From braces to pre-Lie rings

From braces to pre-Lie rings

Aner Shalev, Agata Smoktunowicz

Abstract

Let A be a brace of cardinality p^n where $p > n+1$ is prime and let $ann(p^2)$ be the set of elements of additive order at most p^2 in this brace. We construct a pre-Lie ring related to the brace $A/ann(p^2)$.

In the case of strongly nilpotent braces of nilpotency index $k < p$ the brace $A/ann(p^2)$ can be recovered by applying the construction of the group of flows to the resulting pre-Lie ring. We do not know whether or not our construction is related to the group of flows when applied to braces which are not right nilpotent.

1 Introduction

Let p be a prime. In [22] finite analogs of Lazard's p-adic Lie rings of p-adic Lie groups were constructed. We apply analogous methods to the multiplicative groups of braces, and combine them with methods from [20, 26].

Braces were introduced in 2007 by Wolfgang Rump [19], and they are a generalisation of Jacobson radical rings, with the two-sided braces being exactly the Jacobson radical rings.

It is an open question whether, for $p > n+1$, there is a one-to-one correspondence between left nilpotent pre-Lie rings of cardinality p^n and braces of the same cardinality (see Question 1 in [26] and Question 20.92 in [13]). Such correspondence holds for right nilpotent braces for sufficiently large p, but it is not known whether each not right nilpotent brace of cardinality p^n, where $p > n+1$, corresponds to a pre-Lie algebra [13, 26].

Note that an affirmative answer to this question would yield an extension of the classical Lazard correspondence between p-adic Lie groups and p-adic Lie rings to the correspondence between braces and pre-Lie rings. This would make it possible for braces of this cardinality to be investigated by pre-Lie and Lie algebra researchers who do not have experience with braces.

One of the main motivations for investigating braces is their connections with set-theoretic solutions of the Yang-Baxter equation [19, 4] (see also [6, 7, 8] for some connections with mathematical physics); another motivation is the connections of braces with homological group theory, since braces are precisely bijective 1-cocycles of groups.

The theory of braces is also connected to algebraic number theory and its generalisations through the concept of Hopf-Galois extensions of abelian type [2]. It was shown by Gateva-Ivanova in [9] that braces are in one-to-one correspondence with involutive braided groups, a structure which is used to investigate set-theoretic solutions of the Yang-Baxter equation since 1999. On the other hand, connections between braces and pre-Lie algebras make it possible to find connections between braces and symmetric brace algebras [17], previously unrelated concepts.

The origins of connections between braces and pre-Lie algebras go back to the fundamental paper by Rump [20]. It was he who noticed that pre-Lie k-algebras and pre-Lie k-braces are analogous concepts, and he described a bijective correspondence between these two classes of objects for $k = \mathbb{R}$ (with some additional requirements) [20]. Although it was not explicitly stated in the paper, one direction of this correspondence is obtained by taking the group of flows of the pre-Lie algebra. Furthermore on page 141 of [20] Rump suggests that similar techniques could be used to obtain a passage from pre-Lie $\mathbb{F}_p$-algebras to $\mathbb{F}_p$-braces using Lazard's correspondence, where $\mathbb{F}_p$ is the unique field of order p for some prime p. Such a correspondence was formally obtained in [29] and generalised in [26]. In [29, 26] a new operation $\cdot$ was defined on a left and right nilpotent brace A such that $(A, +, \cdot)$ is a left and right nilpotent pre-Lie ring.

Any brace of prime power order is left nilpotent [19]. For this reason the left nilpotency of the pre-Lie ring is a natural assumption that one can not expect to drop; however, it is an open question as to whether or not the assumption of right nilpotency can be dropped. Namely, it is an open question whether every brace of cardinality p^n where $p > n + 1$ is a prime number can be obtained from some pre-Lie algebra by using the group of flows. The affirmative answer would imply a one-to-one correspondence between braces and pre-Lie rings of such cardinality.

In the case of finite braces, Rump, on page 141 of [20], suggested using the Lazard correspondence and to use the 1-cocycle obtained from the brace to obtain the 1-cocycle in the Lie ring. It is then known that Lie rings with bijective 1-cocycles are pre-Lie rings.

However there are complications, since the additive group of a Lie ring and the additive group of the brace may not be identical in the case where the adjoint group of the brace is obtained by using the Lazard correspondence from this Lie ring.

In this paper we construct a pre-Lie ring associated to the brace $A/ann(p^2)$. This pre-Lie ring is then used in the subsequent paper [31] to show that, if A is a brace of cardinality p^n with $p > n+1$, then the brace $A/ann(p^4)$ can be obtained as in [20] (i.e., as the group of flows) from some left nilpotent pre-Lie ring with the same additive group as the brace $A/ann(p^4)$. This gives an approximation, up to elements which have additive order p^4, to the above questions.

2 Background information

Recall that a *pre-Lie ring* $(A, +, \cdot)$ is an abelian group $(A, +)$ with a binary operation $(x, y) \to x \cdot y$ such that

$$(x \cdot y) \cdot z - x \cdot (y \cdot z) = (y \cdot x) \cdot z - y \cdot (x \cdot z)$$

and $(x + y) \cdot z = x \cdot z + y \cdot z, x \cdot (y + z) = x \cdot y + x \cdot z$, for every $x, y, z \in A$. We say that a pre-Lie ring A is *nilpotent* or *strongly nilpotent* if for some $n \in \mathbb{N}$ all products of n elements in A are zero. We say that A is *left nilpotent* if for some n, we have $a_1 \cdot (a_2 \cdot (a_3 \cdot (\cdots a_n) \cdots)) = 0$ for all $a_1, a_2, \ldots, a_n \in A$.

Braces were introduced by Rump in 2007 [19] to describe all involutive, non-degenerate set-theoretic solutions of the Yang-Baxter equation.

Recall that a set A with binary operations $+$ and $*$ is a *left brace* if $(A, +)$ is an abelian group and the following version of distributivity combined with associativity holds.

$$(a + b + a * b) * c = a * c + b * c + a * (b * c), a * (b + c) = a * b + a * c,$$

for all $a, b, c \in A$; moreover $(A, \circ)$ is a group, where we define $a \circ b = a + b + a * b$. In what follows we will use the definition in terms of the operation '$\circ$' presented in [4] (see [19] for the original definition): a set A with binary operations of addition $+$ and multiplication $\circ$ is a brace if $(A, +)$ is an abelian group, $(A, \circ)$ is a group and for every $a, b, c \in A$

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

All braces in this paper are left braces, and we will just call them braces. Let $(A, +, \circ)$ be a brace. Recall that $I \subseteq A$ is an ideal in A if for $i, j \in I$, $a \in A$ we have $i + j \in I, i - j \in I, i * a, a * i \in I$ where $a * b = a \circ b - a - b$. It follows that A/I is a well defined brace [3]. We will denote by $+, \circ$ the addition and the multiplication in the brace A/I, using the same notation as for addition and multiplication in the brace A. Elements of the brace A/I will be denoted by $[a]_I$ where $[a]_I$ is a coset with $a \in A$ being a representative of this coset. Recall that $[a]_I = \{a + i : i \in I\}$ is a subset of the brace A. Note also that $[a]_I + [b]_I = [a + b]_I$ and $[a]_I * [b]_I = [a * b]_I$.

Let $ann(p^i)$ denote the subset of A consisting of elements whose additive order is p^j where $j \leq i$. Recall that if A is a brace of cardinality p^n, where p is a prime number larger than $n + 1$, then $ann(p^i)$ is an ideal in A for every i by Lemma 17, [25] (Lemma 4, [30]).

3 Some results which will be used later

For the convenience of the reader, in this section we recall some results from other papers, which will be used later.

By a result of Rump [19], for a prime number p, every brace of order p^n is left nilpotent. Recall that Rump introduced *left nilpotent* and *right nilpotent* braces and radical chains A^{i+1} and $A^{(i+1)}$ for a left brace A, where inductively A^i consists of sums of elements $a * b$ with $a \in A, b \in A^{i-1}$, and $A^{(i)}$ consists of sums of elements $a * b$ with $a \in A^{(i-1)}, b \in A$, and $A = A^1 = A^{(1)}$. A left brace A is left nilpotent if there is a number n such that $A^n = 0$. A left brace A is right nilpotent if there is a number n such that $A^{(n)} = 0$.

We recall the definition of a strongly nilpotent brace (defined in [28]). Define $A^{[1]} = A$ and let $A^{[i]}$ consist of sums of elements $a * b$, with $a \in A^{[j]}, b \in A^{[i-j]}$ for all $i > j > 0$. A left brace A is *strongly nilpotent* if there is a number n such that $A^{[n]} = 0$. We recall Lemma 4.1 from [28]:

Lemma 1. *Let $(A, +, \circ)$ be a left brace satisfying $A^s = 0$ for some positive integer s. Let $a, b \in A$, and as usual define $a * b = a \circ b - a - b$. Define inductively elements $d_i = d_i(a, b), d'_i = d'_i(a, b)$ as follows: $d_0 = a$, $d'_0 = b$, and for $i \geq 0$ define $d_{i+1} = d_i + d'_i$ and $d'_{i+1} = d_i * d'_i$. Then for every $c \in A$ we have*

$$(a + b) * c = a * c + b * c + \sum_{i=0}^{2s} (-1)^{i+1}((d_i * d'_i) * c - d_i * (d'_i * c)).$$

For a brace A, an element $a \in A$ and a natural number n, let $a^{\circ n} = a \circ \cdots \circ a$ denote the product of n copies of a under the operation $\circ$. We recall Lemma 14 from [27]:

Lemma 2. *Let A be a left brace, let $a, b \in A$ and let n be a positive integer. Then, $a^{\circ n} * b = \sum_{i=1}^{n} \binom{n}{i} e_i$, where $e_1 = a * b$ and for each i, $e_{i+1} = a * e_i$. Moreover, $a^{\circ n} = \sum_{i=1}^{n} \binom{n}{i} a_i$, where $a_1 = a$ and for each i, $a_{i+1} = a * a_i$.*

For a brace A, denote by $A^{\circ p^i}$ the subgroup of $(A, \circ)$ generated by the elements $a^{\circ p^i}$, where $a \in A$.

Remark 3. *A p-group is said to be regular if $(xy)^p = x^p y^p z$, where z is an element of the commutator subgroup of the subgroup generated by x and y. If G is a group of cardinality p^n where p is a prime number larger than n then G is a regular p-group (see [11] §7. regular p-groups, page 98). By Theorem 7.2 (c) from [11] this implies that*

$$A^{\circ p^i} = \{a^{\circ p_i} : \quad a \in A\},$$

provided that $(A, +, \circ)$ is a brace of cardinality p^n where $p > n + 1$ is a prime number.

For a brace A and a natural number m we denote $mA = \{ma : a \in A\}$. We recall Proposition 15 from [25] (Lemma 2, [30]) and Lemma 4 from [26]:

Lemma 4. *Let i, n be natural numbers. Let A be a brace of cardinality p^n for some prime number $p > n + 1$. Then $p^i A$ is an ideal in A for each i. Moreover $A^{\circ p^i} = p^i A$.*

Let m be a natural number. An integer ξ is a primitive root modulo m if every integer coprime to m is congruent to a power of ξ modulo m. It is known that there exists a primitive root modulo p^j for every j and every odd prime number p (see for example Theorem 6.11 [16]).

Lemma 5. *Let $p > 2$ be a prime number. Let $\xi = \gamma^{p^{p-1}}$, where γ is a primitive root modulo p^p. Then $\xi^{p-1} \equiv 1 \mod p^p$. Moreover, ξ^j is not congruent to 1 modulo p for any natural number $0 < j < p - 1$.*

4 The Braces pA

Assume that B is a brace which is both left nilpotent and right nilpotent; then by a result from [28] it is strongly nilpotent. In other words, there is k such that the product of any k elements, in any order, is zero (where all products are under the operation $*$). If $B^{[k]} = 0$ and $B^{[k-1]} \neq 0$, then we say that B is strongly nilpotent of degree k, and that k is the nilpotency index of B.

Proposition 6. *Let n be a natural number. Let A be a brace of cardinality p^n where p is a prime number larger than $n + 1$. Then pA is a brace, and the product of any $p - 1$ elements of pA is zero. Therefore, pA is a strongly nilpotent brace of nilpotency index not exceeding $p - 1$. Moreover, every product of any i elements from the brace pA and any number of elements from A belongs to $p^i A$. Hence the product of any $p-1$ elements from the brace pA and any number of elements from the brace A is zero. Moreover, $p^{p-1}A = 0$.*

Proof. Let A be a brace of cardinality p^n for $p > n + 1$. Note that $p^n A = 0$ since $(A, +)$ is a group of cardinality p^n, so the additive order of each element in A divides p^n. Since by assumption $p > n + 1$, it follows that $p^{p-1}A = 0$.

By Lemma 4, $p^i A$ is an ideal in A for every i. Therefore, if $a \in p^i A, b \in p^j A$ and $i, j \geq 0$ then $a * b \in p^{i+j} A$, since if $b = p^j c$ then $a * p^j c = p^j (a * c) \in p^j (p^i A) = p^{i+j} A$. This implies that every product of any i elements from pA belongs to $p^i A$, and that every product of any i elements from pA and any number of elements from A belongs to $p^i A$. Hence every product of any $p - 1$ elements from pA and any number of elements from A

belongs to $p^{p-1}A = 0$. It also follows that every product of any $p-1$ elements from pA is zero, and so pA is a nilpotent brace of nilpotency index not exceeding $p-1$.

□

We will now present two results which are related to Lemma 1, which will be used later in the proof of Proposition 9. We first introduce a set W.

Let W denote the set of all non-associative words in non-commuting variables X, Y, Z with any distribution of brackets; moreover, Z appears only once at the very end of each word, and both X and Y appear at least once in each word; furthermore, elements from the set $\{X, Y\}$ appear at least three times in each word. For example, $(XZ)(XY) \notin W$, while $((XY)X)Z \in W$. For $w \in W$ let $w\langle a, b, c\rangle$ denote a specialisation of the word w for $X = a$, $Y = b$, $Z = c$ and the multiplication in $w\langle a, b, c\rangle$ is the same as the operation $*$ in the brace A (recall that $a * b = a \circ b - a - b$). So for example if $w = (((XX)X)Y)Z$ then $w\langle a, b, c\rangle = (((a * a) * a) * b) * c$. Let w be a word in X and Z, then $w\langle a, c\rangle$ is the specialisation of the word w for $X = a$, $Z = c$. So for example if $w = X(X(XZ))$ then $w\langle a, c\rangle = a * (a * (a * c))$.

Lemma 7. *Fix a prime number p. Let W be as above. Then there are integers β_w for $w \in W$, such that only a finite number of them is non zero and the following holds: For each brace $(A, +, \circ)$ of cardinality p^n with $n < p-1$ and for each $a, b \in pA$, $c \in A$ we have*

$$(a+b) * c = a * c + b * c + a * (b * c) - (a * b) * c + \sum_{w \in W} \beta_w w\langle a, b, c\rangle.$$

Proof. By Lemma 1, we have the following formula which holds for any brace of cardinality p^n with $n < p-1$: for every $a, b \in pA$ and $c \in A$ we have

$$(a+b) * c = a * c + b * c + \sum_{i=0}^{2(p-1)} (-1)^{i+1}((d_i * d_i') * c - d_i * (d_i' * c)),$$

where $d_0 = a$, $d_0' = b$, and for $i \geq 1$ we have $d_{i+1} = d_i + d_i'$ and $d_{i+1}' = d_i * d_i'$. By writing the first summand from our sum before the sum we get

$$(a+b) * c = a * c + b * c - (a * b) * c + a * (b * c) + \sum_{i=1}^{2(p-1)} (-1)^{i+1}((d_i * d_i') * c - d_i * (d_i' * c)).$$

We will only use this relation and the relations that products of any $p-1$ elements from the set $\{a, b\}$ and an element c is zero and the relations $p^{p-1}a = 0$ for each $a \in A$ (this holds by Proposition 6). We then apply these relations several times, so that on the right hand side we have a sum of some products of elements a, b and c (where c appears only once at the end and b and a both appear in each product), and then we obtain the result which only depends on p, and which does not depend on a, b or on the brace A. This process will terminate by the last assertion from Proposition 6. □

Next, we obtain the following corollary.

Corollary 8. *Let p be a prime number and let m be a number. Let W' be the set of nonassociative words in variables X, Z where Z appears only once at the end of each word and X appears at least twice in each word. Then there are integers γ_w for $w \in W'$,*

such that only a finite number of them is non zero and the following holds: For each brace $(A, +, \circ)$ *of cardinality* p^n *with* $p > n+1$ *and for each* $a \in pA$, $c \in A$ *we have*

$$(ma) * c = m(a * c) + \sum_{w \in W'} \gamma_w w\langle a, c\rangle.$$

Proof. We will proceed by induction on m. For $m = 1$ the result is true. For $m = 2$ the result follows from Lemma 7 applied for $b = a$. Suppose that the result is true for some m, then by the inductive assumption $(ma) * c = m(a * c) + \sum_{w \in W'} \gamma_w w\langle a, c\rangle$.

We will first prove a supporting Fact 1.

Fact 1. We will show that $Y_t^\alpha \subseteq Y_t^1$ for each t, α where the notation for this is as follows. Denote $X = pA$ as sets. For a natural number t let X_t^1 denote the set consisting of products, under the operation $*$, of t or more elements from the set X and also possibly an element $c \in A$ at the end; and let Y_t^1 denote the set whose elements are (finite) sums of elements from X_t^1. Notice that $X_t^1, Y_t^1 \subseteq p^t A$.

Define X_t^2 to be set consisting of elements u defined as follows. Let $q_1, q_2, \dots q_s$ be such that $q_i \in Y_{j_i}^1$ for each i, where $j_1, \dots, j_s > 0$ are some natural numbers. Let u be a product of elements $q_1, q_2, \dots, q_s$, in this order, with any distribution of brackets, and such that $t \leq j_1 + j_2 + \dots + j_s$ (where s is a natural number which can be different for different elements u) and also possibly element c at the end. Moreover, we only consider u in which element c appears at most once, and if it appears then it appears at the end. Let Y_t^2 denote the set whose elements are (finite) sums of elements from X_t^2. Notice that $X_t^2, Y_t^2 \subseteq p^t A$.

Continuing in this way we define $X_t^\alpha, Y_t^\alpha \subseteq p^t A$. Notice that $X_i^{\alpha-1} \subseteq X_i^\alpha$ for each α, since $X_i^{\alpha-1} \subseteq Y_i^{\alpha-1} \subseteq X_i^\alpha$ for each α.

We will show that $Y_t^{\alpha+1} \subseteq Y_t^\alpha$, for each α, t, by induction on t in the reverse order. Notice that it suffices to show that $X_t^{\alpha+1} \subseteq Y_t^\alpha$.

Observe that this is true for $t \geq p$, since $Y_t^{\alpha+1} \subseteq p^p A = 0$. Suppose that it holds for all numbers $t > j$ for some j. We need to show that $X_j^{\alpha+1} \subseteq Y_j^\alpha$, for each α. Let $u \in X_j^{\alpha+1}$. Then u is a product of $q_1, q_2, \dots q_s$, such that $q_i \in Y_{j_i}^\alpha$, for some integers $j_1, \dots, j_s$, such that $j_1 + \dots + j_s \geq j$ (for some s).

Let $q_i = \sum_k d_{i,k}$ for some $d_{i,k} \in X_{j_i}^\alpha$. By applying Lemma 7 several times we obtain that u equals a sum of all possible products of elements $d_{1,k_1}, d_{2,k_2}, \dots, d_{s,k_s}$ (in this order and with any distribution of brackets) for various $k_1, \dots, k_s$ plus some element $q \in Y_{j+1}^{\alpha+\gamma}$ for some sufficiently large γ. Notice that $d_{i,k_i} \in X_{j_i}^\alpha$ for each i (so it is a product of elements from $Y_\eta^{\alpha-1}$ for some numbers η), so any product of elements $d_{1,k_1}, d_{2,k_2}, \dots, d_{s,k_s}$ (in this order and with any distribution of brackets) is in X_j^α.

We will now show that $X_j^{\alpha+1} \subseteq Y_j^\alpha$, for each α, t. We know that $X_j^{\alpha+1} \subseteq Y_j^\alpha + Y_{j+1}^{\alpha+\gamma}$, for each α and for some $\gamma = \gamma(\alpha)$.

By the inductive induction on j, we have $Y_{j+1}^{\alpha+\gamma} \subseteq Y_{j+1}^{\alpha+\gamma-1} \subseteq Y_{j+1}^{\alpha+\gamma-2} \subseteq \dots \subseteq Y_{j+1}^\alpha$. Since $Y_{j+1}^\alpha \subseteq Y_j^\alpha$ we obtain $X_j^{\alpha+1} \subseteq Y_j^\alpha$ for each α, as required. This completes the inductive argument. Therefore, $X_j^{\alpha+1} \subseteq Y_j^\alpha$ for each j, α. Therefore, $Y_t^\alpha \subseteq Y_t^{\alpha-1} \subseteq \dots \subseteq Y_t^1$. This proves the Fact 1.

We are now ready to prove our result. To calculate $(m+1) * a$ we can apply Lemma 7 for the same a and for $b = ma$ and obtain:

$$((m+1)a)*c = (a+(ma))*c = a*c+(ma)*c+a*((ma)*c)-(a*(ma))*c+\sum_{w \in W} \beta_w w\langle a, ma, c\rangle.$$

We can then apply the inductive assumption and Fact 1 to terms which appear on the right hand side to deduce the conclusion. □

5 The binary operation $\cdot$

We will now introduce a useful notation:

Notation 1. Let p be a prime number. Let X, Y, X be noncommutative variables. Let $E(X, Y, Z)$ denote the set consisting of all non-associative words in X, Y, Z which have length less than p and such that in each word X appears at least once and Y appears at least once, moreover Z appears exactly once in each word and always at the end of this word.

Let $V_{X,Y,Z}$ be a vector obtained from elements of $E(X, Y, Z)$ arranged in a such way that shorter words are situated before longer words.

Let A be a brace of cardinality p^n, where p is a prime number such that $n + 1 < p$. Let $+, \circ, *$ be the operations in this brace. Let $x, y \in pA, z \in A$. By $V_{x,y,z}$ we denote the specialisation of the vector $V_{X,Y,Z}$ for $X = x$, $Y = y$ and $Z = z$. Similarly, by the set $E(x, y, z)$ we denote the specialisation of the set $E_{X,Y,Z}$ for $X = x$, $Y = y$ and $Z = z$.

In this section we will prove the following proposition:

Proposition 9. *Let A be a brace of cardinality p^n, where p is a prime number such that $p > n + 1$. Let $\xi = \gamma^{p^{p-1}}$, where γ is a primitive root modulo p^p. Define the binary operation $\cdot$ on A as follows.*

$$a \cdot b = \sum_{i=0}^{p-2} \xi^{p-1-i}((\xi^i a) * b),$$

for $a, b \in A$. Then $(a+b)\cdot c = a\cdot c+b\cdot c, a\cdot(b'+c) = a\cdot b'+a\cdot c$ and $(a\cdot b)\cdot c-a\cdot(b\cdot c) = (b\cdot a)\cdot c - b\cdot(a\cdot c)$, for every $a, b \in pA$, $b', c \in A$. In particular, $(pA, +, \cdot)$ is a pre-Lie algebra.

Proof. **Part 1.** By the definition of a left brace $x \cdot (y + z) = x \cdot y + x \cdot z$. We will show that $(x + y) \cdot z = x \cdot z + y \cdot z$ for $x, y \in pA, z \in A$. The proof is very similar to the proof of Proposition 5 from [26]. Observe that $(x + y) \cdot z = \sum_{i=0}^{p-2} \xi^{p-1-i}((\xi^i x + \xi^i y) * z)$. When we apply Lemma 7 to $a = \xi^i x$ and $b = \xi^i y$, $c = z$ we get that

$$\xi^{p-1-i}(\xi^i x + \xi^i y) * z = \xi^{p-1-i}((\xi^i x) * z) + \xi^{p-1-i}((\xi^i y) * z) + \xi^{p-1-i}C(i),$$

where $C(i)$ is a sum of some products (under the operation $*$) of elements $a = \xi^i x$, $b = \xi^i y$ and $c = z$.

We would like to prove that $(x + y) \cdot z = x \cdot z + y \cdot z$ for $x, y \in pA$ and $z \in A$. By the above

$$(x + y) \cdot z = \sum_{i=0}^{p-2} \xi^{p-1-i}((\xi^i x) * z) + \xi^{p-1-i}((\xi^i y) * z) + \xi^{p-1-i}C(i),$$

and

$$x \cdot z + y \cdot z = \sum_{i=0}^{p-2} \xi^{p-1-i}((\xi^i x) * z) + \xi^{p-1-i}((\xi^i y) * z).$$

Consequently, it is enough to prove that $\sum_{i=0}^{p-2} \xi^{p-1-i} C(i) = 0$. Let $V_{\xi^i x, \xi^i y, z}$ be a vector constructed as in Notation 1, so entries of this vector are products of elements $\xi^i x$, $\xi^i y$ and z. We assume that $x, y \in pA$, $z \in A$, as mentioned before. By application of Corollary 8 followed by Lemma 7, every element from the set $E(\xi x, \xi y, z)$ can be written as a linear combination of elements from $E(x, y, z)$, with integer coefficients which do not depend on x, y and z, provided that $x, y \in pA$. We can then organize these coefficients into a matrix, which we will call $M = \{m_{i,j}\}$, so that we obtain $MV_{x,y,z} = V_{\xi x, \xi y, z}$, for $x, y \in pA, z \in A$.

Observe that elements from $E(x, y, z)$ (and from $E(\xi x, \xi y, z)$) which are longer appear after elements which are shorter in our vectors $V_{x,y,z}$ and $V_{\xi x, \xi y, z}$. Notice that, by Corollary 8 and Lemma 7, M is an upper triangular matrix.

The first four elements in the vector $V_{\xi x, \xi y, z}$ are $(\xi x) * ((\xi y) * z)$, $((\xi x) * (\xi y)) * z$, $(\xi y) * ((\xi x) * z)$ and $((\xi y) * (\xi x)) * z$ (arranged in some order). Suppose that $(\xi x) * ((\xi y) * z)$ is the first entry in the vector $V_{\xi x, \xi y, z}$ (so $x * (y * z)$ is the first entry in the vector $V_{x,y,z}$). Recall that we have assumed that $x, y \in pA$, $z \in A$. By application of Corollary 8 followed by Lemma 7 several times $(\xi x) * ((\xi y) * z)$ can be written as a sum of element $\xi^2(x * (y * z))$ and some elements from $E(x, y, z)$ of length larger than 3 (so these elements are products of four or more elements from the set $\{x, y, z\}$). Therefore the first diagonal entry in M equals ξ^2, so $m_{1,1} = \xi^2$.

Note that the following diagonal entries of M are ξ^i for some natural numbers i such that $1 < i < p - 1$. Observe that $i < p - 1$, because any product where ξ^{p-1} appears would have $p - 1$ occurrences of elements from the set $\{x, y\}$; however, $x, y \in pA$, and so any such product would belong to $p^{p-1}A = 0$, by Proposition 6, and for this reason such elements were not included in the definition of $E(x, y, z)$ and $V_{x,y,z}$. Note also that $i > 1$, since any element from $E(a, b, c)$ contains both a and b.

Note that $\xi^{p-2+i} \equiv \xi^{i-1} \mod p^p$, since $\xi^{p-1} \equiv 1 \mod p^p$, so the diagonal entries are congruent to ξ^{i-1} modulo p, where $0 < i - 1 < p - 1$. By Lemma 5, diagonal entries of the matrix $\xi^{p-1-1}M$ are not congruent to 1 modulo p.

Note also that M does not depend on x, y and z, as we only used relations from Lemma 7 to construct it.

Consequently, for $x, y \in pA$, $z \in A$ and for every i, we have $V_{\xi^i x, \xi^i y, z} = M^i V_{x,y,z}$. Note that $\xi^{p-1}x = x$ and $\xi^{p-1}y = y$, because ξ^{p-1} is congruent to 1 modulo p^n and $p^n x = p^n y = 0$, since the group $(A, +)$ has cardinality p^n and $n < p - 1$. Consequently, $V_{x,y,z} = V_{\xi^{p-1}x, \xi^{p-1}y, z} = M^{p-1}V_{x,y,z} = (\xi^{(p-1)-1}M)^{p-1}V_{x,y,z}$ for $x, y \in pA$, and $z \in A$.

Notice that there exists a vector V with integer entries such that,

$$C(i) = V^T V_{\xi^i x, \xi^i y, z} = V^T M^i V_{x,y,z},$$

for each i, where V^T is the transpose of V.

Denote $M^0 = I$, the identity matrix. Recall that $\xi^{p-1} \equiv 1 \mod p^n$. It follows that

$$\sum_{i=0}^{p-2} \xi^{(p-1)-i} C(i) = \sum_{i=0}^{p-2} (\xi^{(p-1)-1})^i C(i) = V^T Q_{x,y,z}$$

where $Q_{x,y,z} = \sum_{i=0}^{p-2} (\xi^{(p-1)-1}M)^i V_{x,y,z}$. It remains to prove that all entries of vector $Q_{x,y,z}$

are zero. Notice that

$$(I - \xi^{(p-1)-1}M)\sum_{i=0}^{p-2}(\xi^{(p-1)-1}M)^i = I - (\xi^{(p-1)-1}M)^{p-1},$$

consequently,

$$(I - \xi^{(p-1)-1}M)Q_{x,y,z} = (I - (\xi^{(p-1)-1}M)^{p-1})V_{x,y,z} = 0,$$

where I is the identity matrix of the same dimension as M. Recall that entries of the vector $Q_{x,y,z}$ are elements of A and therefore their additive orders are powers of p. Recall that the diagonal entries of the matrix $I - \xi^{(p-1)-1}M$ are coprime with p, and that this matrix is upper triangular. Therefore $Q_{x,y,z} = 0$.

Part 2. We will show that $(a \cdot b) \cdot c - a \cdot (b \cdot c) = (b \cdot a) \cdot c - b \cdot (a \cdot c)$, for every $a, b \in pA$, $c \in A$. We will use a proof similar to the proof of Theorem 6 from [26]. Assume that $x, y \in pA, z \in A$. By Lemma 7 we get

$$(x + y) * z = x * z + y * z + x * (y * z) - (x * y) * z + d(x, y, z),$$

$$(y + x) * z = x * z + y * z + y * (x * z) - (y * x) * z + d(y, x, z),$$

where $d(x, y, z) = E^T V_{x,y,z}$ for some vector E with integer entries (and these entries do not depend on x, y, z) and where $V_{x,y,z}$ is a vector which occured in part 1 of our proof above. Observe that $d(x, y, z)$ is a combination of elements with three or more occurrences of elements from the set $\{x, y\}$).

We will now use lines 7-27 of the proof of Theorem 6 in [26], the only difference being that in line 18 we need to use part 1 of our proof here (above) instead of Proposition 5 from [26]. We then get that to show that

$$(x \cdot y) \cdot z - x \cdot (y \cdot z) = (y \cdot x) \cdot z - y \cdot (x \cdot z),$$

for every $x, y \in pA$, $z \in A$ it suffices to show that

$$\sum_{i,j=0}^{p-2} \xi^{p-1-i+p-1-j} d(\xi^i x, \xi^j y, z) = 0,$$

for all $x, y \in pA, z \in A$.

Proof that $\sum_{i,j=0}^{p-2} \xi^{p-1-i+p-1-j} d(\xi^i x, \xi^j y, z) = 0$ for $x, y \in pA$, and $z \in A$:

Observe that $d(x, y, z) = w(x, y, z) + v(x, y, z)$, where $w(x, y, z)$ contains all the products of elements x, y, z which appear as summands in $d(x, y, z)$ and in which x appears at least twice, and $v(x, y, z)$ is a sum of products which are summands in $d(x, y, z)$ and in which x appears only once (and consequently y appears at least twice). It is sufficient to show that $\sum_{i,j=0}^{p-2} \xi^{p-1-i+p-1-j} w(\xi^i x, \xi^j y, z) = 0$ and $\sum_{i,j=0}^{p-2} \xi^{p-1-i+p-1-j} v(\xi^i x, \xi^j y, z) = 0$. It suffices to show that $\sum_{i=0}^{p-2} \xi^{p-1-i} w(\xi^i x, y', z) = 0$ and $\sum_{j=0}^{p-2} \xi^{p-1-j} v(x', \xi^j y, z) = 0$ for any $x, x', y, y' \in pA, z \in A$ (note that x', y' should not be confused with inverses of x and y).

We will first show that

$$\sum_{i=0}^{p-2} \xi^{p-1-i} w(\xi^i x, y', z) = 0.$$

Note that there is a vector W with integer entries such that $w(x,y',z) = W^T V'_{x,y',z}$, where $V'_{x,y',z}$ is a vector constructed similarly as in Notation 1 but only including as entries products from $E(x,y',z)$ in which x appears at least twice (namely, for $x, y' \in pA$, $z \in A$, let $\tilde{E}(x,y',z)$ be the subset of $E(x,y',z)$ consisting of these products from $E(x,y',z)$ in which x appears at least twice, and let $V'_{x,y',z}$ be a vector whose entries products from $\tilde{E}(x,y',z)$ arranged in such way that shorter products of elements are situated before longer products). It follows that

$$w(\xi^i x, y', z) = W^T V'_{\xi^i x,y',z} = W^T M^i V'_{x,y',z}$$

for each i, and for all $x, y' \in pA, z \in A$, where W^T is the transpose of W, and M is some upper triangular matrix with integer entries such that $V'_{\xi x,y,z} = MV'_{x,y',z}$ and hence $V'_{\xi^i x,y,z} = M^i V'_{x,y',z}$ for every i (it can be shown that such a matrix M exists as in part 1 of this proof, since $x, y' \in pA$).

Arguing as in the first part of this proof, we see that all diagonal entries of the matrix $I - \xi^{(p-1)-1}M$ are coprime to p, by Lemma 5. It follows because the diagonal entries of M are ξ^i where $i \geq 2$, because x appears more than once in each product which is an entry in $V'_{x,y',z}$ (and $i < p-1$ since all the products which contain ξ^{p-1} have at least $p-1$ occurences of x, and such products were not included in the definition of $V'_{x,y',z}$ as they have length larger than $p-1$. Observe also that all such products are zero by Proposition 6). Now we calculate

$$\sum_{i=0}^{p-2} \xi^{(p-1)-i} w(\xi^i x, y', z) = \sum_{i=0}^{p-2} (\xi^{(p-1)-1})^i w(\xi^i x, y', z) = W^T \sum_{n=0}^{p-2} (\xi^{(p-1)-1} M)^i V'_{x,y',z},$$

where $\xi^0 = 1$ and $M^0 = I$, the identity matrix.

Note that

$$(I - \xi^{(p-1)-1}M) \sum_{i=0}^{p-2} (\xi^{(p-1)-1}M)^i = I - (\xi^{(p-1)-1}M)^{p-1}.$$

Reasoning as in the proof of Theorem 6 in [26] we obtain that

$$\sum_{i=0}^{p-2} \xi^{p-1-i} w(\xi^i x, y', z) = 0.$$

Consequently,

$$0 = W^T \sum_{i=0}^{p-2} \xi^{p-1-i} w(\xi^i x, y', z) = \sum_{i=0}^{p-2} \xi^{p-1-i} w(\xi^i x, y', z),$$

as required.

The proof that

$$\sum_{j=0}^{p-2} \xi^{p-1-j} v(x', \xi^j y, z) = 0$$

for all $x', y \in pA, z \in A$ is very similar to the proof of Theorem 6 from [26], this proof is also very similar to the proof that $\sum_{i=0}^{p-2} \xi^{p-1-i} w(\xi^i x, y', z) = 0$, so it is omitted.

□

6 The pullback $\wp^{-1}$

Let A be a brace of cardinality p^n. For $a \in pA$ let $\wp^{-1}(a)$ denote an element $x \in A$ such that $px = a$. Such an element may not be uniquely determined in A, but we can fix for every $a \in pA$ such an element $\wp^{-1}(a) \in A$. Notice that $p(\wp^{-1}(a)) = px = a$.

For A as above, $ann(p^2)$ consists of all elements of A which have additive order p^j for $j \leq 2$. By Lemma 17 from [25] (Lemma 4, [30]), $ann(p^2)$ is an ideal in A (and so is $ann(p)$), provided that $p > n+1$. Recall that if I is an ideal in the brace A then the factor brace A/I is well defined. In our situation $I = ann(p^2)$, the elements of the brace $A/ann(p^2)$ are cosets $[a]_{ann(p^2)} := a + ann(p^2)$ where $a \in A$, which we will simply denote by $[a]$, so $[a] = [b]$ if and only if $p^2(a-b) = 0$.

Lemma 10. *Let A be a brace and let $A/ann(p^2)$ be defined as above. Let $\wp^{-1} : pA \to A$ be defined as above. Then, for $a, b \in pA$ we have $[\wp^{-1}(a)] + [\wp^{-1}(b)] = [\wp^{-1}(a+b)]$. This implies that, for any integer m we have $[m\wp^{-1}(a)] = [\wp^{-1}(ma)]$.*

Proof. Note that $[\wp^{-1}(a)] + [\wp^{-1}(b)] = [\wp^{-1}(a+b)]$ is equivalent to $\wp^{-1}(a) + \wp^{-1}(b) - \wp^{-1}(a+b) \in ann(p^2)$ which is equivalent to $p^2(\wp^{-1}(a) + \wp^{-1}(b) - \wp^{-1}(a+b)) = 0$. This in turn is equivalent to $pa + pb - p(a+b) = 0$, which holds true (since $p(\wp^{-1}(a)) = a$ for every $a \in A$, by the definition of the function $\wp^{-1}$). □

7 The binary operation $\odot$

Let A be a brace of cardinality p^n where $p > n+1$ is a prime number. In this section we introduce a binary operation $\odot : A/ann(p^2) \times A/ann(p^2) \to A/ann(p^2)$.

Lemma 11. *Let $(A, +, \circ)$ be a brace of cardinality p^n, for a prime number $p > n+1$. Let $\wp^{-1} : pA \to A$ be defined as in the previous section. Let $a, b \in A$. Define*

$$[a] \odot [b] = [\wp^{-1}((pa) * b)].$$

Then this is a well defined binary operation on $A/ann(p^2)$.

Proof. We need to show that $\odot$ is a well defined operation, so that the result does not depend on the choice of coset representatives x, y of cosets $[x], [y]$.

Let $x, x' \in A$ be elements satisfying $[x] = [x']$; then $p^2(x - x') = 0$, which is equivalent to $p(x - x') \in ann(p)$. To show that $[x] \odot [y]$ does not depend on the representative x we need to show that $\wp^{-1}((px) * y) - \wp^{-1}((px') * y) \in ann(p^2)$. This is equivalent to $p((px) * y) - p((px') * y) = 0$. Applying Lemma 1 for $a = p(x - x')$, $b = px'$ and $c = y$, we obtain

$$(px) * y = (p(x - x') + (px')) * y = (px') * y + e,$$

where e belongs to the ideal generated in the brace A by the element $p(x - x')$. It follows that $e \in ann(p)$ since $p(x - x') \in ann(p)$ and $ann(p)$ is an ideal in A by Lemma 17 of [25] (Lemma 4, [30]). We conclude that $pe = 0$, hence

$$p((px) * y) - p((px') * y) = 0,$$

as required. Therefore $[x] \odot [y]$ does not depend on the choice of the representative for the coset $[x]$.

Next we will show that $[x] \odot [y]$ does not depend on the choice of the representative for the coset $[y]$. We need to show that, if $y' \in A$ satisfies $[y] = [y']$ then

$$\wp^{-1}((px) * y) - \wp^{-1}((px) * y') \in ann(p^2).$$

By the above, this is equivalent to $p((px) * y) - p((px) * y') = 0$. By the defining relations of any brace we have $p((px) * y) - p((px) * y') = (px) * (p(y - y'))$. By Lemma 4, $px = u_1^{\circ p} \circ u_2^{\circ p} \circ \cdots \circ u_s^{\circ p}$ for some $u_1, \ldots, u_s \in A$, and by Remark 3 we get $px = u^{\circ p}$ for some $u \in A$. By the formula from Lemma 2 we get $(px) * (p(y - y')) = u^{\circ p} * (p(y - y')) = 0$, since $p^2(y - y') = 0$ (since $A^p = 0$ by [19], page 166). Therefore the result does not depend on the choice of the representative for the coset $[y]$. □

8 Main results

Our main result is the following:

Theorem 12. *Let $(A, +, \circ)$ be a brace of cardinality p^n, where p is a prime number such that $p > n + 1$. Let $\odot$ be defined as in the previous section, so $[x] \odot [y] = [\wp^{-1}((px) * y)]$. Let $\xi = \gamma^{p^{p-1}}$ where γ is a primitive root modulo p^p. Define a binary operation $\bullet$ on $A/ann(p^2)$ as follows:*

$$[x] \bullet [y] = \sum_{i=0}^{p-2} \xi^{p-1-i} [\xi^i x] \odot [y],$$

for $x, y \in A$. Then $A/ann(p^2)$ with the binary operations $+$ and $\bullet$ is a pre-Lie ring.

Proof. **Part 1**. We need to show that $([x]+[y])\bullet[z] = [x]\bullet[z]+[y]\bullet[z]$ and $[x]\bullet([y]+[z]) = [x] \bullet [y] + [x] \bullet [z]$ for every $x, y, z \in A$. Observe that the formula $[x] \bullet ([y] + [z]) = [x]\bullet[y]+[x]\bullet[z]$ follows immediately from the fact that in every brace $x*(y+z) = x*y+x*z$. We will show now that

$$([x] + [y]) \bullet [z] = [x] \bullet [z] + [y] \bullet [z].$$

Notice that $[x]\bullet[y] = [\wp^{-1}(px \cdot y)]$, where operation $\cdot$ is as in Proposition 9. By Proposition 9 and Lemma 10

$$([x] + [y]) \bullet [z] = [\wp^{-1}((px + py) \cdot z)] = [\wp^{-1}(((px) \cdot z) + ((py) \cdot z))] =$$

$$= [\wp^{-1}((px) \cdot z)] + [\wp^{-1}((py) \cdot z)] = [x] \bullet [z] + [y] \bullet [z].$$

Part 2. We need to show that

$$([x] \bullet [y]) \bullet [z] - [x] \bullet ([y] \bullet [z]) = ([y] \bullet [x]) \bullet [z] - [y] \bullet ([x] \bullet [z]),$$

for $x, y, z \in A$. Recall that $[x] \bullet [y] = [\wp^{-1}((px) \cdot y)]$. Consequently,

$$([x] \bullet [y]) \bullet [z] = [\wp^{-1}(px \cdot y)] \bullet [z] = [\wp^{-1}(((px) \cdot y) \cdot z)],$$

and

$$[x] \bullet ([y] \bullet [z]) = [x] \bullet [\wp^{-1}((py) \cdot z)] = [\wp^{-1}((px) \cdot \wp^{-1}((py) \cdot z))].$$

Note that

$$p^2(\wp^{-1}((px)\cdot\wp^{-1}((py)\cdot z)))=p((px)\cdot\wp^{-1}((py)\cdot z))=(px)\cdot((py)\cdot z),$$

On the other hand we have $p^2(\wp^{-1}(((px)\cdot y)\cdot z))=p(((px)\cdot y)\cdot z)$. Note that $(px)\cdot y\in pA$, since, by Lemma 4, pA is an ideal in A.

Let $a\in pA$, $b\in A$, then $(na)\cdot b=n(a\cdot b)$, since

$$(a+a+\cdots+a)\cdot b=a\cdot b+a\cdot b+\cdots+a\cdot b$$

by Proposition 9. Applying this for $n=p$, $a=(px)\cdot y$ and $b=z$, we get that

$$p(((px)\cdot y)\cdot z)=(p((px)\cdot y))\cdot z=((px)\cdot(py))\cdot z.$$

Therefore,

$$([x]\bullet[y])\bullet[z]-[x]\bullet([y]\bullet[z])=([y]\bullet[x])\bullet[z]-[y]\bullet([x]\bullet[z]),$$

written using this notation, and multiplied by p^2 gives an equivalent condition

$$((px)\cdot(py))\cdot z-(px)\cdot((py)\cdot z)=((py)\cdot(px))\cdot z-(py)\cdot((px)\cdot z).$$

This condition holds by Proposition 9 applied for $a=px$, $b=py$, $c=z$. This concludes the proof. □

Connection with the Group of Flows. The group of flows of a pre-Lie algebra was invented in [1] and in [20] Rump suggested to use this construction to obtain a passage from pre-Lie algebras to $\mathbb{F}_p-$ braces. Notice that if A is a strongly nilpotent brace of nilpotency index $k<n$ and cardinality p^n with $n+1<p$ for a prime number p, then we can define a pre-Lie ring $(A,+,\cdot)$ associated to the brace A as in Proposition 5 and Theorem 6 in [26] (a small variation of this pre-Lie ring is obtained by reversing the construction of the group of flows from [20]). Recall the formula from [26]: $x\cdot y=\sum_{i=0}^{p-2}\xi^{p-1-i}(\xi^i x)*y$, for $x,y\in A$. Observe that $[a]\bullet[b]=[\wp^{-1}(\sum_{i=0}^{p-2}\xi^{p-1-i}(\xi^i pa)*b))]=[\wp^{-1}((pa)\cdot b)]=[\wp^{-1}(p(a\cdot b))]=[a\cdot b]$.

It was shown in [26] that by applying the group of flows construction to the pre-Lie ring $(A,+,\cdot_1)$ yields the original brace $(A,+,\circ)$, where $a\cdot_1 b=-(1+p+\cdots+p^n)a\cdot b$, as mentioned in Notation 2 in [26]. Therefore, by applying the group of flows construction to the pre-Lie ring $(A/ann(p^2),+,\bullet_1)$, where $a\bullet_1 b=-(1+p+\cdots+p^n)a\bullet b$ for $a,b\in A$, yields the brace $(A/ann(p^2),+,\circ)$.

The forthcoming paper [31] investigates how to recover the brace $(A/ann(p^2),+,\circ)$ from the obtained pre-Lie ring $(A/ann(p^2),+,\bullet)$ in the general case when A need not be right nilpotent (see also [30]). A correspondence between braces $A/ann(p^2)$ and a subset of left nilpotent pre-Lie rings with the same additive group is also investigated.

Acknowledgements. The first author acknowledges support by the ISF grant 700/21, the BSF grant 2020/037 and the Vinik Chair of mathematics which he holds. The second author acknowledges support from the EPSRC programme grant EP/R034826/1 and from the EPSRC research grant EP/V008129/1. Both authors are grateful to Leandro Vendramin and Wolfgang Rump for useful comments. We are grateful to the referee for many helpful suggestions which improved the original manuscript. In particular we are grateful for improving and clarifying the second page of our introduction and for Remark 3, and for suggestions as to how to use this remark to simplify the proof of Lemma 11.

References

[1] A. Agrachev and R. Gamkrelidze, *Chronological algebras and nonstationary vector fields*, J. Sov. Math. **17** (1981), 1650–1675.

[2] D. Bachiller, *Counterexample to a conjecture about braces*, J. Algebra **453** (2016), 160–176.

[3] D. Bachiller, Ph.D. Thesis entitled *Study of the algebraic structure of left braces and the Yang-Baxter equation*, 2016, Universitat Autónoma de Barcelona.

[4] F. Cedó, E. Jespers and J. Okniński, *Braces and the Yang-Baxter equation*, Comm. Math. Phys. **327** (2014), 101–116.

[5] F. Cedó, E. Jespers and A. del Rio, *Involutive Yang-Baxter groups*, Trans. Amer. Math. Soc. **362** (2010), 2541–2558.

[6] I. Colazzo, E. Jespers and Ł. Kubat, *Set-theoretic solutions of the pentagon equation*, Comm. Math. Phys. **380** (2020), 1003–1024.

[7] A. Doikou, *Set theoretic Yang-Baxter equation, braces and Drinfeld twists*, J. Phys. A, 54 (2021) **41**, Paper No. 415201.

[8] A. Doikou and A. Smoktunowicz, *Set-theoretic Yang-Baxter and reflection equations and quantum group symmetries*, Lett. Math. Phys. **111** (2021), Paper No. 105, 40pp.

[9] T. Gateva-Ivanova, *Set-theoretic solutions of the Yang-Baxter equation*, braces and symmetric groups, Adv. Math. **338** (2018), 649–701.

[10] L. Guarnieri and L. Vendramin, *Skew braces and the Yang-Baxter equation*, Math. Comput. **86** (2017), 2519–2534.

[11] Y. Berkovich, *Groups of prime exponent*, De Gruyter, Berlin, New York, 2008.

[12] E.I. Khukhro, *Nilpotent Groups and their Automorphisms*, De Gruyter expositions in Mathematics **8**, New York, 1993.

[13] E.I. Khukhro and V.D. Mazurov (the Editors), *Unsolved Problems in Group Theory*, the Kourovka Notebook, No. 20, arXiv:1401.0300 [math.GR].

[14] N. Iyudu, *Classification of contraction algebras and pre-Lie algebras associated to braces and trusses*, arXiv: 2008.06033 [math.RA].

[15] P. Jedlicka, A. Pilitowska and A. Zamojska-Dzienio, *The construction of multipermutation solutions of the Yang-Baxter equation of level 2*, J. Comb. Theory Ser. A. **176** (2020), 105295, 35pp.

[16] G. A. Jones and J. M. Jones, *Elementary number theory*, Springer Undergraduate Mathematics Series, 1998.

[17] T. Lada and M. Markl, *Symmetric brace algebras*, Applied Categorical Structures **13** (2005), 351–370.

[18] D. Puljić, A. Smoktunowicz and K. Nejabati-Zenouz, *Some braces of cardinality p^4 and related Hopf-Galois extensions*, New York J. Math. **28** (2022), 494-522

[19] W. Rump, *Braces, radical rings, and the quantum Yang-Baxter equation*, J. Algebra **307** (2007), 153–170.

[20] W. Rump, *The brace of a classical group*, Note Mat. **34** (2014), 115–144.

[21] W. Rump, *Classification of non-degenerate involutive set-theoretic solutions to the Yang-Baxter equation with multipermutation level two*, Algebras Represent. Theory **25** (2022), 1293–1307.

[22] A. Shalev, *On almost fixed point free automorphisms*, J. Algebra **157** (1993), 271–282.

[23] A. Shalev and E.I. Zelmanov, *Pro-p groups of finite coclass*, Math. Proc. Cambridge Phil. Soc. **111** (1992), 417–421.

[24] A. Shalev, *The structure of finite p-groups: effective proof of the coclass conjectures*, Invent. Math. **115** (1994), 315–345.

[25] A. Smoktunowicz, *On passage from finite braces to pre-Lie rings*, arXiv:2202.00085v3 [math.RA].

[26] A. Smoktunowicz, *On the passage from finite braces to pre-Lie rings*, Adv. Math. **409** Part B (2022), 108683.

[27] A. Smoktunowicz, *A note on set-theoretic solutions of the Yang-Baxter equation*, J. Algebra **500** (2018), 3–18.

[28] A. Smoktunowicz, *On Engel groups, nilpotent groups, rings, braces and the Yang-Baxter equation*, Trans. Amer. Math. Soc. **370** (2018), 6535–6564.

[29] A.Smoktunowicz, *A new formula for Lazard's correspondence between finite braces and pre-Lie algebras*, J. Algebra **594** 2022, 202–229.

[30] A. Smoktunowicz, *Classifying braces obtained from pre-Lie algebras*, submitted.

[31] A. Smoktunowicz, *From pre-Lie rings back to braces*, arXiv:2208.02535 [math.RA].

Aner Shalev
Einstein Institute of Mathematics
Edmond J. Safra Campus
The Hebrew University of Jerusalem
Givat Ram. Jerusalem, 9190401, Israel
aner.shalev@mail.huji.ac.il

Agata Smoktunowicz
School of Mathematics, University of Edinburgh
JCMB, Peter Guthrie Tait Road
Edinburgh, EH9 3FD, UK
A.Smoktunowicz@ed.ac.uk