta_y(a)b)$$

where $a, b \in A$ and $x, y \in G$. The inverse of (x, a) is given by

$$(4.3) \quad (x, a)^{-1} = (\sigma_{a^{-1}}(x^{-1}), \delta_{x^{-1}}(a^{-1})).$$

This group will be denoted by $G \bowtie A$ and it is known also as a *biproduct* or *Zappa-Szép product* of G and A . We refer to [Tak03] for details. From equalities (4.1) and (4.2), one gets

$$(4.4) \quad (\sigma_a(x))^{-1} = \sigma_{\delta_x(a)}(x^{-1}),$$

$$(4.5) \quad (\delta_x(a))^{-1} = \delta_{\sigma_a(x)}(a^{-1}).$$

Now we show that every matched pair of groups naturally leads to an irretractable bijective solution to the PE.

Theorem 4.1. *Let (G, A, σ, δ) be a matched pair of groups and let S be the Cartesian product $A \times G$ of A and G . Then the map $s : S \times S \rightarrow S \times S$ defined by*

$$(4.6) \quad s((a, x), (b, y)) = ((a, xy), (b(\delta_x(a))^{-1}, \sigma_{\delta_x(a)}(y)))$$

is an irretractable bijective solution to the PE.

Proof. Let us define on $A \times G$ the following operation

$$(4.7) \quad (a, x)(b, y) = (a, xy).$$

Clearly, the latter endows $A \times G$ with a semigroup structure, even a left group. Hence, (2.2) is satisfied. Moreover, let us also define

$$\theta_{(a,x)}(b, y) = (b(\delta_x(a))^{-1}, \sigma_{\delta_x(a)}(y))$$

for all $a, b \in A$, $x, y \in G$. Then

$$\begin{aligned}
\theta_{(a,x)}(b, y)\theta_{(a,x)(b,y)}(c, z) &= (b(\delta_x(a))^{-1}, \sigma_{\delta_x(a)}(y))\theta_{(a,xy)}(c, z) \\
&= (b(\delta_x(a))^{-1}, \sigma_{\delta_x(a)}(y))(c(\delta_{xy}(a))^{-1}, \sigma_{\delta_{xy}(a)}(z)) \\
&= (b(\delta_x(a))^{-1}, \sigma_{\delta_x(a)}(y)\sigma_{\delta_{xy}(a)}(z)) \\
&= (b(\delta_x(a))^{-1}, \sigma_{\delta_x(a)}(y)\sigma_{\delta_y\delta_x(a)}(z)) \\
&\stackrel{(4.1)}{=} (b(\delta_x(a))^{-1}, \sigma_{\delta_x(a)}(yz)) \\
&= \theta_{(a,x)}(b, yz) = \theta_{(a,x)}((b, y)(c, z)).
\end{aligned}$$

Hence, (2.3) is satisfied. Now, let us first compute

$$\begin{aligned}
\delta_{\sigma_{\delta_x(a)}(y)}(b(\delta_x(a))^{-1}) &= \delta_{\sigma_{(\delta_x(a))^{-1}\sigma_{\delta_x(a)}(y)}}(b)\delta_{\sigma_{\delta_x(a)}(y)}((\delta_x(a))^{-1}) \\
&\stackrel{(4.5)}{=} \delta_y(b)\delta_{\sigma_{\delta_x(a)}(y)}\delta_{\sigma_a(x)}(a^{-1}) \\
&\stackrel{(4.4)}{=} \delta_y(b)\delta_{\sigma_a(x)\sigma_{\delta_x(a)}(y)}(a^{-1}) \\
&= \delta_y(b)\delta_{\sigma_a(xy)}(a^{-1}) \\
&= \delta_y(b)(\delta_{xy}(a))^{-1}.
\end{aligned}$$

It follows that

$$\begin{aligned}
\theta_{\theta_{(a,x)}(b,y)}\theta_{(a,x)(b,y)}(c, z) &= \theta_{(b(\delta_x(a))^{-1}, \sigma_{\delta_x(a)}(y))}(c(\delta_{xy}(a))^{-1}, \sigma_{\delta_{xy}(a)}(z)) \\
&= (c(\delta_{xy}(a))^{-1}(\delta_{\sigma_{\delta_x(a)}(y)}(b(\delta_x(a))^{-1}))^{-1}, \sigma_{\delta_{\sigma_{\delta_x(a)}(y)}(b(\delta_x(a))^{-1})}\sigma_{\delta_{xy}(a)}(z)) \\
&= (c(\delta_{xy}(a))^{-1}(\delta_y(b)(\delta_{xy}(a))^{-1})^{-1}, \sigma_{\delta_y(b)(\delta_{xy}(a))^{-1}}\sigma_{\delta_{xy}(a)}(z)) \\
&= (c(\delta_y(b)(\delta_{xy}(a))^{-1}\delta_{xy}(a))^{-1}, \sigma_{\delta_y(b)(\delta_{xy}(a))^{-1}\delta_{xy}(a)}(z)) \\
&= (c(\delta_y(b))^{-1}, \sigma_{\delta_y(b)}(z)) \\
&= \theta_{(b,y)}(c, z).
\end{aligned}$$

Hence, (2.4) is satisfied.

We show that s is bijective. Let $(a, x), (b, y) \in S$. Then we need to show that there exist unique $(c, u), (d, v) \in S$ such that

$$s((c, u), (d, v)) = ((a, x), (b, y)).$$

Clearly, it is necessary by the definition of s that $c = a$, $uv = x$ and $\sigma_{\delta_u(a)}(v) = y$. Next, the equality $x = uv$ is equivalent via application of σ_a in both terms, by equality (4.1), to

$$\sigma_a(x) = \sigma_a(uv) = \sigma_a(u)\sigma_{\delta_u(a)}(v) = \sigma_a(u)y.$$

Hence,

$$u = \sigma_a^{-1}(\sigma_a(x)y^{-1}).$$

Thus, v is uniquely determined as $\sigma_{\delta_u(a)}^{-1}(y)$. Finally, $d = b\delta_u(a)$, which shows that such $(c, u), (d, v) \in S$ exist and are unique.

Now we are left to prove that $(A \times G, s)$ is irretractable. First note that $A \times \{1\}$ coincides with the set of idempotents of $A \times G$. Indeed

$$(a, x)(a, x) = (a, x) \iff x = x^2 \iff x = 1.$$

Moreover, note that if $(a, 1)$ and $(b, 1)$ are such that

$$\theta_{(a,1)}(c, z) = \theta_{(b,1)}(c, z)$$

for every (c, z) , then it follows that

$$\begin{aligned} (c(\delta_1(a))^{-1}, \sigma_{\delta_1(a)}(z)) &= (c(\delta_1(b))^{-1}, \sigma_{\delta_1(b)}(z)) \\ \iff c(\delta_1(a))^{-1} &= c(\delta_1(b))^{-1} \text{ and } \sigma_{\delta_1(a)}(z) = \sigma_{\delta_1(b)}(z) \\ \iff ca^{-1} &= cb^{-1} \text{ and } \sigma_a(z) = \sigma_b(z) \\ \iff a &= b. \end{aligned}$$

Hence,

$$(a, x) \approx (b, y) \iff \theta_{(a,1)} = \theta_{(b,1)} \text{ and } x = y \iff a = b \text{ and } x = y,$$

which means that $(A \times G, s)$ is irretractable. \square

5. FROM IRRETRACTABLE SOLUTIONS TO MATCHED PAIRS OF GROUPS

In this section, we prove that finite irretractable bijective solutions to the PE define matched pairs of groups. We will use again the element $1 \in S$, introduced before Proposition 2.11 and used in the previous section and the notation $t(x, y) = (x \circ y, \psi_x(y))$ for the map $t = \tau s^{-1} \tau$ introduced in Section 3. We start with a few technical lemmas.

Lemma 5.1. *Let (S, s) be a finite irretractable bijective solution to the PE. Then $G = 1 \cdot S$ is a subgroup of (S, \cdot) and coincides with $E(S, \circ)$. Similarly, $A = 1 \circ S$ is a subgroup of (S, \circ) and coincides with $E(S, \cdot)$.*

Proof. By Proposition 3.3 we have $E(S, \circ) = F = (\ker \theta \cap E(S, \cdot))G_1$. Since (S, s) is irretractable, necessarily $\ker \theta \cap E(S, \cdot) = \{1\}$, hence $E(S, \circ) = G_1 = G$. By symmetry, applying the same argument to the solution $t = \tau s^{-1} \tau$, one also obtains $A = E(S, \cdot)$. \square

Lemma 5.2. *Let (S, s) be a finite irretractable bijective solution to the PE and let $A = 1 \circ S$ and $G = 1 \cdot S$. Then*

- the map $\sigma : A \rightarrow \text{Sym}(G)$ defined by $\sigma_a(x) = 1 \cdot \theta_{(a,1)}(1, x)$ is a left action of (A, \circ) on the set G ,
- the map $\delta : G \rightarrow \text{Sym}(A)$ defined by $\delta_x(a) = (1 \circ \psi_{(1, x^{-1})}(a^{-1}, 1))^{-1}$ is a right action of (G, \cdot) on the set A .

Proof. Let $\sigma : A \rightarrow \text{Sym}(G)$ be defined by $\sigma_a(x) = 1 \cdot \theta_{(a,1)}(1, x)$ and let the map $\delta : G \rightarrow \text{Sym}(A)$ be defined by $\delta_x(a) = (1 \circ \psi_{(1, x^{-1})}(a^{-1}, 1))^{-1}$. Let $a, b \in A$ and $x, y \in G$. Since θ is a homomorphism from (S, \circ) to $\text{Sym}(S)$, it follows that

$$\begin{aligned} \sigma_a \sigma_b(x) &= 1 \cdot \theta_{(a,1)}(1, 1 \cdot \theta_{(b,1)}(1, x)) \\ &= 1 \cdot \theta_{(a,1)}((1, 1) \cdot \theta_{(b,1)}(1, x)) \\ &\stackrel{(2.3)}{=} 1 \cdot \theta_{(a,1)}(1, 1) \cdot \theta_{(a,1) \cdot (1,1)} \theta_{(b,1)}(1, x) \\ &= 1 \cdot \theta_{(a,1) \circ (b,1)}(1, x) \\ &= 1 \cdot \theta_{(a \circ b, 1)}(1, x) \\ &= \sigma_{a \circ b}(x). \end{aligned}$$

Let us define $\sigma' : G \rightarrow \text{Sym}(A)$ by $\sigma'_x(a) = 1 \circ \psi_{(1,x)}(a, 1)$ and prove that it is a left action of (G, \cdot) on the set A . Indeed,

$$\begin{aligned} \sigma'_x \sigma'_y(a) &= 1 \circ \psi_{(1,x)}(1, 1 \circ \psi_{(1,y)}(a, 1)) \\ &= 1 \cdot \psi_{(1,x)}((1, 1) \circ \psi_{(1,y)}(a, 1)) \\ &\stackrel{(3.2)}{=} 1 \circ \psi_{(1,x)}(1, 1) \circ \psi_{(1,x) \circ (1,1)} \psi_{(1,y)}(a, 1) \\ &= 1 \circ \psi_{(1,x)(1,y)}(a, 1) \\ &= 1 \cdot \psi_{(1,xy)}(a, 1) \\ &= \sigma'_{xy}(a). \end{aligned}$$

Finally, as σ' is a left action and $\delta_x(a) = (\sigma'_{x^{-1}}(a^{-1}))^{-1}$, we have

$$\begin{aligned} \delta_x \delta_y(a) &= \delta_x(\sigma'_{y^{-1}}(a^{-1}))^{-1} \\ &= \sigma'_{x^{-1}}(\sigma'_{y^{-1}}(a^{-1}))^{-1} \\ &= \sigma'_{x^{-1}y^{-1}}(a^{-1})^{-1} \\ &= \delta_{yx}(a). \end{aligned}$$

Hence δ is a right action of (G, \cdot) on the set A . \square

Lemma 5.3. *Let (S, s) be a finite irretractable bijective solution to the PE. With the notation of Lemma 5.2 one has for any $a \in A$ and $x \in G$ that*

$$(5.1) \quad \theta_{(a,1)}(1, x) = (1, x) \circ \psi_{(1,x)}^{-1}((a^{-1}, 1))$$

$$(5.2) \quad \theta_{(a,1)(1,x)} = \theta_{\theta_{(a,1)}(1,x)}^{-1}$$

$$(5.3) \quad \psi_{(1,x)}(a, 1) = (a, 1) \cdot \theta_{(a,1)}^{-1}(1, x^{-1})$$

$$(5.4) \quad \psi_{(1,x) \circ (a,1)} = \psi_{\psi_{(1,x)}(a,1)}^{-1}.$$

Proof. First, by definition of s and s^{-1} , one obtains that

$$s^{-1}(\psi_{(1,x)}^{-1}(a^{-1}, 1), (1, x)) = ((a^{-1}, 1), (1, x) \circ \psi_{(1,x)}^{-1}(a^{-1}, 1)).$$

This implies that

$$s((a^{-1}, 1), (1, x) \circ \psi_{(1,x)}^{-1}(a^{-1}, 1)) = (\psi_{(1,x)}^{-1}(a^{-1}, 1), (1, x)).$$

In particular, one finds that $\theta_{(a^{-1},1)}((1, x) \circ \psi_{(1,x)}^{-1}(a^{-1}, 1)) = (1, x)$. As θ is an action of (A, \circ) on the set S , this can be rewritten to

$$\theta_{(a,1)}(1, x) = (1, x) \circ \psi_{(1,x)}^{-1}(a^{-1}, 1),$$

which shows the first equality.

Second, by relation (2.4), one finds that

$$\theta_{\theta_{(a,1)}(1,x)} \theta_{(a,1)(1,x)} = \theta_{(1,x)}.$$

As $\theta_{(1,x)} = \text{id}_S$, due to Proposition 2.11, the previous can be rewritten to

$$\theta_{(a,1)(1,x)} = \theta_{\theta_{(a,1)}(1,x)}^{-1},$$

which shows the second equality.

Third, by definition of s , one finds that

$$s((a, 1), \theta_{(a,1)}^{-1}(1, x^{-1})) = ((a, 1) \cdot \theta_{(a,1)}^{-1}(1, x^{-1}), (1, x^{-1})).$$

Applying s^{-1} on both sides of the equality, one finds in particular that

$$(a, 1) = \psi_{(1,x)^{-1}}((a, 1) \cdot \theta_{(a,1)}^{-1}(1, x^{-1})).$$

As ψ is a left action of (G, \cdot) on S , this can be rewritten to

$$\psi_{(1,x)}(a, 1) = (a, 1) \cdot \theta_{(a,1)}^{-1}(1, x),$$

which shows the third equality.

Finally, by relation (3.3), it follows that

$$\psi_{\psi_{(1,x)}(a,1)}\psi_{(1,x)\circ(a,1)} = \psi_{(a,1)}.$$

As the latter, by a symmetric result to Proposition 2.11, is the identity on S , one finds that

$$\psi_{(1,x)\circ(a,1)} = \psi_{\psi_{(1,x)}(a,1)}^{-1},$$

which shows the result. \square

We are now ready for the main result of this section.

Theorem 5.4. *Let (S, s) be a finite irretractable bijective solution to the PE. Then A and G form a matched pair of groups with respect to σ and δ defined in Lemma 5.2 and (S, s) is isomorphic to the solution associated to (A, G, σ, δ) as in Theorem 4.1.*

Proof. By Lemma 5.2 one has a left action $\sigma : A \rightarrow \text{Sym}(G)$ and a right action $\delta : G \rightarrow \text{Sym}(A)$. To show that the quadruple (G, A, σ, δ) is a matched pair of groups, it remains to show that for any $x, y \in G$ and $a, b \in A$ one has that

$$\begin{aligned} \sigma_a(xy) &= \sigma_a(x)\sigma_{\delta_x(a)}(y) \\ \delta_x(ab) &= \delta_{\sigma_b(x)}(a)\delta_x(b). \end{aligned}$$

We start with the former. Let $a \in A$ and $x, y \in G$.

$$\begin{aligned} \sigma_a(xy) &= 1 \cdot \theta_{(a,1)}(1, xy) \\ &= 1 \cdot \theta_{(a,1)}((1, x)(1, y)) \\ &\stackrel{(2.3)}{=} 1 \cdot \theta_{(a,1)}(1, x)\theta_{(a,1)(1,x)}(1, y) \\ &\stackrel{(5.2)}{=} \sigma_a(x) \cdot \theta_{\theta_{(a,1)}(1,x)}^{-1}(1, y) \\ &\stackrel{(5.1)}{=} \sigma_a(x) \cdot \theta_{(1,x)\circ\psi_{(1,x)}^{-1}(a^{-1},1)}^{-1}(1, y). \end{aligned}$$

As θ is a left action of (S, \circ) on the set S and $\theta_{(1,y)} = \text{id}_S$ for all $y \in G$, one obtains that

$$(5.5) \quad \theta_{(1,x)\circ\psi_{(1,x)}^{-1}(a^{-1},1)}^{-1} = \theta_{(1,1)\circ\psi_{(1,x)}^{-1}(a^{-1},1)}^{-1}.$$

Hence, reprising the earlier calculation,

$$\begin{aligned} \sigma_a(xy) &= \sigma_a(x) \cdot \theta_{(1,x)\circ\psi_{(1,x)}^{-1}(a^{-1},1)}^{-1}(1, y) \\ &= \sigma_a(x) \cdot \theta_{(1,1)\circ\psi_{(1,x)}^{-1}(a^{-1},1)}^{-1}(1, y) \\ &= \sigma_a(x) \cdot \theta_{(\delta_x(a),1)}(1, y), \end{aligned}$$

where we used the fact that ψ is an action of G on S and θ is an action of A on S . As $(1, 1)$ is a right identity of (S, \cdot) , one can continue the chain of equalities as follows.

$$\begin{aligned}\sigma_a(xy) &= \sigma_a(x) \cdot \theta_{(\delta_x(a), 1)}(1, y) \\ &= \sigma_a(x) \cdot (1, 1) \cdot \theta_{(\delta_x(a), 1)}(1, y) \\ &= \sigma_a(x) \cdot \sigma_{\delta_x(a)}(y).\end{aligned}$$

Finally, it remains to show that

$$\delta_x(ab) = \delta_{\sigma_b(x)}(a)\delta_x(b).$$

We have

$$\begin{aligned}\delta_x(a \circ b) &= \sigma'_{x^{-1}}(b^{-1} \circ a^{-1})^{-1} \\ &= ((1, 1) \circ \psi_{(1, x^{-1})}(b^{-1} \circ a^{-1}, 1))^{-1} \\ &\stackrel{(3.2)}{=} ((1, 1) \circ \psi_{(1, x^{-1})}(b^{-1}, 1) \circ \psi_{(1, x^{-1}) \circ (b^{-1}, 1)}(a^{-1}, 1))^{-1} \\ &= ((1, 1) \circ \psi_{(1, x^{-1})}(b^{-1}, 1) \circ (1, 1) \circ \psi_{((1, x^{-1}) \circ (b^{-1}, 1))}(a^{-1}, 1))^{-1} \\ &= ((1, 1) \circ \psi_{((1, x^{-1}) \circ (b^{-1}, 1))}(a^{-1}, 1))^{-1} \circ \delta_x(b) \\ &\stackrel{(5.4)}{=} \left((1, 1) \circ \psi_{\psi_{(1, x^{-1})}^{-1}(b^{-1}, 1)}(a^{-1}, 1) \right)^{-1} \circ \delta_x(b) \\ &\stackrel{(5.3)}{=} \left((1, 1) \circ \psi_{(b^{-1}, 1) \cdot \theta_{(b^{-1}, 1)}^{-1}(1, x)}^{-1}(a^{-1}, 1) \right)^{-1} \circ \delta_x(b).\end{aligned}$$

As ψ is a left action of (S, \cdot) on the set S and $\psi_{(a, 1)} = \text{id}_S$ for all $a \in A$, one obtains that

$$\psi_{(b^{-1}, 1) \cdot \theta_{(b^{-1}, 1)}^{-1}(1, x)}^{-1} = \psi_{(1, 1) \cdot \theta_{(b, 1)}(1, x)}^{-1},$$

where we also applied that θ is a left action of (S, \circ) on S to cancel the inverses of θ and b . Hence, reprising the previous calculation,

$$\begin{aligned}\delta_x(a \circ b) &= \left((1, 1) \circ \psi_{(b^{-1}, 1) \cdot \theta_{(b^{-1}, 1)}^{-1}(1, x)}^{-1}(a^{-1}, 1) \right)^{-1} \circ \delta_x(b) \\ &= \left((1, 1) \circ \psi_{(1, 1) \cdot \theta_{(b, 1)}(1, x)}^{-1}(a^{-1}, 1) \right)^{-1} \circ \delta_x(b) \\ &= \left((1, 1) \circ \psi_{(1, \sigma_b(x))}^{-1}(a^{-1}, 1) \right)^{-1} \circ \delta_x(b),\end{aligned}$$

where one applies the definition of σ . As ψ is an action of G on S , one finds from the previous that

$$\begin{aligned}\delta_x(a \circ b) &= ((1, 1) \circ \psi_{(1, \sigma_b(x))}^{-1}(a^{-1}, 1))^{-1} \circ \delta_x(b) \\ &= \delta_{\sigma_b(x)}(a) \circ \delta_x(b).\end{aligned}$$

Hence, the quadruple (G, A, σ, δ) is a matched pair of groups, as claimed.

Let (S, s') be the solution associated to the matched pair of groups (G, A, σ, δ) constructed in Theorem 4.1 with corresponding map θ' and semigroup (S, \cdot') . It is clear that the semigroups (S, \cdot) and (S, \cdot') coincide. Hence, it remains to show that for any $(a, x) = (a, 1)(1, x) \in S$, one has that $\theta'_{(a, x)} = \theta_{(a, x)}$. Let $b \in A$ and $y \in G$. Then, by relation (2.3), it is sufficient to show that $\theta'_{(a, x)}(b, 1) = \theta_{(a, x)}(b, 1)$ and

$(1, 1) \cdot \theta'_{(a,x)}(1, y) = (1, 1) \cdot \theta_{(a,x)}(1, y)$. We start with the former. By definition of θ' , we have that

$$\begin{aligned}\theta'_{(a,x)}(b, 1) &= (b \circ (\delta_x(a))^{-1}, 1) \\ &= b \circ (1, 1) \circ \psi_{(1,x^{-1})}(a^{-1}, 1).\end{aligned}$$

As $(1, x)$ and $(1, 1)$ are left identities for (S, \circ) one can rewrite the latter into

$$\begin{aligned}\theta'_{(a,x)}(b, 1) &= (b, 1) \circ (1, x) \circ \psi_{(1,x^{-1})}(a^{-1}, 1) \\ &\stackrel{(5.1)}{=} (b, 1) \circ \theta_{(a,1)}(1, x) \\ &= \theta_{\theta_{(a,1)}(1,x)}^{-1}(b, 1) \\ &\stackrel{(5.2)}{=} \theta_{(a,x)}(b, 1),\end{aligned}$$

which shows the first required equality. Finally, let $y \in G$. Then

$$\begin{aligned}(1, 1) \cdot \theta'_{(a,x)}(1, y) &= (1, \sigma_{(\delta_x(a), 1)}(y)) \\ &= (1, 1) \cdot \theta_{(1,1) \circ \psi_{(1,x^{-1})}(a^{-1}, 1)}^{-1}(1, y),\end{aligned}$$

where the latter equality holds by equality (5.5). Continuing the chain of equalities,

$$\begin{aligned}(1, 1) \cdot \theta'_{(a,x)}(1, y) &= (1, 1) \cdot \theta_{(1,1) \circ \psi_{(1,x^{-1})}(a^{-1}, 1)}^{-1}(1, y) \\ &\stackrel{(5.5)}{=} (1, 1) \cdot \theta_{(1,x) \circ \psi_{(1,x^{-1})}(a^{-1}, 1)}^{-1}(1, y) \\ &\stackrel{(5.1)}{=} (1, 1) \cdot \theta_{\theta_{(a,1)}(1,x)}^{-1}(1, y) \\ &\stackrel{(5.2)}{=} (1, 1) \cdot \theta_{(a,x)}(1, y),\end{aligned}$$

which shows that $\theta' = \theta$. Hence, the result follows. \square

Let us now discuss isomorphisms of irretractable solutions. We will see that isomorphic irretractable solutions correspond to isomorphic matched pairs of groups.

Here (and throughout), the notion of isomorphism for matched pairs is the natural one: we say that (A, G, σ, δ) and $(A', G', \sigma', \delta')$ are *isomorphic* matched pairs if there exist group isomorphisms $f : A \rightarrow A'$ and $g : G \rightarrow G'$ such that

$$g(\sigma_a(x)) = \sigma'_{f(a)}(g(x)) \quad \text{and} \quad f(\delta_x(a)) = \delta'_{g(x)}(f(a))$$

for all $a \in A$ and $x \in G$.

Proposition 5.5. *Let (A, G, σ, δ) and $(A', G', \sigma', \delta')$ be isomorphic matched pairs of groups. Then $(A \times G, s)$ and $(A' \times G', s')$, the irretractable bijective solutions to the PE as defined in Theorem 4.1, are isomorphic.*

Proof. Let $a, b \in A$ and $x, y \in G$. By definition of isomorphism of matched pairs we have

$$\begin{aligned}f(a, x)f(b, y) &= (f_1(a), f_2(x))(f_1(b), f_2(y)) = (f_1(a), f_2(x)f_2(y)) \\ &= (f_1(a), f_2(xy)) = f(a, xy) = f((a, x)(b, y)).\end{aligned}$$

Moreover,

$$\begin{aligned}
f\theta_{(a,x)}(b, y) &= f(b(\delta_x(a))^{-1}, \sigma_{\delta_x(a)}(y)) = (f_1(b(\delta_x(a))^{-1}), f_2(\sigma_{\delta_x(a)}(y))) \\
&= (f_1(b)f_1(\delta_x(a))^{-1}, \sigma'_{f_1\delta_x(a)}f_2(y)) \\
&= (f_1(b)(\delta'_{f_2(x)}f_1(a))^{-1}, \sigma'_{\delta'_{f_2(x)}f_1(a)}f_2(y)) \\
&= \theta'_{(f_1(a), f_2(x))}(f_1(b), f_2(y)) = \theta'_{f(a,x)}f(b, y).
\end{aligned}$$

Hence,

$$\begin{aligned}
(f \times f)s((a, x), (b, y)) &= (f \times f)((a, x)(b, y), \theta_{(a,x)}(b, y)) \\
&= (f(a, x)f(b, y), \theta'_{f(a,x)}f(b, y)) = s'(f(a, x), f(b, y)) \\
&= s'(f \times f)((a, x), (b, y)).
\end{aligned}$$

Hence (S, s) and (S', s') are isomorphic solutions. \square

Next, we will prove the converse. First, note that if (S, s) and (S', s') are isomorphic solutions and (S, s) is bijective and irretractable then so is (S', s') .

Proposition 5.6. *Let (S, s) and (S', s') be finite irretractable solutions to the PE. Then there exists an isomorphism of the underlying matched pairs.*

Proof. Without loss of generality (see Theorem 5.4) let us assume that (S, s) and (S', s') are, respectively, the solutions associated to the matched pairs (A, G, σ, δ) and $(A', G', \sigma', \delta')$. Let f be the isomorphism between the solutions (S, s) and (S', s') . Clearly, f defines an isomorphism of the left groups (S, \cdot) and (S', \cdot) . Since f maps $A \times \{1\} = E(S, \cdot)$ onto $E(S', \cdot) = A' \times \{1\}$, f induces a bijective map from A to A' which we denote f_1 . Note that as $(1, 1)$ is the unique idempotent in S with $\theta_{(1,1)} = \text{id}_S$, one finds that $f(1, 1) = (1, 1)$. Hence, f restricts to an isomorphism between $(1, 1)S = \{1\} \times G$ and $\{1\} \times G'$. Thus, f induces an isomorphism f_2 from G to G' . To summarize, for $a \in A$ and $x \in G$ one has $f(a, x) = (f_1(a), f_2(x))$. Next we show that f_1 is an isomorphism between (A, \circ) and (A', \circ) . Let $a, b \in A$. Then,

$$(f \times f)s((a^{-1}, 1), (b, 1)) = (f \times f)((a, 1), (b \circ a, 1)) = ((f_1(a), 1), (f_1(b \circ a), 1)).$$

On the other hand, we obtain that

$$s' \circ (f \times f)((a^{-1}, 1), (b, 1)) = ((f_1(a), 1), (f_1(b) \circ f_1(a), 1)).$$

Hence, f_1 is an isomorphism between A and A' . It remains to show that f respects the actions σ and δ . Let $a \in A$ and $x \in G$. Then

$$(f \times f)s((a, x), (1, 1)) = (f \times f)((a, x), (\delta_x(a)^{-1}, 1)) = (f(a, x), (f_1(\delta_x(a)^{-1}), 1)).$$

Similarly,

$$s'(f \times f)((a, x), (1, 1)) = ((f_1(a), f_2(x)), (\delta'_{f_2(x)}(f_1(a))^{-1}, 1)).$$

As f_1 is a group morphism, this shows that $f_1\delta_x(a) = \delta'_{f_2(x)}(f_1(a))$. Applying a similar reasoning on the tuple $((a, 1), (1, x))$ one finds that $f_2\sigma_a(x) = \sigma'_{f_1(a)}(f_2(x))$. Hence, f is an isomorphism of the matched pairs (A, G, σ, δ) and $(A', G', \sigma', \delta')$. \square

6. A COMPLETE DESCRIPTION OF FINITE BIJECTIVE SOLUTIONS

In this section, we first describe extensions of a finite irretractable bijective solution and then we provide a full classification of all finite bijective solutions (up to isomorphism).

Lemma 6.1. *Let (S, s) be a finite bijective solution to the PE. Let $e \in E(S, \cdot)$. Then, the equivalence class of e under the retract \approx has exactly $|\ker \theta \cap E(S, \cdot)|$ elements. In particular, denoting by \bar{E} the set of idempotents of the retract \bar{S} , one can identify $E(S, \cdot)$ with the Cartesian product of $\ker \theta \cap E(S, \cdot)$ and \bar{E} .*

Proof. Let $a \in E(S, \cdot)$. Let $b \in S$ be in the equivalence class of a under the retract \approx , i.e. $\theta_a = \theta_b$. Then, by definition of \approx , one has that $b \in E(S, \cdot)$. Recall that (S, \circ) is a left group. Hence, there exists an $x \in S$ such that $x \circ a = b$. As θ is a morphism of (S, \circ) to $\text{Sym}(S)$, we find that

$$\theta_a = \theta_b = \theta_{x \circ a} = \theta_x \theta_a.$$

Thus, $\theta_x \in \ker \theta$. Moreover, by Proposition 3.3, $E(S, \cdot)$ is a sub left group of (S, \circ) , which shows that $x \in E(S, \cdot) \cap \ker \theta$. This shows that there are at most $|\ker \theta \cap E(S, \cdot)|$ elements in the equivalence class of a . Vice versa, one sees easily that for any $x \in \ker \theta \cap E(S, \cdot)$ one has that $\theta_{x \circ a} = \theta_a$ and $x \circ a \in E(S, \cdot)$ for any $a \in E(S, \cdot)$. Hence, $x \circ a$ is in the equivalence class of e under \approx . As (S, \circ) is a left group, one obtains at least $|\ker \theta \cap E(S, \cdot)|$ elements in the equivalence class of a , which proves the result. \square

Recall that, for a finite irretractable bijective solution (S, s) , the set S can be identified with the Cartesian product of A and G as in Lemma 5.1.

Proposition 6.2. *Let (S, s) be a finite irretractable bijective solution to the PE, let X be a finite set, and let φ_a be a permutation of X , for every $a \in A$. Then $s' : (X \times S) \times (X \times S) \rightarrow (X \times S) \times (X \times S)$ defined by*

$$s'((\alpha, a, x), (\beta, b, y)) = ((\alpha, a, xy), (\varphi_{b(\delta_x(a))^{-1}}^{-1} \varphi_b(\beta), \theta_{(a,x)}(b, y)))$$

is a solution to the PE.

Proof. By Theorem 5.4, s' can be written as follows

$$s'((\alpha, a, x), (\beta, b, y)) = ((\alpha, a, xy), (\varphi_{b(\delta_x(a))^{-1}}^{-1} \varphi_b(\beta), b(\delta_x(a))^{-1}, \sigma_{\delta_x(a)}(y))).$$

Clearly, $X \times S$ has a structure of a left group with respect to the multiplication given by $(\alpha, a, x)(\beta, b, y) = (\alpha, a, xy)$ and equality (2.2) is satisfied. Hence, it remains to show equalities (2.3) and (2.4). We start with equality (2.3). Let $\alpha, \beta, \gamma \in X, a, b, c \in A$ and $x, y, z \in G$. Then,

$$\begin{aligned} \theta'_{(\alpha, a, x)}((\beta, b, y)(\gamma, c, z)) &= \theta'_{(\alpha, a, x)}(\beta, b, yz) \\ &= (\varphi_{b(\delta_x(a))^{-1}}^{-1} \varphi_b(\beta), \theta_{(a,x)}(b, yz)) \\ &= (\varphi_{b(\delta_x(a))^{-1}}^{-1} \varphi_b(\beta), \theta_{(a,x)}(b, y) \theta_{(a,xy)}(c, z)). \end{aligned}$$

On the other hand, one has that

$$\begin{aligned} &\theta'_{(\alpha, a, x)}(\beta, b, y) \theta'_{(\alpha, a, xy)}(\gamma, c, z) \\ &= (\varphi_{b(\delta_x(a))^{-1}}^{-1} \varphi_b(\beta), \theta_{(a,x)}(b, y)) (\varphi_{c(\delta_{xy}(a))^{-1}}^{-1} \varphi_c(\gamma), \theta_{(a,xy)}(c, z)) \\ &= (\varphi_{b(\delta_x(a))^{-1}}^{-1} \varphi_b(\beta), \theta_{(a,x)}(b, y) \theta_{(a,xy)}(c, z)). \end{aligned}$$

As equality (2.3) holds for (S, s) , it follows indeed that equality (2.3) holds for $(X \times S, s')$. It remains to prove equality (2.4). Note that, by the definition of θ' ,

$$\theta'_{(\alpha, a, x)(\beta, b, y)} \theta'_{(\alpha, a, xy)}(\gamma, c, z) = \theta'_{(\zeta, \theta_{(a, x)}(b, y))}(\varphi_{c\delta_{xy}(a)}^{-1} \varphi_c(\gamma), \theta_{(a, xy)}(c, z)),$$

for some $\zeta \in X$. This in turn is equal to

$$(\varphi_{c\delta_{xy}(a)}^{-1} \delta_{\sigma_{\delta_x(a)}(y)}(b\delta_x(a)^{-1})^{-1} \varphi_{c\delta_{xy}(a)} \varphi_{c\delta_{xy}(a)}^{-1} \varphi_c(\gamma), \theta_{\theta_{(a, x)}(b, y)} \theta_{(a, xy)}(c, z)).$$

This can be simplified to

$$(\varphi_{c\delta_{xy}(a)}^{-1} \delta_{\sigma_{\delta_x(a)}(y)}(b\delta_x(a)^{-1})^{-1} \varphi_c(\gamma), \theta_{\theta_{(a, x)}(b, y)} \theta_{(a, xy)}(c, z)).$$

Note that by equality (4.2), one has that

$$\delta_y(b) = \delta_{\sigma_{\delta_x(a)}(y)}(b\delta_x(a)^{-1})\delta_y\delta_x(a) = \delta_{\sigma_{\delta_x(a)}(y)}(b\delta_x(a)^{-1})\delta_{xy}(a).$$

Applying this formula on the previous expression, one simplifies it to

$$\varphi_{c\delta_y(b)}^{-1} \varphi_c(\gamma), \theta_{\theta_{(a, x)}(b, y)} \theta_{(a, xy)}(c, z)).$$

As

$$\theta'_{(\beta, b, y)}(\gamma, c, z) = (\varphi_{c\delta_y(b)}^{-1} \varphi_c(\gamma), \theta_{(b, y)}(c, z)),$$

one finds that equality (2.4) holds for $(X \times S, s')$ as it holds for (S, s) . Hence, $(X \times S, s')$ is a solution to the PE. Moreover, $(X \times S, s')$ is bijective. Indeed, let $(\alpha, a, x), (\beta, b, y) \in X \times S$ be given. Then we need to show there exist unique $(\gamma, c, z), (\zeta, d, w) \in X \times S$ such that

$$s'((\gamma, c, z), (\zeta, d, w)) = ((\alpha, a, x), (\beta, b, y)).$$

One finds that this implies that

$$s((c, z), (d, w)) = ((a, x), (b, y)).$$

As (S, s) is bijective, it is known that there exist such unique pairs $(c, z), (d, w) \in S$. By the definition of s' it is clear that $\gamma = \alpha$. Finally, as the maps φ are permutations and depend only on the pairs $(c, z), (d, w)$, it follows that there indeed exists a unique $\zeta \in X$ such that

$$s((\gamma, c, z), (\zeta, d, w)) = ((\alpha, a, x), (\beta, b, y)),$$

proving the result. \square

The solution (S', s') constructed in Proposition 6.2 will be called the *extension* of (S, s) by X and $\varphi = \{\varphi_a : a \in A\}$ and denoted by $\text{Ext}_X^\varphi(S, s)$.

Proposition 6.3. *Let (S, s) be a finite irretractable bijective solution to the PE corresponding to the matched pair (A, G, σ, δ) . Let X be a non-empty set. Then, $\text{Ext}_X^\varphi(S, s)$ is isomorphic to $\text{Ext}_X^\rho(S, s)$, for any sets of bijections φ and ρ .*

Proof. Define the map $\xi : \text{Ext}_X^\varphi(S, s) \rightarrow \text{Ext}_X^\rho(S, s)$ by

$$\xi(\alpha, x, a) = (\rho_x^{-1} \varphi_x(\alpha), x, a).$$

Clearly, ξ is a bijective map. Denote $\text{Ext}_X^\varphi(S, s) = (X \times S, s_\varphi)$ and $\text{Ext}_X^\rho(S, s) = (X \times S, s_\rho)$. Then for any $(\alpha, a, x), (\beta, b, y) \in X \times S$, by the definition of s_φ, s_ρ and

ξ , one has that

$$\begin{aligned}
& (\xi \times \xi) s_\rho((\alpha, a, x), (\beta, b, y)) \\
&= (\xi \times \xi)((\alpha, a, xy), (\varphi_{b\delta_x(a)}^{-1} \varphi_b(\beta), b(\delta_x(a))^{-1}, \sigma_{\delta_x(a)}(y))) \\
&= ((\rho_a^{-1} \varphi_a(\alpha), a, xy), (\rho_{b\delta_x(a)}^{-1} \varphi_{b\delta_x(a)} \varphi_b(\beta), b(\delta_x(a))^{-1}, \sigma_{\delta_x(a)}(y))) \\
&= ((\rho_a^{-1} \varphi_a(\alpha), a, xy), (\rho_{b\delta_x(a)}^{-1} \varphi_b(\beta), b(\delta_x(a))^{-1}, \sigma_{\delta_x(a)}(y))) \\
&= ((\rho_a^{-1} \varphi_a(\alpha), a, xy), (\rho_{b\delta_x(a)}^{-1} \rho_b \rho_b^{-1} \varphi_b(\beta), b(\delta_x(a))^{-1}, \sigma_{\delta_x(a)}(y))) \\
&= s_\rho((\rho_a^{-1} \varphi_a(\alpha), a, x), (\rho_b^{-1} \varphi_b(\beta), b, y)) \\
&= s_\rho(\xi \times \xi)((\alpha, a, x), (\beta, b, y)).
\end{aligned}$$

This shows that ξ is an isomorphism of solutions. \square

Hence, up to isomorphism there is only one extension for a given finite irretractable bijective solution (S, s) and a non-empty set X .

Now we show that every finite bijective solution to the PE can be obtained as the extension of its retract. In view of Proposition 6.3, this is in a big contrast to the case of the retract operation on set-theoretic solutions to the Yang–Baxter Equation, see the discussion at the beginning of Section 3.

Theorem 6.4. *Let (S, s) be a finite bijective solution to the PE and let (\bar{S}, \bar{s}) be its retract. Then (S, s) is an extension of (\bar{S}, \bar{s}) by $X = \ker \theta \cap E(S, \cdot)$.*

Proof. Note that, by Lemma 6.1, one can identify the set S with $X \times A \times G$, where the decomposition $\bar{S} = A \times G$ with matched pair of groups (A, G, σ, δ) is such as in Theorem 5.4 and X is the set $\ker \theta \cap E(S, \cdot)$. Let $\alpha, \beta \in X, a, b \in A$ and $x, y \in G$. Then there exist $\gamma \in X, c \in A$ and $z \in G$ such that

$$\theta_{(\alpha, a, x)}(\beta, b, y) = (\gamma, c, z).$$

As taking the retract of a solution is a morphism of solutions, one finds that $(c, z) = \theta_{(a, x)}(b, y)$. Hence,

$$\theta_{(\alpha, a, x)}(\beta, b, y) = (\gamma, \theta_{(a, x)}(b, y)).$$

As $\theta_{(\alpha, a, x)} = \theta_{(\alpha', a, x)}$ for all $\alpha' \in X$, the element γ is independent of α . Moreover, by equality (2.3), one has that

$$\theta_{(\alpha, a, x)}(\beta, b, y) = \theta_{(\alpha, a, x)}(\beta, b, 1) \theta_{(\alpha, a, x)}(\beta, b, y),$$

which shows that γ is independent of y . Finally, notice that

$$\theta_{(\alpha, a, x)} = \theta_{\theta_{(\alpha, a, x)}(\alpha, 1, 1)^{-1}} = \theta_{(\alpha', \delta_x(a), 1)}.$$

Thus, γ depends on $\delta_x(a)$ instead of on a and x separately. Hence, denote

$$\theta_{(\alpha, a, x)}(\beta, b, y) = (\eta_{\delta_x(a), b}(\beta), \theta_{(a, x)}(b, y)).$$

Note that the maps η are bijective, as s is bijective. We examine equality (2.4) to obtain conditions on the maps η . Let $\alpha, \beta, \gamma \in X, a, b, c \in A$ and $x, y, z \in G$. Then for some $\zeta \in X$ one has

$$\begin{aligned}
& \theta_{\theta_{(\alpha, a, x)}(\beta, b, y)} \theta_{(\alpha, a, xy)}(\gamma, c, z) \\
&= \theta_{(\zeta, b\delta_x(a)^{-1}, \sigma_{\delta_x(a)}(y))} (\eta_{\delta_{xy}(a), c}(\gamma), c\delta_{xy}(a)^{-1}, \sigma_{\delta_{xy}(a)}(z)) \\
&= (\eta_{\sigma_{\delta_x(a)}(y)}(b\delta_x(a)^{-1}, c\delta_{xy}(a)^{-1}) \eta_{c\delta_{xy}(a)^{-1}}(\gamma), d, w) \\
&= (\eta_{\delta_y(b)\delta_{xy}(a)^{-1}, c\delta_{xy}(a)^{-1}} \eta_{\delta_{xy}(a), c}(\gamma), d, w),
\end{aligned}$$

with $d \in A$ and $w \in G$. Calculating the right hand side of equality (2.4) and equating its first component with the first component in the previous calculation, one finds the equality

$$\eta_{\delta_y(b)\delta_{xy}(a)^{-1},c\delta_{xy}(a)^{-1}}\eta_{\delta_{xy}(a)^{-1},c} = \eta_{\delta_y(b),c}.$$

Note that as δ_{xy} and δ_y are bijective maps, this can be rewritten such that for any $a, b, c \in A$ one has that

$$\eta_{ba^{-1},ca^{-1}}\eta_{a^{-1},c} = \eta_{b,c}.$$

Note that $\eta_{1,c}(\gamma) = \gamma$ as this corresponds to $\theta_{(\alpha,1,1)}(\gamma, c, 1) = (\gamma, c, 1)$. Moreover, if we let $a = c$, then we see that

$$\eta_{bc^{-1},1}\eta_{c,c} = \eta_{b,c}.$$

Applying this equality for $b = 1$, we find that

$$\eta_{c^{-1},1}\eta_{c,c} = \eta_{1,c} = \text{id}_X.$$

Hence,

$$\eta_{b,c} = \eta_{bc^{-1},1}\eta_{c,c} = \eta_{bc^{-1},1}\eta_{c^{-1},1}^{-1}.$$

Denote $\varphi_t = \eta_{t^{-1},1}^{-1}$. Then, one reformulates the equality to

$$\eta_{b,c} = \varphi_{cb^{-1}}^{-1}\varphi_c.$$

Applying this in the formula for θ , we obtain that

$$\theta_{(\alpha,a,x)}(\beta, b, y) = ((\varphi_{b\delta_x(a)^{-1}}^{-1}\varphi_b(\beta), \theta_{(a,x)}(b, y)).$$

Thus, we have shown that every finite bijective solution can be written as an extension of its retract as in Proposition 6.2. \square

In summary, one obtains our main result which is the following complete characterization of finite bijective solutions to the PE.

Theorem 6.5. *Let (A, G, σ, δ) be a matched pair of groups. Then, for any non-empty set X and set of permutations $\{\varphi_a \mid a \in A\}$, the following defines a bijective solution to the PE on $X \times A \times G$,*

$$s((\alpha, a, x), (\beta, b, y)) = ((\alpha, a, xy), (\varphi_{b(\delta_x(a))^{-1}}^{-1}\varphi_b(\beta), b(\delta_x(a))^{-1}, \sigma_{\delta_x(a)}(y))).$$

Vice versa, every finite bijective solution (S, s) to the PE is such a solution, where the corresponding matched pair (A, G, σ, δ) is determined by the retract of (S, s) , as in Theorem 5.4.

We conclude this section with an explicit description of isomorphism classes of finite bijective solutions to the PE.

Corollary 6.6. *Let (S, s) and (S', s') be finite bijective solutions to the PE. Let (A, G, σ, δ) and $(A', G', \sigma', \delta')$ be the matched pairs determined by the retracts of (S, s) and (S', s') , respectively, and let X, X' be the corresponding extension sets in Theorem 6.5. Then the following are equivalent:*

- (1) $(S, s) \cong (S', s')$ as set-theoretic solutions to the PE,
- (2) $|X| = |X'|$ and $(A, G, \sigma, \delta) \cong (A', G', \sigma', \delta')$ as matched pairs.

In particular, the isomorphism classes of finite bijective solutions to the PE are in a bijection with pairs consisting of an isomorphism class of matched pairs of groups and a positive integer.

Proof. By Theorem 6.5, any finite bijective solution is isomorphic to one of the form $X \times A \times G$ with X a set and (A, G) a matched pair of groups determined by its retract. Its isomorphism class is determined uniquely by the isomorphism class of the matched product, Proposition 5.6, and the cardinality of X , Proposition 6.3. \square

7. CONCLUDING REMARKS AND EXAMPLES

We first show that, as a direct consequence of Proposition 6.3 and Theorem 6.4, one recovers the classification of involutive solutions obtained in [CJK20], in the finite case.

Let (S, s) be a finite bijective solution to the PE such that $s^2 = \text{id}$. Then, by Theorem 6.4, (S, s) is an extension of its retract (\bar{S}, \bar{s}) . Since $s^2 = \text{id}$ then also $\bar{s}^2 = \text{id}$. By Theorem 5.4 we have

$$\bar{s}^2((a, x), (b, y)) = ((a, xy\sigma_{\delta_x(a)}(y)), (b(\delta_x(a))^{-1}(\delta_{xy}(a))^{-1}, \sigma_{\delta_{xy}(a)}\sigma_{\delta_x(a)}(y))).$$

Hence, $y\sigma_{\delta_x(a)}(y) = 1$. Since each δ_x is bijective, it follows that $\sigma_c(y) = y^{-1}$, for every $y \in G$ and $c \in A$. Moreover, we obtain $(\delta_x(a))^{-1}(\delta_{xy}(a))^{-1} = 1$, for all $x, y \in G$ and $a \in A$. Therefore, $\delta_x = \delta_z$ for all $x, z \in G$ and $(\delta_x(a))^2 = 1$. Consequently, A is an elementary abelian 2-group. Since σ is a left action of A on G , we have $\sigma_{ab} = \sigma_a\sigma_b$ and hence $y = y^{-1}$ for every $y \in G$ and $\sigma_a = \text{id}$ for every $a \in A$. In particular, G is an elementary abelian 2-group. Since δ is a right action of G on A , we get that $\delta_{xy} = \delta_y\delta_x$, so that $\delta_x = \text{id}$ for every $x \in G$. Therefore $G \times A$ is an ordinary direct product of groups. Conversely, it is easy to see that if G and A are elementary abelian 2-groups, $\sigma_a = \text{id}$ for every $a \in A$, and $\delta_x = \text{id}$ for every $x \in G$, then conditions (4.1) and (4.2) are satisfied and the solution defined in Theorem 4.1 is involutive. So, in view of Proposition 6.3 and Theorem 6.4, we recover the main result of [CJK20].

We next describe several sources of matched products of groups, and hence of explicit irretractable bijective solutions to the PE via Theorem 4.1. We start with a basic construction (the semidirect product) and then discuss examples arising from skew braces via holomorph/permutation-group methods.

Example 7.1. Let G and A be groups and assume A acts on G by automorphisms, equivalently we are given a group homomorphism $\sigma : A \rightarrow \text{Aut}(G)$. Define a right action $\delta : G \rightarrow \text{Sym}(A)$ to be trivial, i.e. $\delta_x = \text{id}_A$ for all $x \in G$. Then (G, A, σ, δ) is a matched pair of groups: condition (4.1) reduces to $\sigma_a(xy) = \sigma_a(x)\sigma_a(y)$, i.e. $\sigma_a \in \text{Aut}(G)$ and condition (4.2) is trivially satisfied. The corresponding irretractable solution according to Theorem 6.5 is $s : (A \times G)^2 \rightarrow (A \times G)^2$ defined by

$$s((a, x), (b, y)) = ((a, xy), (ba^{-1}, \sigma_a(y))).$$

In this case, our matched product of groups can be identified with the inner semidirect product $G \rtimes A$ of its normal subgroup G and a subgroup A and $\sigma_a(x) = axa^{-1}$ for $a \in A, x \in G$.

More generally, exact factorizations provide one of the most concrete sources of matched pairs. Recall that a group S factorizes through subgroups G and A if $S = GA$, and the factorization is *exact* if moreover $G \cap A = \{1\}$ (equivalently: every $s \in S$ has a unique decomposition $s = xa$ with $x \in G, a \in A$). In this situation one defines mutual actions by the unique decomposition

$$ax = (a \triangleright x)(a \triangleleft x), \quad a \in A, x \in G,$$

with $a \triangleright x \in G$ and $a \triangleleft x \in A$. Then $(G, A, \triangleleft, \triangleright)$ defines a matched pair of groups and the resulting matched product $G \bowtie A$ recovers S .

Clearly, there are many matched pairs of groups that do not come from (semi)direct products, in the sense that neither factor is normal. For example, the alternating group A_5 admits an exact factorization $A_5 = AG$ with $G \cong C_5$ and $A \cong A_4$. In this case, both actions σ and δ are nontrivial.

A particularly rich and well-studied source of such structures comes from skew braces, which are central in the theory of set-theoretic solutions to the Yang–Baxter Equation: given a skew brace one obtains a (non-degenerate) set-theoretic solution, and conversely every non-degenerate such solution yields a skew brace [GV17] (see also the earlier group-with-braiding approach of Lu–Yan–Zhu [LYZ00]). Braces, and later skew braces, were introduced by Rump [Rum07] and by Guarnieri–Vendramin [GV17], and they have played a central role in the subject; see, for instance, [CO21; CJO14; Gat18; LV19] and the recent survey [Ven24] and references therein. Moreover, a skew brace canonically determines a matched pair of groups in which the multiplicative group acts on itself from the left and from the right [SV18, Lemma 5.9]. By Theorem 6.5, this matched pair also produces an irretractable set-theoretic solution to the PE. This highlights an interesting connection between set-theoretic solutions to the Yang–Baxter Equation and to the PE; some connections between the two equations in their general form have already been pointed out in [CMS20; Lau19; VV94].

Example 7.2. Let $(B, +, \circ)$ be a skew brace [GV17]. Recall that we can define a left action $\lambda : (B, \circ) \rightarrow \text{Aut}(B, +)$ by $\lambda_a(b) = -a + a \circ b$ and a right action $\rho : (B, \circ) \rightarrow \text{Sym}(B)$ by $\rho_b(a) = (\lambda_a(b))' \circ a \circ b$. It is known that (B, \circ) with respect to the actions λ and ρ forms a matched pair of groups, see for instance [SV18, Lemma 5.9]. Therefore, any skew brace yields an irretractable bijective solution $(B \times B, s)$ to the PE such that

$$\begin{aligned} s((a, x), (b, y)) &= ((a, x \circ y), (b \circ (\rho_x(a))', \lambda_{\rho_x(a)}(y))) \\ &= ((a, x \circ y), (b \circ (x' \circ a - x'), (a' + x)' \circ (a' + y))). \end{aligned}$$

Skew braces can also be described in terms of regular subgroups of holomorphs. Fix an additive group $(B, +)$. Then skew brace structures on B correspond to regular subgroups of the holomorph $\text{Hol}(B, +) = (B, +) \rtimes \text{Aut}(B, +)$ up to conjugacy; see, for instance, [GV17; BNY20]. Each such regular subgroup determines a skew brace, and Example 7.2 then yields an explicit irretractable solution to the PE.

This holomorph perspective extends further to the notion of skew bracoids. Let H be a group and let $G \leq \text{Hol}(H)$ act transitively on the underlying set of H via the natural holomorph action. Following [Col+25], the pair (G, H) is called a *skew bracoid* if this action is transitive; it is said to *contain a brace* if G contains a regular subgroup of $\text{Hol}(H)$. If (G, H) is a skew bracoid containing a brace, then G admits an exact factorization $G = HS$, where $S = \text{Stab}_G(1)$, which yields a matched pair between H and S [Col+25, Proposition 2.2]. Consequently, skew bracoids containing a brace provide further examples of matched pairs and, via Theorem 6.5, of irretractable bijective solutions to the PE.

This also creates a bridge to Hopf–Galois theory. By the Greither–Pareigis theorem, Hopf–Galois structures on a finite separable field extension correspond to transitive subgroups of a suitable permutation group. Byott’s reformulation [Byo96] expresses this in terms of transitive subgroups inside suitable holomorphs, reducing

classification to the study of transitive holomorph subgroups. In this context, algorithms that enumerate transitive subgroups have been developed; see for instance [Dar25; CRV15]. Therefore, these computational outputs also provide effective input for constructing matched pairs and hence irretractable solutions to the PE via Theorem 6.5.

We conclude by exploring the relation between set-theoretic solutions to the PE and Hopf algebras with positive bases. Recently, the first author and Janssens [CJ26] investigated the relationship between bijective set-theoretic solutions to the PE and Hopf algebras, making explicit at the set-theoretic level a connection originating in work of Militaru [Mil04] and Davydov [Dav01]. In particular, [CJ26] proves that any finite set-theoretic solution gives rise to a Hopf algebra with the so called positive basis property. Even if this is shown without using the full strength of the classification in Theorem 1.1, the argument relies on Theorem 2.4 where we prove that the semigroup S associated to a set-theoretic solution to the PE is a left group. In addition, [CJ26] extends the Lu–Yan–Zhu theory of Hopf algebras with positive bases [LYZ01] to arbitrary fields of characteristic 0 (see [CJ26, Corollary B]).

It is then natural to ask whether the Lu–Yan–Zhu classification [LYZ01] could provide an alternative proof of Theorem 1.1. As explained in the remark following [CJ26, Corollary B] this approach does not directly recover the set-theoretic classification. The obstruction is twofold: first, the Hopf algebra decomposition obtained via the Fundamental Theorem of Hopf modules does not preserve the canonical bases; second, the groups arising in the resulting factorization appear only after a non-explicit rescaling procedure. Overcoming these obstacles would require an explicit description of all set-theoretic bases of the relevant bicrossed product Hopf algebra.

ACKNOWLEDGMENTS

Colazzo acknowledges support from the Engineering and Physical Sciences Research Council [grant number EP/V005995/1] during the early stages of this work. The authors wish to thank Leandro Vendramin for stimulating discussions and computer calculations that began during the “Algebra of the Yang–Baxter equation” conference in Bedlewo in 2022, from which this project originated. The authors wish to thank the anonymous referees for careful reading of the manuscript and for their helpful comments and suggestions.

REFERENCES

- [BS93] S. Baaĵ and G. Skandalis. “Unitaires multiplicatifs et dualité pour les produits croisés de C^* -algèbres”. In: *Ann. Sci. École Norm. Sup. (4)* 26.4 (1993), pp. 425–488. ISSN: 0012-9593.
- [BS98] S. Baaĵ and G. Skandalis. “Transformations pentagonales”. In: *C. R. Acad. Sci. Paris Sér. I Math.* 327.7 (1998), pp. 623–628. ISSN: 0764-4442.
- [BCV18] D. Bachiller, F. Cedó, and L. Vendramin. “A characterization of finite multipermutation solutions of the Yang–Baxter equation”. In: *Publ. Mat.* 62.2 (2018), pp. 641–649. ISSN: 0214-1493,2014-4350.

- [BNY20] V. G. Bardakov, M. V. Neshchadim, and M. K. Yadav. “Computing skew left braces of small orders”. In: *Int. J. Algebra Comput.* 30.4 (2020), pp. 839–851. ISSN: 0218-1967.
- [Byo96] N. P. Byott. “Uniqueness of Hopf Galois structure for separable field extensions”. In: *Commun. Algebra* 24.10 (1996), pp. 3217–3228. ISSN: 0092-7872.
- [Cas26] M. Castelli. “On commutative set-theoretic solutions of the Pentagon Equation”. In: *Semigroup Forum* (2026).
- [CMM20] F. Catino, M. Mazzotta, and M. M. Miccoli. “Set-theoretical solutions of the pentagon equation on groups”. In: *Comm. Algebra* 48.1 (2020), pp. 83–92. ISSN: 0092-7872.
- [CMS20] F. Catino, M. Mazzotta, and P. Stefanelli. “Set-theoretical solutions of the Yang-Baxter and pentagon equations on semigroups”. In: *Semigroup Forum* 101.2 (2020), pp. 259–284. ISSN: 0037-1912.
- [CJO10] F. Cedó, E. Jespers, and J. Okniński. “Retractability of set theoretic solutions of the Yang–Baxter equation”. In: *Adv. Math.* 224.6 (2010), pp. 2472–2484. ISSN: 0001-8708.
- [CJO14] F. Cedó, E. Jespers, and J. Okniński. “Braces and the Yang–Baxter equation”. In: *Comm. Math. Phys.* 327.1 (2014), pp. 101–116. ISSN: 0010-3616.
- [CO21] F. Cedó and J. Okniński. “Constructing finite simple solutions of the Yang-Baxter equation”. In: *Adv. Math.* 391 (2021). Id/No 107968, p. 40. ISSN: 0001-8708.
- [CP61] A. H. Clifford and G. B. Preston. *The algebraic theory of semigroups. Vol. I.* Mathematical Surveys, No. 7. American Mathematical Society, Providence, R.I., 1961, pp. xv+224.
- [CJ26] I. Colazzo and G. Janssens. *On set-theoretic solutions of pentagon equation and positive basis Hopf algebras.* 2026. arXiv: [2601.22089 \[math.RA\]](#).
- [CJK20] I. Colazzo, E. Jespers, and L. Kubat. “Set-theoretic solutions of the pentagon equation”. In: *Comm. Math. Phys.* 380.2 (2020), pp. 1003–1024. ISSN: 0010-3616.
- [Col+25] I. Colazzo, A. Koch, I. Martin-Lyons, and P. J. Truman. “Skew bracoids containing a skew brace”. In: *Journal of Algebra and Its Applications* (2025), p. 2650235.
- [CRV15] T. Crespo, A. Rio, and Montserrat V. “From Galois to Hopf Galois: theory and practice”. In: *Trends in number theory. Fifth Spanish meeting on number theory, Universidad de Sevilla, Sevilla, Spain, July 8–12, 2013. Proceedings.* Providence, RI: American Mathematical Society (AMS); Madrid: Real Sociedad Matemática Española (RSME), 2015, pp. 29–46. ISBN: 978-0-8218-9858-1; 978-1-4704-2729-0.
- [Dar25] A. Darlington. *An Algorithm for Computing Hopf–Galois Structures and Skew Bracoids of Low Degree.* 2025. arXiv: [2508.03372 \[math.GR\]](#).
- [Dav01] A. A. Davydov. “Pentagon equation and matrix bialgebras”. In: *Comm. Algebra* 29.6 (2001), pp. 2627–2650. ISSN: 0092-7872.
- [ESS99] P. Etingof, T. Schedler, and A. Soloviev. “Set-theoretical solutions to the quantum Yang–Baxter equation”. In: *Duke Math. J.* 100.2 (1999), pp. 169–209. ISSN: 0012-7094.

- [Gat18] T. Gateva-Ivanova. “Set-theoretic solutions of the Yang–Baxter equation, braces and symmetric groups”. In: *Adv. Math.* 338 (2018), pp. 649–701. ISSN: 0001-8708.
- [GC12] T. Gateva-Ivanova and P. Cameron. “Multipermutation solutions of the Yang–Baxter equation”. In: *Commun. Math. Phys.* 309.3 (2012), pp. 583–621. ISSN: 0010-3616.
- [GM08] T. Gateva-Ivanova and S. Majid. “Matched pairs approach to set theoretic solutions of the Yang–Baxter equation”. In: *J. Algebra* 319.4 (2008), pp. 1462–1529. ISSN: 0021-8693,1090-266X.
- [GV17] L. Guarnieri and L. Vendramin. “Skew braces and the Yang–Baxter equation”. In: *Math. Comp.* 86.307 (2017), pp. 2519–2534. ISSN: 0025-5718.
- [JL05] L. Jiang and M. Liu. “On set-theoretical solution of the pentagon equation”. In: *Adv. Math. (China)* 34.3 (2005), pp. 331–337. ISSN: 1000-0917.
- [Kas94] R. M. Kashaev. “Quantum dilogarithm as a $6j$ -symbol”. In: *Mod. Phys. Lett. A* 9.40 (1994), pp. 3757–3768. ISSN: 0217-7323.
- [Kas96] R. M. Kashaev. “The Heisenberg double and the pentagon relation”. In: *Algebra i Analiz* 8.4 (1996), pp. 63–74. ISSN: 0234-0852.
- [Kas11] R. M. Kashaev. “Fully noncommutative discrete Liouville equation”. In: *Infinite analysis 2010. Developments in quantum integrable systems*. RIMS Kôkyûroku Bessatsu, B28. Res. Inst. Math. Sci. (RIMS), Kyoto, 2011, pp. 89–98.
- [KR07] R. M. Kashaev and N. Reshetikhin. “Symmetrically factorizable groups and self-theoretical solutions of the pentagon equation”. In: *Quantum groups*. Vol. 433. Contemp. Math. Amer. Math. Soc., Providence, RI, 2007, pp. 267–279.
- [KS98] R. M. Kashaev and S. M. Sergeev. “On pentagon, ten-term, and tetrahedron relations”. In: *Comm. Math. Phys.* 195.2 (1998), pp. 309–319. ISSN: 0010-3616.
- [Kaw10] K. Kawamura. “Pentagon equation arising from state equations of a C^* -bialgebra”. In: *Lett. Math. Phys.* 93.3 (2010), pp. 229–241. ISSN: 0377-9017,1573-0530.
- [Lau19] R. Laugwitz. “Comodule algebras and 2-cocycles over the (braided) Drinfeld double”. In: *Commun. Contemp. Math.* 21.4 (2019), pp. 1850045, 46. ISSN: 0219-1997,1793-6683.
- [LV19] V. Lebed and L. Vendramin. “On structure groups of set-theoretic solutions to the Yang–Baxter equation”. In: *Proc. Edinb. Math. Soc., II. Ser.* 62.3 (2019), pp. 683–717. ISSN: 0013-0915.
- [LYZ00] J.-H. Lu, M. Yan, and Y.-C. Zhu. “On the set-theoretical Yang–Baxter equation”. In: *Duke Math. J.* 104.1 (2000), pp. 1–18. ISSN: 0012-7094.
- [LYZ01] J.-H. Lu, M. Yan, and Y.-C. Zhu. “On Hopf algebras with positive bases”. In: *J. Algebra* 237.2 (2001), pp. 421–445. ISSN: 0021-8693.
- [Mai94] J.-M. Maillet. “On pentagon and tetrahedron equations”. In: *Algebra i Analiz* 6.2 (1994), pp. 206–214. ISSN: 0234-0852.
- [MPS24] M. Mazzotta, V. Pérez-Calabuig, and P. Stefanelli. “Set-theoretical solutions of the pentagon equation on Clifford semigroups”. In: *Semigroup Forum* 108 (2024), pp. 413–431.

- [Mil04] G. Militaru. “Heisenberg double, pentagon equation, structure and classification of finite-dimensional Hopf algebras”. In: *J. London Math. Soc.* (2) 69.1 (2004), pp. 44–64. ISSN: 0024-6107.
- [MS89] G. Moore and N. Seiberg. “Classical and quantum conformal field theory”. In: *Comm. Math. Phys.* 123.2 (1989), pp. 177–254. ISSN: 0010-3616,1432-0916.
- [Rum07] W. Rump. “Braces, radical rings, and the quantum Yang-Baxter equation.” In: *J. Algebra* 307.1 (2007), pp. 153–170. ISSN: 0021-8693.
- [SV18] A. Smoktunowicz and L. Vendramin. “On skew braces (with an appendix by N. Byott and L. Vendramin)”. In: *J. Comb. Algebra* 2.1 (2018), pp. 47–86. ISSN: 2415-6302,2415-6310.
- [Str98] R. Street. “Fusion operators and cocycloids in monoidal categories”. In: *Appl. Categ. Structures* 6.2 (1998), pp. 177–191. ISSN: 0927-2852.
- [Tak03] M. Takeuchi. “Survey on matched pairs of groups—an elementary approach to the ESS-LYZ theory”. In: *Noncommutative geometry and quantum groups (Warsaw, 2001)*. Vol. 61. Banach Center Publ. Polish Acad. Sci. Inst. Math., Warsaw, 2003, pp. 305–331.
- [VV94] A. Van Daele and S. Van Keer. “The Yang-Baxter and pentagon equation”. In: *Compositio Math.* 91.2 (1994), pp. 201–221. ISSN: 0010-437X, 1570-5846.
- [Ven24] L. Vendramin. “Skew braces: a brief survey”. In: *Geometric methods in physics XL, workshop, Białowieża, Poland, June 20–25, 2023*. Cham: Birkhäuser, 2024, pp. 153–175. ISBN: 978-3-031-62406-3; 978-3-031-62409-4; 978-3-031-62407-0.
- [Wor96] S. L. Woronowicz. “From multiplicative unitaries to quantum groups”. In: *Internat. J. Math.* 7.1 (1996), pp. 127–149. ISSN: 0129-167X,1793-6519.

SCHOOL OF MATHEMATICS, UNIVERSITY OF LEEDS, LEEDS, UK. ORCID: 0000-0002-2713-0409
Email address: I.Colazzo@leeds.ac.uk

INSTITUTE OF MATHEMATICS, UNIVERSITY OF WARSAW, BANACHA 2, 02-097 WARSAW, POLAND.
 ORCID: 0000-0002-2434-3425
Email address: okninski@mimuw.edu.pl

DEPARTMENT OF MATHEMATICS AND STATISTICS, NATIONAL UNIVERSITY OF IRELAND - MAYNOOTH,
 MAYNOOTH, IRELAND. ORCID: 0000-0001-7619-6298
Email address: arne.vanantwerpen@mu.ie