From pre-Lie rings back to braces

Agata Smoktunowicz

Abstract

Let \( A \) be a brace of cardinality \( p^n \) where \( p > n + 1 \) is prime, and \( \text{ann}(p^i) \) be the set of elements of additive order at most \( p^i \) in this brace. A pre-Lie ring related to the brace \( A/\text{ann}(p^2) \) was constructed in [8].

We show that there is a formula dependent only on the additive group of the brace \( A \) which reverses the construction from [8]. As an application example it is shown that the brace \( A/\text{ann}(p^4) \) is the group of flows of a left nilpotent pre-Lie algebra.

1 Introduction

Let \( A \) be a brace of cardinality \( p^n \) where \( p > n + 1 \) is prime, and \( \text{ann}(p^i) \) be the set of elements of additive order at most \( p^i \) in this brace. A pre-Lie ring related to the brace \( A/\text{ann}(p^2) \) was constructed in [8]. The aim of this paper is to show that this construction can be reversed to recover the brace \( A/\text{ann}(p^2) \) by applying a formula similar to the formula for the group of flows to the obtained pre-Lie ring. This formula is the same for braces which have the same additive group. The main result of this paper is the following application of this result:

**Theorem 1.** Let \( p \) be a prime number, and \( n < p - 1 \) be a natural number. Let \((A, +, \circ)\) be a brace of cardinality \( p^n \), and let \( \text{ann}(p^i) \) be the set of elements of additive order at most \( p^i \) in this brace. Then the multiplication in the brace \( A/\text{ann}(p^4) \) is the same as the multiplication in the group of flows of some left nilpotent pre-Lie algebra \((A/\text{ann}(p^4), +, \cdot)\). Moreover, the addition in the pre-Lie algebra \((A/\text{ann}(p^4), +, \cdot)\) and in the brace \((A/\text{ann}(p^4), +, \circ)\) is the same (where \((A/\text{ann}(p^4), +, \circ)\) is the factor brace of the brace \((A, +, \circ)\) by the ideal \(\text{ann}(p^4)\)).

Note that, by Lemma 17, [9], \(\text{ann}(p^i)\) is an ideal in the above brace \( A \). Therefore the brace \( A/\text{ann}(p^i) \) is well defined. Recall that the passage from finite pre-Lie algebras to finite braces was first discovered by Wolfgang Rump in [6]. He used the exponential function \( e^a \) to pre-Lie algebras and showed that the obtained structure is a brace. This construction can also be described using the group of flows developed in [1]. For more details, see [9]. It is an open question as to whether or not every brace with such cardinality could be be obtained from some pre-Lie algebra in this way. This is known to be true for right nilpotent braces for sufficiently large \( p \) [9], and it is also known to be true for \( \mathbb{R} \)-braces [8], where for \( \mathbb{R} \)-braces the correspondence is local.

In [6], page 141, Wolfgang Rump suggested a potential way of approaching this question using \( 1 \) cocycles. However, there are complications, because the additive group of a Lie algebra and the additive group of the brace may not be identical in the case when
the adjoint group of the brace is obtained by using the Lazard’s correspondence from this Lie algebra.

Notice that Theorem 10 implies that if \( A \) is a brace of cardinality \( p^n \) for a prime number \( p \) and a natural number \( n < p - 1 \) then the factor brace \( A/\text{ann}(p^2) \) is obtained by the formula from Theorem 11 from some pre-Lie ring with the same additive group. It is not clear whether the formula from Theorem 10 is the same as the formula for the group of flows. We will use the same notation as in \([8]\). For the background section we refer the reader to the background section of \([8]\).

2 Left nilpotency of the pre-Lie rings constructed in \([8]\)

Let \((A, +, \circ)\) be a brace. One of the mappings used in connection with braces are the maps \( \lambda_a : A \to A \) for \( a \in A \). Recall that for \( a, b, c \in A \) we have \( \lambda_a(b) = a \circ b - b \), \( \lambda_{a \circ c}(b) = \lambda_a(\lambda_c(b)) \). Our first result shows that the pre-Lie rings constructed in \([8]\) are left nilpotent. For the reader’s convenience the main result and the construction from \([8]\) is quoted in Theorem 19 at the end of this paper.

**Lemma 2.** Let the notation be as in Theorem 19. Then the obtained pre-Lie ring \((A, +, \bullet)\) is left nilpotent.

**Proof.** By Lemma 14, we have \( pA = A^{op} \). Consequently, if \( a \in A \) then

\[
pa = a_1^{op} \circ a_2^{op} \circ \cdots \circ a_m^{op}
\]

for some \( m \) and some \( a_1, \cdots, a_m \in A \). Recall that \( \circ \) is an associative operation, so we do not need to put brackets in this formula. By Lemma 14 we have that

\[
a^{op} \circ b = \sum_{k=1}^{p-1} \binom{p}{k} e_k,
\]

where \( e_1 = a \circ b, e_2 = a \circ (e_1) \), and for each \( i, e_{i+1} = a \circ e_i \).

Notice that if \( b \in A^i \) then \( e_j \in A^{i+j} \), hence \( e_{p-1} \in A^{p-1} \subseteq A^{p+1} = 0 \).

By using this formula, we see that if \( e \in A, b \in A^i \) and \( c \in A^{i+1} \) for some \( i \) then

\[
\lambda_{c^op}(pc + b) = e^{op} \circ (cp + b) + pc + b = pc' + b,
\]

for some \( c' \in A^{i+1} \) (since \( \binom{p}{k} \) is divisible by \( p \) for \( 0 < k < p \).) Recall that \( A^{i+1} = A \ast A^i \).

Let \( b \in A^i \) for some \( i \). Notice that by the multiplicative property of \( \lambda \) maps we have:

\[
(pa) \circ b + b = \lambda_{pa}(b) = \lambda_{a_1^{op} \circ \cdots \circ a_m^{op}}(b) = \lambda_{a_1^{op}}(\cdots (\lambda_{c^{op}}(\cdots (\lambda_{c^{op}}(b) \cdots )))) \subseteq pA^{i+1} + b.
\]

This implies

\[
(pa) \circ b + b \in pA^{i+1} + b,
\]

hence \( [\gamma^{-1}((pa) \circ b)] \in [A^{i+1}] \), provided that \( b \in A^i \), where \([A^{i+1}] = \{ [a] : a \in A^{i+1} \} \), and, as usual, we use notation \([a] = [a]_{\text{ann}(p^2)} \). Therefore, by the formula for operation \( \bullet \) from Theorem 19 we get

\[
[a] \bullet [b] \in [A^{i+1}],
\]
for $b \in A'$, $a \in A$. Consequently,

$$[b_1] \bullet ([b_2] \bullet (\cdots ([b_n] \bullet [b_{n+1}]))) \in [A^{n+1}] = 0,$$

for all $b_1, \ldots, b_{n+1} \in A$, since $A^{n+1} = 0$ in every brace of cardinality $p^n$ for a prime $p$, by a result of Rump [5].

3 Relations between $\odot$ and $\bullet$

Let $(A, +, \circ)$ be a brace, and let $a \in A$. In this section, by $[a]$, we mean the coset of $A$ in the factor brace $A/\text{ann}(p^2)$, so $[a] = \{a + i : i \in \text{ann}(p^2)\}$. Recall that $[a]$ is an element of the factor brace $A/\text{ann}(p^2)$. We will denote the multiplication and the addition in the brace $A/\text{ann}(p^2)$ by the same symbols as the addition and the multiplication in brace $A$. Recall that $[a] + [b] = [a + b]$ and $[a] \ast [b] = [a \ast b]$, $[a \circ b] = [a \ast b + a + b]$. We recall a lemma from [8].

**Lemma 3.** Let $(A, +, \circ)$ be a brace of cardinality $p^n$, $p$ is a prime number, and $p > n + 1$. Let $\varphi^{-1} : pA \to A$ be defined as in [8]. Let $a, b \in A$, then $[a] = [a]_{\text{ann}(p^2)}$, $[b] = [b]_{\text{ann}(p^2)}$ are elements of $A/\text{ann}(p^2)$. Define

$$[a] \odot [b] = [\varphi^{-1}((pa) \ast b)],$$

then this is a well defined binary operation on $A/\text{ann}(p^2)$.

Notice that $\varphi^{-1}$ can be defined in the same way for all braces whose additive group is the same group $(A, +)$. Recall also that if $a = px$ then $\varphi^{-1}(a)$ is an element in $A$ such that $p(\varphi^{-1}(x)) = a$.

**Remark 1.** Let $(A, +, \circ)$ be a brace of cardinality $p^n$ for some prime number $p$, and for some natural number $n < p - 1$. Note that in the proof of the following Lemma 4 only the following facts are used:

- $p^{p-1}a = 0$ for all $a \in A$.
- The product of any $p - 1$ elements from $pA$, under the operation $\ast$, is zero (by Proposition [16]).
- For every $i$, $p^iA$ is an ideal in $A$, by [11].
- The formula from Lemma [17].
- Operation $\varphi^{-1} : pA \to A$, which only depends on the additive group, and it can be assumed that for all braces with the same additive group this operation $\varphi^{-1}$ is the same.
- The operation of taking the coset $[a] = [a]_{\text{ann}(p^2)}$ of an element $a \in A$. This coset only depends on the additive group of this brace and does not depend on the multiplicative group of this brace.
- The inductive assumption, which gives formulas which only depend on the additive group of brace $A$. 
We proceed on induction, in the decreasing order, on \( p \).

**Proof.** Denote \( p \) since 

\[
\left( \text{number of these integers nonzero, and such that for each brace} \right)
\]

\( X \) each 

\( i \)

\( k \)

We will use this notation in the following lemma.

\[
\text{Let} \quad w(V_1, \ldots, V_j) = \text{the specialisation of} w, \text{on} X_i = [x_i] \text{and under the operation} \circ, \text{and let} w\{x_1, \ldots, x_j\} \text{be the specialisation of} w, \text{for} X_i = x_i \text{and under the operation} \ast. \text{For example, let} w = (X_1X_2)X_3, \text{and let} a, b \in A, \text{then} w([a], [a], [b]) = ([a] \circ [a]) \circ [b] \text{and} wa, a, b = (a \ast a) \ast b. \text{We will use this notation in the following lemma.}
\]

**Lemma 4.** Let \( p \) be a prime number and \( n < p - 1 \) be a natural number. Let \((A, +)\) be an abelian group of cardinality \( p^n \), where \( p \) is a prime number and \( n < p - 1 \) is a natural number. Let \( j > 2 \) and let \( W \in V_j \) be a non-associative word in variables \( X_1, \ldots, X_j \), where each \( X_i \) appears only once, and they appear in the order \( X_1, \ldots, X_j \). Let \( i_1, \ldots, i_{j-1} \geq 0 \), where \( i_j \geq 0 \) are all natural numbers. There are integers \( \beta_v \) for \( v \in V_j \), with only a finite number of these integers nonzero, and such that for each brace \((A, +, \circ)\) with the additive group \((A, +)\) and for each \( x_1, \ldots, x_j \) we have

\[
[p^{-1}W\{p^{i_1}x_1, \ldots, p^{i_j}x_j\}] = p^{i_1 + \ldots + i_j - 1}W([x_1], \ldots, [x_j]) + p^{i_1 + \ldots + i_j} \sum_{v \in V_j} \beta_vv([x_1], \ldots, [x_j]),
\]

**Proof.** Denote

\[
w = W\{p^{i_1}x_1, \ldots, p^{i_j}x_j\}.
\]

We proceed on induction, in the decreasing order, on

\[
i_1 + i_2 + \cdots + i_j.
\]

If \( i_1 + \cdots + i_j \geq p - 1 \geq n + 1 \) then \( w \) is zero by Proposition\[16\] Then

\[
[p^{-1}(w)] = [p^{-1}(0)] = [0] = p^{i_1 + \ldots + i_j - 1}[\bar{w}]
\]

since \( [p^{p-2}A] = [0] \) so \( p^{i_1 + \ldots + i_j - 1}[\bar{w}] = [0] \). Therefore, the result is true.

Let \( k \) be a natural number. Suppose now that the result holds in cases when \( \text{power}(w) > k \), and for all \( j \) and \( \text{we will show that the result holds also in the case when} \text{power}(w) = k \) and for all \( j \). \text{For this fixed} \text{power}(w) = k, \text{we will proceed by induction on} j \text{ (in the usual increasing order). The smallest possible} j \text{ to consider is} j = 2. \text{Recall that} w \text{ is a product of elements} p^{i_1}x_1, \ldots, p^{i_j}x_j \in A \text{ under the operation} \ast. \text{We proceed by induction on} j. \text{Case} j = 2. \text{Notice that for} j = 2 \text{ we have} w = (p^{k'}x_1) \ast (p^{m}x_2), \text{where} k' + m = k. \text{If} k' = 1 \text{ then} w = (px_1) \ast x_2. \text{Consequently}

\[
[p^{-1}(w)] = [p^{-1}((px_1) \ast (p^{m}x_2))] = p^{m}[p^{-1}((px_1) \ast x_2)] = p^{m}[x_1 \circ x_2] = p^{k-1}[x_1 \circ x_2].
\]

It remains to consider the case \( i_1 = k' > 1, i_2 = m. \text{By Lemma} [13]

\[
(px_1)^{k'-1} = p^{k'}x_1 + \sum_{i=2}^{p-1} \binom{k' - 1}{i} y_i,
\]

\[
4
\]
where \( y_2 = (px_1) \ast (px_1, \ldots \ast y_i = (px_1) \ast y_i \) for \( i = 2, 3, \ldots, p - 1 \). Consequently
\[
(px_1)^{ok'-1} = p^{k'} x_1 + \sum_{i=2}^{p-1} \zeta_i p^{k'-1} y_i,
\]
for some integers \( \zeta_i \geq 0 \). This follows because \( -x = (p^p - 1)x = x + \cdots + x \) for \( x \in A \).
Notice that the sum ends at the \( p-1 \)th place since \( y_i \in A^i \) and \( A^{n+1} = 0 \) (since \( A \) has cardinality \( p^n \) by \([5]\), and \( n+1 \leq p-1 \), hence \( A^{p-1} = 0 \)). Therefore
\[
(p^k x_1) \ast (p^m x_2) = ((px_1)^{op^{k-1}} + \sum_{i=2}^{p-1} \zeta_i p^{k'-1} y_i) \ast (p^m x_2).
\]
By Lemma \( 17 \) and Corollary \( 18 \) we have
\[
(p^k x_1) \ast x_2 = (px_1)^{op^{k'-1}} \ast (p^m x_2) + d
\]
where \( d \) is a sum of some products of some number of copies of elements \( p^{k'-1} y_i \) for \( i = 2, 3, \ldots \) and element \( p^m x_2 \) at the end, and also possibly some number of copies of element \((px_1)^{op^{k-1}}\). Observe that \( p^{k'-1} y_i \) is a product of \( i-1 \) copies of element \( px_1 \) and element \( p^{k'-1}(px_1) = p^{k'} x_1 \) at the end, so \( p^{k'-1} y_i = (px_1) \ast ((px_1) \ast (\cdots ((px_1) \ast (p^k x)) \cdots )) \), hence in this presentation \( p \) appears at least \( k'+1 \) times near elements \( x_i \) in this product which is equal to \( p^{k'-1} y_i \) for \( i = 2, 3, \ldots \).

Then, by applying Lemma \( 17 \) several times to the element \( (px_1)^{op^{k'-1}} = p^{k'} x_1 + \sum_{i=2}^{p-1} p^{k'-1} \xi_i y_i \) which appears in these products we get that \( d \) is a sum of some products of elements \( p^{k'-1} y_i \) and the element \( p^m x_2 \) at the end, and possibly also some other elements (which are products of \( y_i \in pA \) and \( p^{k'} x_1 \)). Notice that the process of applying Lemma \( 17 \) will terminate at some stage, because we will obtain longer products of elements from \( pA \), and by Proposition \( 16 \) such products of more than \( p-1 \) elements are zero. Notice also that \( p \) appears at least \( k'+1 + m = k+1 \) times near elements \( x_i \) in such products.

Recall that \([\varphi(x + y)] = [\varphi^{-1}(x)] + [\varphi^{-1}(y)] \) for \( x, y \in pA \), by \([8]\). Observe now that
\[
[\varphi^{-1}((px_1)^{op^{k'-1}} \ast (p^m x_2))] = [\varphi^{-1}(p^{k'-1}((px_1) \ast (p^m x_2))))] + [\varphi^{-1}(c)],
\]
where
\[
c = \sum_{i=2}^{p-1} \zeta_i \varphi^{-1}(p^{k'-1} z_i),
\]
where \( z_2 = (px_1) \ast ((px_1) \ast (p^m x_2)) \) and for \( i = 2, 3, \ldots \) we have \( z_{i+1} = (px_1) \ast z_i \) (by Lemma \( 13 \)). Notice that \( p^{k'-1} z_2 = (px_1) \ast ((px_1) \ast (p^{m+k'-1} x_2)) \) and \( p^{k'-1} z_{i+1} = (px_1) \ast (p^{k'-1} z_i). \) Therefore, in this presentation of elements \( p^{k'-1} z_i \), \( p \) appears at least \( m' + k' + 1 \) times near elements \( x_i \).

Notice also that
\[
[\varphi^{-1}(p^{k'-1}((px_1) \ast (p^m x_2))))] = p^{k'-1 + m}[\varphi^{-1}((px_1) \ast x_2)] = p^{k'-1}[x_1] \circ [x_2].
\]
Combining it all together, we obtain
\[
[\varphi^{-1}((px_1) \ast (p^m x_2))] = p^{k'-1}[x_1] \circ [x_2] + [\varphi^{-1}(d)] + [\varphi^{-1}(c)].
\]
Observe that this equation was proved without using the inductive assumption, so it is true for all $k' > 0, m \geq 0$.

Recall that $k' + m = k$. Remark 1 and the inductive assumption on $k$ (applied for numbers larger than $k$) shows that $[\varphi^{-1}(d)] + [\varphi^{-1}(c)]$ can be written as some sum

$$p^k \sum_{v \in V_j} \beta_{v, t_1, \ldots, t_j, w}([x_1], \ldots, [x_j])$$

This proves the case $j = 2$.

**Case** $j > 2$. Suppose now that $j > 2$. Recall that $w$ is a product of elements $p^{i_1} x_1, \ldots, p^{i_j} x_j \in A$ under the operation $\ast$. Notice that there is $t$ such that $w$ is a product of elements $p^{i_1} x_1, \ldots, p^{i_t} x_{t-1}$ and element $p^{i_t} x_t \ast p^{i_{t+1}} x_{t+1}$ and elements $p^{i_{t+2}} x_{t+2}, \ldots, p^{i_j} x_j \in A$.

Recall that several lines prior we proved that

$$[\varphi^{-1}((p^{k} x_1) \ast (p^m x_2))] = p^{k-1} [x_1] \odot [x_2] + [\varphi^{-1}(d)] + [\varphi^{-1}(c)].$$

Observe that this equation was proved without the use of inductive assumption, so it is true for all $k' > 0, m \geq 0$. We can apply it to $p^{i_t} x_t$ instead of $p^{k} x_1$ and to $p^{i_{t+1}} x_{t+1}$ instead of $p^{m} x_2$, and obtain that:

$$[\varphi^{-1}((p^{i_t} x_t) \ast (p^{i_{t+1}} x_{t+1}))] = p^{i_t+i_{t+1}-1} [x_t] \odot [x_{t+1}] + [\varphi^{-1}(d')] + [\varphi^{-1}(c')],$$

for some $d', c'$ (which were calculated in the same way as $d$ and $c$ above were calculated). Observe that

$$c' + d' = \sum_i r_i$$

where each $r_i$ is a product of some copies of elements from the set $\{p^l x_l, p^l x_{l+1} : l = 1, 2, \ldots\}$ and $p$ appears more than $i_t + i_{t+1}$ times near elements $x_t, x_{t+1}$ in each product (which is equal $r_i$).

Therefore, by multiplying the above equation by $p$ we get

$$(p^{i_t} x_t) \ast (p^{i_{t+1}} x_{t+1}) = p^{i_t+i_{t+1}-1} h + c' + d' + a,$$

for some $h \in A$ such that $[h] = [x_1] \odot [x_2]$ and for some $a \in A$. Moreover $a \in ann(p) = \{x \in A : px = 0\}$, since $a$ is an element from $ann(p^2)$ multiplied by $p$.

By Lemma 17 and Corollary 18 we have that $w = w' + \sum w_i + a'$ where $w'$ (and respectively $w_i$ and $a'$) is a product of elements $p^{i_1} x_1, \ldots, p^{i_{t-1}} x_{t-1}$ and element $p^{i_t+i_{t+1}} h$ (and respectively element $r_i$ and $a'$) and elements $p^{i_{t+2}} x_{t+2}, \ldots, p^{i_j} x_j \in A$. Notice that $a'$ belongs to $ann(p)$, since $ann(p)$ is an ideal in $A$ by [9].

Notice that $w'$ is a product of less than $j$ elements (which are $[x_i]$ for $i \neq t, i \neq t+1$ and the element $[x_t \odot x_{t+1}]$), and $p$ appears $k$ times in this product (near elements $[x_i]$ for $i \neq t, i \neq t+1$ and near the element $[x_t \odot x_{t+1}]$), so we can apply the inductive assumption on $j$ to $w'$ to get

$$[\varphi^{-1}(w')] = p^{k-1} w([x_1], \ldots, [x_j]) + p^k \sum_{v \in V_j} \beta'_v ([x_1], \ldots, [x_j]),$$

for some integers $\beta'_v$.  

6
Theorem 19. By applying this formula we get

\[ w = \prod_{i=1}^{k} \beta_i \sum_{v \in V} \beta_i^n v([x_1], \ldots, [x_j]) \]

for some integers \( \beta_i \). Notice also that \( \varphi^{-1}(a) \in ann(p^2) \) since \( a' \in ann(p) \), hence \( [\varphi^{-1}(a)] = [0] \). Observe that we implicitly used Remark 1. When combined together this concludes the proof.

The aim of this section is to prove the following result:

Theorem 5. Let \( p \) be a prime number and \( n < p - 1 \) be a natural number. Let \( (A, +) \) be an abelian group of cardinality \( p^n \). Let \( V \) denote the set of all non-associative words in non-commuting variables \( X, Y \) (where \( Y \) appears only once at the end of each word and \( X \) appears at least twice in each word in \( V \)). Then there are integers \( \alpha_w \), for \( w \in V \), such that only a finite number of them is non-zero and that the following holds: For each brace \( (A, +, \circ) \) with the additive group \( (A, +) \) and for each \( a, c \in A \) we have

\[ [a] \circ [c] = a \cdot c + p \sum_{w \in V} \alpha_w w([a], [c]), \]

where \( w([a], [c]) \) is a specialisation of the word \( w \) for \( X = [a], Y = [c] \), and the multiplication in \( w(a, c) \) is the same as the multiplication in the pre-Lie ring \( (A/ann(p^2), +, \bullet) \) constructed in Theorem 12 from the brace \( (A, +, \circ) \). So for example if \( w = ((XX)X)Y \) then \( w(a, c) = (([a] \cdot [a]) \cdot [a]) \cdot [c] \).

Proof. Observe that, by applying Corollary 18 and Lemma 17 several times (and using the fact that \( p^n A = 0 \)) we can write each element \( (\xi^i a) \ast c \) as a sum of the element \( \xi^i (pa) \ast c \) and \( t(pa, c, i) \), where \( t(pa, c, i) \) is a sum of products of elements \( pa \) and element \( c \) at the end, with \( ap \) appearing at least two times in each product. Consequently

\[ [\varphi^{-1}((\xi^i pa) \ast c)] = [\xi^i [\varphi^{-1}(pa) \ast c]] + [\varphi^{-1}(t(pa, c, i))]. \]

By Lemma 4 applied to the products which are summands of \( t(pa, c, i) \) we have:

\[ [\varphi^{-1}((\xi^i pa) \ast c)] = [\xi^i [a] \circ [c]] + [f(pa, c, i)] \]

where \( f(pa, c, i) \) is a sum of products of at least two copies of element \( a \) and element \( b \) appearing only once at the end, under operation \( \ast \). Recall the formula for \( [a] \bullet [c] \) from Theorem 19. By applying this formula we get

\[ [a] \bullet [c] = (p - 1)[a] \circ [c] + p \sum_{i=0}^{p-2} \xi^i f(a, c, i). \]

Notice that \( \sum_{i=0}^{p-2} \xi^i f(a, c, i) \) is a sum of some products of \( [a] \) and \( [c] \) under operation \( \circ \) and by Remark 1 the types of these products do not depend on the particular elements \( [a], [c] \) which were used (they only depend on the additive group of \( A \)), moreover a product may appear several times in this sum.
Therefore

\[ \omega^{-1}(\{\xi^3 | a \circ [c] + p \sum_{\zeta \in V} \zeta_{w,i} w([a], [c]) \} \]

for some \( \zeta_{c, w} \) which don’t depend on \( a \) and \( c \) (and \( \zeta_{c, w} \) are the same in all braces with the same additive group \((A, +)\)), where \( w([a], [c]) \) is a specialisation of word \( w \in V \) for \( X = [a], Y = [c], \) and the multiplication in \( w([a], [c]) \) is \( \circ \). For example in \( w = (XX)Y \) then \( w([a], [c]) = ([a] \circ [a]) \circ [c] \). Consequently

\[ [a] \cdot [c] = (p-1)[a] \circ [c] + p \sum_{\zeta \in V} m_{w} w([a], [c]), \]

where \( m_{w} = \sum_{i=0}^{p-2} \xi^{p-1-i} \zeta_{w,i}. \)

**Part 1.** Let \( x_{1}, \ldots, x_{j} \in A \). Let \( u \) be a non-associative word in variables \( X_{1}, \ldots, X_{j} \) (and each \( X_{i} \) appears only once, and they appear in the order \( X_{1}, \ldots, X_{j} \)). Let \( \langle [x_{1}], \ldots, [x_{j}] \rangle \) be the specialisation of \( u \) for \( X_{i} = [x_{i}] \) and under the operation \( \circ \), and \( u([x_{1}], \ldots, [x_{j}]) \) be the specialisation of \( u \) for \( X_{i} = [x_{i}] \) and under the operation \( \circ \).

We will now prove by induction on \( j \), that if \( [x_{1}], \ldots, [x_{j-1}] \in S_{1}, [x_{j}] \in S_{2} \) then there are integers \( m_{w, u} \), such that

\[ u([x_{1}], \ldots, [x_{j}]) = (p-1)^{j-1} u([x_{1}], \ldots, [x_{j}]) + p \sum_{\zeta \in W} m_{w, u} w([x_{1}], \ldots, [x_{j}]]. \]

Moreover, \( W \), the set of non-associative words of length at least 3, and in \( j \) variables \( X_{1}, \ldots, X_{j} \) for some \( j \), and \( w([x_{1}], \ldots, [x_{j}]) \), is a specialisation of \( w \in W \) for \( X_{i} = [x_{i}] \) under the operation \( \circ \).

For \( j = 2 \) the result follows from the first part of our proof, since we have shown that

\[ [a] \cdot [c] = (p-1)[a] \circ [c] + p \sum_{\zeta \in W} m_{w} w([a], [c]). \]

Therefore, for \( u = X_{1}X_{2} \) we take \( m_{v, u} = m_{v} \).

We proceed by induction on \( j \). Let \( j > 2 \). There is \( 1 < t < j \) such that \( u = vy \) for some word \( v \) in variables \( X_{1}, \ldots, X_{t} \), and some word \( y \) in variables \( X_{t+1}, \ldots, X_{j} \). By the inductive assumption:

\[ v([x_{1}], \ldots, [x_{t}]) = (p-1)^{t-1} v([x_{1}], \ldots, [x_{t}]) + p \sum_{\zeta \in W} m_{w, v} w([x_{1}], \ldots, [x_{t}]) \]

and

\[ y([x_{t+1}], \ldots, [x_{j}]) = (p-1)^{j-t-1} y([x_{t+1}], \ldots, [x_{j}]) + p \sum_{\zeta \in W} m_{w, y} w([x_{t+1}], \ldots, [x_{j}]). \]

It follows that,

\[ u([x_{1}], \ldots, [x_{j}]) = v([x_{1}], \ldots, [x_{t}]) \cdot y([x_{t+1}], \ldots, [x_{j}]) = (p-1)^{t-1} v([x_{1}], \ldots, [x_{t}]) + p \sum_{\zeta \in W} m_{w, v} w([x_{1}], \ldots, [x_{t}]) \cdot z \]

8
where
\[ z = (p - 1)^{j-t-1} y([x_{t+1}], \ldots, [x_j]) + p \sum_{w \in W} m_{w,y} w([x_{t+1}], \ldots, [x_j]). \]

Recall that operation \( \circ \) is distributive with respect to addition, since \( \circ \) is a pre-Lie operation. Therefore
\[
 u([x_1], \ldots, [x_j]) = (p - 1)^{j-2} v([x_1], \ldots, [x_i]) \circ y([x_{t+1}], \ldots, [x_j]) +
 + p \sum_{w, w' \in W} m_{w, w', v, y} w([x_1], \ldots, [x_i]) \circ w'([x_{t+1}], \ldots, [x_j]),
\]
for some integers \( m_{w, w', v, y} \). Moreover, in the summation the word \( w \) only depends on variables \( X_1, \ldots, X_j \), and the word \( w' \) depends only on variables \( X_{t+1}, \ldots, X_j \). Therefore,
\[
 w([x_1], \ldots, [x_i]) \circ w'([x_{t+1}], \ldots, [x_j]) = w''([x_1], \ldots, [x_j])
\]
where \( w'' = w w' \) (so \( w' \) is the word which is obtained by putting the word \( w' \) after \( w \), it could be also written as \( w'' = (w)(w') \)).

Observe also that
\[
 v([x_1], \ldots, [x_i]) \circ y([x_{t+1}], \ldots, [x_j]) = u([x_1], \ldots, [x_j]),
\]
since \( u = v y \).

The result now follows from the formula
\[
 [a] \circ [c] = (p - 1) [a] \circ [c] + p \sum_{w \in W} m_{w}([a], [c]),
\]
applied for \( [a] = v([x_1], \ldots, [x_j]) \) and \( [c] = y([x_1], \ldots, [x_j]) \). We obtain
\[
 v([x_1], \ldots, [x_i]) \circ y([x_{t+1}], \ldots, [x_j]) =
 (p-1)v([x_1], \ldots, [x_i]) \circ y([x_{t+1}], \ldots, [x_j]) +
 + p \sum_{w, w' \in W} m_{w, w', v, y} w([x_1], \ldots, [x_i]) \circ w'([x_{t+1}], \ldots, [x_j]),
\]
for some integers \( m_{w, w', v, y} \).

We can apply a similar argument to \( a = w([x_1], \ldots, [x_i]) \) and \( c = w'([x_{t+1}], \ldots, [x_j]) \).
This can then be substituted to the right hand side of the above equation (which has \( u([x_1], \ldots, [x_j]) \) on the left hand side) to obtain:
\[
 u([x_1], \ldots, [x_j]) = (p - 1)^{j-1} u([x_1], \ldots, [x_j]) +
 + p \sum_{w \in W} m_{w,u} w([x_1], \ldots, [x_j]).
\]

**Part 2.** We are now ready to proof our result that
\[
 [a] \circ [c] = (p - 1) [a] \circ [c] + p \sum_{w \in V} \alpha_{w} w([a], [c]).
\]

We start with where \( w([a], [c]) \) is the specialisation under the operation \( \circ \).

Let \( E_{[a], [c]} \subseteq A \) denote the set of products of some copies of element \( [a] \) ([a] appearing at least once) and element \( [c] \) at the end of each word ([c] appearing only once) under the operation \( \circ \). Moreover, we assume that both \( [a] \) and \( [c] \) appear in each product in the set
for some matrix $M$. Let $V_{\alpha,\beta}$ be a vector whose entries are elements from $E_{\alpha,\beta}$ arranged in such a way that longer products appear before shorter products. Let $U_{\alpha,\beta}$ be the corresponding matrix obtained from the corresponding products of $\alpha$ and $\beta$ under the operation $\circ$. So for example if $([\alpha] \circ [\beta]) \circ ([\gamma] \circ [\delta])$ is the $i$-th entry of $V_{\alpha,\beta}$ then $([\alpha] \cdot [\beta] \circ ([\alpha] \cdot [\beta])$ is the $i$-th entry of $U_{\alpha,\beta}$.

Let $RFM$ denote the set of row-finite matrices (where the rows and columns are enumerated by the set of natural numbers) with integer entries. It is known that $RFM$ is a ring, and the product of any copies of matrices $M$ and $D$ is well defined and belongs to $RFM$.

By Part 1 above we obtain

$$U_{\alpha,\beta} = DV_{\alpha,\beta} + pMV_{\alpha,\beta}$$

for some matrix $M$ in $RFM$ and some diagonal matrix $D$ in $RFM$ whose diagonal entries are $(p-1)^i$ for some $i$. Notice that $(p-1)(-1 + p + p^2 + \cdots + p^{p-1})) \equiv 1 \mod p^p$. Recall also that $p^{p^p-1}A = 0$. Therefore

$$V_{\alpha,\beta} = D'U_{\alpha,\beta} - pD'MV_{\alpha,\beta},$$

where $D'$ is a diagonal matrix whose entries are $(-1 + p + p^2 + \cdots + p^{p-1})^i$.

We can now substitute the above formula for $V_{\alpha,\beta}$ in the right hand side and obtain:

$$V_{\alpha,\beta} = D'U_{\alpha,\beta} - pD'MDM'U_{\alpha,\beta} + p^2D'MD'MV_{\alpha,\beta},$$

for some matrix $M'$. We can continue to substitute the expression for $V_{\alpha,\beta}$ on the right hand side. This process will stop after at most $p$ steps, since $p^{p^p-1}A = 0$. This will give

$$V_{\alpha,\beta} = D^{-1}U_{\alpha,\beta} + pM'U_{\alpha,\beta},$$

for some matrix $M'$ from $RFM$ with integer entries. This concludes the proof. □

4 Relations between $\ast$ and $\circ$

In this section we will investigate some properties of the binary operation $\circ$ defined in Lemma 3. Notice that if $p$ is a prime number and $1 \leq i < p$ is a natural number then

$$\binom{p}{i} = \frac{p}{i} \binom{p-1}{i-1},$$

hence $(\binom{p-1}{i-1})/i$ is an integer.

**Lemma 6.** Let $p$ be a prime number. Let $(A, +, \circ)$ be a brace of cardinality $p^n$ with $p > n + 1$. Let $a \in A$, define

$$f(a) = \sum_{i=1}^{p-1} \binom{p-1}{i-1} e_i,$$

where $e_1 = a$, $e_2 = a \ast a$ and $e_{i+1} = a \ast e_i$ for all $i$. Then $pf(a) = a^{op}$. Moreover, there are integers $\alpha_1, \ldots, \alpha_{p-1}$ which only depend on the additive group $(A, +)$ of the brace $A$ (and do not depend on element $a$), and such that

$$[a] = \sum_{i=1}^{p-1} \alpha_i [f_i(a)],$$

10
where \([f_1(a)] = [f(a)], \ [f_2(a)] = [f(a)] \odot [f(a)], \ [f_{i+1}(a)] = [f(a)] \odot [f_i(a)],\) where \(\odot\) is defined as in Lemma \(\text{[3]}\). Moreover, \(\alpha_1 = 1.\) As usual, by \(a\) we mean \([a]_{\text{ann}(p^2)}\).

Proof. We will use a formula from Lemma \(\text{[13]}\) namely

\[
a^{op} = \sum_{i=1}^{p-1} \left( \begin{array}{c} p \\ k \end{array} \right) e_i,
\]

where \(e_1 = a\) and \(e_{i+1} = a \ast e_i\). It works since \(A^p = 0\) as \(n + 1 < p\). Observe also that

\[
[f(a)] \odot [b] = [\varphi^{-1}(a^{op} \ast b)]
\]

by the definition of \(\odot\). By using this formula we see that \([f(a)] = [a] + \sum_{i \geq 1} \beta_i[e_i]\) for some integers \(\beta_i\). Similarly

\[
[f(a)] \odot [f(a)] = [\varphi^{-1}(a^{op} \ast f(a))] = [a \ast a] + \sum_{i \geq 2} \beta'_i[e_i],
\]

for some integers \(\beta'_i\). We proceed by induction on \(j\). Assume that we have proved that

\[
[f_j(a)] = [e_j] + \sum_{i > j} \beta''_i[e_i]
\]

for some integers \(\beta''_i\). It follows that

\[
f_j(a) = e_j + \sum_{i > j} \beta''_i e_i + a',
\]

for some \(a' \in \text{ann}(p^2)\). Recall that for \(x, y \in pA\) we have \([\varphi^{-1}(x+y)] = [\varphi^{-1}(x)] + [\varphi^{-1}(y)]\). It follows that

\[
[f_{j+1}(a)] = [f(a)] \odot [f_j(a)] = [\varphi^{-1}(a^{op} \ast (e_j + \sum_{i > j} \beta''_i e_i + a'))] =
\]

\[
[\varphi^{-1}(a^{op} \ast (e_j))] + \sum_{i > j} \beta''_i [\varphi^{-1}(a^{op} \ast e_i)] + [\varphi^{-1}(a^{op} \ast a')] =
\]

\[
[e_{j+1}] + \sum_{i > j+1} \beta''_i [e_i]
\]

for some integers \(\beta''_i\). Notice that \([\varphi^{-1}(a^{op} \ast a')] = [0]\) since \(p^2 \varphi^{-1}(a^{op} \ast a') = p(a^{op} \ast a') = 0\), since \(a' \in \text{ann}(p^2)\).

Let \(f\) be the vector whose entries are elements \([f_i(a)]\) and let \(E\) be the vector whose entries are elements \([e_i]\). Then

\[
f = ME
\]

for some upper triangular matrix (with integer entries), whose diagonal entries are 1. It follows that \(E = M'f\) for some upper diagonal matrix with integer entries with 1’s on the diagonal (because \(p^n A = 0\)). By looking at the first entry of \(E\) and the first entry of \(M'f\) we get the required conclusion. \(\square\)
Proposition 7. Let notation and assumptions be as in Lemma 6 and let \( b \in A \). Then there are integers \( \gamma_1, \ldots, \gamma_{p-1} \) which only depend on the additive group \((A, +)\) of the brace \( A \) and do not depend on element \( a \) such that

\[
[a \ast b] = \sum_{i=1}^{p-1} \gamma_i[q_i(a, b)]
\]

where \( [q_1(a)] = [f(a)] \circ [b] \), \( [q_2(a)] = [f(a)] \circ [q_1(a, b)] \), \( [q_{i+1}(a, b)] = [f(a)] \circ [q_i(a, b)] \), where \( \circ \) is defined as in Lemma 3. Moreover, \( \gamma_1 = 1 \). As usual by \([a]\) we mean \([a]_{ann(p^2)}\).

Proof. The proof is similar to the proof of Lemma 6. By a formula from Lemma 13,

\[
a^{op} \ast b = \sum_{i=1}^{p-1} \binom{p}{k} e'_i
\]

where \( e'_1 = a \ast b \) and \( e'_{i+1} = a \ast e'_i \) for \( i = 1, 2, \ldots, p-2 \). This formula works since \( n + 1 < p \).

Notice that

\[
[q_1(a, b)] = [f(a)] \circ [b] = [v^{-1}((pf(a)) \ast b)] = [v^{-1}(a^{op} \ast b)] = [a \ast b] + \sum_{i > 1} \beta_i[e'_i]
\]

for some integers \( \beta_i \). We will proceed by induction on \( j \). Assume that

\[
[q_j(a, b)] = [e'_j] + \sum_{i > j} \beta'_i[e'_i]
\]

for some integers \( \beta'_i \). Reasoning similarly as in the proof of Lemma 6 we can show that

\[
[q_{j+1}(a, b)] = [f(a)] \circ [q_j(a, b)] = [e'_{j+1}] + \sum_{i > j+1} \beta''_i[e'_i]
\]

for some integers \( \beta''_i \). Let \( f \) be the vector whose entries are elements \([q_1(a, b)]\) and let \( E \) be the vector whose entries are elements \([e'_i]\). Then

\[
f = ME
\]

for some upper triangular matrix (with integer entries) whose diagonal entries are 1. It follows that

\[
E = M'f
\]

for some upper diagonal matrix with integer entries with 1’s on the diagonal (because \( p^n A = 0 \)).

In this section we investigate properties of this function.

5 Some properties of function \( f \)

Let \( p \) be a prime number. Let \((A, +, \circ)\) be a brace of cardinality \( p^n \) with \( p > n + 1 \). Let \( a \in A \). Recall that

\[
f(a) = \sum_{i=1}^{p-1} \left( \frac{p-1}{i-1} \right) e_i,
\]

where \( e_1 = a \), \( e_2 = a \ast a \) and \( e_{i+1} = a \ast e_i \) for all \( i \). Then \( pf(a) = a^{op} \).

In this section we investigate properties of this function.
Theorem 8. Let \( p \) be a prime number. Let \((A, +, \circ)\) be a brace of cardinality \( p^n \) with \( p > n + 1 \). For \( a \in A \) let \( f(a) = \sum_{i=1}^{p-1} ((p-1)/i)e_i \). Then the map

\[
[a] \rightarrow [f(a)]
\]

is an injective function on \( A/\text{ann}(p^2) \). Consequently, since the set \( A/\text{ann}(p^2) \) is finite, it follows that this function is a bijection. As usual we denote \([a] = [a]_{\text{ann}(p^2)}\).

Proof. Let \( a, b \in A \). Suppose that \([f(a)] = [f(b)]\) then \( f(a) - f(b) \in \text{ann}(p^2)\), hence \( pf(a) - pf(b) = 0\), so \( pf(a) - pf(b) \in \text{ann}(p)\). Recall that \( pf(a) = a^{op} \), hence

\[
a^{op} = b^{op} + e',
\]

for some \( e' \in \text{ann}(p)\).

We will now show that all products

\[
[x_1 * (x_2(*\cdots*(x_{k-1} * x_k)\cdots))]
\]

for \( x_1, \ldots, x_k \in \{a, b\} \) are equal.

For \( k = n + 1 \) the result is true because all such products of length \( n + 1 \) will be zero since \( A^{n+1} = 0 \). We proceed by induction on \( k \) in the decreasing order. Let \( i \) be a natural number, \( i < n + 1 \). We will show the result is true for \( k = i \) provided that it is true for all \( k > i \).

We will first show that

\[
[a * (x_1 *(x_2(*\cdots*(x_{k-2} * x_{k-1})\cdots))] = [b * (x_1 *(x_2(*\cdots*(x_{k-2} * x_{k-1})\cdots)))]
\]

for all \( x_1, \ldots, x_k \in \{a, b\} \).

Observe that \( a^{op} - b^{op} \in \text{ann}(p) \) yields

\[
a^{op} * (x_1 * (x_2(*\cdots*(x_{k-2} * x_{k-1})\cdots)) = \]

\[
b^{op} * (x_1 * (x_2(*\cdots*(x_{k-2} * x_{k-1})\cdots)) + e,
\]

for some \( e \in \text{ann}(p) \), since \( \text{ann}(p) \) is an ideal in the brace \( A \) by \[9\]. It follows from Lemma \[17\] applied to \( a' = a^{op} \) and \( b' = b^{op} - a^{op} \) and \( c' = x_1 * (x_2(*\cdots*(x_{k-2} * x_{k-1})\cdots)\).

By Lemma \[13\] we have:

\[
a^{op} * (x_1 * (x_2(*\cdots*(x_{k-2} * x_{k-1})\cdots)) = \]

\[
= pa*(x_1 *(x_2(*\cdots*(x_{k-2}* x_{k-1})\cdots)) + \frac{p(p-1)}{2} a*(a*(x_1 *(x_2(*\cdots*(x_{k-2}* x_{k-1})\cdots)))) + \cdots.
\]

Similarly,

\[
b^{op} * (x_1 * (x_2(*\cdots*(x_{k-2} * x_{k-1})\cdots)) = \]

\[
= pb*(x_1 *(x_2(*\cdots*(x_{k-2}* x_{k-1})\cdots)) + \frac{p(p-1)}{2} b*(b*(x_1 *(x_2(*\cdots*(x_{k-2}* x_{k-1})\cdots)))) + \cdots.
\]

The above three equations combined together imply after applying \( \varphi^{-1} \) to both sides

\[
[a * (x_1 *(x_2(*\cdots*(x_{k-2}* x_{k-1})\cdots))] + \frac{p-1}{2} a*(a*(x_1 *(x_2(*\cdots*(x_{k-2}* x_{k-1})\cdots)))) + \cdots =
\]
Notice that \([y^{-1}(e)] = [0]\) since \(p^2y^{-1}(e) = pe = 0\). Notice that by the inductive assumption
\[a * (a * (x_1 * (\cdots * (x_{k-2} * x_{k-1}) \cdots))) = [b * (b * (x_1 * (\cdots * (x_{k-2} * x_{k-1}) \cdots)))].\]
This also holds for the next products in the above sum (involving more \(a\) and \(b\)) by the inductive assumption.

The two above arguments show that
\[a * (x_1 * (x_2 * (\cdots * (x_{k-2} * x_{k-1}) \cdots))) = [b * (x_1 * (x_2 * (\cdots * (x_{k-2} * x_{k-1}) \cdots)))].\]
for this fixed \(k\) and for all \(x_1, \ldots, x_{k-1} \in \{a, b\}\). Notice now that we can use a similar argument by putting in the \(i\)th place \(a^{op}\) on the left-hand side and \(b^{op}\) on the right-hand side, without changing the elements \(x_1, x_2, \ldots, x_{k-1}:
\[x_1 * (\cdots * (x_j * (a^{op} * (x_{j+1} * (\cdots * (x_{k-2} * x_{k-1}) \cdots)))) \cdots) =
\]
\[x_1 * (\cdots * (x_j * (b^{op} * (x_{j+1} * (\cdots * (x_{k-2} * x_{k-1}) \cdots)))) \cdots) + e''\]
for all \(x_1, \ldots, x_{k-1} \in \{a, b\}\), for some \(e'' \in A\). Reasoning similarly as when we did to show that \(e \in \text{ann}(p)\), we obtain that \(e'' \in \text{ann}(p)\). By Lemma 13 we have
\[a^{op} * (x_{j+1} * (\cdots * (x_{k-2} * x_{k-1}) \cdots)) = \sum_{i=1}^{p-1} \binom{p}{i} y_i\]
where \(y_1 = a * (x_{j+1} * (\cdots * (x_{k-2} * x_{k-1}) \cdots)))\), and \(y_{i+1} = a \cdot y_i\) for \(i = 1, 2, \ldots, p - 2\).

Similarly
\[b^{op} * (x_{j+1} * (\cdots * (x_{k-2} * x_{k-1}) \cdots)) = \sum_{i=1}^{p-1} \binom{p}{i} y'_i\]
where \(y'_1 = b * (x_{j+1} * (\cdots * (x_{k-2} * x_{k-1}) \cdots)))\), and \(y_{i+1} = b \cdot y_i\) for \(i = 1, 2, \ldots, p - 2\).

By applying \(y^{-1}\) to both sides of equation
\[x_1 * (\cdots * (x_j * (a^{op} * (x_{j+1} * (\cdots * (x_{k-2} * x_{k-1}) \cdots)))) \cdots) =
\]
\[x_1 * (\cdots * (x_j * (b^{op} * (x_{j+1} * (\cdots * (x_{k-2} * x_{k-1}) \cdots)))) \cdots) + e''\]
we obtain after taking cosets
\[[x_1 * (\cdots * (x_j * \sum_{i=1}^{p-1} \alpha_i y_i) \cdots)] = [x_1 * (\cdots * (x_{j-1} * \sum_{i=1}^{p-1} \alpha_i y'_i) \cdots)],\]
where \(\binom{p}{i} = p\alpha_i\) for each \(i\), so \(\alpha_1 = 1\). By the inductive assumption,
\[[x_1 * (\cdots * (x_j * y_i) \cdots)] = [x_1 * (\cdots * (x_j * y'_i) \cdots)]\]
for \(i > 1\). Therefore
\[[x_1 * (\cdots * (x_j * y_1) \cdots)] = [x_1 * (\cdots * (x_{j-1} * y'_1) \cdots)].\]
By the definition of $y_1$, we obtain
\[
[x_1 \ast (\cdots \ast (x_j \ast \cdots (a \ast (x_{j+1} \ast \cdots (x_{k-2} \ast x_{k-1}) \cdots)))))]
\]
for all $x_1, \ldots x_{k-1} \in \{a, b\}$.

We have thus proved that
\[
[x_1 \ast (x_2(\cdots \ast (x_{k-1} \ast x_k) \cdots))] = [x_1' \ast (x_2'(\cdots \ast (x_{k-1}' \ast x_k') \cdots))],
\]
provided that $x_j = x_j'$ in all places except in one place, and all $x_i, x_i' \in \{a, b\}$.

Observe now that when we change one index at a time this implies:
\[
[x_1 \ast (x_2(\cdots \ast (x_{k-1} \ast x_k) \cdots))] = [x_1 \ast (x_2(\cdots \ast (x_{k-1} \ast x_k') \cdots))],
\]
and then
\[
[x_1 \ast (x_2(\cdots \ast (x_{k-1} \ast x_k') \cdots))] = [x_1 \ast (x_2(\cdots \ast (x_{k-2} \ast (x_{k-1}' \ast x_k') \cdots)))]
\]
and continuing to change the $i$-th digit at $i$-th time we eventually get
\[
[x_1' \ast (x_2'(\cdots \ast (x_{k-1}' \ast x_k') \cdots))] = [x_1' \ast (x_2'(\cdots \ast (x_{k-1}' \ast x_k') \cdots))].
\]

These equations imply that
\[
[x_1 \ast (x_2(\cdots \ast (x_{k-1} \ast x_k) \cdots))] = [x_1' \ast (x_2'(\cdots \ast (x_{k-1}' \ast x_k') \cdots))].
\]

This proves the inductive argument.

Notice that for $k = 1$ we have $[a] = [b]$, as required.

**Theorem 9.** Let $p$ be a prime number. Let $(A, +, \circ)$ be a brace of cardinality $p^n$ with $p > n + 1$. For $a \in A$ define
\[
g(a) = f^{(p^n-1)}(a)
\]
where $f^{(1)}(a) = f(a)$ and for every $i$ we denote $f^{(i+1)}(a) = f(f^{(i)}(a))$. Then
\[
[f(g(a))] = [g(f(a))] = [a].
\]

Moreover
\[
[f(x)] = [g^{(p^n-1)}(a)]
\]
where $g^{(1)}(a) = a$ and for every $i$ we denote $g^{(i+1)}(a) = g(g^{(i)}(a))$.

**Proof.** Observe first that since $[a] \rightarrow [f(a)]$ is a bijection on $A/ann(p^2)$, then for every $i$, $[f^{(i)}(a)] \rightarrow [f^{(i+1)}(a)]$ is a bijective function on $A/ann(p^2)$, and hence for every $k > 0$
\[
[a] \rightarrow [f^{(k)}(a)]
\]
is a bijective function on $A/ann(p^2)$.

Notice that there are $p^n + 1$ elements $[f^{(1)}(a)], [f^{(2)}(a)], \ldots , [f^{(p^n+1)}(a)]$, and since brace $A$ has cardinality $p^n$ it follows that
\[
[f^{(i)}(a)] = [f^{(j)}(a)],
\]

15
for some $1 \leq i < j \leq p^n + 1$, hence $j - i \leq p^n \leq p^n$. Notice that the function

$$[f^{(i)}(a)] \to [a]$$

is a bijective function on $A/\text{ann}(p^2)$. Applying this function to both sides of equation

$$[f^{(i)}(a)] = [f^{(j)}(a)],$$

we obtain

$$[a] = [f^{(j-i)}(a)].$$

Notice that $j - i \leq p^n$ implies that $j - i$ divides $p^n$, so it divides $p^n!$. Therefore

$$[f^{(p^n)}(a)] = [a].$$

This shows that

$$[f(g(a))] = [g(f(a))] = [a].$$

On the other hand, by the first part of this proof it follows that $[a] \to [g(a)]$ is a bijective function, since

$$[g(a)] = [f^{(p^n-1)}(a)].$$

Observe now that

$$[g^{(p^n-1)}(a)] = [f^{((p^n-1)^2)}(a)] = [f(a)],$$

since $[f^{(p^n)}(a)] = [a]$. \qed

## 6 Recovering braces from pre-Lie algebras

We are now able to prove the following theorem:

**Theorem 10.** Let $p$ be a prime number and $n < p - 1$ be a natural number. Let $(A, +)$ be an abelian group of cardinality $p^n$. Let $V$ denote the set of all non-associative words in non-commuting variables $X, Y$ (where $Y$ appears only once at the end of each word and $X$ appears at least once in each word in $V$). Then there are integers $e_w$, for $w \in V$, such that only a finite number of them is non-zero and that the following holds: For each brace $(A, +, \circ)$ with the additive group $(A, +)$ and for each $a, c \in A$ we have

$$[a] \star [c] = \sum_{w \in V} e_w w([a], [c]),$$

where $w([a], [c])$ is a specialisation of the word $w$ for $X = [a]$, $Y = [c]$, and the multiplication in $w(a, c)$ is the same as the multiplication in the pre-Lie ring $(A/\text{ann}(p^2), +, \bullet)$ constructed in Theorem 19 from the brace $(A, +, \circ)$. So for example if $w = ((XX)X)Y$ then $w(a, c) = (((a) \bullet [a]) \bullet [a]) \bullet [c])$.

**Proof.** By Lemma 6 we have that

$$[a] = \sum_{i=1}^{p-1} \alpha_i [f_i(a)]$$

16
where \([f_{i+1}(a)] = [f(a)] \odot [f_i(a)]\). By applying it for \(a = g(a)\), where \(g(a)\) is as in Theorem \(9\) so \(g(a) = f^{(p^p - 1)}(a)\) and \([f(g(a))] = [a]\), we obtain:

\[ [g(a)] = \sum_{i=1}^{p-1} \alpha_i [h_i(a)] \]

where \([h_1(a)] = [a]\) and \([h_{i+1}(a)] = [a] \odot [h_i(a)]\) and \(\alpha_i\) are some integers. Observe that integers \(\alpha_i\) only depend on the additive group \((A, +)\) of the brace \(A\) and do not depend on the multiplicative group \((A, \circ)\) and do not depend on element \(a\). Therefore \([g(a)]\) can be obtained by applying the operations \(+\) and \(\odot\) several times to some copies of element \([a]\), and the method is the same for all braces with the same additive group \((A, +)\).

**Fact 1.** By Theorem \(9\) we obtain \([f(a)] = [g^{p^p - 1}(a)]\), therefore \([f(a)]\) can be obtained by applying the operations \(\odot\) and \(+\) several times to some copies of element \([a]\), and the method and order of applying these operations does not depend on element \(a\), and the same method works for all braces with the additive group \((A, +)\).

**Fact 2.** By Lemma \(6\) we have that \([a \ast b] = [a] \ast [b]\) can be written by using operations \(\odot\) and \(+\) applied several times to some copies of element \([f(a)]\) and to the element \([b]\) and to sums of the obtained elements (and the method does not depend on elements \(f(a)\) and \(b\)) and the same method works for all braces with the additive group \((A, +)\).

By combining the above Fact 1 and Fact 2 we obtain that \([a] \ast [b]\) can be obtained by applying operation \(\odot\) to elements \(a\) and \(b\), and the algorithm for which order to apply these operations \(\odot, +\) does not depend on elements \(a, b\). Moreover the same method works for all braces with the additive group \((A, +)\).

By using Theorem \(19\) we can write product \(\odot\) by using the pre-Lie operation \(\bullet\) and \(+\). Notice that the operation \(+\) is this pre-Lie ring is the same as the addition in the factor brace \((A/\text{ann}(p^2), +, \circ)\), so it only depends on the multiplicative group of brace \(A\). Since \(\bullet\) is a pre-Lie algebra multiplication it is distributive with respect to the addition, the obtained result can be simplified and written as:

\[ \sum_{w(a,b) \in W} \beta_w w(a, b), \]

where \(W\) is the set of products of some number of element \([a]\) and element \([b]\) at the end under the pre-Lie operation \(\bullet\), where \(\beta_w\) are some integers which don’t depend on elements \(a, b\) and do not depend on the multiplicative group of the brace \(A\) (and only depend on the additive group \((A, +)\)). This concludes the proof. \(\square\)

### 7 Braces \(A/\text{ann}(p^4)\) and groups of flows

In this section we will prove Theorem \(11\). Notice that, as shown in \(10\), the construction of the group of flows is well defined for every left nilpotent pre-Lie ring \((A, +, \cdot)\). Moreover, the group of flows is a brace with the same addition as in the original pre-Lie ring, and we will call this brace just the group of flows of the pre-Lie ring \((A, +, \cdot)\). The construction of the group of flows was first introduced in \(11\). The connection between braces and groups of flows was discovered by Wolfgang Rump in 2014 \(12\).

We begin with a Lemma similar to the result obtained in the last section of \(8\).
Lemma 11. Let \((A, +, \cdot)\) be a left nilpotent pre-Lie ring of cardinality \(p^n\) for some prime number \(p\) and some natural number \(n < p - 1\). Let \((A/\text{ann}(p^2), +, \cdot)\) be the factor pre-Lie ring by the ideal \(\text{ann}(p^2) = \{a \in A : p^2a = 0\}\). Elements of this pre-Lie ring are cosets \([a] = \{a + i : i \in \text{ann}(p^2)\}\). We denote the multiplication and addition in this pre-Lie ring with the same symbols \(a\) in the original ring:

\[[a] \cdot [b] = [a \cdot b], [a] + [b] = [a + b].\]

Let \((A, +, \circ)\) be the brace obtained from the pre-Lie ring \((A, +, \cdot)\) using the construction of the group of flows. Let \((A/\text{ann}(p^2), +, \bullet)\) be the corresponding pre-Lie ring, constructed as in [8] from the brace \((A, +, \circ)\) (notice that this construction is quoted in Theorem [19]). Then \((A/\text{ann}(p^2), +, \bullet)\) and \((A/\text{ann}(p^2), +, \cdot)\) are the same pre-Lie rings, so

\[[x] \bullet [y] = (p - 1)(x \cdot y),\]

for \([x], [y] \in A/\text{ann}(p^2)\).

Proof. Notice that the addition in both pre-Lie rings is the same as the addition in the additive group \(A/\text{ann}(p^2)\) of the factor brace \(A/\text{ann}(p^2)\). We need to show that

\[[x] \bullet [y] = (p - 1)(x \cdot y),\]

for \([x], [y] \in A/\text{ann}(p^2)\). We will use the same notations for the construction of the group of flows as in [9]. Recall that the formula for the operation \(*\) in the group of flows of pre-Lie algebra \((A, +, \cdot)\) is

\[a * b = \Omega(a) \cdot b + \frac{1}{2!} \Omega(a) \cdot (\Omega(a) \cdot b) + \frac{1}{3!} \Omega(a) \cdot (\Omega(a) \cdot (\Omega(a) \cdot b)) + \ldots\]

where \(a \circ b = a * b + a + b\) in brace \((A, +, \circ)\). By Lemma 20 (11 from [9]) we have that \(\Omega(a) = a + \sum_w \alpha_w w(a)\) for some integers \(\alpha_w\), where \(w\) are finite non associative words in variable \(x\) (of degree at least 2), and \(w(a)\) is a specialisation of \(w\) at \(a\) (so for example if \(w = x \cdot (x \cdot x)\) then \(w(a) = a \cdot (a \cdot a)\)). Moreover, there is \(m\) such that \(\alpha_j = 0\) provided that \(j > m\).

Let \(a, b \in A\), we will denote \(a' = pa\). Observe now that

\[[\xi^i a] \circ [b] = [\varphi^{-1}((\xi^i a') \circ b)] = [\varphi^{-1}(\Omega(\xi^i a') \cdot b + \frac{1}{2!} \Omega(\xi^i a') \cdot (\Omega(\xi^i a') \cdot b) + \ldots)].\]

Observe also that

\[[\Omega(\xi^i a')] = \xi^i a' + \sum_w \alpha_w w(\xi^i a') = \xi^i a + \sum_{k=2}^m (\xi^i)^k f_k(a'),\]

where

\[f_k(a') = \sum_{w \in W_k} \alpha_w w(a')\]

where \(W_k\) consists of words of length \(k\).

Therefore,

\[[\xi^i a] \circ [b] = [\varphi^{-1}(\xi^i a' + \sum_{k=2}^{mp} (\xi^i)^k t_k(a', b))].\]
where \( t_k(a', b) \) is a linear combination (with integer coefficients) of some products of \( j \) copies of \( a' \) and element \( b \) at the end under the operation \( \cdot \). Notice, that for \( j > p - 1 \) each such product will be zero because it will belong to \( p^{p-1}A = 0 \), because \( a' = pa \) and the operation \( \cdot \) is distributive. Therefore,

\[
[\xi^i a] \odot [b] = [\varphi^{-1}(\xi^i a' \cdot b + \sum_{k=2}^{p-2} (\xi^k)^k t_k(a', b))],
\]

Notice that

\[
\xi^{p-1-i}[\xi^i a] \odot [b] = [\varphi^{-1}(a' \cdot b + \sum_{k=2}^{p-2} (\xi^{k-1})^i t_k(a', b))].
\]

Recall also the formula \([a] \bullet [b] = \sum_{i=0}^{p-2} \xi^{p-1-i}[\xi^i a] \odot [b] \), where \( \xi^{p-1} \equiv 1 \mod p^n \). Combining the above equations together we get

\[
[a] \bullet [b] = [\varphi^{-1}(\sum_{i=0}^{p-2} (a' \cdot b + \sum_{k=2}^{p-2} (\xi^{k-1})^i t_k(a', b)))].
\]

Notice that \((1 - \xi^i) \sum_{j=1}^{p-2} (\xi^i)^j = (\xi^i)^{p-1} - 1 = 0\), provided that \( 0 < i < p - 1 \). Consequently

\[
[a] \bullet [b] = [\varphi^{-1}(\sum_{i=0}^{p-1} a' \cdot b)] = [\varphi^{-1}((p - 1)a' \cdot b)] = (p - 1)[a \cdot b],
\]

since \( \cdot \) is a pre-Lie algebra operation, so

\[
a' \cdot b = (pa) \cdot b = p(a \cdot b).
\]

This concludes the proof.

\[\square\]

**Remark 2.** Let \((A, +, \circ_1)\) and \((A, +, \circ_2)\) be two braces with the same additive group \((A, +)\). Suppose that the cardinality of \( A \) is \( p^n \) for some natural number \( n \), and some prime number \( p > n + 1 \). Let \((A/\text{ann}(p^2), +, \bullet_1)\) and \((A/\text{ann}(p^2), +, \bullet_2)\) be the corresponding pre-Lie rings constructed as in \([8]\) (see Theorem \([19]\) for details). Note that the set \( \text{ann}(p^2) = \{a \in A : p^2a = 0\} \) is the same in both braces. Therefore the set \( A/\text{ann}(p^2) \) can be defined only by using the additive group \((A, +)\) without using operations \( \circ_1, \circ_2 \).

Let \((A/\text{ann}(p^2), +, \circ_1)\) be the factor brace obtained from the brace \((A, +, \circ_1)\) and let \((A/\text{ann}(p^2), +, \circ_2)\) be the factor brace obtained from brace \((A, +, \circ_2)\). As usual we use the same notation for operations \(+, \circ\) in the brace and in the factor brace.

Observe that by Theorem \([10]\) if \(x \bullet y = x \circ_2 y\) for all \(x, y \in A/\text{ann}(p^2)\) then \(x \circ_1 y = x \circ_2 y\), for \(x, y \in A/\text{ann}(p^2)\), and hence the braces \((A, +, \circ_1)\) and \((A/\text{ann}(p^2), +, \circ_2)\) are the same.

**Proof of Theorem \([1]\).** As usual we will denote the operations of the addition and of the multiplication in the factor brace by the same symbols as in the original brace. Let

\[
(A, +, \circ)
\]

19
Recall that \(ann(p^2) = \{a \in A : p^2a = 0\}\). Let

\[
(A/ann(p^2), +, \bullet)
\]

be the pre-Lie ring, constructed as in [8] from the brace \((A, +, \circ)\) (notice that this construction is quoted in Theorem [19]). We will denote the subset of elements of order \(p^2\), in the additive group \((A/ann(p^2), +)\), by \(I\). Observe that

\[
I = \{[a] \in A/ann(p^2) : [p^2a] = [0]\}.
\]

Observe that we can define the factor pre-Lie ring \(((A/ann(p^2))/I, +, \bullet_1)\) of the pre-Lie ring \((A/ann(p^2), +, \bullet)\) by the ideal \(I\). In this pre-Lie ring \(((A/ann(p^2))/I, +, \bullet_1)\) we have

\[
[x]_I \bullet_1 [y]_I = [x \bullet y]_I, \quad [x]_I + [y]_I = [x + y]_I \quad \text{for} \quad x, y \in A/ann(p^2) \quad \text{(where \([x]_I, [y]_I\) are elements of this pre-Lie ring \((A/ann(p^2))/I\))}
\]

We will call the pre-Lie ring

\[
((A/ann(p^2))/I, +, \bullet_1)
\]

the pre-Lie ring 1.

On the other hand, let

\[
(A/ann(p^2), +, \circ)
\]

be the factor brace of the brace \((A, +, \circ)\), by the ideal \(ann(p^2)\). Recall that \(I\) denotes the set of elements of the additive order at most \(p^2\) in the group \((A/ann(p^2), +)\). Let

\[
((A/ann(p^2))/I, +, \bullet_2)
\]

be the pre-Lie ring constructed as in [8] (so constructed as in Theorem [19]) from the brace \((A/ann(p^2), +, \circ)\). We will call this pre-Lie ring the pre-Lie ring 2. We also consider the factor brace of the brace

\[
(A/ann(p^2), +, \circ)
\]

by the ideal \(I\). We will call this brace 2, and denote it as \(((A/ann(p^2))/I, +, \circ)\).

We will now show that pre-Lie ring 1 is the same as pre-Lie ring 2. Observe that the additive groups of these pre-Lie rings are the same since the construction of the group of flows does not change the additive group. Observe that for \(x, y \in A\) by \([x], [y]\) we denote elements of the additive group \((A/ann(p^2), +)\) and by \([x]_I, [y]_I\) we denote elements of the additive group \(((A/ann(p^2))/I, +)\). We need to show that

\[
[[x]]_I \bullet_1 [y]_I = [x]_I \bullet_2 [y]_I,
\]

for \(x, y \in A/ann(p^2)\).

Observe that

\[
[x]_I \bullet_2 [y]_I = [[x] \bullet [y]]_I = [[\varphi^{-1}((px) \cdot y)]_I,
\]

where for \(x, y \in A\) we define \(x \cdot y = \sum_{i=0}^{p^2-2} \xi^{p^2-i}((\xi^i x) * y)\).

Observe that

\[
[x]_I \bullet_2 [y]_I = [\varphi^{-1}((px) \cdot [y])_I,
\]

where for \(x, y \in A\) we define \([x] \cdot [y] = \sum_{i=0}^{p^2-2} \xi^{p^2-i}((\xi^i x) * [y])\).

By the definition of \(I\), we know that if \(z, w \in A/ann(p^2)\) then \([z]_I = [w]_I\) if and only if \(z - w \in I\), which means \(p^2z = p^2w\).
Therefore, to show that \([x]_I \bullet_1 [y]_I = [[x]]_I \bullet_2 [[y]]_I\) it suffices to show that
\[
p^2(\phi^{-1}(px) \cdot y) = p^2\phi^{-1}(px \cdot [y]).
\]
This is equivalent to
\[
p((px) \cdot y) = p((px) : [y]),
\]
and this is true by the definition of the factor brace \((A/\text{ann}(p^2), +, \circ)\). Consequently, operations \(\bullet_1\) and \(\bullet_2\) are the same. It follows that the pre-Lie ring \(1\) is the same as the pre-Lie ring \(2\).

We will now introduce pre-Lie ring \(3\). Consider the pre-Lie ring \((A/\text{ann}(p^2), +, \bullet_3)\) such that the addition in this pre-Lie ring is the same as the addition in the pre-Lie ring \(1\), and the multiplication is defined as
\[
[x] \bullet_3 [y] = -(1 + p + p^2 + \ldots + p^{r-1})([x] \cdot_1 [y]),
\]
for \(x, y \in A\). Notice that this gives a well defined pre-Lie ring (see \([12]\) for a proof of this remark). We will call the pre-Lie ring \((A/\text{ann}(p^2), +, \bullet_3)\) pre-Lie ring \(3\).

We will now introduce brace \(1\). Let \((A/\text{ann}(p^2), +, \circ_3)\) be the brace which is constructed as the group of flows from pre-Lie ring \(3\). Let \(((A/\text{ann}(p^2))/I, +, \circ_4)\) be the pre-Lie ring constructed from the brace \((A/\text{ann}(p^2), +, \circ_3)\) by the construction from Theorem \([19]\) (so by the construction from \([8]\) we will call this pre-Lie ring \(((A/\text{ann}(p^2))/I, +, \bullet_4)\) the pre-Lie ring \(4\). By Lemma \([11]\) we obtain that the addition in the pre-Lie ring \(1\) is the same as the addition in the pre-Lie ring \(4\). Observe also that by Lemma \([11]\) we have for \(a, b \in A/\text{ann}(p^2)\)
\[
[a]_I \bullet_4 [b]_I = (p - 1)([a]_I \bullet_3 [b]_I) = -(1 + p + p^2 + \cdots)(p - 1)([a]_I \cdot_1 [b]_I) = [a]_I \cdot_1 [b]_I,
\]
since \(p^a a = a\) for every \(a \in A/\text{ann}(p^2)\). Therefore the pre-Lie ring \(4\) is the same as the pre-Lie ring \(1\).

Let brace \(1\) be the factor brace of the brace \((A/\text{ann}(p^2), +, \circ_3)\) by the ideal \(I\). Observe that brace \(1\) is the group of flows of pre-Lie ring \(5\) which is the factor ring of pre-Lie ring \(3\) by the ideal \(I\) (because the brace \((A/\text{ann}(p^2), +, \circ_3)\) is the group of flows of pre-Lie ring \(3\)).

Recall that pre-Lie ring \(1\) is the same as pre-Lie ring \(2\). Moreover, pre-Lie ring \(4\) is the same as pre-Lie ring \(1\). Therefore pre-Lie ring \(4\) is the same as pre-Lie ring \(2\).

By using Theorem \([10]\) we obtain that brace \(1\) and brace \(2\) are the same, since it is possible to recover brace \(1\) from pre-Lie ring \(4\), and brace \(2\) from pre-Lie ring \(2\) by the formula from Theorem \([10]\).

Therefore the brace \(2\) is the group of flows, since brace \(1\) is the group of flows of a left nilpotent pre-Lie algebra. It remains to show that brace \(2\) is the same as the factor brace of the brace \((A, +, \circ)\) by the ideal \(\text{ann}(p^4)\). Notice that we can map \([[a]]_I \rightarrow [a]_{\text{ann}(p^4)}\) for \(a \in A\). Notice that this map is well defined because if \([[a]]_I = [[b]]_I\) that means that \([a] - [b]\) is in the \(I\), so \([p^2 a] = [p^2 b]\). This in turn means that \(p^2(p^2 a) = p^2(p^2 b)\), which means \([a]_{\text{ann}(p^4)} = [b]_{\text{ann}(p^4)}\). Notice that this map is a homomorphism of braces since \([[a]]_I [[b]]_I = [[a*b]]_I \rightarrow [a*b]_{\text{ann}(p^4)} = [a]_{\text{ann}(p^4)} * [b]_{\text{ann}(p^4)}\). This shows that brace \(2\) is the same as the factor brace \((A/\text{ann}(p^4), +, \circ)\).
For the convenience of the reader we recall some results from other papers used in previous sections. All of these results are also listed in [8].

By a result of Rump [5], 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 $A^{i+1} = A * A^i$ and $A^{(i+1)} = A^{(i)} * A$ for a left brace $A$, where $A = A^1 = A^{(1)}$. A left brace $A$ is left nilpotent if there is a number $n$ such that $A^n = 0$, where inductively $A^i$ consists of sums of elements $a * b$ with $a, b \in A$. A left brace $A$ is right nilpotent if there is a number $n$ such that $A^{(n)} = 0$, where $A^{(i)}$ consists of sums of elements $a * b$ with $a, b \in A$. We recall Lemma 15 from [11]:

**Lemma 12.** [11] Let $s$ be a natural number and let $(A, +, \circ)$ be a left brace such that $A^s = 0$ for some $s$. 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 $1 \leq i$ define $d_{i+1} = d_i + d_i'$ and $d_{i+1}' = d_i * d_i'$. Then for every $c \in A$ we have

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

Let $A$ be a brace, let $a \in A$ and let $n$ be a natural number. 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 [10] (Lemma 15 in the arXiv version)

**Lemma 13.** [10] 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 $e_1 = a * b$, $e_2 = a * e_1$, and for each $i$, $e_{i+1} = a * e_i$. Moreover,

$$a^{\circ n} = \sum_{i=1}^{n} \binom{n}{i} a_i,$$

where $a_1 = a$, $a_2 = a * a_1$, and for each $i$, $a_{i+1} = a * a_i$.

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

We recall Proposition 15 from [9]:

**Lemma 14.** [9] Let $i, n$ be natural numbers. Let $A$ be a brace of cardinality $p^n$ for some prime number $p > n+1$. Then, $p^iA = \{p^ia : a \in A\}$ is an ideal in $A$ for each $i$. Moreover

$$A^{\circ p^i} = p^iA.$$
Lemma 15. [11] Let $p > 2$ be a prime number. Let $\xi = \gamma^{p^{n-1}}$ where $\gamma$ is a primitive root modulo $p^j$, then $\xi^{p^{n-1}} \equiv 1 \mod p^n$. Moreover, $\xi^1$ is not congruent to 1 modulo $p$ for natural $0 < j < p - 1$.

Let $A$ be a brace of cardinality $p^n$ where $p$ is a prime number larger than $n + 1$. Denote $pA = \{pa : a \in A\}$ where $pa$ is the sum of $p$ copies of $a$. We now recall several results from [8]:

Proposition 16. [8] 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 $p^iA$. Hence the product of any $p - 1$ elements from the brace $pA$ and any number of elements from the brace $A$ is zero.

Lemma 17. [8] Fix a prime number $p$. Let $W$ be as above. Then there are integers $\beta_w$ such that only a finite number of them is non zero and that 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

$$(a + b) \circ c = a \circ c + b \circ c + a \circ (b \circ c) - (a \circ b) \circ c + \sum_{w \in W} \beta_w w(a, b, c),$$

where $w(a, b, c)$ is a specialisation of the word $w$ for $X = a$, $Y = b$, $Z = c$ and the multiplication in $w(a, b)$ is the same as the operation $\circ$ in the brace $A$ (recall that $a \circ b = a \circ b - a - b$). So for example if $w = (((XX)X)Y)Z$ then $w(a, b, c) = (((a \circ a) \circ a) \circ b) \circ c$.

Corollary 18. [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 $\gamma_w$ 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 $a, b \in A$ we have

$$(ma) \circ c = m(a \circ c) + \sum_{w \in W} \gamma_w w(a, c),$$

where $w(a, c)$ is a specialisation of the word $w$ for $X = a$, $Y = c$, and the multiplication in $w(a, c)$ is the same as the operation $\circ$ in the brace $A$ (recall that $a \circ c = a \circ c - a - c$).

Theorem 19. [8] Let $(A, +, \circ)$ be a brace of cardinality $p^n$, where $p$ is a prime number such that $p > n + 1$. Let $\text{ann}(p^2)$ be defined as before, so $\text{ann}(p^2) = \{a \in A : p^2a = 0\}$. Let $\otimes$ be defined as [8], so $[x] \otimes [y] = [\gamma^{-1}((px) \circ y)]$. Let $\xi = \gamma^{p^{n-1}}$ where $\gamma$ is a primitive root modulo $p^j$. Define a binary operation $\bullet$ on $A/\text{ann}(p^2)$ as follows:

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

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

The following result was proved in [9]:

23
Lemma 20. Let \((A,+,\circ)\) be a left nilpotent pre-Lie ring of cardinality \(p^n\) for some prime \(p > n + 1\). Let \(\Omega : A \to A\) be the inverse function of \(W\) (so \(W(\Omega(a)) = a\)) where \(W(a) = e^{\ln(1)} - 1\), where \(1 \in A^{\text{identity}}\). Then there are \(\alpha_w \in \mathbb{Z}\) not depending on \(a\) such that \(\Omega(a) = a + \sum_w \alpha_w w(a)\) where \(w\) are finite non-associative words in variable \(x\) (of degree at least 2), and \(w(a)\) is a specialisation of \(w\) at \(a\) (so for example if \(w = x \cdot (x \cdot x)\) then \(w(a) = a \cdot (a \cdot a)\)).

Acknowledgements. The author acknowledges support from the EPSRC programme grant EP/R034826/1 and from the EPSRC research grant EP/V008129/1.

References

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

[2] David Bachiller, PhD thesis entitled Study of the Algebraic Structure of Left Braces and the Yang-Baxter Equation, 2016, Universitat Autóno ma de Barcelona.

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

[4] Kourovka Notebook, in Press, new edition.

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

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

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

[8] A. Shalev, A. Smoktunowicz, From braces to pre-Lie algebras, arXiv:2207.03158 [math.RA].

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

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

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

[12] A. Smoktunowicz, A new formula for Lazard’s correspondence for finite braces and pre-Lie algebras, J. Algebra, Volume 594, 15 March 2022, Pages 202–229.