Journal of Algebra 500 (2018) 3–18

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

A note on set-theoretic solutions of the Yang–Baxter equation

Agata Smoktunowicz

School of Mathematics, University of Edinburgh, James Clerk Maxwell Building, The King's Buildings, Peter Guthrie Tait Road, Edinburgh EH9 3FD, UK

ARTICLE INFO

Article history:
Received 18 January 2016
Available online 6 May 2016
Communicated by
N. Andruskiewitsch, A. Elduque,
E. Khukhro and I. Shestakov

MSC:
16T25
20D15
16N80
16N20

Keywords:
Jacobson radical ring
Braces
Braided groups
The Yang–Baxter equation
Multipermutation solutions

ABSTRACT

This paper shows that every finite non-degenerate involutive set theoretic solution (X, r) of the Yang–Baxter equation whose permutation group $\mathcal{G}(X, r)$ has cardinality which is a cube-free number is a multipermutation solution. Some properties of finite braces are also investigated. It is also shown that if A is a left brace whose cardinality is an odd number and $(-a) \cdot b = -(a \cdot b)$ for all $a, b \in A$, then A is a two-sided brace and hence a Jacobson radical ring. It is also observed that the semidirect product and the wreath product of braces of a finite multipermutation level is a brace of a finite multipermutation level.

1. Introduction

Circa 2005, Wolfgang Rump introduced the notion of braces, a generalization of Jacobson radical rings, as a tool for investigating solutions of the Yang–Baxter equation. We follow his paper [1], p. 128 for the definition of a left brace: Let A be an abelian

E-mail address: A.Smoktunowicz@ed.ac.uk.

http://dx.doi.org/10.1016/j.jalgebra.2016.04.015
0021-8693/

group together with a left distributive multiplication, that is $a \cdot (b + c) = a \cdot b + a \cdot c$ for all $a, b, c \in A$. We call $(A, +, \cdot)$ a *left brace* if the *circle operation* $a \circ b = a \cdot b + a + b$ makes A into a group. As mentioned in [1], p. 129, for a left brace A the associativity of A° is easily seen to be equivalent to the equation $(a \cdot b + a + b) \cdot c = a \cdot (b \cdot c) + a \cdot c + b \cdot c$. The group A° will be called the *adjoint group* of a left brace A. In 2012, Cedó, Jespers and Okniński [2] expressed the definition of a left brace in terms of operation $\circ$. In their paper, the adjoint group A° is called the multiplicative group of the left brace A; their definition is equivalent to the above definition by Rump. We recall the definition from [2]: a left brace is an abelian group $(A, +)$ with a multiplication $\circ$ such that $(A, \circ)$ is a group and

$$a \circ (b + c) + a = a \circ b + a \circ c$$

holds for all $a, b, c \in A$. Another interesting structure related to the Yang–Baxter equation, the braided group, was introduced in 2000, by Lu, Yan, Zhu [3]. In [4], Gateva-Ivanova showed that left braces are in one-to-one correspondence with braided groups with an involutive braiding operator.

Recall that a set-theoretic solution of the Yang–Baxter equation is a pair (X, r) where X is a set and $r(x, y) = (\sigma_x(y), \tau_y(x))$, for $x, y \in X$, is a bijective map such that

$$(r \times id_X)(id_X \times r)(r \times id_X) = (id_X \times r)(r \times id_X)(id_X \times r).$$

A solution (X, r) is non-degenerate if the maps σ_x and τ_x are bijective for each $x \in X$, and (X, r) is involutive if $r^2 = id_{X \times X}$.

Convention. By a solution of the Yang–Baxter equation we will mean a non-degenerate, involutive set-theoretic solution of the Yang–Baxter equation.

For some related results see [5–16].

Let R be a left brace; then the solution (R, r) of the Yang–Baxter equation associated to brace R is defined in the following way: for $x, y \in R$ define $r(x, y) = (u, v)$, where $u = x \cdot y + y$, $v = z \cdot x + x$ and where z is the inverse of $u = x \cdot y + y$ in the adjoint group R° of R, for $x, y \in R$. This solution is called the solution *associated with the left brace* R and will be denoted as (R, r).

The notions of retract of a solution and multipermutation solution were introduced by Etingof, Schedler and Soloviev in [17]. A multipermutation solution is a generalization of Lybashenko's permutation solution. A solution (X, r) is called a multipermutation solution of level m if m is the smallest nonnegative integer that, after applying the operation of retraction m times, the obtained solution has cardinality 1. If such m exists, the solution is also called a *multipermutation solution*, that is a solution which has a finite multipermutation level (for a detailed definition, see [4,2]). Some interesting related results can be found in [18,17,19,2,20,7]; for example, it is known that a finite solution (X, r) is a multipermutation solution, provided that the permutation group $\mathcal{G}(X, r)$ is abelian (Theorem 4.3 [2], for the case when (X, r) is infinite see Theorem 7.1 [20]).

Let A be either a left brace or a right brace. We define $A^{(n)} = A^{(n-1)} \cdot A$ and $A^n = A \cdot A^n$, where $A^{(1)} = 1$, and say that a left brace A has *a finite multipermutation level* if $A^{(n)} = 0$ for some n or equivalently the solution of the Yang–Baxter equation associated to A is a multipermutation solution (for some related results see [21–23]).

Remark. In [22], Rump introduced radical chains A^n and $A^{(n)}$ for a right brace A. Rump showed that, if A is a right brace, then A^n is a two-sided ideal of A, and $A^{(n)}$ doesn't need to be a two-sided ideal of A. Notice that if A is a left brace then $A^{(n)}$ is a two-sided ideal of A, and A^n doesn't need to be a two-sided ideal of A.

A semidirect product of braces and wreath product of braces is an interesting construction. The semidirect product of braces was introduced by Rump in [11]. The wreath product of braces was investigated in 2008 in Corollaries 3.5 and 3.6 [24] (the arXiv version of this paper appeared in 2008) and in Corollary 6.1 [2]. The wreath product of solutions was studied in 2009 in the arXiv version of [20] (see Theorem 8.7). We have the following observation.

Proposition 1. *Let A and B be left braces of a finite multipermutation level. Then the semidirect product $A \rtimes B$ and the wreath product $A \wr B$ of braces A and B is a brace of a finite multipermutation level.*

Braided groups and braces have interesting connections with group theory. In [24], it was shown that every finite nilpotent group can be embedded into an adjoint group of a finite brace whose adjoint group is nilpotent. In Corollary 6.1 [2], it was shown that every finite solvable group is a subgroup of an adjoint group of a finite brace. We notice that, by using the same proof as in Corollary 6.1 in [2] and Proposition 1, it is possible to show a slightly stronger result, namely:

Remark. (Related to Corollary 6.1, [2].) Let G be a finite solvable group. There is a finite left brace A of a finite multipermutation level, such that G is a subgroup of the adjoint group A° of A.

We don't know the answer to the following questions.

Question 2. *Let G be a finite group which is the adjoint group of some left brace A. Does it follow that G is the adjoint group of some left brace of a finite multipermutation level?*

It was shown by Rump that two-sided braces are exactly Jacobson radical rings, see [1], p. 129. By Corollary of [25], for every prime p, a group of order p^4 is the adjoint group of a two-sided brace if and only if it is abelian or has class 2. By Theorem 2.1 of [26], there exists a group of order p^4 of class 3 which is the adjoint group of a left brace, but is not the adjoint group of a two-sided brace, for example

$$\langle x, y | x^3 = y^3 = [x,y]^3 = [x,[x,y]]^3 = [y,[x,y]] = 1, \text{and } [x,[x,y]] \text{ is central } \rangle$$

has order 3^4 and it has class 3 and it is the adjoint group of a left brace.

Question 3. *(Amberg, Kazarin, Sysak [27,28].) If R is a nil ring whose adjoint group R° is finitely generated, is R nilpotent?*

Question 4. *Let F be a field of characteristic not two. An associative F-algebra R gives rise to the commutator Lie algebra $R^- = (R, [a,b] = ab - ba)$. If R is a nil algebra such that R^- is finitely generated Lie algebra, is R nilpotent?*

In [29] Alahmedi, Alsulami, Jain and Zelmanov give sufficient conditions for the Lie algebra R^- to be finitely generated. In [30] Angiono, Galindo and Vendramin provided Lie-theoretical analogs of braces. Some interesting results on Lie rings can be found in [31–35].

We will use the following notation.

$$a^{\circ(n)} = a \circ a \circ \cdots \circ a$$

where a appears n times, so $a^{\circ(n)}$ is the n-th power of a in the adjoint group A° of A. The main result of this paper is the following.

Theorem 5. *Let $(A, +, \cdot)$ be a left brace and let A_p, A_q be the Sylow's subgroups of the additive group of A of cardinalities respectively p^n and q^m for some prime numbers q and p and some natural numbers m, n. Then the following holds:*

1. *If p doesn't divide $q^t - 1$ for any $1 \leq t \leq m$, then*

$$A_p \cdot A_q = 0.$$

2. *Let Let $a \in A_p$, $b \in A_q$ and k be the maximal number such that p^k divides $q^t - 1$ for some $1 \leq t \leq m$. Then $a^{\circ(p^k)} \cdot b = 0$.*

Notice that Theorem 5 implies that if $q < p$ and p doesn't divide $q^t - 1$ for any $0 < t \leq m$, then every left brace of order $p^n q^m$ is not a simple left brace, as A_p is an ideal in A. Moreover, if A_p has a nonzero socle, then A has a nonzero socle. Note that in [36] Bachiller gave the first examples of non-trivial finite simple left braces. Our next result follows from Theorem 5.

Corollary 6. *Let A be a left brace of cardinality $p_1^{\alpha(1)} \dots p_n^{\alpha(n)}$ for some n, some prime numbers $p_1 < p_2 < \ldots < p_n$ and some positive integers $\alpha(1), \ldots, \alpha(n)$. Let A_i denote the Sylow's subgroup of the additive group of A of cardinality $p_i^{\alpha(i)}$. Suppose that for some $m \leq n$ the brace A_m has a nonzero socle and p_m doesn't divide*

$$p_j^i - 1$$

for all $j \leq n$ and each $i \leq \alpha(j)$. Then the socle of A is non-zero.

Recall that the socle of a left brace is defined as $\mathrm{Soc}(A) = \{a \in A : a \cdot b = 0 \text{ for all } b \in A\}$ (see [22], and for left braces [2]). We have the following corollary of Corollary 6.

Corollary 7. *Let A be a left brace of cardinality $p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ for some pairwise distinct prime numbers $p_1, p_2, \ldots, p_n$ and some positive integers $\alpha_1 \ldots \alpha_n$. Assume that for every $i \leq n$, and every $k < i$, p_i doesn't divide*

$$p_k^t - 1$$

for any $t \leq \alpha_k$. If all the Sylow's subgroups of the additive group of A_m are braces of a finite multipermutation level then A is a brace of a finite multipermutation level.

Recall that if A is a finite left brace then all the Sylow's subgroups of the additive group of A are also left braces (see Lemma 17 [23]).

As an application of Theorem 5, we obtain the following corollary.

Corollary 8. *If A is a brace whose cardinality is a cube-free number, then the socle of A is nonzero. Moreover, A is a brace of a finite multipermutation level.*

We can formulate Corollary 8 in the language of braided groups as follows.

Corollary 9. *If (G, σ) is a symmetric group (in the sense of Takeuchi) whose cardinality is a cube-free number, then (G, σ) has a finite multipermutation level.*

Our next result is the following.

Theorem 10. *Every finite solution (X, r) of the Yang–Baxter equation whose permutation group $\mathcal{G}(X, r)$ has cardinality which is a cube-free number is a multipermutation solution.*

Our last application of Theorem 5 is the following.

Corollary 11. *Let A be a finite left brace and let $A_1, \ldots, A_n$ be the Sylow's subgroups of the additive group of A. If for every i, $A_i \cdot A_i = 0$ and the additive group of A_i is cyclic, then A is a left brace of a finite multipermutation level.*

Let A be a left brace and $a \in A$, then we denote $a^1 = a$ and for $i > 1$ we denote $a^{i+1} = a \cdot a^i$. Our next result is related to Theorem 1 from [23].

Theorem 12. *Let A be a finite left brace; then the adjoint group A° is nilpotent if and only if there is a number m such that $a^m = 0$ for every $a \in A$. Moreover, if $a, b \in A$ are*

elements of distinct Sylow's subgroups of the additive group of A, then $(a+b)^n = 0$ for some n implies $a \cdot b = b \cdot a = 0$.

In [37] Guarnieri and Vendramin posed several interesting conjectures. Conjecture 6.4 states that if $p < q$ are prime numbers and p doesn't divide $q-1$, then the number of not isomorphic left braces of order p^2q is 4; notice that then q doesn't divide $p^2 - 1 = (p-1)(p+1)$; so if A_p, A_q are the Sylow's subgroup of the additive group of a brace A of such cardinality p^2q then $A_p \cdot A_q = 0$ and $A_q \cdot A_p = 0$ by Theorem 5. Therefore, A is a direct sum of braces of order p^2 and q, and the truth of Conjecture 6.4 follows from [38], where it was shown that there are exactly 4 nonisomorphic braces of order p^2. We notice that since groups of some cardinalities are nilpotent it is also possible to use Theorem 1 from [23], which asserts that a brace whose adjoint group is nilpotent is a direct sum of the braces which are Sylow's subgroups of its additive group.

Let k be a field. In analogy with k-algebras, Catino and Rizzo [39] introduced braces whose additive groups are k-vector spaces such that $(\alpha a) \cdot b = \alpha(a \cdot b)$, for $\alpha \in K$. Rump called such braces *k-linear* or k-braces; Catino and Rizzo called them circle algebras. In our next result we consider a similar property for left braces.

Theorem 13. *Let A be a left brace whose additive group has no elements of order 2. If $(-a) \cdot b = -(a \cdot b)$ for every $a, b \in A$, then A is a two-sided brace, and hence a Jacobson radical ring. Furthermore, if A is finite, then A is a nilpotent ring.*

2. Notation

Let $(A, +, \cdot)$ be a left brace defined as at the beginning of this paper, and let $\circ$ be the operation such that $a \circ b = a \cdot b + a + b$. We will use the following notation.

$$a^{\circ(n)} = a \circ a \circ \cdots \circ a$$

where a appears n times, and

$$a^n = a \cdot (a \cdot (\cdots (a))),$$

where a appears n times. Let $a, b \in A$, we inductively define elements $e_n = e_n(a, b)$ as $e_0 = b$, $e_1 = a \cdot b$ and

$$e_{i+1} = a \cdot e_i.$$

If n is a natural number and $a \in A$ then $n \cdot a$ denotes the sum of n copies of a, and $(-n) \cdot a$ denotes the sum of n copies of elements $-a$.

Given a prime number q, let F_q denote the field of q elements, and let $F_q[x]$ denote the polynomial ring over F_q in one variable x.

3. Multipermutation solutions

Let A be a left brace, and let $a, b \in A$. Recall that we inductively define elements $e_n = e_n(a,b)$ as $e_0 = b$, $e_1 = a \cdot b$ and $e_{i+1} = a \cdot e_i$. We will start with the following supporting lemma:

Lemma 14. *Let A be a left brace and let $a, b \in A$ and n be a positive integer. Let notation be as above. Then*

$$(a^{\circ(n)}) \cdot b = \sum_{i=1}^{n} \binom{n}{i} \cdot e_i.$$

Moreover,

$$a^{\circ(n)} = \sum_{i=1}^{n} \binom{n}{i} \cdot a^i.$$

Proof. Observe that it can be shown by induction on n that $a^{\circ(n)} = a \circ (a \circ (\ldots \circ (a \circ a))) = \sum_{i=1}^{n} \binom{n}{i} \cdot a^i$, as $a^{\circ(n+1)} = a \circ a^{\circ(n)} = a + a^{\circ(n)} + a \cdot a^{\circ(n)} = a + (\sum_{i=1}^{n} \binom{n}{i} \cdot a^i) + (\sum_{i=1}^{n} \binom{n}{i} \cdot a^{i+1}) = \sum_{i=1}^{n+1} \binom{n+1}{i} \cdot a^i$.

It remains now to show that $\sum_{i=1}^{n} \binom{n}{i} \cdot e_i = (a^{\circ(n)}) \cdot b$. We know that $\circ$ is an associative operation, so $a^{\circ(n)} \circ b = a \circ (a \circ (\cdots \circ (a \circ b)))$. Observe that $(a^{\circ(n)}) \cdot b = (a^{\circ(n)}) \circ b - (a^{\circ(n)}) - b$, so it suffices to show that

$$\sum_{i=1}^{n} \binom{n}{i} \cdot e_i + a^{\circ(n)} + b = a^{\circ(n)} \circ b.$$

We use the induction on n, for $n = 1$ we have $e_1 + a + b = a \circ b$ so the result holds. Suppose that the result holds for some n. We multiply by a from the left to get

$$a \circ (\sum_{i=1}^{n} \binom{n}{i} \cdot e_i + a^{\circ(n)} + b) = a^{\circ(n+1)} \circ b.$$

Observe that the left hand side equals $a \cdot (\sum_{i=1}^{n} \binom{n}{i} \cdot e_i + a^{\circ n} + b) + a + (\sum_{i=1}^{n} \binom{n}{i} \cdot e_i + a^{\circ n} + b) = \sum_{i=1}^{n} \binom{n}{i} \cdot (e_i + e_{i+1}) + a \cdot a^{\circ n} + a \cdot b + a + a^{\circ n} + b = \sum_{i=1}^{n+1} \binom{(n+1)}{i} \cdot e_i + a^{\circ(n+1)} + b$, which finishes the inductive argument. □

Lemma 15. *Let A be a finite left brace, and $a, b \in A$, $a, b \neq 0$, and let p, j be natural numbers. Then $a^{\circ(p^j)} \cdot b = 0$ if and only if $\sum_{i=1}^{p^j} \binom{p^j}{i} \cdot e_i = 0$.*

Proof. It follows because $a^{\circ(p^j)} \cdot b = \sum_{i=1}^{p^j} \binom{p^j}{i} \cdot e_i$ by Lemma 14. □

Lemma 16. *Let A be a left brace and let $a, b \in A$. Suppose that $a^{\circ(p^j)} = 0$ and $q^m \cdot b = 0$ for some distinct prime numbers p, q and some positive integers m, j. If $a \cdot (a \cdot b) = 0$ then $a \cdot b = 0$.*

Proof. By Lemma 14 we have $0 = a^{\circ(n)} \cdot b = \sum_{i=1}^{n} \binom{n}{i} \cdot e_i$ where $n = p^j$ and e_i are defined as in Lemma 14. Observe that $e_i = 0$ for all $i > 1$ as $e_2 = a \cdot (a \cdot b) = 0$. Therefore $n \cdot e_1 = p^j \cdot e_1 = 0$, and since p^j and q are co-prime then $e_1 = 0$, so $a \cdot b = e_1 = 0$. □

For a prime number q, let F_q denote the field of q elements and $F_q[x]$ be the polynomial ring in one variable over F_q. Let $\mathbb{Z}$ be the ring of integers and $\mathbb{Z}[x]$ be the polynomial ring in one variable over $\mathbb{Z}$.

Lemma 17. *Let A be a left brace and $a, b \in A$, $a, b \neq 0$ and let $e_i = e_i(a, b)$ for every i. Let $f(x), g(x), h(x) \in \mathbb{Z}[x]$ be such that $h(x) = g(x)f(x)$ where $f(x) = \sum_{i=0}^{k} j_i x^i$, $h(x) = \sum_{i=0}^{l} l_i x^i$ for some natural numbers k, l. Denote $f = \sum_{i=0}^{k} j_i \cdot e_i$, $h = \sum_{i=0}^{l} l_i e_i$. If $f = 0$ then $h = 0$.*

Proof. Observe that since $f = 0$ then $0 = a \cdot f = \sum_{i=0}^{k} j_i \cdot e_{i+1}$; notice that the element $a \cdot f$ corresponds to the polynomial $x \cdot f(x)$. Similarly the element $0 = a \cdot (a \cdot f) = \sum_{i=0}^{k} j_i \cdot e_{i+2}$ corresponds to the polynomial $x^2 f(x)$. Continuing in this way we get that $h = 0$, since it corresponds to the polynomial $g(x)f(x)$. □

Lemma 18. *Let A be a left brace and $a, b \in A$, $a, b \neq 0$. Suppose that $q \cdot b = 0$ for some natural number q. Let $f(x), g(x), p(x), q(x), h(x) \in \mathbb{Z}[x]$ and let $r(x) = p(x)f(x) + q(x)g(x) + q \cdot h(x)$ where $f(x) = \sum_{i=0}^{k} j_i x^i$, $g(x) = \sum_{i=0}^{l} l_i x^i$ and $h(x) = \sum_{i=0}^{l'} h_i x^i$, $r(x) = \sum_{i=0}^{m} r_i x^i$, for some natural numbers k, l, l', m. Denote $f = \sum_{i=0}^{k} j_i \cdot e_i$, $g = \sum_{i=0}^{l} l_i e_i$ and $r = \sum_{i=0}^{m} r_i e_i$. If $f = 0$ and $g = 0$ then $r = 0$.*

Proof. Observe first that $q \cdot b = 0$ implies $q \cdot e_i = 0$ for all i. Therefore, $t = q \cdot \sum_{i=1}^{l'} h_i e_i = 0$, observe that t corresponds to the polynomial $q \cdot h(x)$. Let $p = \sum_i p_i e_i$ and $q = \sum_i q_i e_i$ be elements corresponding to the polynomials $p(x)f(x)$ and $q(x)g(x)$; by Lemma 17 we get $p = q = 0$. Observe that $r = p + q + t$, and so $r = 0$. □

Theorem 19. *Let A be a finite left brace and $a, b \in A$, $a \cdot b \neq 0$. Suppose that $a^{\circ(p^j)} = 0$ and $q \cdot b = 0$ for some distinct prime numbers p, q and some natural number j. Let A_q be the Sylow's subgroup of the additive group of A, then A_q has cardinality q^m for some m, and $b \in A_q$. Let k be the maximal number such that p^k divides $q^i - 1$ for some $i \leq m$. Then*

$$a^{\circ(p^k)} \cdot b = 0.$$

In particular $a \cdot b = 0$ if p doesn't divide $q^i - 1$ for any $i \leq m$.

Proof. By a slight abuse of notation we can consider natural numbers smaller than q as elements of the field F_q. Denote $e_0 = b$, $e_1 = a \cdot b$ and inductively $e_{i+1} = a \cdot e_i$. Denote $f(x) = (x+1)^{p^j} - 1$, then $f(x) = \sum_{i=1}^{p^j} \binom{p^j}{i} x^i$. Consider elements $\sum_{i=0}^{m} n_i \cdot e_i \in A_q$, where $0 \leq n_0, n_1, \ldots, n_m < q$ then there are q^{m+1} elements in this set, therefore some two of them are equal. Notice that $q \cdot b = 0$ implies $q \cdot e_i = 0$ for every i. Therefore, $\sum_{i=0}^{m} n'_i \cdot e_i = 0$, for some $0 \leq n'_0, n'_1, \ldots, n'_m < q$ (not all equal to zero). Denote $g(x) = \sum_{i=0}^{m} n'_i \cdot x^i$. It is known that an irreducible polynomial of degree α from $F_q[x]$ divides the polynomial $x^{q^\alpha} - x$. Therefore, a polynomial of degree not exceeding m from $F_q[x]$ divides the polynomial $x^m(\prod_{i=1}^{m}(x^{q^i-1} - 1))^m$ in $F_q[x]$. Consequently $h(x+1) = g(x)$ divides the polynomial $(x+1)^m(\prod_{i=1}^{m}((x+1)^{q^i-1} - 1))^m$ in $F_q[x]$. Denote $l(x) = (x+1)^m(\prod_{i=1}^{m}((x+1)^{q^i-1} - 1))^m$ and let $l(x) = \sum_i \alpha_i x^i$ for some $0 \leq \alpha_i < q$, then $\sum_i \alpha_i e_i = 0$ by Lemma 18.

Let $t(x) = \sum_{i=0}^{t} j_i \cdot x^i$ be the greatest common divisor of $f(x)$ and $l(x)$ in $F_q[x]$; then there exist polynomials $h(x), p(x), q(x) \in \mathbb{Z}[x]$ such that

$$t(x) = p(x) \cdot f(x) + q(x) \cdot l(x) + q \cdot h(x).$$

By Lemma 18 we get that $\sum_{i=0}^{l} j_i e_i = 0$, provided that $f = 0$, where in our case $f = \sum_{i=1}^{p^j} \binom{p^j}{i} \cdot e_i$. Recall that $a^{\circ(p^j)} = 0$, by Lemma 15 we get

$$0 = \sum_{i=1}^{p^j} \binom{p^j}{i} \cdot e_i = f,$$

hence $\sum_{i=1}^{l} j_i e_i = 0$, as required.

We will show now that $t(x) = (x+1)^{p^k} - 1$. The greatest common divisor of $f(x) = (x+1)^{p^j} - 1$ and $(x+1)^{q^i} - (x+1) = ((x+1)^{q^i-1} - 1)(x+1)$ equals $(x+1)^{p^s} - 1$ for some s, since $(x+1)$ doesn't divide $f(x)$. Observe that $f(x)$ doesn't have multiple roots in any field extension of F_q because $f(x)$ and $f'(x) = p^k(x+1)^{p^k-1}$ have no common roots. Since $f(x)$ has no multiple roots then $t(x)$ doesn't have multiple roots. Notice also that $(x+1)^{p^i} - 1$ divides polynomial $(x+1)^{p^{i+1}} - 1$. It follows that $t(x) = (x+1)^{p^k} - 1$. By Lemma 15 we get that $a^{\circ(p^k)} \cdot b = 0$.

If p doesn't divide $q^i - 1$ for any $i \leq k$ then $t(x) = (x+1) - 1 = x$ hence $e_1 = a \cdot b = 0$, as required. □

Proof of Theorem 5. Observe that part [1] follows from part [2] applied for $k = 0$. Therefore, we will prove [2]. Let $a' = a^{\circ(p^k)}$, and if $k = 0$ then $a' = a$. Suppose on the contrary that $a' \cdot b' \neq 0$ for some $b' \in A_q$. Let α be such that $a' \cdot (q^\alpha \cdot b') = 0$ and $a' \cdot (q^{\alpha-1} \cdot b') \neq 0$. Denote $b = a' \cdot (q^{\alpha-1} \cdot b') \neq 0$. Observe that $q \cdot b = 0$ and $a' \cdot b = a' \cdot (a' \cdot (q^{\alpha-1} \cdot b')) \neq 0$ by Lemma 16. Therefore $0 \neq a' \cdot b = a^{\circ(p^k)} \cdot b$. This is impossible by Theorem 19. □

Proof of Corollary 6. By Theorem 5 we get $A_m \cdot A_j = 0$ for all $j \leq n$, since p_m doesn't divide $p_j^i - 1$ for each $i \leq \alpha(j)$. Let a be in the socle of the brace A_n, then $a \cdot A_i = 0$ for all i, it follows that a is in the socle of A. □

Proof of Corollary 7. Observe that if a brace A satisfies the assumptions of Corollary 6 then the retraction of A also satisfies the assumptions of Corollary 6. Recall that in [22] Rump has shown that the retraction of a brace A is isomorphic to $A/Soc(A)$. The result now follows from Corollary 6 applied several times. □

Remark. The author is grateful to Leandro Vendramin for providing a list of braces with small cardinalities. In particular it follows from this list that all braces with cardinalities 6, 8, 12, 36 have a finite multipermutation level.

Theorem 20. *Let A be a finite left brace whose cardinality is a cube-free number; then A has a nonzero socle.*

Proof. Let $A = \sum_{i=1}^{n} A_i$ where A_i are Sylow's subgroups of the additive group of A. Let A_i have cardinality $p_i^{\alpha(i)}$ for $i = 1, 2, \ldots, n$ where $p_1 < p_2 < \ldots < p_n$ are prime numbers. It is known that every A_i is a brace (see for example Lemma 17 in [23]). It is known that all groups of order p and p^2 are abelian (see [38] for some related results). Therefore, A_n is a two-sided brace, it follows that the socle of A_n is nonzero. Therefore there is an element $a \in A_n$ such that $a \cdot b = 0$ for all $b \in A_n$. Assume first that $p_n > 3$. We will show that $a \cdot b = 0$ for every $b \in A$. By Theorem 5 we get $A_n \cdot A_i = 0$ for all $i < n$, since p_n doesn't divide $p_i - 1$ nor $p_i^2 - 1 = (p_i - 1)(p_i + 1)$. Therefore $a \cdot A = 0$, as required. Assume now that A_n has cardinality equal to either 3 or 9, and A_{n-1} has cardinality 2 or 4. It follows that A is a brace of one of the following cardinalities: 6, 18, 12, 36. By the remark above it follows that A has a nonzero socle. □

Proof of Corollary 8. It follows from Theorem 20 applied several times. □

Proof of Corollary 9. In [4] Gateva-Ivanova showed that left braces and braided groups with involutive braiding operators are in one-to-one correspondence. Using this correspondence we see that Corollary 9 follows from Corollary 8. □

Proof of Theorem 10. In [4] Gateva-Ivanova showed that a solution (X, r) is a multipermutation solution if and only if the symmetric group $\mathcal{G}(X, r)$ has a finite multipermutation level. It is known that $\mathcal{G}(X, r)$ has a structure of a left brace, and Theorem 10 follows from Corollary 8. □

Proof of Corollary 11. Let the cardinality of A_i be $p_i^{\alpha(i)}$ where p_i is prime. Let A_j have the largest cardinality among braces $A_1, \ldots, A_n$. It follows that $p_j^{\alpha(j)}$ doesn't divide $p_t^i - 1$ for any t and any $i \leq \alpha(t)$. Let a be a generator of the additive group of A_j, then $a^{\circ(p_j{}^{\alpha(j)-1})} \neq 0$ and $a^{\circ(p_j{}^{\alpha(j)})} = 0$, this follows because $A_j \cdot A_j = 0$. By Theorem 5

[2] there is $k \leq \alpha(j) - 1$ such that $a^{\circ(p_j{}^k)} \cdot b = 0$ for every $b \in A_i$ for $i \neq j$. Observe that $a^{\circ(p_j{}^k)} \cdot b = 0$ for $b \in A_j$ because $A_j \cdot A_j = 0$. Therefore $a^{\circ(p_j{}^k)}$ is in the socle of A. Observe that brace $A/Soc(A)$ satisfies the assumptions of this theorem, so it has a nonzero socle. Continuing in this way we get that A has a finite multipermutation level (because the retraction of a brace A equals $A/Soc(A)$ by a result of Rump [22]). □

Proof of Theorem 12. Observe that $(a+b)^n = e_{n-1}(a+b,a) + e_{n-1}(a+b,b)$, where elements $e_{n-1}(a+b,a)$ and $e_{n-1}(a+b,b)$ are defined as in Section 2. Therefore $(a+b)^n = 0$ implies $e_{n-1}(a+b,a) = e_{n-1}(a+b,b) = 0$, since $e_{n-1}(a+b,a)$ and $e_{n-1}(a+b,b)$ are from different Sylow's subgroups of the additive group of A. We can assume that $p^m \cdot a = 0$, $q^{m'} \cdot b = 0$ for some distinct prime numbers p, q and some natural numbers m, m'. We can assume that $m > n$, if necessary taking bigger m. By Lemma 14

$$((a+b)^{\circ(j)}) \cdot b = \sum_{i=1}^{j} \binom{j}{i} \cdot e_i(a+b,b).$$

Let $\alpha = q^t$ where $t > m'$ be such that p^{m+1} divides $q^t - 1$ (we know that p divides $q^{p-1} - 1$ so p^{m+1} divides $q^{(p-1)p^m} - 1$). It follows that $\binom{\alpha}{i}$ is divisible by $p^m \cdot q^{m'}$ for all $1 < i < p^{m+1}$, and so $\binom{\alpha}{i} \cdot (a+b) = 0$ which imply $\binom{\alpha}{i} \cdot (a+b)^i = 0$. By Lemma 14,

$$(a+b)^{\circ(\alpha)} = \sum_{i=1}^{\alpha} \binom{\alpha}{i} (a+b)^i = \alpha \cdot a$$

because $(a+b)^i = 0$ for all $i \geq p^m$ (since $p^m > n$). Therefore, and by Lemma 14,

$$a \cdot b = (\alpha \cdot a) \cdot b = (a+b)^{\circ(\alpha)} \cdot b = \sum_{i=1}^{\alpha} \binom{\alpha}{i} \cdot e_i(a+b,b) = e_\alpha(a+b,b) = 0$$

because $\binom{\alpha}{i}$ is divisible by $q^{m'}$, for $1 \leq i < \alpha$, and $e_\alpha(a+b,b) = 0$ since $\alpha > n$.

Observe that $A = \sum_{i=1}^{n} A_i$ where A_i are Sylow's subgroups of the additive group of A. Recall that every A_i is a brace (see for example Lemma 17 in [23]). Let $a \in A_i$ and $b \in A_j$ for some $i \neq j$. Since $(a+b)^m = 0$ we get $a \cdot b = b \cdot a = 0$, so $A_i \cdot A_j = A_j \cdot A_i = 0$. It follows that A° is the direct product of groups A_i° for $i = 1, \ldots, n$. Notice that every A_i° is a p-group; it follows that A° is a nilpotent group. On the other hand, if A is nilpotent then $A^m = 0$ for some m by Theorem 1 in [23]. □

4. Nilpotent braces

In this section we will investigate the structure of left braces satisfying special conditions. For the following result we use a short proof which was provided by Ferran Cedó, which is much better than the original proof from the previous version of this manuscript,

and which in addition allows the removal of the assumption that A is a brace of a finite multipermutation level.

In this section we will show that if A is a left brace whose additive group has no elements of order two, and moreover $(-a)\cdot b = -(a\cdot b)$ for every $a, b \in A$, then A is a two-sided brace.

Proof of Theorem 13. (Provided by Ferran Cedó: [Ferran Cedó, *Private communication*, 8 January 2016].) Let $a, b, c \in A$. We have that $c \circ (-a) \circ b = (2c - c \circ a) \circ b$ and

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

Hence $(2c - c \circ a) \circ b = 2(c \circ b) - c \circ a \circ b$. In particular, for $a = c^{-1}$ we have that

$$(2c) \circ b = 2(c \circ b) - b.$$

Hence for every $a, b, c \in A$, we have that

$$(2c - c \circ a) \circ b = (2c) \circ b + b - c \circ a \circ b.$$

Let $x, y, z \in A$. Now we have

$$\begin{aligned} (2x - 2y) \circ z &= (2x - x \circ x^{-1} \circ (2y)) \circ z \\ &= (2x) \circ z + z - x \circ x^{-1} \circ (2y) \circ z \\ &= (2x) \circ z + z - (2y) \circ z. \end{aligned}$$

Hence

$$2((x - y) \circ z) - z = 2(x \circ z) - z + z - 2(y \circ z) + z = 2(x \circ z - y \circ z) + z.$$

Thus

$$2((x - y) \circ z) = 2(x \circ z - y \circ z + z).$$

Since the additive group of A has no elements of order two, we have that

$$(x - y) \circ z = x \circ z - y \circ z + z.$$

Note that if $t = x - y$, then $(t + y) \circ z + z = t \circ z + y \circ z$. Therefore, A is a two-sided brace. The result follows. □

5. Semidirect product and wreath product

In this section we will investigate semidirect product and wreath product of left braces. We will use the notation from Section 6 in [2].

Definition 1. Let G and H be two left braces. A map $f : G \to H$ is a homomorphism of left braces if

$$f(a + b) = f(a) + f(b), f(a \circ b) = f(a) \circ f(b).$$

Definition 2. Let N, H be left braces, let $\sigma : H \to Aut(N)$ be a homomorphism of groups from the adjoint group H° of H to the group of automorphisms of the left brace N (see Definition 1). Define the left brace $N \rtimes H$ as follows:

$$(g_1, h_1) + (g_2, h_2) = (g_1 + g_2, h_1 + h_2).$$
$$(g_1, h_1) \circ (g_2, h_2) = (g_1 \circ \sigma(h_1)(g_2), h_1 \circ h_2).$$

Lemma 21. *Let H, N be left braces and let $N \rtimes H$ be the semidirect product of braces H and N constructed via σ. The brace $N \rtimes H$ has a finite multipermutation level if and only if braces H and N have a finite multipermutation level.*

Proof. Let A be a left brace. It can be observed that A is a brace of a finite multipermutation level if and only if $A^{(n)} = 0$ for some n (it follows from results from [22] in the section about the socle of a brace, see also [2] for translation to the left braces). Let $g_i \in N$, $h_i \in H$ and $(g_i, h_i) \in N \rtimes H$ then

$$(\cdots(((g_1, h_1) \cdot (g_2, h_2)) \cdot (g_3, h_3)) \cdot \ldots) \cdot (g_n, h_n) = (d, (\cdots((h_1 \cdot h_2) \cdot h_3) \cdots))$$

for some $d \in N$, where $(g_i, h_i) \cdot (g_j, h_j) = (g_i, h_i) \circ (g_j, h_j) - (g_i, h_i) - (g_j, h_j)$.

Therefore, if brace $A = N \rtimes H$ has a finite multipermutation level then $A^{(n)} = 0$ for some n, and hence $H^{(n)} = 0$. Notice that if $h_1 = 1 = 0$ then

$$(g_1, 1) \circ (g_2, h_2) = (g_1 \circ \sigma(1)(g_2), h_2) = (g_1 \circ g_2, h_2)$$

(since σ is a homomorphism of groups so $\sigma(1) = 1$). It follows that

$$(g_1, 1) \cdot (g_2, h_2) = (g_1, 1) \circ (g_2, h_2) - (g_1, 1) - (g_2, h_2) = (g_1 \cdot g_2, 1).$$

Recall that $A = N \rtimes H$. Therefore, if $A^{(n)} = 0$ then

$$(\cdots(((g_1, 1) \cdot (g_2, h_2)) \cdot (g_3, h_3)) \cdots) \cdot (g_n, h_n) = ((\cdots((g_1 \cdot g_2) \cdot g_3) \cdots) \cdot g_n, 1)$$

therefore $N^{(n)} = 0$ and so N has a finite multipermutation level. We have shown that if $N \rtimes H$ has a finite multipermutation level then N and H are braces of a finite multipermutation level.

Assume now that H has a finite multipermutation level, so $H^{(m)} = 0$ for some m. Then

$$(\cdots(((g_1,h_1)\cdot(g_2,h_2))\cdot(g_3,h_3))\cdots)\cdot(g_m,h_m) = (d,1)$$

for some $d \in N$. Assume that N has a finite multipermutation level, so $N^{(m')} = 0$ for some m'. Then

$$(\cdots(((d,1)\cdot(g_{m+1},h_{m+1}))\cdot(g_{+2},h_{m+2}))\cdots)\cdot(g_{m+m'},h_{m+m'}) = (1,1) = (0,0).$$

Therefore,

$$(\cdots(((g_1,h_1)\cdot(g_2,h_2))\cdot(g_3,h_3))\cdots)\cdot(g_{m+m'},h_{m+m'}) = (1,1) = (0,0),$$

and hence $A^{(m+m')} = 0$ and so $N \rtimes H$ is a brace of finite multipermutation level. □

We follow definition from [2] for the wreath product of left braces.

Definition 3. Let G, H be two left braces. Then the wreath product $G \wr H$ of G by H is the semidirect product $W \rtimes H$, where

$$W = \{f : H \to G : |\{h \in H : f(h) \neq 1\}| < \infty\}$$

and the action of H of W is given by the homomorphism $\sigma : H \to Aut(W)$ defined by $\sigma(h)(f)(x) = f(hx)$, for all $x \in H$ and $f \in W$.

Recall that the multiplication on W is defined as $(f_1 \circ f_2)(x) = f_1(x) \circ f_2(x)$ and the sum is defined $(f_1 + f_2)(x) = f_1(x) + f_2(x)$ for $f_1, f_2 \in W$ and $x \in H$.

Lemma 22. *Let G, H be left braces. Then the wreath product $G \wr H$ of G by H is a left brace of a finite multipermutation level if and only if G and H are braces of a finite multipermutation level.*

Proof. By Lemma 21, it suffices to show that the left brace W defined as in Definition 3 is of a finite multipermutation level if and only if G is of a finite multipermutation level. Notice that if $f_1, f_2 \in W$ and $x \in H$, then $(f_1 \cdot f_2)(x) = (f_1 \circ f_2 - f_1 - f_2)(x) = (f_1 \circ f_2)(x) - f_1(x) - f_2(x) = f(x) \cdot f_2(x)$. Suppose that G is of a finite multipermutation level. That means that $G^{(m)} = 0$ for some m. For $f_1, f_2, \ldots, f_m \in W$ and $x \in H$ we get

$$0 = (\cdots(((f_1(x)\cdot f_2(x))\cdot f_3(x))\cdots)f_m(x) = ((\cdots((f_1 \cdot f_2)\cdot f_3)\cdots)\cdot f_m)(x).$$

Hence $(\cdots((f_1 \cdot f_2) \cdot f_3)\cdots)f_m = 0$, and thus $W^{(m)} = 0$. Therefore W is of a finite multipermutation level.

Conversely, assume that W is of a finite multipermutation level. That means that $W^{(m)} = 0$ for some m. Let $g_1, \ldots, g_m \in G$. Let f_{g_i} be the element of W defined by $f_{g_i}(x) = g_i$ if $x = 1$ and $f_{g_i}(x) = 1$ otherwise. Then

$$(\cdots((g_1 \cdot g_2) \cdot g_3)\cdots) \cdot g_m - ((\cdots((f_{g_1} \cdot f_{g_2}) \cdot f_{g_3})\cdots) \cdot f_{g_m})(1) = 0.$$

Hence $G^{(m)} = 0$ and the result follows. □

Acknowledgments

I am very grateful to David Bachiller, Ferran Cedó, Tatiana Gateva-Ivanova, Jan Okniński and Leandro Vendramin for many helpful suggestions which have improved the previous version of this paper. I am especially grateful to David Bachiller for his suggestion that the assumption that the cardinality of A is an odd number was not necessary in the previous version of Corollary 8, and to Ferran Cedó for providing a shorter and better proof of Theorem 13, which in addition allows the removal of the assumption that the solution associated to A is a multipermutation solution. I am also grateful to Leandro Vendarmin for providing a list of braces with small cardinalities. I would also like to thank Michael West for reviewing the English-language aspects of this paper. I am very grateful to the unknown referee for their many helpful comments and suggestions which have improved the paper. This research was supported with ERC grant 320974, and I would like to thank them for their support.

References

[1] W. Rump, Modules over braces, Algebra Discrete Math. 2 (2006) 127–137.
[2] F. Cedó, E. Jespers, J. Okniński, Braces and the Yang–Baxter equation, Comm. Math. Phys. 327 (1) (2014) 101–116.
[3] J.-H. Lu, M. Yan, Y.-C. Zhu, et al., On the set-theoretical Yang–Baxter equation, Duke Math. J. 104 (1) (2000) 1–18.
[4] T. Gateva-Ivanova, Set-theoretic solutions of the Yang–Baxter equation, braces, and symmetric groups, arXiv:1507.02602.
[5] D. Bachiller, Counterexample to a conjecture about braces, J. Algebra 453 (2016) 160–176, http://dx.doi.org/10.1016/j.jalgebra.2016.01.011.
[6] D. Bachiller, F. Cedo, E. Jespers, Solutions of the Yang–Baxter equation associated with a left brace, arXiv:1503.02814.
[7] L. Vendramin, Extensions of set-theoretic solutions of the Yang–Baxter equation and a conjecture of Gateva-Ivanova, J. Pure Appl. Algebra 220 (5) (2016) 2064–2076.
[8] N. Iyudu, S. Shkarin, Finite dimensional semigroup quadratic algebras with the minimal number of relations, Monatsh. Math. 168 (2) (2012) 239–252.
[9] F. Catino, M. Miccoli, Y.P. Sysak, On the adjoint group of semiprime rings, Comm. Algebra 35 (1) (2006) 265–270.
[10] W. Rump, Classification of cyclic braces, J. Pure Appl. Algebra 209 (3) (2007) 671–685.
[11] W. Rump, Semidirect products in algebraic logic and solutions of the quantum Yang–Baxter equation, J. Algebra Appl. 7 (04) (2008) 471–490.
[12] T. Gateva-Ivanova, M. Van den Bergh, Semigroups of I-type, J. Algebra 206 (1) (1998) 97–112.

[13] T. Gateva-Ivanova, S. Majid, Matched pairs approach to set theoretic solutions of the Yang–Baxter equation, J. Algebra 319 (4) (2008) 1462–1529.
[14] W. Rump, The brace of a classical group, Note Mat. 34 (1) (2014) 115–145.
[15] J. Ault, J. Watters, Circle groups of nilpotent rings, Amer. Math. Monthly 80 (1) (1973) 48–52.
[16] B. Amberg, O. Dickenschied, Y.P. Sysak, Subgroups of the adjoint group of a radical ring, Canad. J. Math. 50 (1) (1998) 3–15.
[17] P. Etingof, T. Schedler, A. Soloviev, Set-theoretical solutions to the quantum Yang–Baxter equation, Duke Math. J. 100 (2) (1999) 169–209, http://dx.doi.org/10.1215/S0012-7094-99-10007-X.
[18] D. Bachiller, F. Cedo, E. Jespers, J. Okninski, A family of irretractable square-free solutions of the Yang–Baxter equation, arXiv:1511.07769.
[19] F. Cedó, E. Jespers, J. Okniński, Retractability of set theoretic solutions of the Yang–Baxter equation, Adv. Math. 224 (6) (2010) 2472–2484.
[20] T. Gateva-Ivanova, P. Cameron, Multipermutation solutions of the Yang–Baxter equation, Comm. Math. Phys. 309 (3) (2012) 583–621.
[21] F. Cedó, T. Gateva-Ivanova, A. Smoktunowicz, On the Yang–Baxter equation and left nilpotent left braces, arXiv:1601.07131.
[22] W. Rump, Braces, radical rings, and the quantum Yang–Baxter equation, J. Algebra 307 (1) (2007) 153–170.
[23] A. Smoktunowicz, On Engel groups, nilpotent groups, rings, braces and the Yang–Baxter equation, arXiv:1509.00420.
[24] F. Cedó, E. Jespers, A. Del Rio, Involutive Yang–Baxter groups, Trans. Amer. Math. Soc. 362 (5) (2010) 2541–2558.
[25] R. Kruse, On the circle group of a nilpotent ring, Amer. Math. Monthly 77 (2) (1970) 168–170.
[26] F. Cedó, E. Jespers, J. Okniński, et al., Nilpotent groups of class three and braces, Publ. Mat. 60 (1) (2016) 55–79.
[27] B. Amberg, L. Kazarin, Nilpotent p-Algebras and Factorized p-Groups, Groups St. Andrews, vol. 1, London Math. Soc. Lecture Note Ser., vol. 339, 2005, pp. 130–147.
[28] B. Amberg, Y.P. Sysak, Radical Rings and Products of Groups, London Math. Soc. Lecture Note Ser., 1999, pp. 1–19.
[29] A. Alahmadi, H. Alsulami, S. Jain, E. Zelmanov, Finite generation of Lie algebras associated with associative algebras, J. Algebra 426 (2015) 69–78.
[30] I. Angiono, C. Galindo, L. Vendramin, Hopf braces and Yang–Baxter operators, arXiv:1604.02098.
[31] L. Bartholdi, R.I. Grigorchuk, et al., Lie methods in growth of groups and groups of finite width, in: Computational and Geometric Aspects of Modern Algebra, in: London Math. Soc. Lecture Note Ser., vol. 275, 2000, pp. 1–27.
[32] C. Martinez, E. Zelmanov, et al., Nil algebras and unipotent groups of finite width, Adv. Math. 147 (2) (1999) 328–344.
[33] V. Petrogradsky, Examples of self-iterating Lie algebras, J. Algebra 302 (2) (2006) 881–886.
[34] V.M. Petrogradsky, I.P. Shestakov, E. Zelmanov, Nil graded self-similar algebras, Groups Geom. Dyn. 4 (4) (2010) 873–900.
[35] I.P. Shestakov, E. Zelmanov, Some examples of nil Lie algebras, J. Eur. Math. Soc. (JEMS) 10 (2) (2008) 391–398.
[36] D. Bachiller, Examples of simple left braces, arXiv:1511.08477.
[37] L. Guarnieri, L. Vendramin, Braces, generalizations and applications to the Yang–Baxter equation, arXiv:1511.03171.
[38] D. Bachiller, Classification of braces of order p3, J. Pure Appl. Algebra 219 (8) (2015) 3568–3603.
[39] F. Catino, R. Rizzo, Regular subgroups of the affine group and radical circle algebras, Bull. Aust. Math. Soc. 79 (01) (2009) 103–107.