Proceedings of the Edinburgh Mathematical Society (2019) **62**, 595–608
doi:10.1017/S0013091518000664

LEFT BRACES AND THE QUANTUM YANG–BAXTER EQUATION

H. MENG*, A. BALLESTER-BOLINCHES AND R. ESTEBAN-ROMERO†

Departament de Matemàtiques, Universitat de València, 46100 Burjassot, València, Spain (hangyangmenges@gmail.com; Adolfo.Ballester@uv.es; Ramon.Esteban@uv.es)

(Received 19 April 2018; first published online 3 December 2018)

Abstract Braces were introduced by Rump in 2007 as a useful tool in the study of the set-theoretic solutions of the Yang–Baxter equation. In fact, several aspects of the theory of finite left braces and their applications in the context of the Yang–Baxter equation have been extensively investigated recently. The main aim of this paper is to introduce and study two finite brace theoretical properties associated with nilpotency, and to analyse their impact on the finite solutions of the Yang–Baxter equation.

Keywords: p-nilpotent group; braces; Yang–Baxter equation

2010 *Mathematics subject classification:* Primary 16T25; 20F16

1. Introduction

The quantum Yang–Baxter equation (YBE), first appearing in the paper by Yang [**11**], is an important equation in mathematical physics that lays the foundations of some interesting mathematical theories. One of the fundamental open problems is to find all the solutions of the YBE. A subclass of solutions, the involutive and non-degenerate ones, have received a lot of attention in recent years. This type of solution is of interest not only for applications of the YBE to physics but also for its connections with some mathematical topics of recent interest such as radical rings [**7**], trifactorized groups [**10**] and Hopf algebras [**6**].

Let X be a non-empty set. A map $r\colon X \times X \longrightarrow X \times X$ is a *set-theoretic solution* of the YBE if

$$r_{12}r_{23}r_{12} = r_{23}r_{12}r_{23},$$

where the maps $r_{12}, r_{23}\colon X \times X \times X \longrightarrow X \times X \times X$ are defined as $r_{12} = r \times \mathrm{id}_X$, $r_{23} = \mathrm{id}_X \times r$. For all $x, y \in X$, we define two maps $f_x\colon X \longrightarrow X$ and $g_y\colon X \longrightarrow X$ by setting $r(x, y) = (f_x(y), g_y(x))$.

* Corresponding author.
† Permanent address: Institut Universitari de Matemàtica Pura i Aplicada, Universitat Politècnica de València, Camí de Vera, s/n, 46022 València, Spain, email: resteban@mat.upv.es.

We say that the solution (X, r) is *involutive* if $r^2 = \mathrm{id}_{X^2}$, where $X^2 = X \times X$; (X, r) is *non-degenerate* if f_x, g_y are bijective maps for all x, $y \in X$.

By a solution of the YBE we mean a non-degenerate involutive set-theoretic solution of the YBE, as in [2, 3].

The solutions of the YBE can be studied using group theory by considering two fundamental groups: the structure group and the permutation group (see [4]).

Let (X, r) be a solution of the YBE and assume that X is finite. The *structure group* of (X, r) is the group $G(X, r)$ with the presentation

$$\langle X \mid xy = f_x(y)g_y(x) \text{ for all } x, y \in X \rangle.$$

The *permutation group* of (X, r) is the subgroup $\mathcal{G}(X, r)$ of $\mathrm{Sym}(X)$ generated by the bijections f_x for all $x \in X$, that is,

$$\mathcal{G}(X, r) = \langle f_x \mid x \in X \rangle \leqslant \mathrm{Sym}(X).$$

On the other hand, Rump [7] introduced a new algebraic structure as a generalization of radical rings that turns out to be an important tool to study the solutions of the YBE. This structure is called a *left brace* and it is defined as a set B with two binary operations, $+$ and $\cdot$, such that $(B, +)$ is an abelian group, $(B, \cdot)$ is a group and

$$a \cdot (b + c) = a \cdot b + a \cdot c - a \quad \text{for all } a, b, c \in B. \tag{1}$$

The class of Jacobson radical rings coincides with the class of all *two-sided braces*, that is, left braces in which the symmetric version of condition (1) holds.

Let (X, r) be a solution of the YBE. Then $G(X, r)$ and $\mathcal{G}(X, r)$ are left braces (see [3, § 3]). Moreover, the results of [1] show that every finite left brace is isomorphic to the left brace $\mathcal{G}(X, r)$ for some finite solution of the YBE, allowing us to conclude that the problem of constructing all the finite solutions of the YBE is reduced to describing all the finite left braces.

The main goal of this paper is to introduce and analyse two brace theoretical properties that are natural extension of the well-known brace properties of left and right nilpotency, and to apply them to the study of the solutions of the YBE. Our first main result (Theorem 14) can be regarded as an improvement of a recent result of Smoktunowicz [9, Theorem 1] characterizing nilpotency of finite braces by means of the nilpotency of their multiplicative groups. It also provides an alternative shorter proof of this result that confirms the important role of abstract group theory in the study of braces. The study of a local right nilpotency in § 5 allows us to determine a large class of groups whose associated finite solutions of the YBE are multipermutation ones, and it can be considered as a significant improvement on one of the main results of [3].

Throughout the paper, the word 'brace' always means 'left brace'.

2. Basic results on braces

We shall lead up to proofs of our main results through a series of elementary lemmas. Some of them are surely well known, but include short proofs for completeness.

Let $(B, +, \cdot)$ be a brace. It is rather easy to check that the identity 0 of the additive group $(B, +)$ and the identity 1 of the multiplicative group $(B, \cdot)$ are equal.

https://doi.org/10.1017/S0013091518000664 Published online by Cambridge University Press

As usual, we denote by $-a, a^{-1}$ the inverse element of a in $(B,+),(B,\cdot)$, respectively.

We say a subset B_0 of B is a *sub-brace* of B if $(B_0,+)$ is a subgroup of $(B,+)$ and $(B_0,\cdot)$ is a subgroup of $(B,\cdot)$.

Let A, B be two braces. A map $f\colon A \longrightarrow B$ is a *homomorphism of braces* if $f(a+b) = f(a)+f(b)$ and $f(ab) = f(a)f(b)$ for all a, $b \in A$. The *kernel* of f is defined as the set $\mathrm{Ker}(f) = \{a \in A \mid f(a) = 1\}$. If f is bijective, f is called an *isomorphism*.

We say that A and B are *isomorphic* ($A \cong B$) if there is an isomorphism between A and B.

Let $*$ be the binary operation on B defined by setting

$$a * b = a \cdot b - a - b,$$

for a, $b \in B$.

We begin with some essential properties of the operation $*$.

Lemma 1. *Let $(B,+,\cdot)$ be a brace. Then for every a, b, $c \in B$, we have:*

(1) $a * (b+c) = a * b + a * c$;

(2) $a * 0 = 0 * a = 0$;

(3) $a * (-b) = -(a * b)$;

(4) $(a \cdot b) * c = a * (b * c) + a * c + b * c$.

Proof. Only Statement (4) is in doubt.

$$\begin{aligned}(a \cdot b) * c &= (a \cdot b) \cdot c - (a \cdot b) - c \\ &= a \cdot (b \cdot c) - (a \cdot b) - c \\ &= a \cdot (b * c + b + c) - (a \cdot b) - c \\ &= a \cdot (b * c) + a \cdot b + a \cdot c - 2a - (a \cdot b) - c \\ &= a * (b * c) + a + b * c - 2a - c + a \cdot c \\ &= a * (b * c) + a * c + b * c.\end{aligned}$$

□

We shall say that a non-empty subset I of B is a *left* (*right*) *ideal* of B if $(I,+)$ is a subgroup of $(B,+)$ and $b * a \in I$ ($a * b \in I$) for every $a \in I$ and $b \in B$; I is an *ideal* of B if I is both a left and right ideal of B.

Let I be an ideal of the brace A; we have that $a + I = aI$ for all $a \in A$. We may define $A/I = \{a + I \mid a \in A\}$ with the operations:

$$(a+I) + (b+I) = (a+b) + I, \quad (a+I) \cdot (b+I) = (ab) + I.$$

Then $(A/I,+,\cdot)$ is a brace called the *quotient brace* of A modulo I.

It is clear that if $f\colon A \longrightarrow B$ is a homomorphism of braces, then $\mathrm{Ker}(f)$ is an ideal of A and $f(A)$ is a sub-brace of B. Moreover, we have the following.

Lemma 2. $A/\mathrm{Ker}(f) \cong f(A)$.

https://doi.org/10.1017/S0013091518000664 Published online by Cambridge University Press

Lemma 3. *Let B be a brace and I, J be ideals of B such that $I \subseteq J$. Then*

$$(B/I)/(J/I) \cong B/J.$$

In [3, Definition 3], an alternative notion of an ideal in terms of some useful automorphisms of $(B,+)$ is given. For $a \in B$, let

$$\lambda_a \colon B \longrightarrow B; \quad b \longmapsto a \cdot b - a, \quad b \in B.$$

According to [3, Lemma 1], λ_a is an automorphism of $(B,+)$, and the map

$$\lambda \colon (B,\cdot) \longrightarrow \mathrm{Aut}((B,+)); \quad a \longmapsto \lambda_a,$$

is a group homomorphism. Thus we have a natural group action of $(B,\cdot)$ on $(B,+)$ via the homomorphism λ.

The next lemma shows that in fact the two definitions are equivalent.

Lemma 4. *Let $(B,+,\cdot)$ be a brace and let I be a non-empty subset of B.*

(1) *I is a left ideal of B if and only if $(I,+)$ is a subgroup of $(B,+)$ and $\lambda_a(i) \in I$ for every $a \in B$, $i \in I$.*

(2) *I is an ideal of B if and only if $(I,\cdot)$ is a normal subgroup of $(B,\cdot)$ and $\lambda_a(i) \in I$ for every $a \in B$, $i \in I$.*

Proof.

(1) Note that for every $a \in B, i \in I$,

$$a * i \in I \iff \lambda_a(i) = a \cdot i - a = a * i + i \in I.$$

(2) If I is an ideal of B, then I is a left ideal of B. Then $\lambda_a(i) \in I$ for every $a \in B, i \in I$. We prove that $(I,\cdot)$ is a normal subgroup of $(B,\cdot)$. Let $a \in B, i \in I$. Then

$$\begin{aligned} a^{-1} \cdot i \cdot a &= a^{-1}(i * a + i + a) - a^{-1} + a^{-1} \\ &= \lambda_{a^{-1}}(i * a) + \lambda_{a^{-1}}(i) + \lambda_{a^{-1}}(a) + a^{-1} \\ &= \lambda_{a^{-1}}(i * a) + \lambda_{a^{-1}}(i) \in I. \end{aligned}$$

Conversely, assume that $(I,\cdot)$ is a normal subgroup of $(B,\cdot)$ and $\lambda_a(i) \in I$ for all $a \in B$, $i \in I$. Then $i * a = i \cdot a - i - a = a \cdot (a^{-1} \cdot i \cdot a) - a - i = \lambda_a(a^{-1} \cdot i \cdot a) - i \in I$. Let i, $j \in I$. Then

$$i - j = j \cdot (j^{-1} \cdot i) - j = \lambda_j(j^{-1} \cdot i) \in I \quad \text{for all } i, j \in I.$$

Therefore $(I,+)$ is a subgroup of $(B,+)$. □

An interesting and useful application of Lemma 4 is the following.

Lemma 5. *Let $(B,+,\cdot)$ be a finite brace. Then $mB = \{mb \mid b \in B\}$ is a left ideal of B for all $m \in \mathbb{N}$. In particular, every Hall subgroup of $(B,+)$ is a left ideal of B.*

https://doi.org/10.1017/S0013091518000664 Published online by Cambridge University Press

Proof. Note that $(mB,+)$ is a characteristic subgroup of $(B,+)$. Thus $(mB,+)$ is invariant under the action of $(B,\cdot)$ via λ. Consequently, mB is a left ideal of B by Lemma 4. □

Let X, Y be subsets of the brace B. Define

$$X+Y=\{x+y \mid x\in X, y\in Y\}$$
$$X*Y=\langle x*y \mid x\in X, y\in Y\rangle_+,$$

where $\langle S\rangle_+$ denotes the subgroup generated by the set $S\subseteq B$ in $(B,+)$. Note that if $(Y,+)$ is a subgroup of $(B,+)$, it follows from Lemma 1(3) that

$$X*Y=\left\{\sum_{i=1}^{m} x_i*y_i \mid x_i\in X, y_i\in Y\right\}.$$

Lemma 6. *Let B be a brace. Suppose that L is a left ideal of B and I is an ideal of B. Then $I*L$ is a left ideal of B. Moreover, $I*B$ is an ideal of B.*

Proof. Let $x=\sum_{i=1}^{n} a_i*b_i\in I*L$, where $a_i\in I, b_i\in L$. If $y\in B$, then $\lambda_y(x)=\lambda_y(\sum_{i=1}^{n} a_i*b_i)=\sum_{i=1}^{n}\lambda_y(a_i*b_i)$. Therefore, by Lemma 4(1), it is enough to prove that $\lambda_y(a*b)\in I*L$ for each $a\in I, b\in L$.

$$\begin{aligned}\lambda_y(a*b)&=\lambda_y(\lambda_a(b)-b)=(\lambda_y\circ\lambda_a)(b)-\lambda_y(b)\\&=\lambda_{ya}(b)-\lambda_y(b)=\lambda_{(yay^{-1})y}(b)-\lambda_y(b)\\&=\lambda_{yay^{-1}}(\lambda_y(b))-\lambda_y(b)\\&=(yay^{-1})*\lambda_y(b).\end{aligned}$$

Since I is an ideal of B, $(I,\cdot)\trianglelefteq(B,\cdot)$. Hence $yay^{-1}\in I$. Since L is a left ideal of B, we have that $\lambda_y(b)\in L$. Thus $\lambda_y(a*b)\in I*L$, as desired.

We prove now that $I*B$ is an ideal of B. By Lemma 4(2), it is enough to show that $(I*B,\cdot)\trianglelefteq(B,\cdot)$. Let $x\in I*B$ and $y\in B$. Then

$$\begin{aligned}y^{-1}xy&=y^{-1}(xy)-y^{-1}+y^{-1}=\lambda_{y^{-1}}(xy)+y^{-1}\\&=\lambda_{y^{-1}}(x*y+x+y)+y^{-1}\\&=\lambda_{y^{-1}}(x*y)+\lambda_{y^{-1}}(x)+\lambda_{y^{-1}}(y)+y^{-1}\\&=\lambda_{y^{-1}}(x*y)+\lambda_{y^{-1}}(x).\end{aligned}$$

Note that $x\in I$ since I is an ideal of B. Since $I*B$ is a left ideal of B, we have that $\lambda_{y^{-1}}(x*y), \lambda_{y^{-1}}(x)\in I*B$. Thus $y^{-1}xy\in I*B$. □

https://doi.org/10.1017/S0013091518000664 Published online by Cambridge University Press

We define inductively:

$$L_0(X,Y) = Y; \qquad L_n(X,Y) = X * L_{n-1}(X,Y) \quad (n \geq 1);$$
$$\mathrm{R}_0(X,Y) = X; \qquad \mathrm{R}_n(X,Y) = \mathrm{R}_{n-1}(X,Y) * Y \quad (n \geq 1).$$

Observe that if $x,\ y \in B$, then $L_n(\{x\},\{y\})$ coincides with $\{e_n(x,y)\}$, with $e_n(x,y)$ defined as in [8, § 2]. Note that if Y and Z are subgroups of $(B,+)$, we have that $X * (Y+Z) = (X*Y) + (X*Z)$ by Lemma 1(1). Hence the following.

Proposition 7. *Let $(B,+,\cdot)$ be a brace. Assume that Y and Z are subgroups of $(B,+)$. Then*

$$L_n(X, Y+Z) = L_n(X,Y) + L_n(X,Z)$$

for all $n \in \mathbb{N}$.

Proof. We argue by induction on n. If $n = 0$, then the result is clear. We may assume that $n \geq 1$ and $L_{n-1}(X, Y+Z) = L_{n-1}(X,Y) + L_{n-1}(X,Z)$ holds. Then

$$\begin{aligned} L_n(X, Y+Z) &= X * L_{n-1}(X, Y+Z) \\ &= X * (L_{n-1}(X,Y) + L_{n-1}(X,Z)) \\ &= X * L_{n-1}(X,Y) + X * L_{n-1}(X,Z) \\ &= L_n(X,Y) + L_n(X,Z). \end{aligned}$$

□

The following description of the sets $L_n(X,Y)$ in terms of commutators of the semidirect product $G = (B,+) \rtimes (B,\cdot)$ with respect to the action of $(B,\cdot)$ on $(B,+)$ via λ turns out to be crucial in our approach.

Let $a \in (B,+)$ and $b \in (B,\cdot)$. Then

$$[a, b^{-1}] = -a + \lambda_b(a) = -a + b \cdot a - b = b * a.$$

If Y is a subgroup of $(B,+)$ and X is a subgroup of $(B,\cdot)$, then

$$[Y,X] = \langle [y, x^{-1}] \mid x \in X, y \in Y \rangle_+ = \langle x * y \mid x \in X, y \in Y \rangle_+ = X * Y;$$

furthermore,

$$L_n(X,Y) = [\ldots[[Y,X],X],\ldots,X] = [Y,X,\ldots,X] \quad (X \text{ appears } n \text{ times}).$$

It easily follows from Lemma 6 that $L_n(B,B) = B^{n+1}$ [7] is a left ideal of B, and also a normal subgroup of G contained in $(B,+)$ for all n.

Assume now that B has order p^n for some prime p, $n \geq 1$. Then G is a p-group and so it is nilpotent. Applying [5, 5.1.6 (iii)], we obtain that if $L_i(B,B) \neq 0$, then $(L_{i+1}(B,B),+)$ is a proper subgroup of $(L_i(B,B),+)$. Therefore we have the following.

Lemma 8 (see [7, Corollary]). *Let B be a finite brace such that $|B| = p^n$ for some prime p and $n \geq 0$. Then $L_n(B,B) = 0$.*

https://doi.org/10.1017/S0013091518000664 Published online by Cambridge University Press

Let B be a brace. Rump [7] defined the socle series of the brace B by setting $\mathrm{Soc}_0(B) = 0$, $\mathrm{Soc}(B) = \mathrm{Soc}_1(B)$ and

$$\mathrm{Soc}_{n+1}(B) := \{x \in B \mid x * a \in \mathrm{Soc}_n(B) \text{ for all } a \in B\},$$

for all $n \geq 1$.

Note that if $s \in \mathrm{Soc}(B)$, then $sx = s + x$ for all $x \in B$. Therefore, by Lemma 4, $\mathrm{Soc}_n(B)$ is an ideal of B for all n.

The following proposition is elementary.

Proposition 9. *Let B be a brace and let X be a non-empty subset of B. Assume that $m, n \geq 0$. Then $\mathrm{R}_n(X, B) \subseteq \mathrm{Soc}_m(B)$ if and only if $X \subseteq \mathrm{Soc}_{m+n}(B)$.*

3. Braces and solutions of the Yang–Baxter equation

Let (X, r), (Y, s) be two solutions of the YBE. Following [3, § 3], we say that a *homomorphism* from (X, r) to (Y, s) is a map $\varphi\colon X \longrightarrow Y$ such that

$$s(\varphi(x_i), \varphi(x_j)) = (\varphi(x_k), \varphi(x_l)),$$

if x_i, x_j, x_k, $x_l \in X$ satisfy $r(x_i, x_j) = (x_k, x_l)$.

In this case, $(\varphi(X), s|_{\varphi(X)^2})$ is also a solution of the YBE. The solution (X, r) is said to be *embedded* in (Y, s) if φ is injective. If φ is bijective, then we say that (X, r) and (Y, s) are isomorphic.

If B is a brace, then the map $r\colon B \times B \longrightarrow B \times B$ defined by

$$r(x, y) = (\lambda_x(y), \lambda^{-1}_{\lambda_x(y)}(x))$$

provides a solution of the YBE called *the solution of the YBE associated with the brace B* (see [3, Lemma 2]). Clearly, if the braces A and B are isomorphic, then the solutions of the YBE associated with A and B are isomorphic.

Let (X, r) be the solution of the YBE. Denote by $\mathbb{Z}^X$ the additive free abelian group with basis X. Note that $\mathrm{Sym}(X)$ induces a group of automorphisms of $\mathbb{Z}^X$ by

$$\sigma\left(\sum_{x \in X} a_x x\right) = \sum_{x \in X} a_x \sigma(x), \sigma \in \mathrm{Sym}(X), \quad a_x \in \mathbb{Z}, x \in X.$$

Write the group $M_X = \{(a, \sigma) \mid a \in \mathbb{Z}^X, \sigma \in \mathrm{Sym}(X)\}$ with the product defined by:

$$(a, \sigma)(b, \tau) = (a + \sigma(b), \sigma\tau) \quad \text{for all } a, b \in \mathbb{Z}^X, \sigma, \tau \in \mathrm{Sym}(X).$$

By [4, Propositions 2.4 and 2.5], $G(X, r)$ is isomorphic to a subgroup of M_X of the form

$$H = \{(a, \phi(a)) \mid a \in \mathbb{Z}^X\},$$

for some function $\phi\colon \mathbb{Z}^X \longrightarrow \mathrm{Sym}(X)$ such that $\phi(x) = f_x$. We can define a sum in H by setting

$$(a, \phi(a)) + (b, \phi(b)) = (a + b, \phi(a + b)) \quad \text{for all } a, b \in \mathbb{Z}^X.$$

Then $(H, +, \cdot)$ is an (infinite) left brace (see [3, § 3]). In [3, Theorem 1] it is stated that the solution (X, r) of the YBE can be embedded in the solution of the YBE associated with H. The following result can be considered as a slight extension of that theorem.

https://doi.org/10.1017/S0013091518000664 Published online by Cambridge University Press

Proposition 10. *With the above notation, assume that (H, s) is the solution of the YBE associated with the brace H. Then there exists an $\mathcal{G}(H, s)$-invariant subset $Y \subseteq H$ such that $(Y, s|_{Y^2})$ is isomorphic to (X, r).*

Proof. Let $\psi\colon X \longrightarrow H$ be the map defined by $\psi(x) = (x, f_x) = (x, \phi(x))$ and set $Y = \psi(X)$.

Recall that $s\colon H \times H \longrightarrow H \times H$ is the map defined by $s(h, g) = (\lambda_h(g), \lambda^{-1}_{\lambda_h(g)}(h))$. Thus $\mathcal{G}(H, s) = \langle \lambda_h \mid h \in H\rangle = \langle \lambda_{(a,\phi(a))} \mid a \in \mathbb{Z}^X\rangle$. For every $h = (a, \phi(a)) \in H$ and $y = \psi(x) \in Y$, where $a \in \mathbb{Z}^X$ and $x \in X$, we have

$$\begin{aligned}\lambda_h(y) &= (a, \phi(a))(x, \phi(x)) - (a, \phi(a))\\ &= (a + \phi(a)(x), \phi(a)\phi(x)) - (a, \phi(a))\\ &= (a + \phi(a)(x), \phi(a + \phi(a)(x))) - (a, \phi(a))\\ &= (\phi(a)(x), \phi(\phi(a)(x))).\end{aligned}$$

Note that $\phi(a)(x) \in X$ and so $\lambda_h(y) = \psi(\phi(a)(x)) \in Y$. Thus Y is $\mathcal{G}(H, s)$-invariant. Moreover, $\psi(f_x(y)) = \lambda_{\psi(x)}(\psi(y))$ for all $x,\ y \in X$. This implies that φ is an embedding of (X, r) in (H, s), and so $(Y, s|_{Y^2})$ is a solution of the YBE that is isomorphic to (X, r). □

We bring this section to a close with the notions of retraction of a solution and multipermutation solutions introduced in [4]. Let (X, r) be a solution of the YBE and assume that $r(x, y) = (f_x(y), g_y(x))$ for all $x,\ y \in X$. The *retraction* relation $\sim$ on X with respect to r is an equivalence relation defined by $x \sim y$ if $f_x = f_y$.

If $[x]$ denotes the $\sim$-class of $x \in X$, then a natural induced solution $\mathrm{Ret}(X, r) = (X/\!\sim, \widetilde{r})$ called the *retraction* of (X, r), where $\widetilde{r}$ is defined by

$$\widetilde{r}([x], [y]) = ([f_x(y)], [g_y(x)]) \quad \text{for all } [x],\ [y] \in X/\!\sim,$$

emerges.

Define

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

and

$$\mathrm{Ret}^m(X, r) = \mathrm{Ret}(\mathrm{Ret}^{m-1}(X, r)), \quad m \geq 2.$$

Then a solution (X, r) is said to be a *multipermutation solution of level m* if m is the smallest non-negative m such that $\mathrm{Ret}^m(X, r)$ has cardinality 1.

The following lemma is an easy application of [3, Lemmas 3 and 4].

Lemma 11. *Let B be a brace and let (B, r) be the solution of the YBE associated with B. Then $Ret^m(B, r)$ is isomorphic to the solution of the YBE associated with the brace $B/\mathrm{Soc}_m(B)$.*

Proof. We argue by induction on m. By [3, Lemma 3], the result is true for $m = 1$. Now suppose that $\mathrm{Ret}^{m-1}(B, r)$ is isomorphic to the solution of the YBE associated with the brace $\overline{B} = B/\mathrm{Soc}_{m-1}(B)$. By [3, Lemma 4], $\mathrm{Ret}^m(B, r)$ is isomorphic to the

https://doi.org/10.1017/S0013091518000664 Published online by Cambridge University Press

solution of the YBE associated with $\overline{B}/\mathrm{Soc}(\overline{B})$. By Lemma 3, $\overline{B}/\mathrm{Soc}(\overline{B})$ is isomorphic to $B/\mathrm{Soc}_m(B)$. Thus, $\mathrm{Ret}^m(B,r)$ is isomorphic to the solution of the YBE associated with $B/\mathrm{Soc}_m(B)$. □

4. Left p-nilpotent braces

A brace B is called *left nilpotent* if $L_n(B,B)=0$ for some $n\in\mathbb{N}$. Smoktunowicz [**9**, Theorem 1] characterized nilpotency of finite braces by means of the nilpotency of their multiplicative groups.

Our main result of this section shows that this result is not accidental and can be obtained owing to a local completeness property of the finite braces.

Recall that a property of groups is said to be *local* if it is generalized in a form referring to a prime. An interesting property in this context is to find out whether the original property can be described as the conjunction of all the local properties for all primes. If we consider the property of finite groups of being nilpotent, a local version is that of being p-nilpotent, for p a prime. A finite group G is said to be *p-nilpotent* if G has a normal Hall p'-subgroup.

It is clear that every finite nilpotent group is p-nilpotent and that a finite p-nilpotent group for all primes p is nilpotent. Therefore, the following definition turns out to be natural in this context.

Definition 12. Let B be a finite brace and let p be a prime. B is called left p-nilpotent if $L_n(B,B_p)=0$ for some positive integer n, where B_p is the Sylow p-subgroup of the additive group of B.

Our next result shows that left nilpotency of finite braces is a local property. It can also be deduced from [**8**, Theorem 12].

Lemma 13. *Let B be a finite brace. Then B is left nilpotent if and only if B is left p-nilpotent for all primes p.*

Proof. Denote by $\pi(B)$ the set of all the primes dividing the order of B. It is easy to see that the lemma holds when $B=\{0\}$. Thus we may assume that $B\neq\{0\}$.

Assume that B is left nilpotent. Then $L_n(B,B)=0$ for some integer $n\geq 1$. For every prime p dividing the order of B, we have that $L_n(B,B_p)\subseteq L_n(B,B)=0$, where B_p is the Sylow p-subgroup of the additive group of B. Hence B is left p-nilpotent.

Conversely, assume that $L_{n(p)}(B,B_p)=0$ for every prime $p\in\pi(B)$, where B_p is the Sylow p-subgroup of the additive group of B and $n(p)$ is an positive integer (depending on p). Let $m=\max\{n(p)\mid p\in\pi(B)\}$. Then

$$L_m(B,B_p)=0 \quad \text{for all } p\in\pi(B).$$

Observe that $B=\sum_{p\in\pi(B)}B_p$. It follows from Proposition 7 that

$$L_m(B,B)=L_m\left(B,\sum_{p\in\pi(B)}B_p\right)=\sum_{p\in\pi(B)}L_m(B,B_p)=0.$$

Hence B is left nilpotent. □

https://doi.org/10.1017/S0013091518000664 Published online by Cambridge University Press

Our main result of this section characterizes left p-nilpotent finite braces. It is an extension of [9, Theorem 1] and also provides an alternative shorter proof of that result.

Theorem 14. *Let $(B,+,\cdot)$ be a finite brace and let p be a prime. Assume that $B_{p'}, B_p$ are the Hall p'-subgroup and Sylow p-subgroup of the group $(B,+)$, respectively. Then the following statements are pairwise equivalent.*

(1) *B is a left p-nilpotent brace.*

(2) $B_{p'} * B_p = 0$.

(3) $B_{p'} * \Omega((B_p,+)) = 0$, *where $\Omega((B_p,+))$ is the group generated by all elements of order p in $(B_p,+)$.*

(4) *The multiplicative group $(B,\cdot)$ is p-nilpotent.*

Proof. (1) implies (2). If B is p-nilpotent, then $L_n(B,B_p) = 0$ for some positive integer n. In particular, $L_n(B_{p'},B_p) = 0$. Considering the action of $(B_{p'},\cdot)$ on $(B_p,+)$, we have that $[B_p, B_{p'}, \ldots, B_{p'}] = L_n(B_{p'},B_p) = 0$. It follows from [5, 8.2.7 (b)] that $[B_p, B_{p'}] = 0$. Hence $B_{p'} * B_p = 0$.

It is clear that (2) implies (3).

(3) implies (4). Considering the action of $(B_{p'},\cdot)$ on $(B_p,+)$, we have that

$$[\Omega((B_p,+)), B_{p'}] = B_{p'} * \Omega((B_p,+)) = 0.$$

This implies that $B_{p'}$ acts trivially on $\Omega((B_p,+))$. Then it follows from [5, 8.4.3] that $B_{p'}$ acts trivially on $(B_p,+)$, so that $B_{p'} * B_p = 0$. Hence we have $B_{p'} * B = B_{p'} * (B_p + B_{p'}) = B_{p'} * B_{p'} \subseteq B_{p'}$. We have by Lemma 5 that $B_{p'}$ is an ideal of B, and so $(B_{p'},\cdot)$ is a normal subgroup of $(B,\cdot)$ by Lemma 4. Hence $(B,\cdot)$ is p-nilpotent.

(4) implies (1). Since $(B,\cdot)$ is p-nilpotent, we have that $(B_{p'},\cdot)$ is a normal subgroup of $(B,\cdot)$. By Lemma 5, $B_{p'}$ is a left ideal of B. Hence we can apply Lemma 4 to conclude that $B_{p'}$ is an ideal of B. Consequently, $B_{p'} * B_p \subseteq B_{p'} \cap B_p = 0$ since B_p is a left ideal of B by Lemma 5. Now we claim that

$$L_n(B,B_p) = L_n(B_p,B_p) \quad \text{for all } n \geq 1.$$

It suffices to prove that $L_n(B,B_p) \subseteq L_n(B_p,B_p)$ for all $n \geq 1$. We argue by induction on n. Assume that $n = 1$ and let $x = ab \in B$ and $y \in B_p$, where $a \in B_p, b \in B_{p'}$. Then, by Lemma 1,

$$x * y = (ab) * y = a * (b * y) + a * y + b * y = a * y \in B_p * B_p$$

since $b * y = 0$. Thus we have $L_1(B,B_p) = B * B_p \subseteq B_p * B_p = L_1(B_p,B_p)$. Now we may assume that the result holds for $n-1$, that is, $L_{n-1}(B,B_p) \subseteq L_{n-1}(B_p,B_p)$. Arguing as above, we obtain that $B * L_{n-1}(B_p,B_p) \subseteq B_p * L_{n-1}(B_p,B_p)$. Therefore,

$$L_n(B,B_p) = B * L_{n-1}(B,B_p) \subseteq B * L_{n-1}(B_p,B_p) \subseteq B_p * L_n(B_p,B_p).$$

Since $L_m(B_p,B_p) = 0$ for some m by Lemma 8, we have that $L_m(B,B_p) = L_m(B_p,B_p) = 0$. Consequently, B is a left p-nilpotent brace and the circle of implications is complete. □

https://doi.org/10.1017/S0013091518000664 Published online by Cambridge University Press

We will draw a series of conclusions from Theorem 14.

Corollary 15 (see [9, Theorem 1]). *Let $(B, +, \cdot)$ be a finite brace. Then B is left nilpotent if and only if the multiplicative group $(B, \cdot)$ is nilpotent.*

Another application of left p-nilpotent finite braces is the following non-simplicity criterion.

Corollary 16. *Let $(B, +, \cdot)$ be a finite brace and let p be the smallest prime dividing the order of B. If the Sylow p-subgroups of $(B, \cdot)$ are cyclic, then B is left p-nilpotent. In particular, B is not simple if $|B| \neq p$.*

Proof. Applying [5, 7.2.2], we have that $(B, \cdot)$ is p-nilpotent. By Theorem 14 and its proof, B is left p-nilpotent and then $B_{p'}$ is an ideal of B, where $B_{p'}$ is the Hall p'-subgroup of the additive subgroup of B. If $|B| \neq p$, then $B_{p'} \neq 1$. Hence B is not simple. □

5. Right p-nilpotent braces

Recall that a brace B is said to be *right nilpotent* if $\mathrm{R}_n(B, B) = 0$ for some $n \geq 0$. Applying Proposition 9, we conclude that B is right nilpotent if and only if $\mathrm{Soc}_n(B) = B$ for some $n \geq 0$.

Right nilpotency has a strong impact on the solutions of the YBE. In fact, as is proved in [2, Proposition 6], a brace B is right nilpotent if and only if the solution of the YBE associated with B is a multipermutation solution.

The aim of this section is to introduce right p-nilpotent braces and to prove a characterization theorem that includes an extension of [2, Proposition 6] and can be used to show a significant improvement on [3, Theorem 3] concerning finite solutions of YBE whose associated permutation group is abelian.

Definition 17. Let B be a finite brace and let p be a prime. B is called *right p-nilpotent* if $\mathrm{R}_n(B_p, B) = 0$ for some positive integer n, where B_p is the Sylow p-subgroup of the additive group of B.

Our first result in this section gives a criterion for a finite brace B to be right p-nilpotent, and confirms that right p-nilpotency and left p-nilpotency are very different brace theoretical properties.

Theorem 18. *Let B be a finite brace. Assume that the multiplicative group of B has an abelian normal Sylow p-subgroup for some prime p. Then B is right p-nilpotent.*

Proof. Assume the theorem is false and choose for B a counterexample of least order. Let B_p be the Sylow p-subgroup of $(B, +)$. Then B_p is a left ideal of B by Lemma 5. In particular, B_p is closed under taking products. Therefore $(B_p, \cdot)$ is also a Sylow p-subgroup of $(B, \cdot)$ and so $(B_p, \cdot)$ is abelian and normal in $(B, \cdot)$. By Lemma 4, B_p is an ideal of B.

Let $B_{p'}$ be the Hall p'-subgroup of $(B, +)$. Since $B_{p'}$ is a left ideal of B by Lemma 5, it follows that $B_p * B_{p'} \subseteq B_p \cap B_{p'} = 0$. Thus, by Proposition 7, we have $\mathrm{Soc}(B_p) * B =$

https://doi.org/10.1017/S0013091518000664 Published online by Cambridge University Press

$\mathrm{Soc}(B_p) * (B_p + B_{p'}) = \mathrm{Soc}(B_p) * B_p + \mathrm{Soc}(B_p) * B_{p'} = 0$. Since B_p is abelian, we have that

$$\begin{aligned}\mathrm{Soc}(B_p) &= \{a \in B_p \mid a * b = 0 \text{ for all } b \in B_p\}\\ &= \{a \in B_p \mid b * a = 0 \text{ for all } b \in B_p\}\\ &= \{a \in B_p \mid \lambda_b(a) = a \text{ for all } b \in B_p\}.\end{aligned}$$

Now, considering the action of $(B_p, \cdot)$ on $(B_p, +)$, we have that $\mathrm{Soc}(B_p) = \mathrm{C}_{(B_p,+)}((B_p, \cdot))$. It follows from [5, 8.1.4 (a)] that $0 \neq \mathrm{Soc}(B_p) \subseteq B_p \cap \mathrm{Soc}(B)$. Denote $I = B_p \cap \mathrm{Soc}(B)$ and observe that I is an ideal of B since B_p and $\mathrm{Soc}(B)$ are both ideals of B. Considering the quotient brace of B modulo I, we have that $(B/I, \cdot) \cong (B, \cdot)/(I, \cdot)$. Hence B/I satisfies the hypothesis of the theorem. The minimal choice of B implies that B/I is right p-nilpotent. Then $\mathrm{R}_n(B_p/I, B/I) = 0$ for some $n \geq 0$. Thus $\mathrm{R}_n(B_p, B) \subseteq I \subseteq \mathrm{Soc}(B)$ so that $\mathrm{R}_{n+1}(B_p, B) = \mathrm{R}_n(B_p, B) * B \subseteq \mathrm{Soc}(B) * B = 0$, and then B is right p-nilpotent, contrary to assumption. □

Theorem 19. *Let B be a finite brace and let (B, r) be the solution of the YBE associated with B. Assume that p is a prime and B_p is the Sylow p-subgroup of $(B, +)$. Then the following statements are pairwise equivalent.*

(1) *B is right p-nilpotent.*

(2) *$B_p \subseteq \mathrm{Soc}_n(B)$ for some $n \geq 0$.*

(3) *There exists some $n \geq 0$ such that the cardinality of $\mathrm{Ret}^n(B, r)$ is a p'-number.*

Proof. (1) implies (2). Let $n \geq 0$ such that $\mathrm{R}_n(B_p, B) = 0 = \mathrm{Soc}_0(B)$. Applying Proposition 9, we conclude that $B_p \subseteq \mathrm{Soc}_n(B)$.

(2) implies (3). By Lemma 11, $\mathrm{Ret}^n(B, r)$ is isomorphic to the solution of the YBE associated with the left brace $B/\mathrm{Soc}_n(B)$. Since $B_p \subseteq \mathrm{Soc}_n(B)$, we have that $B/\mathrm{Soc}_n(B)$ is of order a p'-number. Hence the cardinality of $\mathrm{Ret}^n(B, r)$ is a p'-number.

(3) implies (1). By Lemma 11, we have that $B/\mathrm{Soc}_n(B)$ is of order a p'-number, and then $B_p \subseteq \mathrm{Soc}_n(B)$ for some $n \geq 0$. Applying Lemma 9, we conclude that $\mathrm{R}_n(B_p, B) = 0$. □

We now derive some consequences of the characterization theorem. The first one confirms that right p-nilpotency, like left p-nilpotency, is a local property.

Proposition 20. *Let B be a finite brace. Then B is right nilpotent if and only if B is right p-nilpotent for all primes p.*

Proof. Let B_p be the Sylow p-subgroup of $(B, +)$ for each prime p. If B is right nilpotent, then $B_p \subseteq B = \mathrm{Soc}_n(B)$ for some $n \geq 0$ and all primes p by Proposition 9. Therefore B is p-right nilpotent for all primes p.

Assume that B is right p-nilpotent for all primes p. It follows from Theorem 19 that $B_p \subseteq \mathrm{Soc}_{n(p)}(B)$ for some $n(p) \geq 0$ (depending on p). Let $m = \max\{n(p) \mid p \in \pi(B)\}$. Hence $B = \sum_p B_p \subseteq \mathrm{Soc}_m(B)$. Hence B is right nilpotent. □

https://doi.org/10.1017/S0013091518000664 Published online by Cambridge University Press

Recall that a finite group is called an *A-group* if all its Sylow subgroups are abelian. Let $\preceq$ be a total order relation on the set $\mathbb{P}$ of all primes. Recall that a finite group G is said to satisfy the *Sylow tower property with respect to* $\preceq$ if G has a normal Hall π_p-subgroup for each prime p, where $\pi_p = \{q \mid p \preceq q\}$.

Corollary 21. *Let B be a finite brace. Assume that $(B, \cdot)$ is an A-group with the Sylow tower property. Then B is right nilpotent.*

Proof. We argue by induction on the order of B. Assume that $(B, \cdot)$ satisfies the Sylow tower property with respect to the total relation $\preceq$ on $\mathbb{P}$. Write $\pi(B) = \{p_1, \ldots, p_s\}$ and assume that $p_1 \preceq p_2 \preceq \cdots \preceq p_s$. Let B_{p_s} be the Sylow p_s-subgroup of $(B, +)$. By Theorem 18, B is right p_s-nilpotent. Consequently, by Theorem 19, $B_{p_s} \subseteq \mathrm{Soc}_m(B)$ for some $m \geq 0$. Then the quotient brace $\overline{B}$ of B modulo B_{p_s} satisfies the hypothesis of the theorem. By induction, $\overline{B}$ is right nilpotent. Hence $\mathrm{R}_n(\overline{B}, \overline{B}) = 0$ for some $n \geq 0$, and so $\mathrm{R}_n(B, B) \subseteq B_{p_s} \subseteq \mathrm{Soc}_m(B)$. By Proposition 9, $B \subseteq \mathrm{Soc}_{m+n}(B)$. Therefore, B is right nilpotent. □

The following corollary is a significant improvement on [**3**, Theorem 3].

Corollary 22. *Let (X, r) be a finite solution of the YBE. Assume that $\mathcal{G}(X, r)$ is an A-group with the Sylow tower property. Then (X, r) is a multipermutation solution.*

Proof. Set $H = G(X, r)$ and let (H, s) be the solution of the YBE associated with the brace H. By Proposition 10, we can find a $\mathcal{G}(H, s)$-subset $Y \subseteq H$ such that $(Y, s|_{Y^2})$ is isomorphic to (X, r). If (H, s) is a multipermutation solution, it follows from [**3**, Lemma 5] that $(Y, s|_{Y^2})$ is a multipermutation solution. Then we can conclude that (X, r) is a multipermutation solution. Thus it suffices to prove that (H, s) is a multipermutation solution. According to [**2**, Proposition 6], it is enough to show that H is right nilpotent.

Observe that $\mathcal{G}(X, r) \leqslant \mathrm{Sym}(X)$ is a finite brace since X is a finite set. By Corollary 21, $\mathcal{G}(X, r)$ is right nilpotent. It is well known (see, for instance, the comments before [**3**, Lemma 2]) that $H/\mathrm{Soc}(H)$ and $\mathcal{G}(X, r)$ are isomorphic as braces. Hence $H/\mathrm{Soc}(H)$ is right nilpotent. Hence

$$\mathrm{R}_n(H/\mathrm{Soc}(H), H/\mathrm{Soc}(H)) = 0$$

for some $n \geq 0$. Then $\mathrm{R}_n(H, H) \subseteq \mathrm{Soc}(H)$. By Proposition 9, $H \subseteq \mathrm{Soc}_{n+1}(H)$ and H is right nilpotent.

The proof of the corollary is complete. □

Acknowledgements. This work was supported by the research grant MTM2014-54707-C3-1-P from the *Ministerio de Economía y Competitividad*, Spanish Government, and FEDER, European Union, and PROMETEO/2017/057 from *Generalitat* (Valencian Community, Spain). The first author was supported by grant number 201606890006 of the China Scholarship Council.

References

1. D. Bachiller, F. Cedó and E. Jespers, Solutions of the Yang–Baxter equation associated with a left brace, *J. Algebra* **463** (2016), 80–102.

2. F. Cedó, T. Gateva-Ivanova and A. Smoktunowicz, On the Yang–Baxter equation and left nilpotent left braces, *J. Pure Appl. Algebra* **221**(4) (2017), 751–756.
3. F. Cedó, E. Jespers and J. Okniński, Braces and the Yang–Baxter equation, *Commun. Math. Phys.* **327** (2014), 101–116.
4. P. Etingof, T. Schedler and A. Soloviev, Set theoretical solutions to the quantum Yang–Baxter equation, *Duke Math. J.* **100** (1999), 169–209.
5. H. Kurzweil and B. Stellmacher, *The theory of finite groups. An introduction.* Universitext (Springer-Verlag, New York, 2004).
6. D. E. Radford, *Hopf algebras* (World Scientific, 2012).
7. W. Rump, Braces, radical rings, and the quantum Yang–Baxter equation, *J. Algebra* **307** (2007), 153–170.
8. A. Smoktunowicz, A note on set-theoretic solutions of the Yang–Baxter equation, *J. Algebra* **500** (2018), 3–18.
9. A. Smoktunowicz, On Engel groups, nilpotent groups, rings, braces and Yang–Baxter equation, *Trans. Amer. Math. Soc.* **370** (2018), 6535–6564.
10. Y. Sysak, Products of groups and local nearrings, *Note Mat.* **28** (2008), 181–216.
11. C. N. Yang, Some exact results for many-body problem in one dimension with repulsive delta-function interaction, *Phys. Rev. Lett.* **19** (1967), 1312–1315.