International Journal of Algebra and Computation
Vol. 22, No. 7 (2012) 1250075 (23 pages)

DOI: 10.1142/S0218196712500750

World Scientific
www.worldscientific.com

THE SUBPOWER MEMBERSHIP PROBLEM FOR MAL'CEV ALGEBRAS

PETER MAYR*
CAUL, Centro de Álgebra da Universidade de Lisboa
Av. Prof. Gama Pinto 2, 1649-003 Lisboa, Portugal
pxmayr@gmail.com

Received 11 May 2011
Accepted 10 September 2011
Published 12 November 2012

Communicated by R. McKenzie

Given tuples $a_1, \ldots, a_k$ and b in $\mathbf{A}^n$ for some algebraic structure $\mathbf{A}$, the subpower membership problem asks whether b is in the subalgebra of $\mathbf{A}^n$ that is generated by $a_1, \ldots, a_k$. For $\mathbf{A}$ a finite group, there is a folklore algorithm which decides this problem in time polynomial in n and k. We show that the subpower membership problem for any finite Mal'cev algebra is in NP and give a polynomial time algorithm for any finite Mal'cev algebra with finite signature and prime power size that has a nilpotent reduct. In particular, this yields a polynomial algorithm for finite rings, vector spaces, algebras over fields, Lie rings and for nilpotent loops of prime power order.

Keywords: Subalgebras of powers; membership test; generators; partial functions; interpolation; Mal'cev algebras

Mathematics Subject Classification 2010: 08A40 (20B40)

1. Introduction

How can we decide whether a given partial operation is the restriction of a term function on some algebra? What is the complexity of the interpolating term function if it exists? We will consider these questions in a formulation that Ross Willard proposed at the Conference on Order, Algebra, and Logics in Nashville 2007 [13].

Fix a finite algebra $\mathbf{A}$. Then the *subpower membership problem* for $\mathbf{A}$ is the following decision problem:

INPUT	$\{a_1, \ldots, a_k\} \subseteq A^n, b \in A^n$
PROBLEM	Is b in the subalgebra $\langle a_1, \ldots, a_k \rangle$ of $\mathbf{A}^n$ that is generated by $a_1, \ldots, a_k$?

*Current address: Institute for Algebra, JKU Linz, Altenberger Straße 69, 4040 Linz, Austria.

So the size of the input is basically given by $n(k+1)$. For any $\mathbf{A}$ we can solve this problem in exponential time by enumerating all the elements in $\langle a_1, \ldots, a_k \rangle$ (at most $|A|^n$). In [9] Kozik constructed algebras for which the problem is in fact Exptime-complete. For algebras with near-unanimity term it is clearly polynomial by the Baker–Pixley Theorem [2]. Adapting the algorithm for testing membership for permutation groups in [7], Willard obtained a polynomial time algorithm for the subpower membership for groups expanded with multilinear operations (in particular, for groups, rings, modules, K-algebras,...). In his talk he asked whether the subpower membership problem for any finite Mal'cev algebra is in P.

We provide the following partial answers.

Theorem 1.1. *The subpower membership problem for every finite Mal'cev algebra is in NP.*

Theorem 1.1 will be proved in Sec. 2. For certain cases that behave very much like p-groups with additional operations we will give a polynomial time algorithm (see [6] for the definition of commutators and nilpotence for general algebraic structures).

Theorem 1.2. *Let $\langle A, m \rangle$ be a nilpotent Mal'cev algebra of prime power order. Then every expansion of $\langle A, m \rangle$ with finitely many functions has subpower membership problem in P.*

Theorem 1.2 is proved in Sec. 3. We state some consequences for classical algebras.

Corollary 1.3. *Every expansion of a finite p-group with finitely many functions has subpower membership problem in P.*

Corollary 1.4 (Willard, unpublished). *Every finite ring, vector space, algebra over a field, or Lie ring has subpower membership problem in P.*

Corollary 1.5. *Every nilpotent loop of prime power size has subpower membership problem in P.*

The problem whether subpower membership can be decided in polynomial time for any finite Mal'cev algebra remains open.

We also note that investigating Post's classification of the algebras of size 2 yields that the subpower membership problem for each of them is solvable in polynomial time. Note in particular that each of the 11 term-inequivalent Mal'cev algebras of size 2 is either abelian or has a majority term [12].

2. The Subpower Membership Problem is in *NP*

For proving Theorem 1.1 we will use the small generating sets for subpowers of a Mal'cev algebra that already appeared in [1, 3]. A ternary function m on a set A is said to be a *Mal'cev function* if $m(x, y, y) = m(y, y, x) = x$ for all $x, y \in A$.

Recall that an algebra $\mathbf{A}$ generates a congruence permutable variety if and only if it has a term operation that is a Mal'cev function. In that case we call $\mathbf{A}$ a *Mal'cev algebra*. For every group $\langle G, \cdot, ^{-1} \rangle$ we have a Mal'cev term operation defined by $m(x, y, z) := xy^{-1}z$.

We denote the set of all k-ary term operations on an algebra $\mathbf{A}$ by $\mathrm{Clo}_k(\mathbf{A})$ and put $\mathrm{Clo}(\mathbf{A}) := \bigcup_{k\in\mathbb{N}} \mathrm{Clo}_k(\mathbf{A})$ [11, Definition 4.2].

Let $\mathbf{A}$ be an algebra with Mal'cev term operation m, and let $n \in \mathbb{N}$. For $i \in \{2, \ldots, n\}$ and $a, b \in A^n$ we call (a, b) a *fork* at index i if $a_1 = b_1, \ldots, a_{i-1} = b_{i-1}$. Let $R_1 \subseteq A^n$, and let $R_2, \ldots, R_n \subseteq (A^n)^2$ be a set of forks at $2, \ldots, n$, respectively. We say $a \in A^n$ is *representable* with respect to $R_1, \ldots, R_n$ if there exist $r_1 \in R_1, (s_2, r_2) \in R_2, \ldots, (s_n, r_n) \in R_n$ such that

(1) $a(i) = r_i(i)$ for all $i \in \{1, \ldots, n\}$ and
(2) $m(\cdots m(r_1, s_2, r_2), \ldots, s_{i-1}, r_{i-1})(i) = s_i(i)$ for all $i \in \{2, \ldots, n\}$.

Note that under these assumptions

$$a = m(\cdots m(r_1, s_2, r_2), \ldots, s_n, r_n).$$

Let B be a subuniverse of $\mathbf{A}^n$, let $R_1 \subseteq B$, and let $R_2, \ldots, R_n \subseteq B^2$ be a set of forks at $2, \ldots, n$, respectively. Then we call $R_1, \ldots, R_n$ a *canonical representation* for B if

(1) $\forall\, r, r' \in R_1 \colon r_1 = r'_1 \Rightarrow r = r'$,
(2) $\forall\, i \in \{2, \ldots, n\} \forall\, (s, r), (s', r') \in R_i \colon (s_i, r_i) = (s'_i, r'_i) \Rightarrow (s, r) = (s', r')$,
(3) every $a \in B$ is representable with respect to $R_1, \ldots, R_n$.

We reformulate the representation results from [1, 3] for our purposes.

Lemma 2.1 (cf. [1, Lemma 3.1; 3, Lemma 3.1]). *Let $\mathbf{A}$ be an algebra with Mal'cev operation m, let $n \in \mathbb{N}$, and let $B \leq \mathbf{A}^n$. Then B has a canonical representation $R_1, \ldots, R_n$ with $|R_1| \leq |A|$ and $|R_i| \leq |A|^2$ for all $i \in \{2, \ldots, n\}$.*

Proof. We choose $R_1 \subseteq B$ and choose $R_2, \ldots, R_n \subseteq B^2$ to be a set of forks at $2, \ldots, n$, respectively, such that the following holds:

(1) for every $a \in B$ there exists a unique $r \in R_1$ such that $a_1 = r_1$,
(2) $\forall\, i \in \{2, \ldots, n\}$: for every $(a, b) \in B^2$ that is a fork at i there exists a unique $(s, r) \in R_i$ such that $(a_i, b_i) = (s_i, r_i)$.

Then $R_1, \ldots, R_n$ is a canonical representation with the asserted properties. □

By Lemma 2.1 every subuniverse of $\mathbf{A}^n$ is generated as a subuniverse of $\langle A, m \rangle$ by at most $|A| + 2(n-1)|A|^2$ elements.

Algorithm 1 IsRepresentable$(m, (R_1, \dots, R_n), a)$

Input: m a Mal'cev operation on A, $R_1 \subseteq A^n, R_2, \dots, R_n \subseteq A^n \times A^n$ sets of forks at $2, \dots, n$, respectively, $a \in A^n$
Output: true if a is representable with respect to $R_1, \dots, R_n$

```
if ∃ r ∈ R_1 : a_1 = r_1 then
  b := r
else
  return (1, a)
end if
for i ∈ {2, ..., n} do
  if ∃ (s, r) ∈ R_i : s_i = b_i, r_i = a_i then
    b := m(b, s, r)
  else
    return (i, (b, a))
  end if
end for
return true
```

Given a canonical representation of a subuniverse B of $\mathbf{A}^n$ the algorithm IsRepresentable verifies membership in B.

The conditions in the if-statements in IsRepresentable can be checked by a sequential search through the at most $|A|$ elements in R_1 and the at most $|A|^2$ elements in R_i for $i > 1$. Hence the complexity of IsRepresentable is polynomial in n.

Note that $a \in A^n$ may not be representable for one of two reasons. Either there does not exists $r \in R_1$ such that $a_1 = r_1$ in which case the algorithm simply returns $(1, a)$. Or there exist $r_1 \in R_1, (s_2, r_2) \in R_2, \dots, (s_{i-1}, r_{i-1}) \in R_{i-1}$ with $b := m(\cdots m(r_1, s_2, r_2), \dots, s_{i-1}, r_{i-1})$ satisfying $b_1 = a_1, \dots, b_{i-1} = a_{i-1}$ but there is no $(s, r) \in R_i$ such that $(s_i, r_i) = (b_i, a_i)$. In this case the algorithm returns the missing fork $(i, (b, a))$. With these adaptations IsRepresentable can be used to build a canonical representation by adding missing generators. This is done by the next algorithm, CanonicalRepresentation, which computes a canonical representation for a subuniverse of $\mathbf{A}^n$ that is given by generators.

For checking the correctness of CanonicalRepresentation assume that $R_1, \dots, R_n$ is returned. Clearly

$$B := \{a \in A^n : a \text{ is representable with respect to } R_1, \dots, R_n\}$$

contains $\{a_1, \dots, a_k\}$, is closed under the basic operations of $\mathbf{A}$, and all the elements of $R_1, \dots R_n$ are obtained by applying operations of $\mathbf{A}$ to $a_1, \dots, a_k$. Hence B is the subalgebra of $\mathbf{A}^n$ that is generated by $\{a_1, \dots, a_k\}$. By construction $R_1, \dots, R_n$ is a canonical representation of B.

Note that CanonicalRepresentation in fact enumerates all elements in $B := \langle a_1, \ldots, a_k \rangle$. Hence its running time is potentially exponential in the input size.

Proof of Theorem 1.1. We will use the intermediate results of the algorithm CanonicalRepresentation to show that $b \in \langle a_1, \ldots, a_k \rangle$ can be verified in polynomial time.

Let us fix $R_1, \ldots, R_n$ for a particular step during the running time of CanonicalRepresentation. Any possible new addition r to R_1 is either some a_j from the input or of the form $f(v_1, \ldots, v_t)$ where $v_1, \ldots, v_t$ are representable with respect to $R_1, \ldots, R_n$. Hence we have a term whose length is at most linear in tn which allows us to verify that r is generated by the elements that are already in $R_1, R_2, \ldots, R_n$.

Algorithm 2 CanonicalRepresentation($\mathbf{A}, \{a_1, \ldots, a_k\}$)

Input: $\mathbf{A}$ algebra with Mal'cev operation m, $a_1, \ldots, a_k \in A^n$
Output: a canonical representation $R_1, \ldots, R_n$ for $\langle a_1, \ldots, a_k \rangle \leq \mathbf{A}^n$

```
R_i := ∅
for a ∈ {a_1, ..., a_k} do
  while IsRepresentable(m, (R_1, ..., R_n), a) ≠ true do
    if IsRepresentable(m, (R_1, ..., R_n), a) = (i, r) then
      Add r to R_i
    end if
  end while
end for
closed := false
while not closed do
  closed := true
  for f a basic operation of A do
    t := arity of f
    for v_1, ..., v_t representable with respect to R_1, ..., R_n do
      a := f(v_1, ..., v_t)
      while IsRepresentable(m, (R_1, ..., R_n), a) ≠ true do
        if IsRepresentable(m, (R_1, ..., R_n), a) = (i, r) then
          Add r to R_i
        end if
        closed := false
      end while
    end for
  end for
end while
return R_1, ..., R_n
```

Likewise for every new addition (s, r) to $R_i\,(i > 1)$ we have that $s = m(\cdots m(r_1, s_2, r_2), \ldots, s_{i-1}, r_{i-1})$ with $r_1 \in R_1, (s_2, r_2) \in R_2, \ldots, (s_{i-1}, r_{i-1}) \in R_{i-1}$ and either $r = a_j$ with $j \in \{1, \ldots, k\}$ or $r = f(v_1, \ldots, v_t)$ for $v_1, \ldots, v_t$ representable with respect to $R_1, \ldots, R_n$. Hence we have a term of length at most $3n-2$ to check that s is generated by $R_1, R_2, \ldots, R_n$ and a term whose length is at most linear in tn to verify that r is generated by $R_1, R_2, \ldots, R_n$.

A canonical representation of B comprises at most $|A| + (n-1)|A|^2$ elements. Given the terms above, we can verify that all elements in $R_1, R_2, \ldots, R_n$ are in B in time polynomial in n. Since every element in a canonical representation is obtained from $a_1, \ldots, a_k$ in finitely many steps, this is true even if $\mathbf{A}$ has infinitely many basic operations.

Note that we cannot check that $R_1, R_2, \ldots, R_n$ generates all of B in polynomial time. However, if $b \in B$, then this can be verified in time polynomial in n given the witnesses for $R_1 \subseteq B$ and $R_2, \ldots, R_n \subseteq B^2$ and the term $b = m(\cdots m(r_1, s_2, r_2), \ldots, s_n, r_n)$ with $r_1 \in R_1, (s_2, r_2) \in R_2, \ldots, (s_n, r_n) \in R_n$. Hence we have proved Theorem 1.1. □

We continue with some observations on the structure of term functions. For a fixed signature S and variables x_i $(i \in \mathbb{N})$ we define the *depth* $d(f)$ of a term f recursively:

(1) If $f = s(t_1, \ldots, t_k)$ for $s \in S$ of arity k and terms $t_1, \ldots, t_k$, then $d(f) = \max\{d(t_i) : i \in \{1, \ldots, k\}\} + 1$.
(2) $d(x_i) = 0$ for $i \in \mathbb{N}$.

So we may consider the depth of a term f as the height of the tree that represents f.

Given a finite algebra $\mathbf{A}$ and $a_1, \ldots, a_k \in A^n$ we may enumerate all elements in $\langle a_1, \ldots, a_k \rangle$ by starting with the set $B := \{a_1, \ldots, a_k\}$ and iteratively closing it under the basic operations of $\mathbf{A}$. In the case of a Mal'cev algebra we can now state an *a priori* bound on the number of iterations needed for this straightforward closure algorithm.

Theorem 2.2. *Let* $\mathbf{A}$ *be a finite algebra with a Mal'cev operation* m *among its basic operations, let* $k, n \in \mathbb{N}$, *and let* $a_1, \ldots, a_k \in A^n$.

Then for every $b \in \langle a_1, \ldots, a_k \rangle$ *there exists a term* f *in the signature of* $\mathbf{A}$ *such that* $d(f) \leq |A|^2 n^2 - (|A|^2 - |A| - 1)n - 1$ *and the operation* $\bar{f}$ *induced by* f *on* A *satisfies* $\bar{f}(a_1, \ldots, a_k) = b$.

Proof. From the proof of Theorem 1.1 we see that CanonicalRepresentation yields a canonical representation $R_1, \ldots, R_n$ of $\langle a_1, \ldots, a_k \rangle$ with the following property: All $r \in R_1$ and all r, s with (r, s) in some R_i for $i \in \{2, \cdots, n\}$ can be represented by a term with depth at most n in the previous generators. Since $\sum_{i=1}^{n} |R_i| \leq |A| + (n-1)|A|^2$, every element in $R_1, \ldots, R_n$ can be written as term with depth at

most $n(|A|+(n-1)|A|^2)$ in $a_1, \ldots, a_k$. Finally every $b \in \langle a_1, \ldots, a_k \rangle$ is representable with respect to $R_1, \ldots, R_n$ by a term of depth $n-1$. The result follows. □

Since an algebra $\mathbf{A}$ has at most $|A|^{|A|^k}$ many k-ary term operations, we have the trivial bound that every term operation can be represented by a term of depth at most $|A|^{|A|^k}$. For Mal'cev algebras we obtain the following improvement.

Corollary 2.3. *Let $\mathbf{A}$ be a finite algebra with a Mal'cev operation m among its basic operations, and let $k \in \mathbb{N}$. Then every k-ary term function f on $\mathbf{A}$ can be represented by a term of depth at most $|A|^{2k+2} - (|A|^2 - |A| - 1)|A|^k - 1$.*

Proof. This follows from Theorem 2.2 by considering the term function f as an element in the subuniverse of $\mathbf{A}^{A^k}$ that is generated by the k-ary projections. □

3. Nilpotent Mal'cev Algebras

In this section we will prove Theorem 1.2 for expansions $\mathbf{A}$ of nilpotent algebras using a specialization of the representation results and algorithms from Sec. 2 as well as techniques from Freese and McKenzie's finite basis result for nilpotent algebras (see [6, Chap. 14]).

In the following four subsections we address these subproblems:

(1) Defining an appropriate "canonical" generator set (which we will call a group representation) for $B \leq \mathbf{A}^n$ (Sec. 3.1).
(2) Closing the set of representable elements under the Mal'cev operation m of $\mathbf{A}$ (Sec. 3.2).
(3) Closing the set of representable elements under other basic operations of $\mathbf{A}$ (Sec. 3.3).
(4) Formulating a polynomial-time algorithm to obtain a group representation for $B \leq \mathbf{A}^n$ (Sec. 3.4).

3.1. *The group representation*

Let $\mathbf{A}$ be an algebra with Mal'cev term operation m, let $n \in \mathbb{N}$, let $B \leq \mathbf{A}^n$, and let $z \in B$. Consider

$$B = B_0 \supseteq B_1 \supseteq \cdots \supseteq B_n = \{z\},$$

where $B_i = \{a \in B : a(1) = z(1), \ldots, a(i) = z(i)\}$[a] for all $i \in \{1, \ldots, n\}$. For $i \in \{1, \ldots, n\}$ let $T_i \subseteq B_{i-1}$ such that

(1) $z \in T_i$,
(2) $\forall\, a \in B_{i-1}\, \exists !\, t \in T_i : a(i) = t(i)$.

[a]Here we denote tuples in A^n as functions $\{1, \ldots, n\} \to A$ to avoid excessive indices in the following.

Then we call $T_1, \dots, T_n$ a *group representation* of B with respect to z (The name is motivated by the following connection with groups; see also Lemma 3.1).

Suppose that we have group operations $+, -$ and 0 on A such that $m(x_1, x_2, x_3) = x_1 - x_2 + x_3$. Let $n \in \mathbb{N}$, and let $z = (0, \dots, 0)$ be the zero vector in A^n. For $B \leq \mathbf{A}^n$ with $z \in B$, the sets $B_0, \dots, B_n$ above form subgroups of $\langle A, +, -, 0\rangle$. Assume $T_1, \dots, T_n$ is a group representation of B with respect to $(0, \dots, 0)$. This is equivalent to saying that T_i is a transversal through the cosets of B_i in B_{i-1} for every $i \in \{1, \dots, n\}$. Now it is immediate that

$$B = T_1 + \cdots + T_n.$$

For arbitrary Mal'cev algebras we do not have a representation like this but are required to use the slightly more complicated notion of forks and canonical representations as in Sec. 2. However for nilpotent Mal'cev algebras we have the following result, which is quite similar to the group case.

Lemma 3.1. *Let* $\mathbf{A}$ *be a nilpotent algebra with Mal'cev operation* m *and a central series* $1_A = \alpha_0 > \alpha_1 > \cdots > \alpha_q = 0_A$ *for some* $q \in \mathbb{N}$. *Let* $n \in \mathbb{N}$, $B \leq \mathbf{A}^n$, $z \in B$, *and let* $T_1, \dots, T_n$ *be a group representation of* B. *Denoting* $x + y := m(x, z, y)$ *we*

Algorithm 3 IsGroupRepresentable$(m, z, (T_1, \dots, T_n), a)$

Input: m a Mal'cev operation on A such that $\langle A, m\rangle$ is nilpotent with central series of length q and $a, z \in A^n$
$T_1, \dots, T_n$ subsets of A^n that contain z such that
$\forall\, i \leq n \forall\, b \in T_i \forall\, j < i \colon b(j) = z(j)$
Output: true if $a \in T_1 + q \cdot T_2 + \cdots + q \cdot T_n$

```
if ∃ t_1 ∈ T_1 : a(1) = t_1(1) then
  b := t_1
else
  return (1, a)
end if
for i ∈ {2, ..., n} do
  for j ∈ {1, ..., q} do
    u := m(z, b, a)
    if ∃ t_ij ∈ T_i : t_ij(i) = u(i) then
      b := m(b, z, t_ij)
    else
      return (i, u)
    end if
  end for
end for
return true
```

have

$$B = T_1 + \underbrace{T_2 + \cdots + T_2}_{q} + \cdots + \underbrace{T_n + \cdots + T_n}_{q},$$

where the sum is associated left to right.

Proof. Let $a \in B$. We claim that the algorithm IsGroupRepresentable returns true for the group representation $T_1, \ldots, T_n$ of B and that

$$a = t_1 + \sum_{j=1}^{q} t_{2j} + \cdots + \sum_{j=1}^{q} t_{nj} \tag{3.1}$$

with t_1 and t_{ij} as in the algorithm.

By assumption we have $t_1 \in T_1$ such that $t_1(1) = a(1)$. We show that

$$\forall\, i \in \{1, \ldots, n\} \forall\, j \in \{0, \ldots, q\} : \left(t_1 + \sum_{k=1}^{q} t_{2k} + \cdots + \sum_{k=1}^{j} t_{ik} \right)(i) \equiv_{\alpha_j} a(i). \tag{3.2}$$

We will use induction first on i and then on j. For $i = 1$ or $j = 0$ the assertion is clearly true. Assume the congruence in (3.2) is satisfied for some $i \in \{2, \ldots, n\}, j \in \{0, \ldots, q-1\}$. Let $b = t_1 + \sum_{k=1}^{q} t_{2k} + \cdots + \sum_{k=1}^{j} t_{ik}$. Then $u := m(z, b, a)$ is in B. Since a and b are equal at every index in $\{1, \ldots, i-1\}$, we have $u(1) = z(1), \ldots, u(i-1) = z(i-1)$. By definition of a group representation there exists $t_{i,j+1} \in T_i$ such that $u(i) = t_{i,j+1}(i)$. Now

$$\begin{aligned} (b + t_{i,j+1})(i) &= m(b(i), z(i), m(z(i), b(i), a(i))) \\ &\equiv a(i) \pmod{[1_A, \alpha_j]} \\ &\equiv a(i) \pmod{\alpha_{j+1}}. \end{aligned}$$

Here the first congruence follows from [10, Lemma 4.1] and second from the assumption that α_j induces a central congruence in $\mathbf{A}/\alpha_{j+1}$. This proves (3.2) and eventually (3.1). □

3.2. *Partial term functions*

Throughout this section we use the following conventions: p is a prime, $\underline{p} := \{0, \ldots, p-1\}$, A is set of p-power size, m is a Mal'cev operation on A such that $\mathbf{A}_0 := \langle A, m \rangle$ is nilpotent with central series $1_A = \alpha_0 \succ \alpha_1 \succ \cdots \succ \alpha_q = 0_A$ for some $q \in \mathbb{N}$. Here α_{i-1} covers α_i, that is, there are no congruences of $\mathbf{A}_0$ properly in between α_{i-1} and α_i. We fix $r \in \mathbb{N}$ and $S \subseteq A^r$. Our aim is to prove Corollary 3.4 which describes the r-ary term functions on $\mathbf{A}_0$ which reduce to projections on S.

As in [6, p. 124] we call the function $c \in \mathrm{Clo}_k(\mathbf{A}_0)$ a *commutator* if

$$\forall\, x_1, \dots, x_{k-1} \in A, \quad \forall\, x_k \in \{x_1, \dots, x_{k-1}\} \colon c(x_1, \dots, x_k) = x_k.$$

For notational convenience we introduce the set of r-ary essential commutators,

$$\mathrm{Com}_r(\mathbf{A}_0) := \left\{ g \in \mathrm{Clo}_r(\mathbf{A}_0) \colon \begin{array}{r} \exists\, S \subseteq \{1, \dots, r-1\}, \quad S \neq \emptyset, \\ \exists \text{ a commutator } c \in \mathrm{Clo}_{|S|+1}(\mathbf{A}_0), \\ \forall\, x \in A^r \colon g(x_1, \dots, x_r) = c(x_S, x_r) \end{array} \right\}.$$

For $i \in \{1, \dots, q\}$ let

$$C_i := \{c \in \mathrm{Com}_r(\mathbf{A}_0) : \forall\, x \in A^r \colon c(x) \equiv_{\alpha_{i-1}} x_r\}.$$

Let $r \in \mathbb{N}$, and let $p_r \colon A^r \to A,\ (x_1, \dots, x_r) \mapsto x_r$ denote the projection on the rth coordinate. For $a, b \colon A^r \to A$, we use the shorthand notation $a + b := m(a, p_r, b)$. We recall from [6] that every term function on a nilpotent algebra is a sum of commutators with respect to this addition.

Lemma 3.2 ([cf. 6, Lemma 14.6]). *Let $g, h \in \mathrm{Clo}_r(\mathbf{A}_0)$, and let $i \in \{1, \dots, q\}$.*

(1) *If $g \equiv_{\alpha_{i-1}} h$, then there exists $\mu_i \in \underline{p}^{C_i}$ such that $g \equiv_{\alpha_i} h + \sum_{c \in C_i} \mu_{i,c} c$ (with the sum associated left to right).*
(2) *There exist $\mu_1 \in \underline{p}^{C_1}, \dots, \mu_q \in \underline{p}^{C_q}$ such that*

$$g = \sum_{c \in C_1} \mu_{1,c} c + \cdots + \sum_{c \in C_q} \mu_{q,c} c$$

(with the sum associated left to right).

Proof. For proving (1) we adapt the proof of Lemma 14.6 in [6]. We use induction on the arity r. Since the only unary term operation of $\mathbf{A}_o$ is the identity map, the assertion holds for $r = 1$. So consider $r > 1$. By [6, Corollary 7.4] we have $e \in \mathrm{Clo}_r(\mathbf{A}_0)$ such that

$$g = h + e \quad \text{and} \quad e \equiv_{\alpha_{i-1}} p_r.$$

We will show that e is congruent to a sum of operations in C_i modulo α_i. Let $e_o := e$, and for $j \in \{1, \dots, r-1\}$ define $e_j \in \mathrm{Clo}_r(\mathbf{A}_0)$ iteratively by

$$e_j(x_1, \dots, x_r) := m(e_{j-1}(x_1, \dots, x_r), e_{j-1}(x_1, \dots, x_{j-1}, x_r, x_{j+1}, \dots, x_r), x_r).$$

Then $e_j \equiv_{\alpha_{i-1}} p_r$ and $e_j(x_1, \dots, x_r) = x_r$ whenever $x_l = x_r$ for some $l \leq j$. In particular e_{r-1} is a commutator in C_i.

For an operation $v \colon A^r \to A$ define $v_{\alpha_i} \colon A^r \to A/\alpha_i$ by $v_{\alpha_i}(x) := v(x)/\alpha_i$. Since α_{i-1} covers α_i by assumption, $+$ induces an elementary abelian group operation on

$V := \{f_{\alpha_i} : f \in \mathrm{Clo}_r(\mathbf{A}_0), f \equiv_{\alpha_{i-1}} p_r\}$. For $S \subseteq \{1, \ldots, r-1\}$ define $\delta_S \colon A^r \to A^r$ by

$$(\delta_S(x))_j := \begin{cases} x_r & \text{if } j \in S, \\ x_j & \text{else.} \end{cases}$$

From the definitions it is straightforward that

$$e_{r-1} \equiv_{\alpha_i} \sum_{S \subseteq \{1,\ldots,r-1\}} (-1)^{|S|} e\delta_S$$

with the order of the sum irrelevant because $+$ is commutative on V. Since $e\delta_\emptyset = e$, we obtain

$$e \equiv_{\alpha_i} e_{r-1} - \sum_{\emptyset \neq S \subseteq \{1,\ldots,r-1\}} (-1)^{|S|} e\delta_S.$$

From the induction assumption for $r-1$ it follows that each $e\delta_S$ for $S \neq \emptyset$ is congruent modulo α_i to a sum of operations from C_i. Thus e is a sum of elements from C_i modulo α_i. The multiplicities of the summands may be chosen from $\underline{p} = \{0, \ldots, p-1\}$ since $\langle V, + \rangle$ is an elementary abelian p-group. This proves (1).

Item (2) follows from (1) and the fact that $g(z, \ldots, z) = z$ for all $z \in A$. □

To characterize the term functions that act as projections on S we need a slightly more complicated representation. Let $j \in \{1, \ldots, q\}$. Consider the following set of equations for $x \in S$:

$$\sum_{c \in C_j} \mu_c c(x) \equiv_{\alpha_j} x_r. \tag{3.3}$$

Since the functions in C_j commute with respect to $+$ modulo α_j and since α_{j-1} covers α_j, the solutions $\mu \in \mathbb{Z}^{C_j}$ of (3.3) form a vectorspace V modulo p. We have $v^{(1)}, \ldots, v^{(s)} \in \underline{p}^{C_j}$ which form a basis for V modulo p. Note that $s \leq |C_j|$. We define

$$D_{j,j} := \left\{ \sum_{c \in C_j} v_c^{(k)} c : k \in \{1, \ldots, s\} \right\}.$$

Next we define lists of functions $D_{i,j}$ for $1 \leq i < j \leq q$ iteratively with respect to j. Assume $D_{1,j-1}, \ldots, D_{j-1,j-1}$ are already defined and that

$$\forall\, 1 \leq i < j \forall\, d \in D_{i,j-1} \forall\, x \in S : d \equiv_{\alpha_{i-1}} p_r \quad \text{and} \quad d(x) \equiv_{\alpha_{j-1}} x_r. \tag{3.4}$$

This is certainly satisfied for the smallest value, $j = 2$. For $x \in S$ consider the set of equations

$$\sum_{d \in D_{i,j-1}} \mu_{i,d} d(x) + \cdots + \sum_{d \in D_{j-1,j-1}} \mu_{j-1,d} d(x) + \sum_{c \in C_j} \mu_{j,c} c(x) \equiv_{\alpha_j} x_r. \tag{3.5}$$

By (3.4) every summand on the left-hand side of every equation is congruent to x_r modulo α_{j-1}. So the solutions $(\mu_i, \dots, \mu_j) \in \mathbb{Z}^{D_{i,j-1}} \times \cdots \times \mathbb{Z}^{D_{j-1,j-1}} \times \mathbb{Z}^{C_j}$ of (3.5) form a vectorspace V' modulo p. Let $v^{(1)}, \dots, v^{(s')} \in \underline{p}^{D_{i,j-1}} \times \cdots \times \underline{p}^{D_{j-1,j-1}} \times \underline{p}^{C_j}$ form a basis for V' modulo p. Define

$$D_{i,j} := \left\{ \sum_{d \in D_{i,j-1}} v_d^{(k)} d(x) + \cdots + \sum_{d \in D_{j-1,j-1}} v_d^{(k)} d(x) + \sum_{c \in C_j} v_c^{(k)} c(x) : k \in \{1, \dots, s'\} \right\}.$$

Then $|D_{i,j}| \leq |D_{i,j-1}| + \cdots + |D_{j-1,j-1}| + |C_j|$ and for every $d \in D_{i,j}$ we have $d \equiv_{\alpha_{i-1}} p_r$ and for every $x \in S$: $d(x) \equiv_{\alpha_j} x_r$.

Lemma 3.3. *Let $1 \leq i \leq j \leq q$, and let $g \in \mathrm{Clo}_r(\mathbf{A}_0)$ such that $g \equiv_{\alpha_{i-1}} p_r$ and $g(x) \equiv_{\alpha_j} x_r$ for all $x \in S$.*

Then there exist $\lambda_i \in \underline{p}^{D_{i,j}}, \dots, \lambda_j \in \underline{p}^{D_{j,j}}$ such that

$$g \equiv_{\alpha_j} \sum_{d \in D_{i,j}} \lambda_{i,d} d + \cdots + \sum_{d \in D_{j,j}} \lambda_{j,d} d$$

(*with the sum associated left to right*).

Proof. We use induction on $j - i$. For $i = j$ there exists $\mu_i \in \underline{p}^{C_i}$ such that $g \equiv_{\alpha_i} \sum_{c \in C_i} \mu_{i,c} c$ by Lemma 3.2(1). Now the assertion follows from the definition of $D_{i,i}$ and the fact that the functions in C_i commute with respect to $+$ modulo α_i.

So assume $i < j$ in the following. First we claim that

$$\exists\, \lambda_i \in \underline{p}^{D_{i,j}} : g \equiv_{\alpha_i} \sum_{d \in D_{i,j}} \lambda_{i,d} d. \tag{3.6}$$

Note that trivially $g(x) \equiv_{\alpha_{j-1}} x_r$ for all $x \in S$. So by the induction assumption we have $\mu_i \in \underline{p}^{D_{i,j-1}}, \dots, \mu_{j-1} \in \underline{p}^{D_{j-1,j-1}}$ such that

$$g \equiv_{\alpha_{j-1}} \sum_{d \in D_{i,j-1}} \mu_{i,d} d + \cdots + \sum_{d \in D_{j-1,j-1}} \mu_{j-1,d} d.$$

By Lemma 3.2(1) there exists $\mu_j \in \underline{p}^{C_j}$ such that

$$g \equiv_{\alpha_j} \sum_{d \in D_{i,j-1}} \mu_{i,d} d + \cdots + \sum_{d \in D_{j-1,j-1}} \mu_{j-1,d} d + \sum_{c \in C_j} \mu_{j,c} c.$$

Now (3.6) follows from the definition of $D_{i,j}$ since the operations in $D_{i,j-1} \cup \cdots \cup D_{j-1,j-1} \cup C_j$ commute with respect to $+$ modulo α_i.

Let $\lambda_i \in \underline{p}^{D_{i,j}}$ as in (3.6). By [6, Lemma 7.3] there exists $g' \in \mathrm{Clo}_r(\mathbf{A}_0)$ such that

$$g = \sum_{d \in D_{i,j}} \lambda_{i,d} d + g'. \tag{3.7}$$

Further by [6, Corollary 7.4] $g' \equiv_{\alpha_i} p_r$ and $g'(x) \equiv_{\alpha_j} x_r$ for all $x \in S$. Using the induction assumption on g', we have $\lambda_{i+1} \in \underline{p}^{D_{i+1,j}}, \ldots, \lambda_j \in \underline{p}^{D_{j,j}}$ such that

$$g' \equiv_{\alpha_j} \sum_{d \in D_{i+1,j}} \lambda_{i+1,d} d + \cdots + \sum_{d \in D_{j,j}} \lambda_{j,d} d.$$

Together with (3.7) this yields the result. □

From Lemma 3.3 we immediately obtain the following.

Corollary 3.4. *Let $g \in \mathrm{Clo}_r(\mathbf{A}_0)$ such that $g(x) = x_r$ for all $x \in S$. Then there exist $\lambda_1 \in \underline{p}^{D_{1,q}}, \ldots, \lambda_q \in \underline{p}^{D_{q,q}}$ such that*

$$g = \sum_{d \in D_{1,q}} \lambda_{1,d} d + \cdots + \sum_{d \in D_{q,q}} \lambda_{q,d} d$$

(*with the sum associated left to right*).

If $\mathbf{A}$ is a nilpotent Mal'cev algebra of prime power order and finite signature, then there exists an integer D such that every commutator of arity greater than D is the projection on the last argument by [6, Theorem 14.16]. From this the following bounds are straightforward.

Lemma 3.5. *There exists $D \in \mathbb{N}$ such that for all $r \in \mathbb{N}$ and $c := |\mathrm{Com}_r(\mathbf{A}_0)|$ the following hold*:

(1) *If $r \geq D$, then $c \leq \binom{r-1}{D-1} \cdot |\mathrm{Clo}_D(\mathbf{A}_0)|$; otherwise $c \leq |\mathrm{Clo}_D(\mathbf{A}_0)|$.*
(2) *$|D_{i,j}| \leq 2^{j-i} c$ for all $1 \leq i \leq j \leq q$.*

Proof. We prove (2) by induction on $j - i$. For $j = i$ the definition of $D_{j,j}$ yields $|D_{j,j}| \leq |C_j| \leq c$. For $j > i$ we have

$$\begin{aligned} |D_{i,j}| &\leq |D_{i,j-1}| + \cdots + |D_{j-1,j-1}| + |C_j| \\ &\leq 2^{j-i-1} c + \cdots + 2^0 c + c \\ &= 2^{j-i} c. \end{aligned}$$

□

Lemma 3.6. *Let $f : S \to A$. The algorithm TermExtension determines $g \in \mathrm{Clo}_r(\mathbf{A}_0)$ with $g|_S = f$ if such a function g exists, and returns fail otherwise. The running time of TermExtension is bound by a polynomial in $|S|$ and r.*

Algorithm 4 TermExtension(m, f)

Input: m a Mal'cev operation on a set A of prime power order
$f\colon S \to A$ where $S \subseteq A^r$
Output: $g \in \mathrm{Clo}_r(\langle A, m\rangle)$ with $g|_S = f$ if existent; fail otherwise
Let $1_A = \alpha_0 \succ \alpha_1 \succ \cdots \succ \alpha_q = 0_A$ be a central series for $\langle A, m\rangle$.
For $1 \le i \le j \le q$ determine C_i and D_{ij} for S by solving (3.5).
$f_1 := f, g_0 := p_r$
for $i \in \{1, \dots, q\}$ **do**
For $x \in S$ solve the following system of linear equations in $\mathbb{Z}_p$:

$$f_i(x) \equiv_{\alpha_i} \sum_{d \in D_{1,i-1}} \mu_{1,d} d(x) + \cdots + \sum_{d \in D_{i-1,i-1}} \mu_{i-1,d} d(x) + \sum_{c \in C_i} \mu_{i,c} c(x)$$

if $\mu_1, \dots, \mu_i$ is a solution **then**
$g_i := g_{i-1} + \sum_{d \in D_{1,i-1}} \mu_{1,d} d + \cdots + \sum_{d \in D_{i-1,i-1}} \mu_{i-1,d} d + \sum_{c \in C_i} \mu_{i,c} c$
Let $f_{i+1}\colon S \to A$ with $f(x) = m(g_i(x), x_r, f_{i+1}(x))$ for all $x \in S$.
else if no solution exists **then**
return fail
end if
end for
return g_q

Proof. *Correctness*: First assume that f is the restriction of a term function on $\mathbf{A}_0$. We claim that

$$\forall\, i \in \{0, \dots, q\} \forall\, x \in S\colon f(x) \equiv_{\alpha_i} g_i(x). \tag{3.8}$$

For $i = 0$ this is trivially true. Assume the assertion holds for $i - 1 \ge 0$. By [6, Lemma 7.3] the function $f_i\colon S \to A$ such that $f(x) = m(g_{i-1}(x), x_r, f_i(x))$ for all $x \in S$ is the restriction of some term function g'. Moreover by [6, Corollary 7.4] and the induction assumption we have $g'(x) \equiv_{\alpha_{i-1}} x_r$ for all $x \in S$. By the Lemmas 3.2 and 3.3 there exist $\mu_1 \in \underline{p}^{D_{1,i-1}}, \dots, \mu_{i-1} \in \underline{p}^{D_{i-1,i-1}}, \mu_i \in \underline{p}^{C_i}$ such that

$$g' \equiv_{\alpha_i} \sum_{d \in D_{1,i-1}} \mu_{1,d} d + \cdots + \sum_{d \in D_{i-1,i-1}} \mu_{i-1,d} d + \sum_{c \in C_i} \mu_{i,c} c.$$

Now

$$f_i(x) \equiv_{\alpha_i} \sum_{d \in D_{1,i-1}} \mu_{1,d} d(x) + \cdots + \sum_{d \in D_{i-1,i-1}} \mu_{i-1,d} d(x) + \sum_{c \in C_i} \mu_{i,c} c(x)$$

implies $f(x) \equiv_{\alpha_i} g_i(x)$ for all $x \in S$. Hence (3.8) is proved and $f = g_q|_S$.

The same reasoning shows that if TermExtension returns the term function g_q, then (3.8) holds. Consequently f is the restriction of a term function.

Complexity: To determine $C_1, \ldots, C_q$ we first find D such that every commutator of arity greater than D is a projection. Note that D is an invariant of $\mathbf{A}_0$ that is independent of $|S|$ and r. Given all commutators of arity at most D, it is then straightforward to list $\mathrm{Com}_r(\mathbf{A})$ and $C_1, \ldots, C_q$. Since $|\mathrm{Com}_r(\mathbf{A})|$ is bound by a polynomial in the arity r by Lemma 3.5, this can be done in polynomial time.

Let $1 \leq i \leq j \leq q-1$. Now $D_{i,j}$ is defined from the solutions of (3.5), a system of $|S|$ linear equations over $\mathbb{Z}_p$ with the number of variables bound by a polynomial in r by Lemma 3.5. A system of linear equations over a field can be solved in a number of steps that is polynomial in its dimension. Hence solutions for (3.5) and consequently $D_{i,j}$ can be determined in time polynomial in $|S|$ and r. We note that we must not represent the functions in $D_{i,j}$ by their graphs which are elements of A^{r+1} and whose size is exponential in r. Instead we consider the elements of $D_{i,j}$ as terms in $+$ and $\mathrm{Com}_r(\langle A, m\rangle)$. By Lemma 3.5 the length of this representation is bounded by a polynomial in r.

Similarly the term representation of g_i for $1 \leq i \leq q$ is found in time polynomial in $|S|$ and r. □

TermExtension is a polynomial time algorithm to solve the subpower membership problem for $\mathbf{A}_0$. It can also be used to build a group representation for some $B \leq \mathbf{A}_0^n$. The algorithm IsGroupRepresentation will be used in Sec. 3.4 to obtain a group representation in an even more general setting.

Algorithm 5 IsGroupRepresentation$(m, z, (T_1, \ldots, T_n))$

Input: m a Mal'cev operation on a set A of prime power size,
$\{z\} \subseteq T_1, \ldots, T_n \subseteq A^n$,
$\forall\, i \in \{1, \ldots, n\} \forall\, s, t \in T_i \colon t(1) = z(1), \ldots, t(i-1) = z(i-1)$, and $t(i) \neq s(i)$
Output: true if $T_1, \ldots, T_n$ is a group representation with respect to z for $\langle \bigcup_{i=1}^n T_i \rangle \leq \langle A, m\rangle^n$

```
Let T := ⋃_{i=1}^n T_i, say T = {t_1, ..., t_{r-1}, z}.
S := ((t_1(1), ..., t_{r-1}(1), z(1)), ..., (t_1(n), ..., t_{r-1}(n), z(n)))
for i ∈ {1, ..., n} do
  for a ∈ A such that ∄ t ∈ T_i : t(i) = a do
    Define f : {S(1), ..., S(i)} → A by f(S(j)) := z_j for 1 ≤ j ≤ i − 1,
    f(S(i)) := a
    if TermExtension(m, f) ≠ fail then
      g := TermExtension(m, f)
      return (i, (g(S(1)), ..., g(S(n))))
    end if
  end for
end for
return true
```

Lemma 3.7. *Let* $\{z\} \subseteq T_1, \ldots, T_n \subseteq A^n$, *and let* $B := \langle \bigcup_{i=1}^n T_i \rangle \leq \langle A, m \rangle^n$. *Assume that* $\forall\, i \in \{1, \ldots, n\} \forall\, s, t \in T_i \colon t(1) = z(1), \ldots, t(i-1) = z(i-1)$, *and* $t(i) \neq s(i)$. *The algorithm IsGroupRepresentation returns true if* $T_1, \ldots, T_n$ *is a group representation with respect to* z *for* B; *and it returns* $(i, r) \in \{1, \ldots, n\} \times B$ *such that* $r(1) = z(1), \ldots, r(i-1) = z(i-1)$ *and* $\forall\, t \in T_i \colon t(i) \neq r(i)$ *otherwise.*

The running time of IsGroupRepresentation is bound by a polynomial in n *and* $|\bigcup_{i=1}^n T_i|$.

Proof. Straightforward. □

3.3. *Functions of finite degree*

When searching for a group representation for an algebra $\mathbf{A}$ we will apply operations f on A to sums as in Lemma 3.1 to check for closure. Assume for a moment that $+$ is an actual group operation on A and that f is linear. By $f(\sum_{i=1}^n x_i) = \sum_{i=1}^n f(x_i)$ verifying $f(T_1 + \cdots + T_n) \subseteq T_1 + \cdots + T_n$ can be reduced to checking $f(T_i) \subseteq T_1 + \cdots + T_n$ for all $i \in \{1, \ldots, n\}$ and the closure of $T_1 + \cdots + T_n$ with respect to $+$. Even for nonlinear functions, $f(\sum_{i=1}^n x_i)$ may be split into a sum of functions applied to shorter subsums of some fixed length. For example consider the following equation for taking squares on a ring:

$$\left(\sum_{i=1}^n x_i\right)^2 = \sum_{1 \leq i < j \leq n} (x_i + x_j)^2 - (n-2) \sum_{i=1}^n x_i^2.$$

We will show that such a weak kind of linearity holds for every function on a p-group (Corollary 3.10). This follows from an even more general result for nilpotent Mal'cev algebras of prime power order which we will state as Lemma 3.9.

Let m be a Mal'cev operation on the set A, and let $\mathbf{A}_0 := \langle A, m \rangle$. Let f be an l-ary operation on A. We define the *degree* of f with respect to $\mathbf{A}_0$ as the smallest $d \in \mathbb{N}_0$ for which there exists $g \in \mathrm{Clo}_{2^{d+1}}(\mathbf{A}_0)$ such that for all $x_1, \ldots, x_{d+1}, z \in A^l$:

$$f\left(\sum_{i=1}^{d+1} x_i\right) = g\left(\left(f\left(\sum_{i \in S} x_i\right)\right)_{S \subsetneq \{1, \ldots, d+1\}}, z_l\right). \tag{3.9}$$

Here all sums are taken with respect to $a +_z b := m(a, z, b)$ for $a, b \in A^l$ and associated left to right, i.e.

$$\sum_{i=1}^{d+1} x_i = m(\ldots, m(m(x_1, z, x_2), z, x_3), \ldots, x_{d+1}).$$

The sum over the empty index set is understood as $\sum_{i \in \emptyset} x_i = z$. We consider an arbitrary but fixed linear order on the proper subsets S of $\{1, \ldots, d+1\}$. Now $(f(\sum_{i \in S} x_i))_{S \subsetneq \{1, \ldots, d+1\}}$ denotes a tuple of length $2^{d+1} - 1$ over A whose entries are ordered with respect to this linear order on subsets. Then we apply g to the

concatenation of that tuple followed by z_l, the last entry of $z \in A^l$, to obtain the right-hand side of (3.9).

If no $d \in \mathbb{N}_0$ (and $g \in \mathrm{Clo}(\mathbf{A}_0)$) exists for which (3.9) holds, we say that f has *infinite degree with respect to* $\mathbf{A}_0$.

For an operation f of finite degree d, f applied to a sum of arbitrary length can be expressed by applications of f to sums of length at most d as follows:

Lemma 3.8. *Let A be a set with a Mal'cev operation m, let f be an l-ary operation on A. If f has degree d with respect to $\mathbf{A}_0 := \langle A, m\rangle$, then for all $n \in \mathbb{N}$ there exist $r \in \mathbb{N}$, subsets $S_1, \dots, S_r$ of $\{1, \dots, n\}$ with $|S_1| \leq d, \dots, |S_r| \leq d$ and $g \in \mathrm{Clo}_{r+1}(\mathbf{A}_0)$ such that for all $x_1, \dots, x_n, z \in A^l$:*

$$f\left(\sum_{i=1}^{n} x_i\right) = g\left(f\left(\sum_{i\in S_1} x_i\right), \dots, f\left(\sum_{i\in S_r} x_i\right), z_l\right).$$

(*All sums are taken with respect to $+_z$ and associated left to right.*)

Proof. Straightforward from the definition of degree (3.9). □

At first sight, having finite degree seems to be a very strong condition. Still for certain Mal'cev algebras there exists a finite constant that bounds the degree of any operation.

Lemma 3.9. *Let A be a set of prime power size with a Mal'cev operation m such that $\mathbf{A}_0 := \langle A, m\rangle$ is nilpotent. Then there exists $d \in \mathbb{N}_0$ such that every finitary operation on A has degree at most d with respect to $\mathbf{A}_0$.*

Proof. We fix a central series $1_A = \alpha_0 \succ \alpha_1 \succ \cdots \succ \alpha_q = 0_A$ for some $q \in \mathbb{N}_0$ for $\mathbf{A}_o$. Let $o \in A$ be arbitrary. For $a \in A$ define $\rho_{o,a} \colon A \to A,\ x \mapsto m(x, o, a)$. Since $\mathbf{A}_0$ is nilpotent, every function $\rho_{o,a}$ is bijective on A by [6, Corollary 7.4]. Let $R_o(A)$ denote the subgroup of the full symmetric group on A that is generated by $\{\rho_{o,a} : a \in A\}$. Note that $\rho_{o,o} = 1$ is the identity in $R_o(A)$. If the order of A is a power of the prime p, then $R_o(A)$ is a p-group by [6, Lemma 14.8]. The augmentation ideal of the group ring $\mathbb{Z}_p(R_o(A))$ is equal to its Jacobson radical [4, Theorem 5.24], hence nilpotent by finiteness. Thus there exists $e_o \in \mathbb{N}$ such that for all $g_1, \dots, g_{e_o} \in R_o(A)$ we have $(1 - g_1) \cdots (1 - g_{e_o}) = 0$ in $\mathbb{Z}_p(R_o(A))$. Let e be the greatest element in $\{e_o : o \in A\}$. We note that q and e depend only on $\mathbf{A}_0$.

In preparation for proving the full result, we first consider certain operations on A as elements in a module over some group ring. For this, fix $k \in \{0, \dots, q-1\}$, $l \in \mathbb{N}$, $z \in A^l$, and write $\beta := \alpha_{k+1}$. For $v \colon A^l \to z_l/\alpha_k$ we define $v_\beta \colon A^l \to A/\beta, x \mapsto v(x)/\beta$. Since α_k covers β, $x +_{z_l} y := m(x, z_l, y)$ induces an elementary abelian group operation on $\{x/\beta : x \equiv_{\alpha_k} z_l\}$. Consequently $V := \{v_\beta : v \in (z_l/\alpha_k)^{A^l}\}$ forms a vector space over the field $\mathbb{Z}_p$. The addition of functions in V is pointwise, and the zero vector in V is induced by the constant function that maps everything to z_l/β.

Next we let the group $R_{z_1}(A) \times \cdots \times R_{z_l}(A)$ act on V. For $(g_1, \ldots, g_l) \in R_{z_1}(A) \times \cdots \times R_{z_l}(A)$ and $v\colon A^l \to A$ define $v * (g_1, \ldots, g_l)\colon A^l \to A$, $(x_1, \ldots, x_l) \mapsto v(g_1^{-1}(x_1), \ldots, g_l^{-1}(x_l))$. This induces a group action on V. Hence V forms a module for the group ring $\mathbb{Z}_p(R_{z_1}(A) \times \cdots \times R_{z_l}(A))$.

For $b := (b_1, \ldots, b_l)$ in A^l, define $\tau_b := (\rho_{z_1,b_1}, \ldots, \rho_{z_l,b_l})$. Then τ_z is the identity in $R_{z_1}(A) \times \cdots \times R_{z_l}(A)$. Let $y_1, \ldots, y_e \in A^l$. Since, for every $i \in \{1, \ldots, l\}$, the augmentation ideal I of $\mathbb{Z}_p(R_{z_i}(A))$ satisfies $I^e = 0$, we have $(\tau_z - \tau_{y_1}^{-1}) \cdots (\tau_z - \tau_{y_e}^{-1}) = 0$ in $\mathbb{Z}_p(R_{z_1}(A) \times \cdots \times R_{z_l}(A))$. Let $v\colon A^l \to z_l/\alpha_k$. Then we obtain

$$v * (\tau_z - \tau_{y_1}^{-1}) \cdots (\tau_z - \tau_{y_e}^{-1}) \equiv_\beta z_l.$$

Hence for all $x \in A^l$ we have

$$\sum_{T \subseteq \{1,\ldots,e\}} (-1)^{|T|} v\left(x +_z \sum_{i \in T} y_i\right) \equiv_\beta z_l.$$

Note that the order of the outer sum may be chosen arbitrarily since v_β is an element of the abelian group $\langle V, +_{z_l} \rangle$. Setting $x = z$, we finally obtain for all $y_1, \ldots, y_e, z \in A^l$ and for all $v\colon A^l \to z_l/\alpha_k$:

$$v\left(\sum_{i=1}^{e} y_i\right) \equiv_\beta \sum_{T \subsetneq \{1,\ldots,e\}} (-1)^{|T|+e+1} v\left(\sum_{i \in T} y_i\right). \tag{3.10}$$

Now consider an arbitrary l-ary operation f on A. We claim that for every $k \in \{0, \ldots, q\}$ there exists $g \in \mathrm{Clo}_{2^{k(e-1)+1}}(\mathbf{A}_0)$ such that for all $x_1, \ldots, x_{k(e-1)+1}, z \in A^l$:

$$f\left(\sum_{i=1}^{k(e-1)+1} x_i\right) \equiv_{\alpha_k} g\left(\left(f\left(\sum_{i \in S} x_i\right)\right)_{S \subsetneq \{1,\ldots,k(e-1)+1\}}, z_l\right). \tag{3.11}$$

Here all sums are taken with respect to $+_z$ and associated left to right. For the proof we use induction on k. For $k = 0$ we have $f(x_1) \equiv_{\alpha_0} z_l$, and the assertion is true. So assume we have (3.11) for k. Let $d' := k(e-1) + 1$. Since $\mathbf{A}_0$ is nilpotent, by [6, Lemma 7.3] there exists $r \in \mathrm{Clo}_3(\mathbf{A}_0)$ such that for all $a, b, c \in A$:

$$m(a, b, r(a, b, c)) = c. \tag{3.12}$$

Define an operation h of arity $l(d'+1)$ on A by

$$h(x_1, \ldots, x_{d'}, z) := r\left(g\left(\left(f\left(\sum_{i \in S} x_i\right)\right)_{S \subsetneq \{1,\ldots,d'\}}, z_l\right), z_l, f\left(\sum_{i=1}^{d'} x_i\right)\right).$$

Then (3.12) yields for all $x_1, \ldots, x_{d'}, z \in A^l$:

$$f\left(\sum_{i=1}^{d'} x_i\right) = g\left(\left(f\left(\sum_{i\in S} x_i\right)\right)_{S\subsetneq\{1,\ldots,d'\}}, z_l\right) +_{z_l} h(x_1, \ldots, x_{d'}, z). \tag{3.13}$$

Hence we have $g' \in \mathrm{Clo}_{2^{d'+e-1}}(\mathbf{A}_0)$ such that for all $x_1, \ldots, x_{d'+e-1}, z \in A^l$:

$$f\left(\sum_{i=1}^{d'+e-1} x_i\right) = g'\left(\left(f\left(\sum_{i\in S} x_i\right)\right)_{S\subsetneq\{1,\ldots,d'+e-1\}}, z_l\right) + {}_{z_l}h\left(x_1, \ldots, x_{d'-1}, \sum_{i=d'}^{d'+e-1} x_i, z\right). \tag{3.14}$$

For fixed $x_1, \ldots, x_{d'-1}, z \in A^l$ consider $v\colon A^l \to A$ defined by $v(x) := h(x_1, \ldots, x_{d'-1}, x, z)$. From (3.11), (3.13) and [6, Corollary 7.4] we have $h(x_1, \ldots, x_{d'}, z) \equiv_{\alpha_k} z_l$. Then $v(x) \equiv_{\alpha_k} z_l$ for all $x \in A^l$ and (3.10) yields

$$h\left(x_1, \ldots, x_{d'-1}, \sum_{i=d'}^{d'+e-1} x_i, z\right) \equiv_{\alpha_{k+1}} \sum_{T\subsetneq\{d',\ldots,d'+e-1\}} (-1)^{|T|+e+1} h\left(x_1, \ldots, x_{d'-1}, \sum_{i\in T} x_i, z\right) \tag{3.15}$$

for all $x_1, \ldots, x_{d'+e-1}, z \in A^l$. From the definition of h it follows that for every proper subset T of $\{d', \ldots, d'+e-1\}$ there exists $h_T \in \mathrm{Clo}_{2^{d'+e-1}}(\mathbf{A}_0)$ such that

$$h\left(x_1, \ldots, x_{d'-1}, \sum_{j\in T} x_j, z\right) = h_T\left(\left(f\left(\sum_{i\in S} x_i\right)\right)_{S\subsetneq\{1,\ldots,d'+e-1\}}, z_l\right).$$

Hence, by (3.15), we have $h' \in \mathrm{Clo}_{2^{d'+e-1}}(\mathbf{A}_0)$ such that

$$h\left(x_1, \ldots, x_{d'-1}, \sum_{i=d'}^{d'+e-1} x_i, z\right) \equiv_{\alpha_{k+1}} h'\left(\left(f\left(\sum_{i\in S} x_i\right)\right)_{S\subsetneq\{1,\ldots,d'+e-1\}}, z_l\right).$$

Together with (3.14) this yields the induction step for our claim (3.11). The assertion of the lemma follows for $k = q$. □

The specialization of the previous lemma for groups yields that every finitary function on a p-group satisfies some weak form of the homomorphism property.

Corollary 3.10. *Let* $\mathbf{A} := \langle A, +, -, 0\rangle$ *be a finite p-group, let* $l \in \mathbb{N}$, *and let* $f : A^l \to A$. *Assume that* $A = A_0 > A_1 > \cdots > A_q = 0$ *is a central series with* A_i/A_{i+1} *elementary abelian for all* $i \in \{0, \ldots, q-1\}$. *Let* $e \in \mathbb{N}$ *be such that the augmentation ideal* I *of the group ring* $\mathbb{Z}_p(\mathbf{A}^l)$ *satisfies* $I^e = 0$.

Then there exists $r \in \mathbb{N}$ *and proper subsets* $S_1, \ldots, S_r$ *of* $\{1, \ldots, q(e-1)+1\}$ *such that for all* $x_1, \ldots, x_{q(e-1)+1} \in A^l$:

$$f\left(\sum_{i=1}^{q(e-1)+1} x_i\right) = \sum_{j=1}^{r} f\left(\sum_{i\in S_j} x_i\right).$$

Proof. This is straightforward from the proof of Lemma 3.9 specialized for the Mal'cev operation $m(a, b, c) := a - b + c$ on A and $z := (0, \ldots, 0)$. □

3.4. *The algorithm*

Lemma 3.11. *Let* A *be a set of prime power size with Mal'cev operation* m *such that* $\langle A, m\rangle$ *is nilpotent, let* F *be a finite set of finitary operations on* A, *let* $k, n \in \mathbb{N}$ *and* $a_1, \ldots, a_k \in A^n$.

The algorithm GroupRepresentation returns a group representation of the subalgebra $B := \langle a_1, \ldots, a_k\rangle$ *of* $\langle A, m, F\rangle^n$ *with the running time bound by a polynomial in* k *and* n.

Proof. *Correctness*: Assume that $T_1, \ldots, T_n$ is returned. By construction we have for all $i \in \{1, \ldots, n\}$ that $z \in T_i$, $T_i \subseteq \{a \in B : a(1) = z(1), \ldots, a(i-1) = z(i-1)\}$, and for all $s, t \in T_i$: $s(i) = t(i) \Rightarrow s = t$.

Let C be the subalgebra of $\langle A, m\rangle^n$ that is generated by $T := \bigcup_{i=1}^{n} T_i$. Then $C \subseteq B$ and $T_1, \ldots, T_n$ is a group representation for C by Lemma 3.7. So we have $q \in \mathbb{N}$ such that

$$C = T_1 + \underbrace{T_2 + \cdots + T_2}_{q} + \cdots + \underbrace{T_n + \cdots + T_n}_{q} \tag{3.16}$$

by Lemma 3.1. Next let f be an l-ary operation in F and let $c_1, \ldots, c_l \in C$. By (3.16) we have $x_1, \ldots, x_{q(n-1)+1} \in \bigcup_{i=1}^{n} T_i^l$ such that $(c_1, \ldots, c_l) = \sum_{j=1}^{q(n-1)+1} x_j$. By Lemma 3.9 we have $d \in \mathbb{N}$ such that f has degree d. Hence, by Lemma 3.8 there exist $r \in \mathbb{N}$, $S_1, \ldots, S_r \subseteq \{1, \ldots, q(n-1)+1\}$ with $|S_1| \leq d, \ldots, |S_r| \leq d$, and $g \in \mathrm{Clo}_{r+1}(\langle A, m\rangle)$ such that

$$f\left(\sum_{j=1}^{q(n-1)+1} x_j\right) = g\left(f\left(\sum_{i\in S_1} x_i\right), \ldots, f\left(\sum_{i\in S_r} x_i\right), z\right).$$

Since S_j has size at most d, the algorithm guarantees that $f(\sum_{i\in S_j} x_i) \in C$ for all $j \in \{1, \ldots, r\}$. Since C is closed under the Mal'cev operation m and hence under

g, we obtain $f(\sum_{j=1}^{q(n-1)+1} x_j) \in C$. Hence C is also closed under all operations in F and $C = B$. Thus $T_1, \ldots, T_n$ is a group representation of B.

Running time: Since we are only interested in using GroupRepresentation for applying it to the subpower membership problem, we may consider the algebra

Algorithm 6 GroupRepresentation($\langle A, m, F\rangle, \{a_1, \ldots, a_k\}$)

Input: A of prime power size with Mal'cev operation m such that $\langle A, m\rangle$ is nilpotent
F a finite set of finitary operations on A
$a_1, \ldots, a_k \in A^n$
Output: group representation $T_1, \ldots, T_n$ for $\langle a_1, \ldots, a_k\rangle \leq \langle A, m, F\rangle^n$
$z := a_k$, $T_i := \{z\}$ for all $i \in \{1, \ldots, n\}$
for $a \in \{a_1, \ldots, a_k\}$ **do**
  while IsGroupRepresentable$(m, z, (T_1, \ldots, T_n), a) \neq$ true **do**
    if IsGroupRepresentable$(m, z, (T_1, \ldots, T_n), a) = (i, t)$ **then**
      Add t to T_i
    end if
  end while
end for
closed := false
while not closed **do**
  while IsGroupRepresentation$(m, z, (T_1, \ldots, T_n)) \neq$ true **do**
    if IsGroupRepresentation$(m, z, (T_1, \ldots, T_n)) = (i, t)$ **then**
      Add t to T_i
    end if
  end while
  closed := true
  for $f \in F$ **do**
    $l :=$ arity of f, $d :=$ degree of f
    for $r_1, \ldots, r_l$ sums of d elements in $\bigcup_{i=1}^{n} T_i$ **do**
      $a := f(r_1, \ldots, r_l)$
      while not IsGroupRepresentable$(m, z, (T_1, \ldots, T_n), a)$ **do**
        if IsGroupRepresentable$(m, z, (T_1, \ldots, T_n), a) = (i, t)$ **then**
          Add t to T_i
          closed := false
        end if
      end while
    end for
  end for
end while
return $(T_1, \ldots, T_n)$

$\langle A, m, F\rangle$ and all its invariants as constants. We analyze the running time of the algorithm only with respect to the parameters n and k.

If $T_1, \ldots, T_n$ is a group representation of B, then $T := \bigcup_{i=1}^{n} T_i$ has at most $n|A|$ elements. Hence the number of elements that are added to $T_1, \ldots, T_n$ is bound by a linear function in n, and so is the number of repetitions of all while-loops in the algorithm. The running time of IsGroupRepresentable is easily seen to be polynomial in n. So the for-loop over all generators $a_1, \ldots, a_k$ only takes time that is polynomial in n and k.

By Lemma 3.7 the running time of IsGroupRepresentation is bound by a polynomial in n and $|T| \leq n|A|$.

We note that the arity l and degree d of an operation $f \in F$ are invariants of the algebra $\langle A, m, F\rangle$, in particular, independent of n and k. Consequently the for-loop over all sums $r_1, \ldots, r_l$ of length d is completed in time polynomial in n. □

3.5. *The theorem and some consequences*

Proof of Theorem 1.2. The result follows from Lemma 3.11 since given a group representation for $B := \langle a_1, \ldots, a_k\rangle \leq \mathbf{A}^n$, the algorithm IsGroupRepresentable determines whether some b is in B in polynomial time in n. □

Proof of Corollary 1.3. If $\langle A, +\rangle$ is a p-group, then $\langle A, x - y + z\rangle$ is a nilpotent Mal'cev algebra of p-power order. So every expansion of $\langle A, +\rangle$ is term equivalent to an expansion of $\langle A, x - y + z\rangle$ and Theorem 1.2 applies. □

Proof of Corollary 1.4. Let $\langle A, +\rangle$ be a finite abelian group, and let F be a finite set of operations on A that are multilinear with respect to $+$. We consider the expanded group $\mathbf{A} := \langle A, +, F\rangle$. All rings, algebras over fields, vector spaces and Lie rings are of this form.

By multilinearity every $f \in F$ preserves the Sylow subgroups $A_1, \ldots, A_r$ of $\langle A, +\rangle$. It follows that $\mathbf{A}$ is a direct product of expanded groups $\mathbf{A}_1, \ldots, \mathbf{A}_r$ of pairwise coprime, prime power order. Now $b \in A^n$ is member of the subuniverse of $\mathbf{A}^n$ generated by some $a_1, \ldots, a_k \in A^n$ if and only if we have membership for every projection on $\mathbf{A}_1, \ldots, \mathbf{A}_r$. By Corollary 1.3 we have a polynomial algorithm for the subpower membership problem on $\mathbf{A}_i$ for every $i \in \{1, \ldots, k\}$. Hence subpower membership for $\mathbf{A}$ can be solved in polynomial time. □

Proof of Corollary 1.5. Let $\mathbf{A} := \langle A, \cdot, 1\rangle$ be a finite loop. Then $\mathbf{A}$ is a Mal'cev algebra by [8, Lemma 4.6]. In the theory of quasigroups, the center $Z(\mathbf{A})$ of $\mathbf{A}$ is defined as the set of elements x such that for all $y, z \in A$:

$$xy = yx, \quad (xy)z = x(yz), \quad (yx)z = y(xz), \quad (yz)x = y(zx)$$

(see [5]). Also $\mathbf{A}$ is called nilpotent if there exist $n \in \mathbb{N}$ such that $\mathbf{A}$ has a series

$$\{1\} = Z_0(\mathbf{A}) < Z_1(\mathbf{A}) < \cdots < Z_{n-1}(\mathbf{A}) < Z_n(\mathbf{A}) = A$$

with $Z_{i+1}(\mathbf{A})/Z_i(\mathbf{A}) = Z(\mathbf{A}/Z_i(\mathbf{A}))$ for all $i \in \{0, \ldots, n-1\}$.

It is straightforward to check that $\zeta := \{(a, b) \in \mathbf{A} : b = aZ(A)\}$ is a congruence of $\mathbf{A}$ and that ζ is central with respect to the term condition commutator of [6]. Hence a loop that is nilpotent in the sense of [5] is also nilpotent in the sense of [6]. (The converse is true as well.) Now the result follows from Theorem 1.2. □

Acknowledgments

The author acknowledges support from the Portuguese Project POCTI-ISFL-1-143 of CAUL financed by FCT and FEDER as well as from grant P24285 of the Austrian Science Fund FWF.

I want to thank Erhard Aichinger for discussions on the finite basis result for nilpotent algebras in [6, Chap. 14] and the anonymous referee for his diligent reading of the manuscript and for suggesting several improvements.

References

[1] E. Aichinger, Constantive Mal'cev clones on finite sets are finitely related, *Proc. Amer. Math. Soc.* **138**(10) (2010) 3501–3507.

[2] K. A. Baker and A. F. Pixley, Polynomial interpolation and the Chinese remainder theorem for algebraic systems, *Math. Z.* **143**(2) (1975) 165–174.

[3] A. Bulatov and V. Dalmau, A simple algorithm for Mal′tsev constraints, *SIAM J. Comput.* **36**(1) (2006) 16–27 (electronic).

[4] C. W. Curtis and I. Reiner, *Methods of Representation Theory: With Applications to Finite Groups and Orders*, Vol. I (John Wiley & Sons, New York, 1981).

[5] D. Daly and P. Vojtěchovský, Enumeration of nilpotent loops via cohomology, *J. Algebra* **322**(11) (2009) 4080–4098.

[6] R. Freese and R. McKenzie, *Commutator Theory for Congruence Modular Varieties, London Mathematical Society Lecture Note Series*, Vol. 125 (Cambridge University Press, 1987).

[7] M. Furst, J. Hopcroft and E. Luks, Polynomial-time algorithms for permutation groups, in 21*st Annual Symp. Foundations of Computer Science*, Syracuse, New York, October 13–15, 1980 (IEEE, New York, 1980), pp. 36–41.

[8] D. Hobby and R. McKenzie, *The Structure of Finite Algebras, Contemporary Mathematics*, Vol. 76 (American Mathematical Society, 1988).

[9] M. Kozik, A finite set of functions with an EXPTIME-complete composition problem, *Theoret. Comput. Sci.* **407**(1–3) (2008) 330–341.

[10] P. Mayr, Mal'cev algebras with supernilpotent centralizers, *Algebra Universalis* **65** (2011) 193–211.

[11] R. N. McKenzie, G. F. McNulty and W. F. Taylor, *Algebras, Lattices, Varieties*, Vol. I (Wadsworth & Brooks/Cole Advanced Books & Software, Monterey, California, 1987).

[12] E. L. Post, *The Two-Valued Iterative Systems of Mathematical Logic*, Annals of Mathematics Studies, Vol. 5 (Princeton University Press, Princeton, NJ, 1941).

[13] R. Willard, Four unsolved problems in congruence permutable varieties, Talk at International Conference on Order, Algebra, and Logics, Vanderbilt University, Nashville (June 12–16, 2007).