Math. Proc. Camb. Phil. Soc. (2022), **173**, 201–211
doi:10.1017/S0305004121000517
First published online 16 July 2021

The restricted Burnside problem for Moufang loops

BY ALEXANDER GRISHKOV

Department of Mathematics, University of São Paulo, Caixa Postal 66281*, São Paulo-SP,* 05311-970*, Brazil. and Omsk F.M. Dostoevsky State University, Neftezavodskaya* 11*, Omsk, Omskaya obl.,* 644053*, Russia.*
e-mail: grishkov@ime.usp.br

LIUDMILA SABININA†

Department of Mathematics, Autonomous University of the State of Morelos, Avenida Universidad 1001*, Cuernavaca,* 62209 *Morelos, Mexico.*
e-mail: liudmila@uaem.mx

AND EFIM ZELMANOV

Department of Mathematics, University of California, San Diego, 9500 *Giman Dr. La Jolla, California* 92093-0112*, U.S.A.*
e-mail: ezelmanov@math.ucsd.edu

(*Received* 20 *April* 2020; *revised* 14 *June* 2021; *accepted* 7 *April* 2021)

Dedicated to the memory of Peter Plaumann

Abstract

We prove that for positive integers $m \geq 1$, $n \geq 1$ and a prime number $p \neq 2, 3$ there are finitely many finite m-generated Moufang loops of exponent p^n.

2020 Mathematics Subject Classification: 20N05 (Primary); 17D10 (Secondary)

1. *Introduction*

A loop U is called a *Moufang loop* if it satisfies the following identities:

$$((zx)y)x = z((xy)x) \text{ and } x(y(xz)) = (x(yx))z.$$

In this paper we solve the restricted Burnside problem for Moufang loops of exponent p^n, $p > 3$.

THEOREM 1. *For an arbitrary prime power p^n, $p > 3$, there exists a function $f(m)$ such that any finite m-generated Moufang loop of exponent p^n has order $< f(m)$.*

For groups this assertion was proved by E. Zelmanov ([20, 21]). For Moufang loops of prime exponent it was proved by A. Grishkov [6] (if $p \neq 3$) and G. Nagy [15] (if $p = 3$).

†Corresponding author

In [16, 17] the restricted Burnside problem was solved for a subclass of Moufang loops and related Bruck loops.

2. *Groups with triality*

A group G with automorphisms ρ and σ is called a *group with triality* if $\rho^3 = \sigma^2 = (\rho\sigma)^2 = 1$ and

$$[x, \sigma][x, \sigma]^{\rho}[x, \sigma]^{\rho^2} = 1$$

for every $x \in G$, where $[x, \sigma] = x^{-1}x^{\sigma}$.

Let G be a group with triality. Let $U = \{[x, \sigma] | x \in G\}$. Then the subset U endowed with the multiplication

$$a \cdot b = (a^{-1})^{\rho} b (a^{-1})^{\rho^2};\ a, b \in U$$

becomes a Moufang loop.

Every Moufang loop U can be obtained in this way from a suitable group with triality, which is finite if U is finite. Moreover, if p is a prime number, then a finite Moufang p-loop can be obtained from a finite p-group with triality ([3, 5, 10]).

3. *Lie and Malcev algebras*

Let $\mathbb{F}_p$ be a field of order p, let G be a group. Consider the group algebra $\mathbb{F}_p G$ and its fundamental ideal ω, spanned by all elements $1 - g,\ g \in G$. The Zassenhaus filtration is the descending chain of subgroups

$$G = G_1 > G_2 > \cdots ,$$

where $G_i = \{g \in G \mid 1 - g \in \omega^i\}$. Then $[G_i, G_j] \subseteq G_{i+j}$ and each factor G_i/G_{i+1} is an elementary abelian p-group. Hence,

$$L = L_p(G) = \sum_{i \geq 1} L_i,\ \ L_i = G_i/G_{i+1}$$

is a vector space over $\mathbb{F}_p$. The bracket

$$[x_i G_{i+1}, y_j G_{j+1}] = [x_i, y_j] G_{i+j+1};\ \ x_i \in G_i,\ y_j \in G_j,$$

makes L a Lie algebra. Notice that the bracket [,] on the left-hand side of the last equality is a Lie bracket whereas [,] on the right-hand side denotes the group commutator.

Let x, y be generators of a free associative algebra over $\mathbb{F}_p$. Then $(x + y)^p = x^p + y^p + \{x, y\}$, where $\{x, y\}$ is a Lie element. Following [12], we call a Lie $\mathbb{F}_p$−algebra L with an operation $a \to a^{[p]}$, $a \in L$, a Lie p-algebra if

$$(ka)^{[p]} = k^p a^{[p]},$$
$$(a + b)^{[p]} = a^{[p]} + b^{[p]} + \{a, b\},$$
$$[a^{[p]}, b] = [\underbrace{a, [a, \ldots [a}_{p}, b] \ldots]$$

for arbitrary $k \in \mathbb{F}_p$; $a, b \in L$. The mapping $L_i \to L_{ip}$, $(g_i G_{i+1})^{[p]} = g_i^p G_{ip+1}$, extends to the operation $a \to a^{[p]}$, $a \in L$, making L a Lie p-algebra. For more details about this construction see [2, 11, 22].

https://doi.org/10.1017/S0305004121000517 Published online by Cambridge University Press

We call a Lie algebra (resp. Lie p-algebra) L with automorphisms ρ, σ a *Lie algebra with triality* if $\rho^3 = \sigma^2 = (\rho\sigma)^2 = 1$ and for an arbitrary element $x \in L$ we have

$$(x^\sigma - x) + (x^\sigma - x)^\rho + (x^\sigma - x)^{\rho^2} = 0.$$

LEMMA 3·1. *Let G be a group with triality and let p be a prime number. Then $L_p(G)$ is a Lie p-algebra with triality.*

Proof. The automorphisms ρ, σ of the group G give rise to automorphisms ρ, σ of the Lie algebra $L_p(G)$. For an element $x_i \in G_i$ we have

$$[x_i, \sigma][x_i, \sigma]^\rho [x_i, \sigma]^{\rho^2} = 1.$$

It implies that for the element $x = x_i G_{i+1} \in L_i$ we have

$$(x^\sigma - x) + (x^\sigma - x)^\rho + (x^\sigma - x)^{\rho^2} = 0.$$

This completes the proof of the lemma.

Recall that a (nonassociative) algebra is called a *Malcev algebra* if it satisfies the identities:

(1). $xy = -yx$;
(2). $(xy)(xz) = ((xy)z)x + ((yz)x)x + ((zx)x)y$,

see [4, 14, 23].

LEMMA 3·2 (see [7]). *Let L be a Lie algebra with triality over a field of characteristic $\neq 2, 3$. Let $H = \{x \in L | x^\sigma = -x\}$. Recall, that for any $x \in H$, $x + x^\rho + x^{\rho^2} = 0$. Then H is a Malcev algebra with multiplication*

$$a * b = [a + 2a^\rho, b] = [a^\alpha, b],$$

where $a, b \in H$, $\alpha = 1 + 2\rho$.

LEMMA 3·3. *For arbitrary elements $a, b, c \in H$ we have*

$$3[[a, b], c] = 2(a * b) * c + (c * b) * a + (a * c) * b.$$

We remark that in a Lie algebra with triality over a field F, for arbitrary elements $a_1, \ldots, a_n \in H$ the subspace

$$\sum_{i=1}^{n} F a_i + \sum_{i=1}^{n} F a_i^\alpha = \sum_{i=1}^{n} F a_i + \sum_{i=1}^{n} F a_i^\rho$$

is invariant with respect to the group of automorphisms $\langle \sigma, \rho \rangle$.

Proof. Let's prove that for any $x, y, z \in H$:

$$(x * y) * z = 2[[x^{\rho^2}, y^\rho], z] + [[x, y], z]. \tag{3·1}$$

https://doi.org/10.1017/S0305004121000517 Published online by Cambridge University Press

Using $x + x^{\rho} + x^{\rho^2} = 0$ and $y + y^{\rho} + y^{\rho^2} = 0$, we get

$$v = [x^{\rho}, y] - [x, y^{\rho}] = -[x^{\rho^2}, y] - [x, y] + [x, y^{\rho^2}] + [x, y] = [x, y^{\rho^2}] - [x^{\rho^2}, y];$$
$$v^{\rho} = [x^{\rho^2}, y^{\rho}] - [x^{\rho}, y^{\rho^2}] = -[x^{\rho}, y^{\rho}] - [x, y^{\rho}] + [x^{\rho}, y^{\rho}] + [x^{\rho}, y] = [x^{\rho}, y] - [x, y^{\rho}] = v.$$

Then

$$v^{\sigma} = [x^{\rho\sigma}, y^{\sigma}] - [x^{\sigma}, y^{\rho\sigma}] = [x^{\rho^2}, y] - [x, y^{\rho^2}] = -v,$$

hence $v \in H$ and, by triality, we have $v + v^{\rho} + v^{\rho^2} = 3v = 0$. Since the characteristic of the field is not 3 then $v = 0$ and we proved that

$$[x^{\rho}, y] = [x, y^{\rho}], \;\; [x^{\rho^2}, y^{\rho}] = [x^{\rho}, y^{\rho^2}]. \tag{3·2}$$

Finally, we have by (3·2)

$$\begin{aligned}(x * y) * z &= [x + 2x^{\rho}, y] * z \\ &= [[x + 2x^{\rho}, y], z + 2z^{\rho}] \\ &= [[x, y], z] + 2[[x^{\rho}, y], z] + 2[[x + 2x^{\rho}, y], z^{\rho}] \\ &= [[x, y], z] + 2[[x^{\rho}, y], z] + 2[[x^{\rho} + 2x^{\rho^2}, y^{\rho}], z] \\ &= [[x, y], z] + 2[[x^{\rho}, y], z] + 2[[-x + x^{\rho^2}, y^{\rho}], z] \\ &= 2[[x^{\rho^2}, y^{\rho}], z] + [[x, y], z].\end{aligned}$$

Let $J = J(x, y, z) = (x * y) * z + (y * z) * x + (z * x) * y$, then by (3·1) we get

$$J = 2([[x^{\rho^2}, y^{\rho}], z] + [[y^{\rho^2}, z^{\rho}], x] + [[z^{\rho^2}, x^{\rho}], y]).$$

But $t = [[x^{\rho^2}, y^{\rho}], z] - [[z^{\rho^2}, x^{\rho}], y] = 0$, indeed, we have

$$\begin{aligned}t - t^{\rho} &= ([[x^{\rho^2}, y^{\rho}], z] - [[z^{\rho^2}, x^{\rho}], y])^{\rho} - [[x^{\rho^2}, y^{\rho}], z] + [[z^{\rho^2}, x^{\rho}], y] \\ &= [[x, y^{\rho^2}], z^{\rho}] - [[z, x^{\rho^2}], y^{\rho}] - [[x^{\rho^2}, y^{\rho}], z] + [[z^{\rho^2}, x^{\rho}], y] \\ &= [[x^{\rho^2}, y], z^{\rho}] - [[z, x^{\rho^2}], y^{\rho}] - [[x^{\rho^2}, y^{\rho}], z] + [[z^{\rho^2}, x^{\rho}], y] \\ &= [[x^{\rho^2}, z^{\rho}], y] + [x^{\rho^2}, [y, z^{\rho}]] - [[z, y^{\rho}], x^{\rho^2}] - [z, [x^{\rho^2}, y^{\rho}]] \\ &\quad - [[x^{\rho^2}, y^{\rho}], z] + [[z^{\rho^2}, x^{\rho}], y] \\ &= [x^{\rho^2}, [y, z^{\rho}]] - [[z, y^{\rho}], x^{\rho^2}] \\ &= 0.\end{aligned}$$

Hence, $t \in H \cap \{v | v^{\rho} = v\}$. As above we can prove that $v = 0$, since the characteristic of the field is $\neq 3$.

Then

$$J(x, y, z) = (x * y) * z + (y * z) * x + (z * x) * y = 6[[x^{\rho^2}, y^{\rho}], z]. \tag{3·3}$$

https://doi.org/10.1017/S0305004121000517 Published online by Cambridge University Press

Now we are ready to prove the Lemma. By (3·1) and (3·3) we get

$$\begin{aligned}2(x*y)*z+(z*y)*x+(x*z)*y &= 3(x*y)*z+(z*y)*x+(x*z)*y+(y*x)*z\\ &= 3(x*y)*z+J(x,y,z)\\ &= 6[[x^{\rho^2},y^{\rho}],z]+3[[x,y],z]-6[[x^{\rho^2},y^{\rho}],z]\\ &= 3[[x,y],z],\end{aligned}$$

which proves the lemma.

LEMMA 3·4. *If a Lie algebra L with triality is generated by elements*

$$a_1,\ldots,a_m,a_1^{\alpha},\ldots,a_m^{\alpha},$$

where $a_1,\ldots,a_m\in H$, then the Malcev algebra H is generated by $a_1,\ldots,a_m$.

Proof. We have $L=H\dot{+}S$, where $S=\{a\in L|a^{\sigma}=a\}$ and $H^{\alpha}\subseteq S$. Hence the subspace H of L is spanned by left-normed commutators $b=[\ldots[b_1,b_2],b_3],\ldots,b_r]$, where $b_1,\ldots,b_r\in\{a_1,\ldots,a_m,a_1^{\alpha},\ldots,a_m^{\alpha}\}$ and elements from $\{a_1,\ldots,a_m\}$ occur in b an odd number of times.

(1) Suppose that $b_r=a_i^{\alpha}$, $1\le i\le m$, $b'=[\ldots[b_1,b_2],\ldots,b_{r-1}]$. Then by the induction assumption on r the element b' lies in the Malcev algebra H' generated by $a_1,\ldots,a_m$ and $b=[b',a_i^{\alpha}]=-a_i*b'$;

(2) Suppose that $b_r\in\{a_1,\ldots,a_m\}$. If the element b_{r-1} also lies in $\{a_1,\ldots,a_m\}$ and $b''=[\ldots[b_1,\ldots],b_{r-2}]$ then by the induction assumption $b''\in H'$. In this case it remains to use Lemma 3·3.

Let $b_{r-1}\in\{a_1^{\alpha},\ldots,a_m^{\alpha}\}$. Then

$$b=[[b'',b_{r-1}],b_r]=[b'',[b_{r-1},b_r]]+[b_{r-1},[b_r,b'']]$$

By the induction assumption on r applied to the elements $a_1,\ldots,a_m,a_{m+1}=[b_{r-1},b_r]\in H'$ the first summand lies in H'. The second summand was considered in case (1). This completes the proof of the lemma.

4. *Commutator identities in groups*

Let Fr be the free group on free generators x_i, $i\ge 1$; y,z_1,z_2. Recall the Hall commutator identity

$$[xy,z]=[y,[z,x]][x,z][y,z],$$

where $[x,y]=x^{-1}y^{-1}xy$ is the group commutator.

Let N be the normal subgroup of Fr generated by the element y and let N' by the subgroup of N generated by $[N,N]$ and by all elements g^p, $g\in N$. Then N/N' is a vectors space over the finite field $\mathbb{F}_p$. For an element $g\in Fr$ consider the linear transformation

$$g':N/N'\longrightarrow N/N',\ \ hN'\longrightarrow[g,h]N'.$$

https://doi.org/10.1017/S0305004121000517 Published online by Cambridge University Press

Then the Hall identity implies

$$(ab)' = a' + b' - b'a',$$

or, equivalently, $1-(ab)' = (1-b')(1-a')$, where 1 is the identity map. Hence, $1-(a^{p^n})' = (1-a')^{p^n}$. This implies the following well known lemma

LEMMA 4·1. $\underbrace{[x_1, [x_1, [\dots [x_1}_{p^n}, y]]\dots] = [x_1^{p^n}, y] \mod N'$.

COROLLARY. $[[x_1, z_1], [[x_1, z_1], [\dots, [[x_1, z_1], y]\dots] = [[x_1, z_1]^{p^n}, y] \mod N'$.

Applying the so called "collection process" of G. Higman [11] (see also [22]) we linearize this equality in x_1.

LEMMA 4·2. *The product*

$$\prod_{\pi \in S_{p^n}} [[x_{\pi(1)}, z_1], [[x_{\pi(2)}, z_1], [\dots, [[x_{\pi(p^n)}, z_1], y]\dots]$$

with an arbitrary order of factors lies in the subgroup generated by elements

$$[[x_{i_1}\cdots x_{i_r}, z_1]^{p^n}, y],$$

$1 \le i_1 < \cdots < i_r \le p^n$, *and commutators* c *in* $y, z_1, x_1, \dots, x_{p^n}$ *such that:*

(i) c involves all elements $y, x_1, \dots, x_{p^n}$*;*
(ii) some element y *or* x_j, $1 \le j \le p^n$, *occurs in* c *at least twice.*

Consider again a group with triality G and the Lie algebra with triality $L = L_p(G) = \sum_{i=1}^{\infty} L_i$. The subspace $H = \{a \in L \mid a^\sigma + a = 0\}$ is graded, i.e. $H = \sum_{i=1}^{\infty} H_i$, $H_i = H \cap L_i$.

LEMMA 4·3. *Suppose that for an arbitrary element* $g \in G$ *we have* $[g, \sigma]^{p^n} = 1$. *Then*

(i) for an arbitrary homogeneous element $a \in H_i$, $i \ge 1$, *we have* $\mathrm{ad}(a)^{p^n} = 0$,
(ii) for arbitrary homogeneous elements $a_1, \dots, a_{p^n}$ *from* H *we have*

$$\sum_{\pi \in S_{p^n}} \mathrm{ad}(a_{\pi(1)}) \cdots \mathrm{ad}(a_{\pi(p^n)}) = 0.$$

Proof. For a homogeneous element $a \in H_i$ there exists an element $g \in G_i$ such that $a = [g, \sigma]G_{i+1}$. Then $a^{[p^n]} = [g, \sigma]^{p^n} G_{p^n i+1} = 0$. This implies $ad(a)^{p^n} = ad(a^{[p^n]}) = 0$.

Let $a_1, \dots, a_{p^n}$ be homogeneous elements from H, $a_i = [g_i, \sigma]G_{n(i)+1}$, $g_i \in G_{n(i)}$, $b = g'G_{j+1}$, $g' \in G_j$. Applying Lemma 4·2 to $x_i = g_i$, $z_1 = \sigma$, $y = g'$ we get the assertion (ii).

LEMMA 4·4. *For an arbitrary element* $a \in H$ *we have* $[a, a^\rho] = 0$.

Proof. We have already mentioned that for an arbitrary element $g \in [G, \sigma]$ we have $[g, g^\rho] = 1$, see [8]. Hence, $[g, g^\rho] = 0$ in $L(G)$.

Let $a_i \in H_i$, $a_j \in H_j$ be homogeneous elements. We need to show that $[a_i, a_j^\rho] + [a_j, a_i^\rho] = 0$. There exist elements $g_i \in G_i$, $g_j \in G_j$ such that $a_i = [g_i, \sigma]G_{i+1}$, $a_j =$

https://doi.org/10.1017/S0305004121000517 Published online by Cambridge University Press

$[g_j, \sigma]G_{j+1}$. In the free group Fr consider the element

$$X = [[x_1, z_1], [x_2, z_1]^{z_2}][[x_2, z_1], [x_1, z_1]^{z_2}].$$

Applying the Hall identity and the Collection Process in the free group Fr we get

$$[[x_1x_2, z_1], [x_1x_2, z_1]^{z_2}] = [[x_1, z_1], [x_1, z_1]^{z_2}][[x_2, z_1], [x_2, z_1]^{z_2}] \cdot X \cdot c_1 \cdots c_r,$$

where $c_1, \ldots, c_r$ are commutators in x_1, x_2, z_1, z_2; each of these commutators involved both elements x_1, x_2 and at least one of these elements occurs more than once.

Substitute $x_1 = g_i, x_2 = g_j, z_1 = \sigma, z_2 = \rho$. Then the equality above in the free group Fr implies $X \in G_{i+j+1}$. Hence $[a_i, a_j^\rho] + [a_j, a_i^\rho] = 0$, which completes the proof of the lemma.

Example 4·1. Let L be a nilpotent 3-dimensional Lie algebra with basis a, b, c and multiplication $[a, b] = c$, $[a, c] = [b, c] = 0$. The group S_3 acts on L via $a^\sigma = -a$, $b^\sigma = a + b$, $c^\sigma = c$, $a^\rho = b$, $b^\rho = -a - b$, $c^\rho = c$. The straightforward computation shows that L is a Lie algebra with triality and that $[a, a^\rho] = -c \neq 0$.

LEMMA 4·5.

(i) *For an arbitrary element $a \in H$, arbitrary $k \geq 1$, we have*

$$\mathrm{ad}(a^\alpha)^{p^k} = \mathrm{ad}(a)^{p^k} + 2\rho^{-1}\mathrm{ad}(a)^{p^k}\rho;$$

(ii) *for arbitrary elements $a_1, \ldots, a_{p^k} \in H$ we have*

$$\sum_{\pi \in S_{p^k}} \mathrm{ad}(a^\alpha_{\pi(1)}) \cdots \mathrm{ad}(a^\alpha_{\pi(p^k)})$$
$$= \sum_{\pi \in S_{p^k}} \mathrm{ad}(a_{\pi(1)}) \cdots \mathrm{ad}(a_{\pi(p^k)}) + 2\rho^{-1} \sum_{\pi \in S_{p^k}} \mathrm{ad}(a_{\pi(1)}) \cdots \mathrm{ad}W(a_{\pi(p^k)})\rho.$$

Proof. We only need to prove part (i). Part (ii) is obtained from (i) by linearization. We have $a^\alpha = a + 2a^\rho$. By Lemma 4·4 $[a, a^\rho] = 0$. Hence,

$$ad(a^\alpha)^{p^k} = ad(a)^{p^k} + 2^{p^k} ad(a^\rho)^{p^k} = ad(a)^{p^k} + 2\rho^{-1} ad(a)^{p^k}\rho.$$

This completes the proof of the lemma.

We remark that the proof of linearised Engel identity in [6] contains a gap that is filled in this paper.

For an element $a \in H$ let $ad^*(a)$ denote the operator of multiplication by a in the Malcev algebra, $ad^*(a) : h \to a * h$, $ad^*(a) = ad(a^\alpha)$.

LEMMA 4·6.

(i) *For an arbitrary homogeneous element $a \in H_i$, $i \geq 1$, we have* $\mathrm{ad}^*(a)^{p^n} = 0$;

(ii) *for arbitrary elements $a_1, \ldots, a_{p^n} \in H$ we have*

$$\sum_{\pi \in S_{p^n}} ad^*(a_{\pi(1)}) \cdots \mathrm{ad}^*(a_{\pi(p^n)}) = 0.$$

https://doi.org/10.1017/S0305004121000517 Published online by Cambridge University Press

Proof. Assertion (i) follows from Lemma 4·3 and Lemma 4·5. Assertion (ii) follows from Lemma 4·3 and Lemma 4·5.

5. *Local nilpotence in Malcev algebras*

PROPOSITION 1. *Let $M = M_1 + M_2 + \cdots$ be a finitely generated graded Malcev algebra over a field of characteristic $p \neq 2, 3$, such that:*

(i) $\mathrm{ad}^*(a)^{p^n} = 0$ *for an arbitrary homogeneous element* $a \in M$*;*

(ii) $\sum_{\pi \in S_{p^n}} \mathrm{ad}^*(a_{\pi(1)}) \cdots \mathrm{ad}^*(a_{\pi(p^n)}) = 0$ *for arbitrary* $a_1, \ldots, a_{p^n} \in M$.

Then the Malcev algebra M is nilpotent and finite dimensional.

If I is an ideal of a Malcev algebra M then $\widetilde{I} = I^2 + I^2 \cdot M$ is also an ideal of M. Consider the descending chain of ideals $M^{[0]} = M$, $M^{[i+1]} = \widetilde{M^{[i]}}$. We say that a Malcev algebra M is *solvable* if $M^{[n]} = (0)$ for some $n \geq 1$.

LEMMA 5·1 (Filippov, [4]). *A finitely generated solvable Malcev algebra over a field of characteristic > 3 is nilpotent if and only if each of its Lie homomorphic images is nilpotent.*

Consider the free Malcev algebra $M(m)$ on m free generators $x_1, \ldots, x_m$. As always $\mathbb{N} = \{1, 2, \ldots\}$ is the set of positive integers. The algebra $M(m)$ is $\mathbb{N}^m$-graded via

$$\deg(x_i) = (0, 0, \ldots, \underset{i}{1}, 0, \ldots, 0), \quad 1 \leq i \leq m, \quad M(m) = \bigoplus_{\gamma \in \mathbb{N}^m} M(m)_\gamma .$$

Let I be the ideal of $M(m)$ generated by elements $\underbrace{a(a(\cdots a}_{p^n}\, b) \cdots)$ and elements

$$\sum_{\pi \in S_{p^n}} a_{\pi(1)}(a_{\pi(2)}(\cdots (a_{\pi(p^n)} b) \cdots),$$

where $a, a_1, \ldots, a_{p^n}, b$ run over all homogeneous elements of $M(m)$. Let

$$M(m, p^n) = M(m)/I$$

LEMMA 5·2. *The algebra $M(m, p^n)^2$ is finitely generated.*

Proof. Kuzmin (see [14]) showed that for an arbitrary Malcev algebra M we have $M^{[3]} \subseteq M^2 \cdot M^2$. By [20] every Lie homomorphic image of $M(m, p^n)$ is a nilpotent algebra. Hence by Lemma 5·1 of Filippov there exists $t \geq 1$ such that

$$M(m, p^n)^t \subseteq M(m, p^n)^{[3]} \subseteq M(m, p^n)^2 M(m, p^n)^2 .$$

Since the algebra $M(m, p^n)$ is $\mathbb{N}^m$-graded it implies that $M(m, p^n)^2$ is generated by products of $x_1, \ldots, x_m$ of length ℓ, $2 \leq \ell \leq t - 1$. This completes the proof of the lemma.

Recall that an algebra is said to be *locally nilpotent* if every finitely generated subalgebra is nilpotent.

https://doi.org/10.1017/S0305004121000517 Published online by Cambridge University Press

LEMMA 5·3. *Let $M = M_1 + M_2 + \cdots$ be a graded Malcev algebra that satisfies assumptions* (i) *and* (ii) *of Proposition* 1. *Let I be an ideal of M such that both I and M/I are locally nilpotent. Then the algebra M is locally nilpotent.*

Proof. Let M' be a subalgebra of M generated by m homogeneous elements. Then M' is a homomorphic image of the Malcev algebra $M(m, p^n)$. By Lemma 5·2 the algebra $(M')^2$ is finitely generated.

Let's prove that the algebra M' is solvable. Since the factor M/I has been assumed to be locally nilpotent the algebra $(M' + I)/I$ is nilpotent and finite dimensional. We will prove solvability of M' by induction on $\dim_F(M' + I/I)$. If $\dim_F(M' + I)/I = 0$ then the subalgebra M' is nilpotent since it lies in I. If $\dim_F(M' + I)/I > 0$ then $\dim_F(M')^2 + I/I < \dim_F(M' + I)/I$. Hence the algebra $(M')^2$ is solvable which implies solvability of M'.

Since M' is solvable then by [20] all Lie homomorphic images of the algebra M' are nilpotent. Hence by Lemma 5·1 the algebra M' is nilpotent, which completes the proof of the lemma.

LEMMA 5·4. *Let $M = M_1 + M_2 + \cdots$ be a graded Malcev algebra that satisfies assumptions (i) and (ii) of Proposition 1. Then M contains a largest graded locally nilpotent ideal $Loc(M)$ such that the factor algebra $M/Loc(M)$ does not contain nonzero locally nilpotent ideals.*

REMARK. For Lie algebras this assertion was proved in [13, 18]

Proof. Let I_1, I_2 be graded locally nilpotent ideals of M. Since the factor algebra $I_1 + I_2/I_1 \cong I_2/I_1 \cap I_2$ is locally nilpotent it follows from Lemma 5·3 that the algebra $I_1 + I_2$ is locally nilpotent.

Let $\mathrm{Loc}(M)$ be the sum of all graded locally nilpotent ideals of M. We showed that the ideal $\mathrm{Loc}(M)$ is locally nilpotent. By Lemma 5·3 the factor algebra $\overline{M} = M/\mathrm{Loc}(M)$ does not contain nonzero graded locally nilpotent ideals. Let J be a nonzero (not necessarily graded) locally nilpotent ideal of $\overline{M}$. Let J_{gr} be the ideal of $\overline{M}$ generated by nonzero homogeneous components of elements of J of maximal degree. It is easy to see that the ideal J_{gr} of $\overline{M}$ is locally nilpotent, a contradiction. This completes the proof of the lemma.

Recall that an algebra A is called *prime* if for any nonzero ideals I, J of A we have $IJ \neq (0)$. A graded algebra $A = A_1 + A_2 + \cdots$ is *graded prime* if for any nonzero graded ideals I, J we have $IJ \neq (0)$. Passing to ideals $I_{\mathrm{gr}}, J_{\mathrm{gr}}$ we see that a graded prime algebra is prime.

The proof of the following lemma follows a well-known scheme (see [21]). We still include it for the sake of completeness.

LEMMA 5·5. *Let $M = M_1 + M_2 + \cdots$ be a graded Malcev algebra satisfying assumptions (i) and (ii) of Proposition 1. Then the ideal $Loc(M)$ is an intersection $Loc(M) = \bigcap P$ of graded ideals $P \lhd M$ such that the factor algebra M/P is prime.*

Proof. Choose a homogeneous element $a \in M \setminus \mathrm{Loc}(M)$. Since the ideal $I(a)$ generated by the element a in M is not locally nilpotent there exists a finitely generated graded subalgebra $B \subseteq I(a)$ that is not nilpotent. Since the algebra B satisfies assumptions (i) and (ii) it follows from Filippov's Lemma 5·1 that the algebra B is not solvable.

https://doi.org/10.1017/S0305004121000517 Published online by Cambridge University Press

Consider the descending chain of subalgebras $B^{(0)} = B$, $B^{(i+1)} = (B^{(i)})^2$. Since the algebra B is not solvable we conclude that $B^{(i)} \neq (0)$ for all $i \geq 0$.

By Zorn's Lemma there exists a maximal graded ideal P of M with the property that $B^{(i)} \nsubseteq P$ for all i. Indeed, let $P_1 \subseteq P_2 \subseteq \cdots$ be an ascending chain of graded ideals such that B is not solvable modulo each of them. If B is solvable modulo $\bigcup_{i\geq 1} P_i$ then $B^{(s)} \subseteq \bigcup_{i\geq 1} P_i$ for some $s \geq 1$. By Lemma 5·2 the subalgebra $B^{(s)}$ is finitely generated, hence $B^{(s)} \subseteq P_i$ for some i, a contradiction.

We claim that the factor algebra M/P is graded prime. Indeed, suppose that I, J are graded ideals of M, $P \subsetneq I$, $P \subsetneq J$, and $IJ \subseteq P$. By maximality of P there exists $i \geq 1$ such that $B^{(i)} \subseteq I$ and $B^{(i)} \subseteq J$. Then $B^{(i+1)} \subseteq P$, a contradiction. This completes the proof of the lemma.

Proof of Proposition 1. Let M be a graded Malcev algebra satisfying assumptions (i) and (ii). If M is not nilpotent then $M \neq \mathrm{Loc}(M)$. By Lemma 5·5, M has a nonzero prime homomorphic image. Filippov [4] showed that every prime non-Lie Malcev algebra over a field of characteristic $p > 3$ is 7-dimensional over its centroid. Now it remains to refer to the result of Stitzinger [19] on Engel's Theorem in the form of Jacobson for Malcev algebras. This completes the proof of Proposition 1.

6. *Proof of Theorem 1*

Let $U(m, p^n)$ be the free Moufang loop of exponent p^n on m free generators $x_1, \ldots, x_m$. Let $E = E(U(m, p^n))$ be the minimal group with triality that corresponds to the loop $U(m, p^n)$ (see [9]). The group E is generated by elements $x_1, \ldots, x_m, x_1^\rho, \ldots, x_m^\rho$. Consider the Zassenhaus descending chain of subgroups $E = E_1 > E_2 > \cdots$. Let

$$G = E/\bigcap_{i\geq 1} E_i, \quad U = [G, \sigma].$$

Theorem 4 from [5] implies that an arbitrary finite m-generated Moufang loop of exponent p^n is a homomorphic image of the loop U. We will show that the loop U is finite.

As above, consider the Lie p-algebra

$$L = L_p(G) = \bigoplus_{i\geq 1} L_i, \qquad L_i = G_i/G_{i+1},$$

over the field $\mathbb{F}_p$, $|\mathbb{F}_p| = p$, and the Malcev algebra $H = \{a - a^\sigma | a \in L\}$. The Malcev algebra H is graded, $H = \bigoplus_{i\geq 1} H_i$, $H_i = H \cap L_i$, and satisfies assumptions (i) and (ii) of Proposition 1.

Consider the Lie subalgebra L' of L generated by the set $I_m = \{a_1, \ldots, a_m, a_1^\alpha, \ldots, a_m^\alpha\}$, where $a_i = x_i E_2 \in L_1$, $1 \leq i \leq m$. The whole Lie algebra L is generated by I_m as a p-algebra.

Since the subalgebra L' is S_3-invariant it follows that L' is a Lie algebra with triality. Therefore L' gives rise to the Malcev algebra $H' = L' \cap H$. By Lemma 3·4 the elements $a_1, \ldots, a_m$ generate H' as a Malcev algebra. Hence, by Proposition 1 the algebra H' is nilpotent and finite dimensional. Let $\dim_{\mathbb{F}_p} H' = d$.

Since the Lie algebra L is generated by $a_1, \ldots, a_m$ as a p-algebra it follows that L is spanned by p powers $c^{[p^k]}$, where c is a commutator in $a_1, \ldots, a_m$ of length $\leq 2d$, $k \geq 0$. The space H is spanned by pth powers $c^{[p^k]}$, where the commutators c have odd length.

https://doi.org/10.1017/S0305004121000517 Published online by Cambridge University Press

An arbitrary homogeneous element $a \in H_i$ can be represented as $[g, \sigma]G_{i+1}$, where $g \in G_i$. Hence $[g, \sigma]^{p^n} = 1$ implies $a^{[p^n]} = 0$. Then H is spanned by p-powers $c^{[p^k]}$, where c is a commutator in $a_1, \ldots, a_m$ of odd length $\leq 2d$ and $k < n$. Hence, $\dim_{\mathbb{F}_p} H < \infty$. Since $|H| = |U|$ we conclude that $|U| < \infty$. This concludes the proof of Theorem 1.

Acknowledgements. The first author was supported by CNPq (grant 307824/2016-0), by FAPESP (Brazil) and Russian Foundation for Basic Research (under grant 16-01-00577a). The second author was supported in part by SNI-CONACyT, PRODEP-UAEM "Estancias cortas de investigacion de integrantes de Cuerpos Academicos Consolidados-2020", FAPESP 2019/24418-0 and UC MEXUS grants. The third author gratefully acknowledges the support of the NSF grant DMS 1601920.

The authors are grateful to the referee for helpful remarks.

REFERENCES

[1] R. H. BRUCK. *A survey of binary systems,* vol. 20, (Springer, 1971).

[2] J. D. DIXON, M. P. F. DU SAUTOY, A. MANN, and D. SEGAL. *Analytic pro-p groups,* second ed., Cambridge Studies in Advanced Math., no. 61, (Cambridge University Press, Cambridge, 1999).

[3] S. DORO. Simple Moufang loops. *Math. Proc. Camb. Phil. Soc.* **83** (1978), no. 3, 377–392.

[4] V. T. FILIPPOV. The Engel algebras of Malcev. *Algebra and Logic* **15** (1976), no. 1, 89–109.

[5] G. GLAUBERMAN. On loops of odd order. II. *J. Algebra* **8** (1968), 393–414.

[6] A. N. GRISHKOV. The weakened Burnside problem for Moufang loops of prime period. *Sibirsk. Mat. Zh.* **28** (1987), no. 3, 60–65, 222.

[7] A. GRISHKOV. Lie algebras with triality. *J. Algebra* **266** (2003), no. 2, 698–722.

[8] A. N. GRISHKOV and A. V. ZAVARNITSINE. Lagrange's theorem for Moufang loops. *Math. Proc. Cambridge Philos. Soc.* **139** (2005), no. 1, 41–57.

[9] A. N. GRISHKOV and A. V. ZAVARNITSINE. Groups with triality. *J. Algebra Appl.* **5** (2006), no. 4, 441–463.

[10] A. N. GRISHKOV and A. V. ZAVARNITSINE. Sylow's theorem for Moufang loops. *J. Algebra* **321** (2009), no. 7, 1813–1825.

[11] G. HIGMAN. Lie ring methods in the theory of finite nilpotent groups Proc. Internat. Congress Math. 1958. (Cambridge Univ. Press, New York, 1960), pp. 307–312.

[12] N. JACOBSON. *Lie algebras.* Interscience Tracts in Pure and Applied Math., no. 10, (Interscience Publishers, New York-London, 1962).

[13] A. I. KOSTRIKIN. On Lie rings satisfying the Engel condition. *Dokl. Akad. Nauk SSSR* (N.S.) **108** (1956), 580–582.

[14] E. N. KUZMIN. Structure and representations of finite dimensional Malcev algebras. *Quasigroups Related Systems* **22** (2014), no. 1, 97–132.

[15] G. P. NAGY. Burnside problems for Moufang and Bol loops of small exponent. *Acta Sci. Math.* (Szeged) **67** (2001), no. 3-4, 687–696.

[16] P. PLAUMANN and L. SABININA. On nuclearly nilpotent loops of finite exponent. Comm. Algebra **36** (2008), no. 4, 1346–1353.

[17] P. PLAUMANN and L. SABININA. *Some remarks on the Burnside problem for loops,* Advances in Algebra and Combinatorics, (World Sci. Publ., Hackensack, NJ, 2008), pp. 293–302.

[18] B. I. PLOTKIN. Algebraic sets of elements in groups and Lie algebras. *Uspehi Mat. Nauk* **13** (1958), no. 6 (84), 133-138.

[19] E. L. STITZINGER. On nilpotent and solvable Malcev algebras. *Proc. Amer. Math. Soc.* **92** (1984), no. 2, 157–163.

[20] E. I. ZELMANOV. Solution of the restricted Burnside problem for groups of odd exponent. *Izv. Akad. Nauk SSSR Ser. Mat.* **54** (1990), no. 1, 42–59, 221.

[21] E. I. ZELMANOV. Solution of the restricted Burnside problem for 2-groups. *Mat. Sb.* **182** (1991), no. 4, 568–592.

[22] E. ZELMANOV. *Nil rings and periodic groups.* KMS Lecture Notes in Mathematics. (Korean Mathematical Society, Seoul, 1992).

[23] K. A. ZHEVLAKOV, A. M. SLINKO, I. P. SHESTAKOV, and A. I. SHIRSHOV. *Rings that are nearly associative*. Pure Appl. Math., vol. 104, (Academic Press, Inc., New York-London, 1982).