Programming Research Group

MAL'TSEV CONSTRAINTS ARE TRACTABLE

Bulatov A. Andrei

PRG-RR-02-05

Oxford University Computing Laboratory
Wolfson Building, Parks Road, Oxford OX1 3QD

Abstract

A wide variety of combinatorial problems can be represented in the form of Constraint Satisfaction Problems (CSP). The general CSP is known to be NP-complete, however, some restrictions on the possible form of constraints may lead to a tractable subclass. In [23] and then in [5, 3], it was shown that the complexity of subclasses of the constraint satisfaction problem depends only on certain algebraic invariance properties of constraints. The tractability of the problem class raised from a finite group has been proved in [12, 11]. In this paper we show that an arbitrary family of constraints invariant with respect to a Mal'tsev operation, that is a ternary operation $f(x, y, z)$ satisfying $f(y, y, x) = f(x, y, y) = x$ for any x, y, gives rise to a tractable problem class. Since any group constraint considered in [12, 11] is invariant with respect to a certain Mal'tsev operation, this result implies the mentioned result of [12, 11].

[0]This research has been carried out whilst visiting Oxford University Computing Laboratory in 2001.

1 Introduction

The Constraint Satisfaction Problem (CSP) provides a common framework for a wide variety of combinatorial problems from across all the computer science, including database theory [40, 28, 17], temporal and spatial reasoning [38], machine vision [34], belief maintenance [8], technical design [36], natural language comprehension [1], programming language analysis [35], etc. The CSP can be posed in many different forms, but the most concise one is probably the following: given a finite relational structure $\mathbb{A}$ and a relational structure $\mathbb{B}$ (not necessarily finite) decide whether there is a homomorphism from $\mathbb{A}$ to $\mathbb{B}$.

The general CSP is known to be NP-complete, and hence, intractable [30, 34]. However, certain restrictions on the possible type of the relational structures may affect the complexity of the corresponding problem class and give rise to a tractable subclass of the general CSP. There is, therefore, a fundamental research direction aiming to recognise tractable subclasses of the constraint satisfaction problem. A progress in this direction may help in speeding up of general superpolynomial algorithms, and provide efficient algorithms for those applications, which fall in one of the known tractable classes. This problem is also important from a theoretical perspective, as it helps to clarify the boundary between tractability and intractability in a wide range of combinatorial search problems.

There are two natural ways to restrict the general CSP corresponding to restrictions on the source and the target structure. In the first direction a remarkable progress has been recently achieved [16, 17, 18, 15]. In this paper we explore the second approach. The first result in this direction has been obtained by Schaefer [37] in the important case of Boolean CSP, that is when the target structure is 2-element. Schaefer established that for Boolean constraint satisfaction problems (which he called "Generalised Satisfiability Problems") there are exactly six different families of structures that give rise to a tractable problem class, and any problem involving structures not contained in these six families is NP-complete. This important result is known as Schaefer's Dichotomy Theorem for Boolean relations.

In the same paper [37], Schaefer raised the question of how this result could be generalised to larger structures (that is, sets with more than 2 elements). Feder and Vardi [12] identified two broad families of tractable structures that contain all of Schaefer's six classes. The first family, the class of problems of *bounded width*, is defined via *Datalog*, and each problem from this class can be solved by a simple algorithm that determines the *local consistency* of a problem instance. The second family, is defined to be the class of problems satisfying the property of the *ability to count*. A large class of problems with the ability to count consists of structures endowed with the operation of a certain group, and the relations of structures are defined via this operation (as subgroups, near-subgroups, and their cosets). Such group problem classes were proved to be tractable in [12] in the case of groups of odd order, and in [11] in the case of general finite groups.

Another approach to characterising tractable CSPs has been suggested by P.Jeavons and co-authors in [26, 23, 24, 6, 4]. This approach relies upon closure properties of relations with respect to certain operations. In [26, 23, 24, 25, 27], several types of operations have been identified which guarantee the tractability of the corresponding problem classes.

Subgroups and their cosets can be characterised making use of their invariance properties: a subset H of a group G is a coset of a subgroup if and only if H is invariant with respect to the operation $xy^{-1}z$ of the group. The group operation $xy^{-1}z$ provides a standard example of a *Mal'tsev* operation, that is a ternary operation $f(x, y, z)$ satisfying the conditions $f(x, y, y) = f(y, y, x) = x$. Moreover, in [11], near-subgroups and their cosets have been shown to be invariant with respect to a Mal'tsev operation which is not necessarily equals $xy^{-1}z$. Mal'tsev operations frequently appear in various areas of mathematics and computer science, because most of the 'classical' algebraic structures such as groups, quasigroups, rings, near-rings, fields, modules, vector spaces, modals etc. possess a Mal'tsev operation.

In this paper we show that every class of CSPs arising from a Mal'tsev operation is tractable. Moreover, there is an algorithm that, for every problem instance from such a class, finds a basis of the solution space such that each solution can be uniquely decomposed.

The paper is organised as follows. In Section 2, we give the definition of the CSP in the relational form convenient for proving, and describe how to restrict the general CSP using invariance properties of relations. Section 3 contains all required algebraic definitions and results, both general and concerning particularly Mal'tsev algebras. In Section 4, we sketch the algorithm solving Mal'tsev problems instances, and define a special form of a basis of the solution space. Finally, details, subroutines, proofs of soundness, and estimation of the time complexity are provided in Section 5.

2 Preliminaries

2.1 Constraint satisfaction problem

For a class of sets, $\mathcal{A} = \{A_i \mid i \in I\}$, a subset ϱ of $A_{i_1} \times \ldots \times A_{i_k}$ together with the list $(i_1, \ldots, i_k)$ is called a k-ary *relation over* $\mathcal{A}$ with *signature* $(i_1, \ldots, i_k)$. Elements of relations will be called *tuples* or *vectors*, and denoted in boldface. Then $\mathbf{a}[i]$ stands for the ith component of a tuple $\mathbf{a}$.

The 'constraint satisfaction problem' was introduced by Montanari in 1974 [34] and has been widely studied [9, 12, 32, 29, 30, 31, 39]. We define the constraint satisfaction problem in a slightly more general form.

Definition 1 *The* constraint satisfaction problem (CSP) *is the combinatorial decision problem with*

Instance: *a quadruple* $(V; \mathcal{A} = \{A_i: i \in I\}; \sigma; \mathcal{C})$ *where*

- V *is a set of* variables*;*
- $\mathcal{A}$ *is a collection of sets of* values *[*domains*] of a variables from* V*;*
- $\sigma: V \to I$ *is a* sort function*;*
- $\mathcal{C}$ *is a set of* constraints, $\{C_1, \ldots, C_q\}$.

  Each constraint $C_i \in \mathcal{C}$ *is a pair* $\langle s_i, \varrho_i \rangle$*, where*

- $s_i = (v_1, \ldots, v_{m_i})$ *is a tuple of variables of length* m_i, *called the* constraint scope*;*
- ρ_i *is an* m_i*-ary relation on* $\mathcal{A}$, $\varrho_i \subseteq A_{\sigma(v_1)} \times \ldots \times A_{\sigma(v_{m_i})}$, *called the* constraint relation*.*

Question: *does there exist a* solution, *i.e. a function* f, *from* V *to* $\bigcup_{i \in I} A_i$, *such that, for each variable* $v \in V$, $f(v) \in A_{\sigma(v)}$, *and for each constraint* $\langle s_i, \varrho_i \rangle \in \mathcal{C}$, *with* $s_i = (v_1, \ldots, v_{m_i})$, *the tuple* $(f(v_1), \ldots, f(v_{m_i}))$ *belongs to* ϱ_i*?*

Often all the variables can be supposed to have a common set of values. To distinguish this important particular case, we will refer to the general case as to the *multi-sorted* CSP, while to the case with a common domain as the *one-sorted* CSP. A one-sorted problem instance is then written as $(V, A, \mathcal{C})$ where A is the common domain and V, $\mathcal{C}$ are as before.

The constraint satisfaction problem is NP-complete in general, as was proved in [34] and will be seen from the examples below. However, some restrictions may affect the complexity of the problem. One way to restrict the problem is to impose some conditions on the possible form of constraint relations.

Let Γ be a set of relations over a collection of sets $\mathcal{A} = \{A_i : i \in I\}$. Then CSP($\Gamma$) denotes the subclass of the CSP defined by the property: for any instance $\mathcal{P} \in$ CSP(Γ), any variable has one of the sets from $\mathcal{A}$ as the domain, and every constraint relation of $\mathcal{P}$ belongs to Γ. If all A_i are finite then the size of a problem instance is the length of the encoding of all tuples in all constraints. The set Γ is said to be *tractable* if, for each finite subset $\Gamma' \subseteq \Gamma$, there exists a polynomial time algorithm solving any problem from CSP(Γ'); Γ is said to be *NP-complete* if CSP(Γ') is NP-complete for certain finite subset $\Gamma' \subseteq \Gamma$. If there is a uniform polynomial time algorithm that solves CSP(Γ), then Γ is said to be *globally tractable*.

Example 1 The binary disequality relation, denoted by $\neq_D$, is defined as

$$\neq_D = \{(d_1, d_2) \in D^2 : d_1 \neq d_2\}.$$

Note that CSP($\{\neq_D\}$) corresponds to the Graph $|D|$-Colorability problem [14]. Thus CSP($\neq_D$) is tractable when $|D| = 2$ and NP-complete when $|D| \geq 3$.

Example 2 An instance of Graph Unreachability consists of a graph $G = (V, E)$ and a pair of vertices, $v, w \in V$. The question is whether there is no path in G from v to w. This can be expressed as the CSP instance $(V, \{0, 1\}, C)$ where

$$\mathcal{C} = \{\langle e, \{(0,0),(1,1)\}\rangle : e \in E\} \cup \{\langle (v), \{(0)\}\rangle, \langle (w), \{(1)\}\rangle\}.$$

Thus, Graph Unreachabitity is equivalent to a subclass of CSP($\{\underline{0}_D, \{0\}, \{1\}\}$) where $\underline{0}_D$ stands for the equality relation on $D = \{0, 1\}$.

Example 3 A system of linear equations over a field F can be expressed as the CSP instance $(V, F, \mathcal{C})$ where V is the set of variables of the system, and each constraint $\langle s, \varrho \rangle$ from $\mathcal{C}$ corresponds to an equation. Then s is the set of variables appearing in the equation, and ϱ is the set of solutions of the equation, that is, a hyperplane.

For further examples including essentially multi-sorted CSP the reader is referred to [4, 3].

2.2 Transformations of problem instances

For a tuple $\mathbf{a} = (\mathbf{a}[1], \ldots, \mathbf{a}[n])$, and a set $I = \{i_1, \ldots, i_k\} \subseteq \{1, \ldots, n\}$, we denote by $\mathbf{a}\big|_I$ the *projection* $(\mathbf{a}[i_1], \ldots, \mathbf{a}[i_k])$ of $\mathbf{a}$ onto I. Analogously, for an n-ary relation ϱ, $\varrho\big|_I$ denotes the relation $\{\mathbf{a}\big|_I : \mathbf{a} \in \varrho\}$. Often we use tuples whose components are indexed not by natural numbers, but elements of a certain set, for example, by variables of a CSP instance. In this case the notation $(\mathbf{a}[i])_{i\in I}$ where I is the index-set will be used. For the algorithms below we need a particular kind of problem instances.

Let $\mathcal{P} = (V; \mathcal{A} = \{A_i \mid i \in I\}; \sigma; \mathcal{C})$ where $\mathcal{C} = (C_1, \ldots, C_q)$, $C_i = \langle s_i, \varrho_i \rangle$ be a problem instance, and $V' \subseteq V$. A *partial solution* of $\mathcal{P}$ on V' is a function $\varphi \colon V' \to \bigcup_{v\in V'} A_{\sigma(v)}$ such that, for any $i \le q$, $\varphi(s_i \cap V') \in \varrho_i\big|_{s_i\cap V'}$. Notice that a partial solution can be treated as a solution to the *restricted problem instance* $\mathcal{P}_{V'} = (V'; \mathcal{A}; \sigma\big|_{V'}; \mathcal{C}_{V'})$ where $\sigma\big|_{V'}$ is the restriction of σ onto V', and $\mathcal{C}_{V'} = (C'_1, \ldots, C'_q)$, $C'_i = (s_i \cap V', \varrho_i\big|_{V'})$, $s_i \cap V'$ is ordered in the natural way. Let us denote the set of all partial solutions on V' by $\mathcal{S}_{V'}$. We call a problem instance $\mathcal{P}$ *k-minimal* if, for any at most k-element subset V' of V, there is $t \in \{1, \ldots, q\}$ such that $V' \subseteq s_t$, and for any $l \in \{1, \ldots, q\}$, we have $\varrho_l\big|_{V'\cap s_l} = \mathcal{S}_{V'}\big|_{V'\cap s_l}$.

Any problem instance $\mathcal{P}$ can be transformed to an equivalent k-minimal instance $\mathcal{P}'$. To do this we first add the constraint $(V', \mathcal{S}_{V'})$, for each k-element set $V' \subseteq V$; and second repeat the following procedure until the obtained problem instance coincide with the previous one: for each k-element set $V' \subseteq V$, calculate the relation $\mathcal{S}_{V'}$, and then, throw out "superfluous" tuples from all the constraint relations. It is easily seen, that $\mathcal{P}'$ is k-minimal and the time complexity of this procedure is $O(m^2 n^k r)$ where n is the number of variables, m is the total number of tuples in the constraint relations, and r is the maximal arity of the constraint relations. The obtained instance is referred to as *associated* with $\mathcal{P}$. As is easily seen the solution set of the associated instance is equal to that of the original instance.

Another transformation of a problem instance sometimes allows one to reduce the number of variables. Suppose that $\mathcal{P}$ is 3-minimal. For each constraint relation ϱ_i define the digraph $G(\varrho_i)$ as follows: the set of vertices is s_i, and (v, w) is an edge if and only if there is a mapping $\pi \colon A_{\sigma(v)} \to A_{\sigma(w)}$ such that $\varrho\big|_{\{v,w\}}$ is a subset of the *graph* of π, that is the relation $\{(a, \pi(a) \colon a \in A_{\sigma(v)}\}$. By $G(\mathcal{P})$ we denote the transitive closure of the union $G(\varrho_1) \cup \ldots \cup G(\varrho_q)$. Clearly, values of any two variables from the same strongly connected component are related by a one-to-one mapping. Formally this fact can be expressed as follows. Choose a representative from each strongly connected component, the set of all representatives will be denoted by V'. For each $v \in V$, there is $v' \in V'$ and a mapping $\pi_v \colon A_{\sigma(v')} \to A_{\sigma(v)}$ such that $\mathcal{S}_{\{v',v\}}$ is the graph of π_v. Then we transform $\mathcal{P}$ to the instance $\mathcal{P}' = (V'; \mathcal{A}; \sigma'; \mathcal{C}')$ where $\sigma' = \sigma\big|_{V'}$, for each $C_i = (s_i, \varrho_i) \in \mathcal{C}$ we replace each variable $v \in s_i = (v_1, \ldots, v_m)$ with v', replace ϱ_i with the relation $\{(\pi_{v_1}^{-1}(\mathbf{a}[v_1]), \ldots, \pi_{v_m}^{-1}(\mathbf{a}[v_m])) \colon \mathbf{a} \in \varrho_i\}$, and then remove all repetitions of entries from the obtained constraint scope and corresponding coordinate positions of the obtained relation; the resulted constraint is denoted by C'_i. Obviously, every solution of $\mathcal{P}$ can be restricted to a solution of $\mathcal{P}'$, and vice versa, every solution of $\mathcal{P}'$ can be extended to a solution of $\mathcal{P}$.

2.3 Algebraic structure of constraint satisfaction problem

A way how to describe problem classes of the form CSP(Γ) via their algebraic invariance properties has been exhibited in [26, 27, 23, 5] for the case of the one-sorted CSP, and in [3] for the case of multi-sorted CSP. We use the multi-sorted version of the CSP as an auxiliary tool. So we describe in details the one-sorted case and give only some basics for the multi-sorted one.

2.3.1 One-sorted case

An m-ary relation ϱ is said to be *invariant* with respect to an operation $f(x_1,\dots,x_n)$ [or f *preserves* ϱ] if, for every $(a_{11},\dots,a_{m1}),\dots,(a_{1n},\dots,a_{mn}) \in \varrho$, we have

$$\begin{pmatrix} f(a_{11},a_{12},\dots,a_{1n}) \\ f(a_{21},a_{22},\dots,a_{2n}) \\ \vdots \\ f(a_{m1},a_{m2},\dots,a_{mn}) \end{pmatrix} \in \varrho.$$

Given a set of relations, Γ, the set of all operations preserving Γ is denoted by $\mathsf{Pol}\,\Gamma$. Analogously, given a set of operations, C, on A, the set of all relations which are preserved by operations from C is denoted by $\mathsf{Inv}\,C$.

Theorem 1 ([23]) *For any set of relations Γ over a finite set, and any finite set of relations $\Gamma' \subseteq \mathsf{Inv}\ \mathsf{Pol}\,\Gamma$, there is a polynomial time reduction from* CSP(Γ) *to* CSP(Γ').

Corollary 1 *A set of relations, Γ, is tractable if and only if $\mathsf{InvPol}\,\Gamma$ is tractable.*

It is often useful to deal with not just a set of operations, but a set endowed with operations.

Definition 2 *A* universal algebra *(or simply* algebra*) is an ordered pair $\mathbb{A} = (A; F)$ where A is a nonempty set and F is a family of finitary operations on A. The set A is called the* universe *(or the* base set*), and the operations from F are called* basic*. An algebra is said to be* finite *if its universe is finite.*

For an algebra $\mathbb{A} = (A; F)$, the set $\mathsf{Pol}\ \mathsf{Inv}\ F$ is closed with respect to substitution, and each operation from this set is said to be *term* operation of $\mathbb{A}$. Two algebras with the same universe are said to be *term equivalent*, if the sets of their term operations are equal. The universe of an algebra $\mathbb{A}$ will be denoted by A.

Thus, for any set of relation, Γ, over a set A the algebra corresponding to the problem class CSP(Γ) is $(A; \mathsf{Pol}\ \Gamma)$, and conversely, any finite algebra $\mathbb{A} = (A; F)$ gives rise to a problem class $\mathsf{Inv}\ F$. By Theorem 1, if sets Γ_1, Γ_2 correspond to term equivalent algebras, then they are either tractable or intractable simultaneously. An algebra $\mathbb{A}$ is said to be *(globally) tractable* [*NP-complete*] if $\mathsf{Inv}\ F$ is (globally) tractable [NP-complete].

We are now able to reformulate the main result of this paper. An algebra is said to be *Mal'tsev* if it has a Mal'tsev term operation.

Theorem 2 *Any finite Mal'tsev algebra is globally tractable.*

2.3.2 Multi-sorted case

To introduce the algebraic structure of problem classes in the multi-sorted case we need more algebraic terminology.

First we note that algebras can be grouped into families according to the arities of their operations.

Definition 3 *Algebras* $\mathbb{A}_1 = (A_1, F_1)$, $\mathbb{A}_2 = (A_2, F_2)$ *are said to be* similar *(or of the* same type*) if there exists a set* I *such that* $F_1 = \{f_i^1 \mid i \in I\}$, $F_2 = \{f_i^2 \mid i \in I\}$ *and, for all* $i \in I$, f_i^1, f_i^2 *are of the same arity.*

Let $\mathcal{A}$ be a class of similar algebras. The index-set for the basic operations of algebras from $\mathcal{A}$ is often called the set of basic operations of $\mathcal{A}$. For each $\mathbb{A} \in \mathcal{A}$, the concrete operation corresponding to an index f will be called the $\mathbb{A}$-*interpretation* of f and denoted $f^{\mathbb{A}}$. We will also use *terms* of $\mathcal{A}$, constructed from basic operations of $\mathcal{A}$ in the standard way (see, for example, [19, 10]). Again, for each $\mathbb{A} \in \mathcal{A}$, the $\mathbb{A}$-interpretation of a term t is a concrete operation derived by the usual rules. The $\mathbb{A}$-interpretation of t is a term operation of $\mathbb{A}$, and denoted by $t^{\mathbb{A}}$.

We say that an (n-ary) term t preserves an (m-ary) multi-sorted relation ϱ with the signature $(i_1, \ldots, i_m)$ over the collection of the universes of algebras from $\mathcal{A}$ if, for any $(a_{11}, \ldots, a_{m1}), \ldots, (a_{1n}, \ldots, a_{mn}) \in \varrho$ we have

$$t \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix} = \begin{pmatrix} t^{\mathbb{A}_{i_1}}(a_{11}, \ldots, a_{1n}) \\ \vdots \\ t^{\mathbb{A}_{i_m}}(a_{m1}, \ldots, a_{mn}) \end{pmatrix} \in \varrho.$$

For a class $\mathcal{A}$ of similar algebras, $\mathsf{Inv}\ (\mathcal{A})$ denotes the class of multi-sorted relations over the class of the universes of algebras from $\mathcal{A}$ invariant with respect to terms of $\mathcal{A}$. Further, we can define the associated multi-sorted CSP just by setting $\mathrm{CSP}(\mathcal{A}) = \mathrm{CSP}(\mathsf{Inv}\ (\mathcal{A}))$.

Definition 4 *A collection of algebras* $\mathcal{A}$ *is said to be* tractable *if* $\mathsf{Inv}\ (\mathcal{A})$ *is tractable. It is said to be NP-complete if* $\mathsf{Inv}\ (\mathcal{A})$ *is NP-complete.*

3 Properties of Mal'tsev algebras

To describe the algorithm solving the CSP over Mal'tsev algebras, we need some algebraic terminology and results. All these notions are standard, and can be found in [7, 33], but we give all the required definitions so that the paper is self-contained.

3.1 Basic definitions

We shall make use of four standard constructions on algebras which are defined as follows:

Definition 5 *Let* $\mathbb{A}_1 = (A_1, F^{\mathbb{A}_1})$, $\mathbb{A}_2 = (A_2, F^{\mathbb{A}_2})$ *be similar algebras. A mapping* $\varphi: A_1 \to A_2$ *is called a* homomorphism *from* $\mathbb{A}_1$ *to* $\mathbb{A}_2$ *if* $\varphi f^{\mathbb{A}_1}(a_1, \ldots, a_k) = f^{\mathbb{A}_2}(\varphi(a_1), \ldots, \varphi(a_k))$ *holds for all* $f \in F$ *and all* $a_1, \ldots, a_k \in A_1$, *where* k *is the arity of* f. *If the mapping* φ *is surjective then* $\mathbb{A}_2$ *is called a* homomorphic image *of* $\mathbb{A}_1$.

Definition 6 *Let* $\mathbb{A} = (A, F)$ *be an algebra and* B *a subset of* A *such that, for any* $f \in F$, *with arity* k, *and for any* $b_1, \ldots, b_k \in B$, *we have* $f(b_1, \ldots, b_k) \in B$. *Then the algebra* $\mathbb{B} = (B, F|_B)$, *where* $F|_B$ *consists of restrictions of the operations in* F *onto the set* B, *is called a* subalgebra *of* $\mathbb{A}$.

The least subalgebra containing a set $C \subseteq A$ *is called the subalgebra* generated by C, *and denoted by* $\langle C \rangle$.

Definition 7 *Let* $\mathbb{A}_1, \ldots, \mathbb{A}_n$ *be similar algebras, and* F *a set of basic operations. The* direct product *of* $\mathbb{A}_1, \ldots, \mathbb{A}_n$ *is the algebra* $\mathbb{B} = (B; F^{\mathbb{B}})$ *where* $B = A_1 \times \ldots \times A_n$ *and the* $\mathbb{B}$*-interpretation of a basic operation* $f \in F$ *of arity* k *is defined as follows*

$$f^{\mathbb{B}}\left(\begin{pmatrix} a_{11} \\ \vdots \\ a_{n1} \end{pmatrix}, \ldots, \begin{pmatrix} a_{1k} \\ \vdots \\ a_{nk} \end{pmatrix}\right) = \begin{pmatrix} f^{\mathbb{A}_1}(a_{11}, \ldots, a_{1k}) \\ \vdots \\ f^{\mathbb{A}_n}(a_{n1}, \ldots, a_{nk}) \end{pmatrix}$$

where $a_{11}, \ldots, a_{1k} \in A_1, \ldots, a_{n1}, \ldots, a_{nk} \in A_n$. *The direct product of* $\mathbb{A}_1, \ldots, \mathbb{A}_n$ *is denoted by* $\mathbb{A}_1 \times \ldots \times \mathbb{A}_n$ *or* $\prod_{i \in \{1, \ldots, n\}} \mathbb{A}_i$.

Definition 8 *An equivalence relation* θ *is called a* congruence *of an algebra* $\mathbb{A} = (A; F)$ *if* $\theta \in \mathsf{Inv}\, F$.

The equality relation $\underline{0}_{\mathbb{A}}$ *and the total binary relation* $\underline{1}_{\mathbb{A}}$ *are congruences of* $\mathbb{A}$.

For any $a \in \mathbb{A}$ *and a congruence* θ, *the* θ*-block containing* a *is denoted by* $a/_{\theta}$.

For any congruence θ of an algebra $\mathbb{A} = (A; F)$, the algebra $\mathbb{A}/_{\theta} = (A/_{\theta}; F^{\theta})$ where $A/_{\theta} = \{a/_{\theta}: a \in A\}$, $F^{\theta} = \{f^{\theta}: f \in F\}$, $f^{\theta}(a_1/_{\theta}, \ldots, a_n/_{\theta}) = f(a_1, \ldots, a_n)/_{\theta}$, is called the *factor algebra* of $\mathbb{A}$. The factor algebra is known to be a homomorphic image of $\mathbb{A}$, and the (*canonical*) homomorphism is defined through the formula $a \mapsto a/_{\theta}$. Conversely, the kernel of every homomorphism is a congruence.

Example 4 *A group is an algebra of the form* $(G; \{\cdot, ^{-1}, e\})$. *Homomorphisms, subalgebras, and direct products of groups as universal algebras are homomorphisms, subgroups, and direct products in usual sense. A congruence of a group is the equivalence relation whose classes are the cosets of a normal subgroup.*

It is not hard to see that, for an algebra $\mathbb{A} = (A; F)$, every (n-ary) relation $\varrho \in \mathsf{Inv}\ F$ can be viewed as a subalgebra of the nth direct power $\mathbb{A}^n = \underbrace{\mathbb{A} \times \ldots \times \mathbb{A}}_{n \text{ times}}$. Analogously, every relation from $\mathsf{Inv}\ \mathcal{A}$ for a class of similar algebras $\mathcal{A}$ is a subalgebra of the direct product of some algebras from $\mathcal{A}$. We therefore will use the algebraic notation for relations; relations will be denoted by $\mathbb{D}, \mathbb{R}, \ldots$

3.2 Simple properties of Mal'tsev algebras

The following proposition contains three basic properties of Mal'tsev algebras, which will be constantly used. For a natural number n, by $\underline{n}$ we denote the set $\{1, \ldots, n\}$. For $\mathbf{a} = (\mathbf{a}[1], \ldots, \mathbf{a}[n])$ and $\mathbf{b} = (\mathbf{b}[1], \ldots, \mathbf{b}[m])$, $(\mathbf{a}, \mathbf{b})$ denotes the tuple $(\mathbf{a}[1], \ldots, \mathbf{a}[n], \mathbf{b}[1], \ldots, \mathbf{b}[m])$, while $\langle \mathbf{a}, \mathbf{b} \rangle$ denotes the pair of tuples.

A subalgebra $\mathbb{D}$ of the direct product $\mathbb{D}_1 \times \ldots \times \mathbb{D}_n$ is called a *subdirect product* if, for any $i \in \underline{n}$ and $a \in \mathbb{D}_i$, there is $\mathbf{a} \in \mathbb{D}$ such that $\mathbf{a}[i] = a$.

Proposition 1 *Let $\mathbb{D}$ be a subdirect product of Mal'tsev algebras $\mathbb{D}_1, \ldots, \mathbb{D}_n$ and $I \subseteq \underline{n}$. Then the following properties hold.*
1. $\mathbb{D}$ is rectangular*, that is if $\mathbf{a}, \mathbf{b} \in \mathbb{D}|_I, \mathbf{c}, \mathbf{d} \in \mathbb{D}|_{\underline{n}-I}$ and $(\mathbf{a}, \mathbf{c}), (\mathbf{a}, \mathbf{d}), (\mathbf{b}, \mathbf{c}) \in \mathbb{D}$, then $(\mathbf{b}, \mathbf{d}) \in \mathbb{D}$.*
2. The relation $\theta_I = \{\langle \mathbf{a}, \mathbf{b} \rangle \in (\mathbb{D}|_I)^2$: there is $\mathbf{c} \in \mathbb{D}|_{\underline{n}-I}$ such that $(\mathbf{a}, \mathbf{c}), (\mathbf{b}, \mathbf{c}) \in \mathbb{D}\}$ is a congruence of $\mathbb{D}_I$.
3. $\mathbb{D}$ is a disjoint union of sets of the form $B \times C$ where B is a θ_I-block and C is a $\theta_{\underline{n}-I}$-block.

We are going to prove that every finite Mal'tsev algebra is tractable. However, it is clear that the less basic (and term) operations an algebra has, the wider and harder problem class it corresponds to. Therefore, we may restrict ourselves with those Mal'tsev algebras that have only one basic operation, the Mal'tsev operation.

3.3 Types of prime quotients and the structure of relations

A pair of congruences (α, β) of an algebra $\mathbb{A}$ is said to be *prime quotient* if $\alpha \subset \beta$ and there is no congruence γ such that $\alpha \subset \gamma \subset \beta$. In this case we write $\alpha \prec \beta$. Tame congruence theory [21] allows one to assign to each prime quotient of an algebra one of five types $\mathbf{1}, \ldots, \mathbf{5}$. The type of the prime quotient (α, β) is denoted by $\mathsf{typ}(\alpha, \beta)$.

The types of prime quotients strongly affect the properties of an algebra. For example, in [3], it is proved that if there is a prime quotient of type $\mathbf{1}$ then the algebra is NP-complete.

As we do not need the general definition of types, we define them only in the particular case of Mal'tsev algebras. Let $\mathbb{A} = (A; \mathbf{d})$ be a finite Mal'tsev algebra, $\mathbf{d}$ a Mal'tsev operation, and (α, β) a prime quotient. Let also $\beta/_\alpha$ denote the congruence of $\mathbb{A}/_\alpha$ defined as follows ([20, 13]): $(a/_\alpha, b/_\alpha) \in \beta/_\alpha$ if and only if $(a, b) \in \beta$. Then $\mathsf{typ}(\alpha, \beta) = \mathbf{2}$ if and only if, for any $\beta/_\alpha$-block B of $\mathbb{A}/_\alpha$ and any $a \in \mathbb{A}/_\alpha$, the algebra

$(B; \mathbf{d}^\theta(x,a,y), \mathbf{d}^\theta(a,x,a), a)$ is an Abelian group; otherwise $\mathsf{typ}(\alpha,\beta) = \mathbf{3}$. The types **1**,**4**,**5** cannot appear in a Mal'tsev algebra.

If the intersection $\theta_1 \cap \ldots \cap \theta_k$ of congruences of an algebra $\mathbb{A}$ equals $\underline{0}_{\mathbb{A}}$ then $\mathbb{A}$ can be represented as a subdirect product of $\mathbb{A}/_{\theta_1}, \ldots, \mathbb{A}/_{\theta_k}$. An algebra is called *subdirectly irreducible* if the intersection of all nontrivial congruences is nontrivial. In this case there is the least nontrivial congruence which is called the *monolith*. As is well known, every algebra can be decomposed in a subdirect product of subdirectly irreducible algebras. In fact, if congruences $\alpha_1, \ldots, \alpha_k$ of $\mathbb{A}$ are *meet-irreducible*, that is for α_i there exists a unique β_i such that (α_i, β_i) is a prime quotient, and $\alpha_1 \wedge \ldots \wedge \alpha_k = \underline{0}_{\mathbb{A}}$, then $\mathbb{A}$ is a subdirect product of $\mathbb{A}/_{\alpha_1}, \ldots, \mathbb{A}/_{\alpha_k}$ and all $\mathbb{A}_i$ are subdirectly irreducible.

We will use the following folklore fact.

Proposition 2 *Let $\mathbb{A}$ be a subdirectly irreducible Mal'tsev algebra, μ its monolith, and $(a,b) \in \mu$. Then for any $c,d \in \mathbb{A}$ such that $(c,d) \in \mu$, there are a term operation $f(x,y_1,\ldots,y_n)$ and $e_1,\ldots,e_n \in \mathbb{A}$ such that $f(a,e_1,\ldots,e_n) = c$, $f(b,e_1,\ldots,e_n) = d$.*

A subdirect product $\mathbb{D}$ of $\mathbb{D}_1, \ldots, \mathbb{D}_n$ is said to be *reduced*, if for no two-element subset $I \subseteq \underline{n}$ the projection $\mathbb{D}|_I$ is the graph of a mapping.

Let $\mathbb{D}$ be a reduced subdirect product of subdirectly irreducible Mal'tsev algebras $\mathbb{D}_1, \ldots, \mathbb{D}_n$; μ_i the monolith of $\mathbb{D}_i$; and $\underline{0}_i$ the equality relation on $\mathbb{D}_i$, $i \in \underline{n}$. Let also $I \subseteq \underline{n}$, and δ be a congruence of $\mathbb{D}|_I$. We say that $\mathbb{D}$ is *I-rectangular* modulo δ, if $\delta \subseteq \theta_I$.

Lemma 1 *If $i \in \underline{n}$ is such that $\mathsf{typ}(\underline{0}_i, \mu_i) = \mathbf{3}$, then $\mathbb{D}$ is $\{i\}$-rectangular modulo μ_i.*

Proof. Without loss of generality we may suggest that $i = 1$. Suppose $\mathbb{D}$ is not $\{1\}$-rectangular modulo μ_1. This means $\mu_1 \not\subseteq \theta_{\{1\}}$, therefore, $\theta_{\{1\}} = \underline{0}_1$. Let $J \subseteq \underline{n}$ be minimal such that $1 \in J$ and $\mathbb{D}|_J$ is not $\{1\}$-rectangular. Since by the assumption $\mathbb{D}$ is reduced, and therefore each binary projection $\mathbb{D}|_{\{i,j\}}$ of $\mathbb{D}$ is i- and j-rectangular modulo μ_i, μ_j respectively, J has at least 3 elements. It will not be loss of generality, if we assume $J = \underline{n}$.

For a term operation $\mathbf{f}$ of $\mathbb{D}$ we denote by f_i the corresponding term operation of $\mathbb{D}_i$. By the results of [21, 2], for any μ_1-block B containing more than one element, there are $N = \{0,1\} \subseteq B$, a term operation $\mathbf{g}(x,y,z_1,\ldots,z_k)$ of $\mathbb{D}$, and $\mathbf{a}_1,\ldots,\mathbf{a}_k \in \mathbb{D}$ such that the operation $\mathbf{f}(x,y) = \mathbf{g}(x,y,\mathbf{a}_1,\ldots,\mathbf{a}_k)$ satisfies the following conditions: $f_1(\mathbb{D}_1,\mathbb{D}_1) \subseteq N$; f_1 is a semilattice operation on N, that is $f_1(0,1) = f_1(1,0) = f_1(1,1) = 1$, $f_1(0,0) = 0$; $f_i(a,b) = f_i(c,d)$ for any $i \neq 1$ and any $a,b,c,d \in \mathbb{D}_i$ such that $(a,c),(b,d) \in \mu_i$; and $\mathbf{f}(x,x)$ is idempotent, that is $\mathbf{f}(\mathbf{f}(x,x),\mathbf{f}(x,x)) = \mathbf{f}(x,x)$. Take $\mathbf{a} = (\mathbf{a}[3],\ldots,\mathbf{a}[n]) \in \mathbb{D}|_{\underline{n}-\{1,2\}}$ such that $\begin{pmatrix} 0 \\ \mathbf{a} \end{pmatrix}, \begin{pmatrix} 1 \\ \mathbf{a} \end{pmatrix} \in \mathbb{D}|_{\underline{n}-\{2\}}$ and denote by A $[B]$ the set of all $c \in \mathbb{A}_2$ such that $\begin{pmatrix} 0 \\ c \\ \mathbf{a} \end{pmatrix} \in \mathbb{D}$ $\left[\begin{pmatrix} 1 \\ c \\ \mathbf{a} \end{pmatrix} \in \mathbb{D}\right]$. Notice that A, B are $\theta_{\{2\}}$-blocks, and by the assumption $\theta_{\{1\}} = \underline{0}_1$, we have $A \cap B = \varnothing$. Replacing $\mathbf{a}$ with $f(\mathbf{a},\mathbf{a})$ we may assume $\mathbf{f}(\mathbf{a},\mathbf{a}) = \mathbf{a}$ and, therefore, $f_2(A,A) \subseteq A$, $f_2(B,B), f_2(A,B), f_2(B,A) \subseteq B$.

Further, $\begin{pmatrix} 0 \\ b \end{pmatrix}, \begin{pmatrix} 1 \\ a \end{pmatrix} \in \mathbb{D}|_{\{1,2\}}$, for any $a \in A, b \in B$, since $\mathbb{D}|_{\{1,2\}}$ is 1-rectangular modulo μ_1. Take $\mathbf{b} \in \mathbb{D}_{\underline{n}-\{1,2\}}$ such that $\begin{pmatrix} 0 \\ b \\ \mathbf{b} \end{pmatrix} \in \mathbb{D}$. Denoting $\mathbf{d}(0,1,0)$ by d, we have

$$\mathbf{d}\left(\begin{pmatrix} 0 \\ a \\ \mathbf{a} \end{pmatrix}, \begin{pmatrix} 1 \\ b \\ \mathbf{a} \end{pmatrix}, \begin{pmatrix} 0 \\ b \\ \mathbf{b} \end{pmatrix}\right) = \begin{pmatrix} d \\ a \\ \mathbf{b} \end{pmatrix} \in \mathbb{D}.$$

Then $\mathbf{f}\left(\begin{pmatrix} d \\ a \\ \mathbf{b} \end{pmatrix}, \begin{pmatrix} d \\ a \\ \mathbf{b} \end{pmatrix}\right) = \begin{pmatrix} d' \\ a' \\ \mathbf{b}' \end{pmatrix} \in \mathbb{D}$ where $d' \in \{0,1\}$. Set $f_2(b,b) = b'$, and note that $a' \in A$, $b' \in B$. If $d' = 0$ then

$$\begin{pmatrix} 0 \\ b' \\ \mathbf{b}' \end{pmatrix} = \mathbf{f}\left(\begin{pmatrix} 0 \\ b \\ \mathbf{b} \end{pmatrix}, \begin{pmatrix} 0 \\ b \\ \mathbf{b} \end{pmatrix}\right) \in \mathbb{D} \quad \text{and} \quad \begin{pmatrix} 0 \\ a' \\ \mathbf{b}' \end{pmatrix} \in \mathbb{D},$$

hence $a' \overset{\theta_{\{2\}}}{\equiv} b'$, that contradicts the assumption $A \cap B = \varnothing$. Therefore $d' = 1$. So, we have $\begin{pmatrix} 0 \\ b' \\ \mathbf{b}' \end{pmatrix}, \begin{pmatrix} 1 \\ a' \\ \mathbf{b}' \end{pmatrix} \in \mathbb{D}$.

Then,

$$\mathbf{f}\left(\begin{pmatrix} 0 \\ b' \\ \mathbf{b}' \end{pmatrix}, \begin{pmatrix} 1 \\ a' \\ \mathbf{b}' \end{pmatrix}\right) = \begin{pmatrix} 1 \\ b'' \\ \mathbf{b}' \end{pmatrix} \in \mathbb{D}$$

where $b'' \in B$. On the other hand,

$$\mathbf{f}\left(\begin{pmatrix} 1 \\ a' \\ \mathbf{b}' \end{pmatrix}, \begin{pmatrix} 1 \\ a' \\ \mathbf{b}' \end{pmatrix}\right) = \begin{pmatrix} 1 \\ a'' \\ \mathbf{b}' \end{pmatrix} \in \mathbb{D}$$

where $a'' \in A$. Due to rectangularity, since $\begin{pmatrix} 1 \\ b'' \\ \mathbf{a} \end{pmatrix}, \begin{pmatrix} 1 \\ b'' \\ \mathbf{b}' \end{pmatrix}, \begin{pmatrix} 1 \\ a'' \\ \mathbf{b}' \end{pmatrix} \in \mathbb{D}$, the tuple $\begin{pmatrix} 1 \\ a'' \\ \mathbf{a} \end{pmatrix}$ is also in $\mathbb{D}$, and therefore $a'' \in B$. This again contradicts the assumption $A \cap B = \varnothing$. $\square$

4 Results

In fact, we will obtain more than just the tractability of a Mal'tsev algebra. We exhibit an algorithm that finds a basis of the solution space of a problem instance, and moreover, any solution can be uniquely decomposed.

Let $\mathbb{A} = (A; F)$ be a Mal'tsev algebra with a Mal'tsev operation $\mathbf{d}$, $\mathcal{P} = (V; A; \mathcal{C}) \in \mathrm{CSP}(\mathbb{A})$, and $V = \{v_1, \ldots, v_n\}$. Let also $\mathcal{S}$ denote the set of all solutions to $\mathcal{P}$. We denote $\mathbb{B}_i$ the set $\mathcal{S}_i = \{\varphi(v_i) \mid \varphi \in \mathcal{S}\}$. As is easily seen $\mathbb{B}_i$ is a subalgebra of $\mathbb{A}$. For any i, choose a chain $\underline{0}_{\mathbb{B}_i} = \alpha^i_0 \prec \alpha^i_1 \prec \ldots \prec \alpha^i_{q_i} = \underline{1}_{\mathbb{B}_i}$ of congruences of $\mathbb{B}_i$, and consider the direct product $\mathbb{B} = \mathbb{B}_1 \times \ldots \times \mathbb{B}_n$. For any sequence $(\beta^1, \ldots, \beta^n)$ where $\beta^i \in \{\alpha^i_0, \ldots, \alpha^i_{q_i}\}$, the congruence $\overline{\beta}$ of $\mathbb{B}$ is defined as follows: $((a[1], \ldots, a[n]), (b[1], \ldots, b[n]))$ if and only if $(a[i], b[i]) \in \beta^i$, for all $i \in \underline{n}$.

A basis of the set $\mathcal{S}$ of solutions to $\mathcal{P}$ we are looking for is of the following form. There is a chain $\overline{\beta}_0 \subset \overline{\beta}_1 \subset \ldots \subset \overline{\beta}_k$ of congruences of $\mathbb{B}$ such that $\overline{\beta}_l$ corresponds to a sequence $(\beta_{l1}, \ldots, \beta_{ln})$, $\beta_{li} \in \{\alpha^i_0, \ldots, \alpha^i_{q_i}\}^n$, and

- $\beta_{k1} = \alpha^1_{q_1} = \underline{1}_{\mathbb{B}_1} \ldots \beta_{kn} = \alpha^n_{q_n} = \underline{1}_{\mathbb{B}_n}$, $\beta_{01} = \alpha^1_0 = \underline{0}_{\mathbb{B}_1} \ldots \beta_{0n} = \alpha^n_0 = \underline{0}_{\mathbb{B}_n}$;
- for any $l \in \{0, \ldots, k-1\}$ and $i \in \{1, \ldots, n\}$, either $\beta_{li} = \beta_{l+1i}$ or $\beta_{li} \prec \beta_{l+1i}$;
- the set $I_l = \{i \in \underline{n} \colon \beta_{li} \prec \beta_{l+1i}\}$ is a strictly connected component of $G(\mathcal{S}/_{\overline{\beta}_l})$.

Then the basis consist of k parts, $B = B^k \cup \ldots \cup B^1$ where

- $B^k = \{\mathbf{a}_k\}$ where $\mathbf{a}$ is an arbitrary tuple from $\mathcal{S}$;
- $B^l = B^l_1 \cup \ldots \cup B^l_{r_l}$ where r_l is the number of classes of the congruence $\beta_{l+1s}/_{\beta_{ls}}$, for certain $s \in I_l$.
- Let $C^l_1, \ldots, C^l_{r_l}$ be $\beta_{l+1s}/_{\beta_{ls}}$-classes. Then one of the following two possibilities holds:
  - for any $1 \le j \le r_l$, $B^l_j = \{\mathbf{a}\}$ with $\mathbf{a}[s]/_{\beta_{ls}} \in C_j$;
  - for any $1 \le j \le r_l$,
  $$B^l_j = \{\mathbf{a}_1, \ldots, \mathbf{a}_t\}$$
  where $t = |C^l_j|$, $\mathbf{a}_1[i], \ldots, \mathbf{a}_t[i]$ lie in the same β_{li}-class for $i \notin I_l$, and for any $b \in C^l_j$ there is $u \in \underline{t}$ with $\mathbf{a}_u[s]/_{\beta_{ls}} = b$.

In the next section we show that an arbitrary tuple $\mathbf{a} \in \mathcal{S}$ can be represented in the form

$$\mathbf{d}(\mathbf{d}(\ldots \mathbf{d}(\mathbf{d}(\ldots \mathbf{d}(\mathbf{a}_k, \mathbf{a}_{k-1}, \mathbf{b}_{k-1}), \ldots), \mathbf{a}_l, \mathbf{b}_l), \ldots), \mathbf{a}_1, \mathbf{b}_1)$$

where, $\{\mathbf{a}^k\} = B^k$, for each $1 \le l < k$, if $\mathbf{c}_{l+1}$ denotes the tuple

$$\mathbf{d}(\mathbf{d}(\ldots \mathbf{d}(\mathbf{a}_k, \mathbf{a}_{k-1}, \mathbf{b}_{k-1}), \ldots), \mathbf{a}_{l+1}, \mathbf{b}_{l+1})$$

then $(\mathbf{c}_{l+1}, \mathbf{a}) \in \overline{\beta}_{l+1}$, and $\mathbf{a}_l, \mathbf{b}_l \in B^l$ are such that $(\mathbf{a}_l[s], \mathbf{c}_{l+1}[s]) \in \beta_{ls}$, $(\mathbf{b}_l[s], \mathbf{a}[s]) \in \beta_{ls}$ for $s \in I_l$. Obviously, such a representation is unique.

Example 5 *Let S_3 denote the full symmetric group on the 3-element set $\{1,2,3\}$. The elements of S_3 are*

$$\varepsilon = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \beta_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \beta_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$
$$\gamma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \gamma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad \gamma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

The group S_3 is a Mal'tsev algebra with a Mal'tsev operation $\mathbf{d}(x,y,z) = xy^{-1}z$. We consider the algebra $\mathbb{A} = (S_3; \{\mathbf{d}\})$. As is easily seen, the only proper congruence α of $\mathbb{A}$ and S_3 has the classes $\{\varepsilon, \beta_1, \beta_2\}, \{\gamma_1, \gamma_2, \gamma_3\}$, and the corresponding normal subgroup of S_3 is $\{\varepsilon, \beta_1, \beta_2\}$.

A basis of a subalgebra

$$\mathbb{D} = \begin{pmatrix} \varepsilon & \varepsilon & \varepsilon & \beta_1 & \beta_1 & \beta_1 & \beta_2 & \beta_2 & \beta_2 & \gamma_1 & \gamma_1 & \gamma_1 & \gamma_2 & \gamma_2 & \gamma_2 & \gamma_3 & \gamma_3 & \gamma_3 \\ \gamma_1 & \gamma_2 & \gamma_3 & \gamma_1 & \gamma_2 & \gamma_3 & \gamma_1 & \gamma_2 & \gamma_3 & \varepsilon & \beta_1 & \beta_2 & \varepsilon & \beta_1 & \beta_2 & \varepsilon & \beta_1 & \beta_2 \\ \beta_2 & \beta_2 & \beta_2 & \varepsilon & \varepsilon & \varepsilon & \beta_1 & \beta_1 & \beta_1 & \gamma_2 & \gamma_2 & \gamma_2 & \gamma_3 & \gamma_3 & \gamma_3 & \gamma_1 & \gamma_1 & \gamma_1 \end{pmatrix}$$

can be chosen as follows

$$\underbrace{\begin{matrix} \varepsilon \\ \gamma_3 \\ \beta_2 \end{matrix}}_{B^5} \Bigg| \underbrace{\begin{matrix} \beta_1 & \gamma_1 \\ \gamma_1 & \varepsilon \\ \varepsilon & \gamma_2 \end{matrix}}_{B^4} \Bigg| \underbrace{\begin{matrix} \beta_1 & \beta_2 & \varepsilon \\ \gamma_1 & \gamma_1 & \gamma_2 \\ \varepsilon & \beta_1 & \beta_2 \end{matrix}}_{B^3_1} \quad \underbrace{\begin{matrix} \gamma_3 & \gamma_1 & \gamma_2 \\ \beta_1 & \beta_2 & \beta_2 \\ \gamma_1 & \gamma_2 & \gamma_3 \end{matrix}}_{B^3_2} \Bigg| \underbrace{\begin{matrix} \beta_1 & \beta_1 & \beta_1 \\ \gamma_1 & \gamma_2 & \gamma_3 \\ \varepsilon & \varepsilon & \varepsilon \end{matrix}}_{B^2_1} \quad \underbrace{\begin{matrix} \gamma_3 & \gamma_3 & \gamma_3 \\ \varepsilon & \beta_1 & \beta_2 \\ \gamma_1 & \gamma_1 & \gamma_1 \end{matrix}}_{B^2_2} \Bigg| \underbrace{\begin{matrix} \beta_1 \\ \gamma_1 \\ \varepsilon \end{matrix}}_{B^1_1} \quad \underbrace{\begin{matrix} \gamma_3 \\ \varepsilon \\ \gamma_1 \end{matrix}}_{B^1_2}$$

The strictly connected components are $I_1 = \{1\}, I_2 = \{2\}, I_3 = \{3\}, I_4 = \{1,2,3\}$, and the chain of congruences is $(\underline{0},\underline{0},\underline{0}) \subset (\alpha,\underline{0},\underline{0}) \subset (\alpha,\alpha,\underline{0}) \subset (\alpha,\alpha,\alpha) \subset (\underline{1},\underline{1},\underline{1})$.

Theorem 3 *Let $\mathbb{A}$ be a finite Mal'tsev algebra. Then a basis of the solution space of any problem instance $\mathcal{P} \in \mathrm{CSP}(\mathbb{A})$ can be found in polynomial time, and each solution to $\mathcal{P}$ is uniquely decomposable.*

If the Mal'tsev algebra $\mathbb{A}$ satisfies some additional restrictions then Theorem 3 may assists in finding the number of solutions. The algebra $\mathbb{A}$ is said to be *uniform* if, for any subalgebra $\mathbb{B}$ of $\mathbb{A}$, and any congruence β of $\mathbb{B}$, all the classes of β are of the same size. Groups and quasigroups provide examples of uniform Mal'tsev algebras. Moreover, let G be a finite group or quasigroup, and d its Mal'tsev operation, that is $d(x,y,z) = xy^{-1}z$ if G is a group; if G is a quasigroup then d is defined in a more sorhisticated way. Then the algebra $(G; d)$ is also uniform.

Another example of uniform Mal'tsev algebra is found in [11]. Let G be a finite group. A subset K of G is said to be a *near-subgroup* if the intersection of K with the Abelian sections of G forms subgroups [12, 11]. There is a Mal'tsev operations d on G such that the near-subgroups of G and their cosets are invariant under d [11]. It is not hard to check that $(G; d)$ is uniform.

Theorem 4 *For any finite uniform Mal'tsev algebra $\mathbb{A}$, there is a polynomial time algorithm that computes the number of solutions to any problem instance $\mathcal{P} \in \mathrm{CSP}(\mathbb{A})$.*

Proof. Let $B = B^k \cup \ldots \cup B^1$ be a basis of the set of solutions to cP; and let N_l denote the number of different $(B^k \cup \ldots \cup B^l)$-decompositions. By Theorem 3, a B-decomposition of a solution is unique, therefore, N_1 equals the number of solutions.

Obviously, $N_k = 1$. Then, if N_{l+1} is already known, notice that any $(B^k \cup \ldots \cup B^{l+1})$-decomposition has a unique extension if each B^l_j is a singleton, and has $|C^l_j|$ extensions otherwise. Since all the classes C^l_j are of the same size, we have $N_l = N_{l+1}$ in the first case, and $N_l = N_{l+1} \cdot |C^l_j|$ in the second case. $\square$

5 Algorithm

In the following two sections we describe an algorithm that solves, in polynomial time, arbitrary problem from $\mathrm{CSP}(\mathbb{A})$ where $\mathbb{A}$ is a Mal'tsev algebra with a Mal'tsev term $\mathbf{d}$. As is known, the less term operations has an algebra, the large problem class of CSPs it determines. Therefore we shall assume that $\mathbf{d}$ is the only basic operation of $\mathbb{A}$. Furthermore, for the sake of convenience we describe our algorithm for multi-sorted problem instances. However, all the domains are supposed to be homomorphic images of subalgebras of $\mathbb{A}$. This means, in particular, that we can precalculate all the required parameters and objects connected with the domains: subalgebras, congruences, types of prime quotients, and so on, even if such a calculation takes superpolynomial time on the size of an algebra.

The procedure of constructing a basis is sophisticated, and at first sight it might seem to be quite different from what was described in Section 4. However, it can be shown that the result of this procedure satisfies all the requirements of the definition from Section 4.

5.1 Planning

The aim of the algorithm we describe is to build a basis of the solution space of a problem instance over Mal'tsev algebras. A basis will be built inductively. For this we will simplify the given problem instance by decomposing the algebras if they are not subdirectly irreducible, and factorising modulo the monolith otherwise. In each step we choose a variable and factorise the algebra corresponding to this variable. During the first phase of the algorithm we build a "plan", that is a sequence of decompositions and factorisations.

Suppose that we are given a problem instance $\mathcal{P} = (V; \mathcal{A}; \delta; \{C_1, \ldots, C_q\})$. For short we will denote the algebra $\mathbb{A}_{\delta(v)}$ by $\mathbb{A}_v$ and omit the sort-function. We may assume that all $\mathbb{A}_v$s are subdirectly irreducible, and all the strongly connected components of the graph $G(\mathcal{P})$ are 1-element. Otherwise, we should reduce $\mathcal{P}$ to such a problem as is described in Steps 1–5 of the algorithm in Section 5.3. As we possibly will partially rearrange the plan, the procedure of planning will be applied several times. So, we describe it as a subroutine.

Informally, in each step we do the following. First, we take a variable with indegree 0 in $G(\mathcal{P})$, and factorise the algebra corresponding to this variable modulo its monolith. Second, we decompose the algebra which has become not subdirectly irreducible in the previous step to obtain a problem instance over subdirectly irreducible algebras. Third, we find the graph $G(\varrho)$ for each constraint relation ϱ of the obtained problem instance, and then the transitive closure G of the union of the graphs, and the strongly connected components of G. So, we find those variables whose values are connected by one-to-one mappings. Second, we choose a representative from each strongly connected component, and remove all other variables. During all this process we correspondingly change the problem instance.

INPUT: $\mathcal{P}^1 = (V^1; \{\mathbb{A}_v^1 : v \in V^1\}, \{C_1^1, \dots, C_q^1\})$ where each $\mathbb{A}_v^1$ is subdirectly irreducible, and all the strongly connected components of $G(\mathcal{P})$ are 1-element.

OUTPUT: Sequences

- $(\mathcal{P}'^2, \dots, \mathcal{P}'^k)$, where $\mathcal{P}'^l = (W^l; \{\mathbb{A}_v^l : v \in W^l\}; \{C_1'^l, \dots, C_q'^l\})$, $C_t^l = (s_t^l, \varrho_t^l)$, and $|\mathbb{A}_v^k| = 1$ for all $v \in W^k$;
- $(G^1, \dots, G^{k-1})$ where $G^l = (W^l, E^l)$ is the graph such that $(v, w) \in E^l$ if and only if $\mathcal{P}^l_{\{v,w\}}$ is the graph of a mapping $\varphi_{v,w} \colon \mathbb{A}_v^l \mapsto \mathbb{A}_w^l$;
- $(V^2, \dots, V^k)$ where $V^l \subseteq W^l$ consists of representatives of strongly connected components of G^l;
- $(\mathcal{P}^2, \dots, \mathcal{P}^k)$ where $\mathcal{P}^l = \mathcal{P}'^l\big|_{V^l}$;
- $(v^1, \dots, v^{k-1})$ where $v^l \in V^l$ form a strongly connected component of G^l;
- $(\Delta^1, \dots, \Delta^{k-1})$ where Δ^l is a set of meet-irreducible congruences of $\mathbb{A}^l_{v^l}$ such that $\bigwedge_{\delta \in \Delta^l} \delta = \mu^l_{v^l}$.

ALGORITHM

Repeat the following steps **until** $|\mathbb{A}_v^l| = 1$ for all $v \in V^l$.

Step 1 **Fix** $v^l \in V^l$, a vertex of $G(\mathcal{P}^l)$ of indegree 0.
/* If $\mathsf{typ}(\underline{0}^l_{v^l}, \mu^l_{v^l}) = \mathbf{3}$ where $\underline{0}^l_v, \mu^l_v$ denote the equality relation and the monolith of $\mathbb{A}^l_v$, $v \in V^l$, respectively, then we say that lth step is of type **3**, otherwise lth step is of type **2** */

Step 2 **Set**

$$\mathbb{B}_v = \begin{cases} \mathbb{A}^l_{v^l} / \mu^l_{v^l}, & \text{if } v = v^l, \\ \mathbb{A}^l_v, & \text{otherwise,} \end{cases}$$

$\overline{\varrho}_t'^l = \{(\mathbf{a}[v])_{v \in s_t'^l} \colon$ there is $\mathbf{b} \in \varrho_t'^l$ such that $\mathbf{a}[v^l] = \mathbf{b}[v^l]/_{\mu^l_v}$ and $\mathbf{a}[v] = \mathbf{b}[v]$ if $v \neq v^l\}$.

Step 3 Let $\theta_{v^l,1},\dots,\theta_{v^l,t_{v^l}}$ be meet-irreducible congruences of $\mathbb{B}_{v^l}$ such that $\theta_{v^l,1}\wedge\dots\wedge\theta_{v^l,t_{v^l}}=\underline{0}_{v^l}$ where $\underline{0}_{v^l}$ denotes the equality relation on $\mathbb{B}_{v^l}$. **Set** $\Delta^l=\{\theta_{v^l,1},\dots,\theta_{v^l,t_{v^l}}\}$, and $\mathbb{A}^{l+1}_{(v^l,1)}=\mathbb{B}_{v^l}/_{\theta_1},\dots,\mathbb{A}^{l+1}_{(v^l,t_{v^l})}=\mathbb{B}_{v^l}/_{\theta_{t_{v^l}}}$. Then $\mathbb{B}_{v^l}$ is a subdirect product of $\mathbb{A}^{l+1}_{(v^l,1)},\dots,\mathbb{A}^{l+1}_{(v^l,t_{v^l})}$. **For** $v\in V'^l-\{v^l\}$, **set** $t_v=1$, $\theta_{v,1}=\underline{0}^l_v$, $\Delta^l_v=\{\theta_{v,1}\}$, **and** $\mathbb{A}^{l+1}_{(v,1)}=\mathbb{A}^l_v$.

Step 4 **Set**

$$W^{l+1}=\bigcup_{v\in V'^l}\{(v^l,j)\colon 1\le j\le t_v\}.$$

$$C'^{l+1}_t=(s'^{l+1}_t,\varrho'^{l+1}_t),\text{ for each }1\le t\le q,\text{ where}$$

$$\begin{aligned} s'^{l+1}_t &= \bigcup_{v\in s'^l_t}\{(v,l)\colon 1\le l\le t_v\};\\ \varrho'^{l+1}_t &= \{(\mathbf{a}[v]/_{\theta_{v,1}},\dots,\mathbf{a}[v]/_{\theta_{v,t_v}})_{v\in s'^l_t}\colon(\mathbf{a}[v])_{v\in s'^l_t}\in\overline{\varrho}'^l_t\}.\end{aligned}$$

$$\mathcal{P}'^{l+1}=(W^{l+1};\{\mathbb{A}^{l+1}_v\colon v\in W^{l+1}\},\{C'^{l+1}_1,\dots,C'^{l+1}_q\}).$$

Step 5 **Establish 3-minimality**.

Step 6 **Find** the digraph $G^{l+1}=G(\mathcal{P}'^{l+1})=(W^{l+1},E^{l+1})$ where $(v,w)\in E^{l+1}$ if and only if $\mathcal{S}'^{l+1}_{\{v,w\}}$ is the graph of a mapping $\varphi_{v,w}\colon\mathbb{A}^{l+1}_v\mapsto\mathbb{A}^{l+1}_w$.

Step 7 **Choose** a representative from each strongly connected component of G^{l+1}; let V^{l+1} denote the set of the representatives. **Set** $\mathcal{P}^{l+1}=(V^{l+1};\{\mathbb{A}^{l+1}_v\colon v\in V^{l+1}\};C^{l+1}_1,\dots,C^{l+1}_q\}$ that is obtained from $\mathcal{P}'^{l+1}$ as follows. For each $C'^{l+1}_t=(s'^{l+1}_t,\varrho'^{l+1}_i)$ we **replace** each variable $v\in s'^{l+1}_i=(v_1,\dots,v_m)$ with v', replace ϱ'^{l+1}_i with the relation $\{(\varphi^{-1}_{v'_1,v_1}(\mathbf{a}[v_1]),\dots,\varphi^{-1}_{v'_m,v_m}(\mathbf{a}[v_m]))\colon\mathbf{a}\in\varrho'^{l+1}_i\}$, and then **remove** all repetitions of entries from the obtained constraint scope and corresponding coordinate positions of the obtained relation.

5.2 Basis of the solution space

All objects involved in the problem instance: variables, tuples, domains, relations change from step to step of the procedure of planning. It will be convenient for us to use a special notation for what the listed objects turn to.

Suppose $\mathcal{P}^l$ is the problem instance in lth step. Then

- $v{\Uparrow}^{l+1}$ is the tuple $((v,1)',\dots,(v,t_v)')$ where (v,i) denotes the representative from V^{l+1} of the strongly connected component of G^{l+1} containing (v,i) for $v\in V^l$ with $t_v=|\Delta^l_v|$;
- $a{\Uparrow}^{l+1}$ is $(a/_{\theta_{v,1}},\dots,a/_{\theta_{v,t_v}})$ where $a\in\mathbb{A}^l_v$ and $\{\theta_{v,1},\dots,\theta_{v,t_v}\}=\Delta^i_v$;
- $\mathbf{a}{\Uparrow}^{l+1}=(\mathbf{a}[v]{\Uparrow}^{l+1})_{v\in W}$ where $\mathbf{a}=(\mathbf{a}[v])_{v\in W}$, $W\subseteq V^l$;

- $\varrho\!\uparrow^{l+1} = \{\mathbf{a}\!\uparrow^{l+1} : \mathbf{a} \in \varrho\}$ where ϱ is a relation on $\{\mathbb{A}^l_v : v \in V^l\}$.

Suppose that $v\!\uparrow^j$, $a\!\uparrow^j$, $\mathbf{a}\!\uparrow^j$, $\varrho\!\uparrow^j$ are already defined. Then

- $v\!\uparrow^{j+1} = (v_1\!\uparrow^{j+1}, \ldots, v_t\!\uparrow^{j+1})$ where $v\!\uparrow^j = (v_1, \ldots, v_t)$;
- $a\!\uparrow^{j+1} = (\mathbf{a}[w]\!\uparrow^{j+1})_{w \in v\uparrow^j}$ where $a \in \mathbb{A}^l_v$, $(\mathbf{a}[w])_{w \in v\uparrow^j} = a\!\uparrow^j$;
- $\mathbf{a}\!\uparrow^{j+1} = (\mathbf{a}[v]\!\uparrow^{j+1})_{v \in W\uparrow^{j+1}}$ where $\mathbf{a} = (\mathbf{a}[w])_{w \in W}$, $W \subseteq V^l$;
- $\varrho\!\uparrow^{j+1} = \{\mathbf{a}\!\uparrow^{j+1} : \mathbf{a} \in \varrho\}$ where ϱ is a relation on $\{\mathbb{A}^l_v : v \in V^l\}$.

We are going to find a basis of the solution space $\mathcal{S}^l$ of the problem instance $\mathcal{P}^l$ in each step. Since all the constraint relations are subalgebras of corresponding direct products, $\mathcal{S}^l$ is also a subalgebra of $\mathbb{A}^l = \prod_{v \in V^l} \mathbb{A}^l_v$, and the basis will be a generating set of $\mathcal{S}^l$. The basis we look for should be of a very special form. Let B be a basis of $\mathcal{S}^l$. Then

$$B = B^k \cup \ldots \cup B^l$$

where $B^k\!\uparrow^i \cup \ldots \cup B^i\!\uparrow^i$ is a basis of $\mathcal{S}^l\!\uparrow^i$ (which is not necessarily equals $\mathcal{S}^i$) for each $l < i \le k$. Since all $\mathbb{A}^k_v$ are trivial, if $l = k$ we have $\mathcal{S}^k = B^k = \{\mathbf{a}\}$. In this case we say that $\mathbf{a}$ can be *B-decomposed*.

Let $C_1, \ldots, C_s$ be the $\mu^l_{v^l}$-blocks. Then

$$B^l = B^l_1 \cup \ldots \cup B^l_s$$

where for each $1 \le p \le s$ there is $(\mathbf{a}_p[w])_{w \in V^l - \{v^l\}} \in \prod_{w \in V^l - \{v^l\}} \mathbb{A}^l_w$ such that

$$B^l_p = \{\mathbf{a}_b : b \in C'_p \subseteq C_p\},$$

$$\mathbf{a}_b[w] = \begin{cases} b, & \text{if } w = v^l, \\ \mathbf{a}_p[w], & \text{if } w \neq v^l \end{cases}$$

and $C'_p = C_p$ or $|C'_p| = 1$.

Let $B - B^l = \{\mathbf{c}_1, \ldots, \mathbf{c}_n\}$. We say that $\mathbf{b}$ can be *B-decomposed* if

$$\mathbf{b} = \mathbf{d}(\mathbf{b}', \mathbf{a}_b, \mathbf{a}_c)$$

where $b = \mathbf{b}'[v^l]$, $c = \mathbf{b}[v^l]$, and $\mathbf{b}'$ is such that (a) $\mathbf{b}'\!\uparrow^{l+1}$ can be $(B - B^l)\!\uparrow^{l+1}$-decomposed, (b) if $\mathbf{b}'\!\uparrow^{l+1} = f(\mathbf{c}_1\!\uparrow^{l+1}, \ldots, \mathbf{c}_n\!\uparrow^{l+1})$ is a $(B - B^l)\!\uparrow^{l+1}$-decomposition, then $\mathbf{b}' = f(\mathbf{c}_1, \ldots, \mathbf{c}_n)$.

Such a decomposition of $\mathbf{a}$ will be called a *standard B-decomposition.* If $B \subseteq \mathcal{S}^l$ and each vector $\mathbf{a} \in \mathcal{S}^l$ has a standard B-decomposition, then B is said to be a *standard basis* of $\mathcal{S}^l$.

Lemma 2 *Let $B \subseteq \mathcal{S}^l$ be constructed as above; $\mathcal{S}$ a subdirect product of $\mathbb{A}^l_v$, $v \in V^l$; $C'_p = C_p$ whenever lth step is of type* **3**, *or lth step is of type* **2** *and $\mathcal{S}^l$ is v^l-rectangular modulo $\mu^l_{v^l}$, and C'_p one-element whenever lth step is of type* **2** *and the congruence θ_{v^l} of $\mathbb{A}^l_{v^l}$ is the equality relation. Then B is a standard basis of $\mathcal{S}^l$.*

Proof. We prove by induction that, for any $\mathbf{b} \in \mathcal{S}$ and any $1 \leq l \leq k$, the tuple $b^l = b\!\uparrow^l$ can be $((B^k \cup \ldots B^l)\!\uparrow^l)$-decomposed. The base case of induction, $l = k$, is obvious, because $\mathcal{S}\!\uparrow^k = B^k\!\uparrow^k = \{\mathbf{b}^k\}$. Suppose that $\mathbf{b}\!\uparrow^{l+1}$ is $((B^k \cup \ldots B^{l+1})\!\uparrow^{l+1})$-decomposed, $f(\mathbf{c}_1\!\uparrow^{l+1}, \ldots, \mathbf{c}_m\!\uparrow^{l+1})$ where $B^k \cup \ldots \cup B^{l+1} = \{\mathbf{c}_1, \ldots, \mathbf{c}_m\}$ is its decomposition, and set $f(\mathbf{c}_1\!\uparrow^l, \ldots, \mathbf{c}_m\!\uparrow^l) = \mathbf{c}$.

Let C_j^l be the $\mu_{v^l}^l$-class containing $\mathbf{c}[v^l]$. Notice that $\mathbf{c}[v] = \mathbf{b}^l[v]$ for all $v \neq v^l$. Therefore, if $\theta_{v^l} = \underline{0}_{v^l}$ then $\mathbf{c} = \mathbf{b}^l$, and $\mathbf{b}^l = \mathbf{d}(\mathbf{c}, \mathbf{a}\!\uparrow^l, \mathbf{a}\!\uparrow^l)$ where $B_j^l = \{\mathbf{a}\}$.

Otherwise, $\mathbf{b}^l = \mathbf{d}(\mathbf{c}, \mathbf{a}_c\!\uparrow^l, \mathbf{a}_b\!\uparrow^l)$ where $c = \mathbf{c}[v^l]$, $b = \mathbf{b}^l[v^l]$, and $\mathbf{a}_b, \mathbf{a}_c \in B_j^l$. $\square$

The coordinates of $\mathbf{a}$ in the basis B we will denote by $K(\mathbf{a})$. The tuple $K(\mathbf{a})$ consists of parts $K^k(\mathbf{a}), \ldots, K^l(\mathbf{a})$ which correspond to the parts $B^k, \ldots, B^l$ of B. Further, each $K^i(\mathbf{a})$ consists of $K_1^i(\mathbf{a}), \ldots, K_s^i(\mathbf{a})$ which in their turn correspond to $B_1^i, \ldots, B_s^i$. Finally, each $K_p^i(\mathbf{a})$ is a tuple of integers $(\alpha_1, \ldots, \alpha_m)$. By the construction of the standard basis, at most one of $K_1^i(\mathbf{a}), \ldots, K_s^i(\mathbf{a})$ is non-zero, and this non-zero tuple, $K_p^i(\mathbf{a})$, contains two non-zero components, -1 and 1.

When solving equations we shall need a notation for the coordinates of an unknown vector. These unknown coordinates will be denoted by $K(x)$.

Let $K_p^i(\mathbf{a}) = (\alpha_1, \ldots, \alpha_m)$, $B_p^i = \{\mathbf{a}_1, \ldots, \mathbf{a}_m\}$. Sometimes we will use the notation $\mathbf{b}+K_p^i(\mathbf{a})\cdot B_p^i$ which denotes just $\mathbf{b}$ if $K_p^i(\mathbf{a})$ is a zero tuple, and $\mathbf{d}(\mathbf{b}, \mathbf{a}_i, \mathbf{a}_j)$ where $\alpha_i = -1$, $\alpha_j = 1$. Since at most one of $K_1^i(\mathbf{a}), \ldots, K_s^i(\mathbf{a})$ is non-zero, we may define $\mathbf{b} + K^i(\mathbf{a}) \cdot B^i$ to be $\mathbf{b} + K_p^i(\mathbf{a}) \cdot B_p^i$ where $K_p^i(\mathbf{a})$ is the non-zero part of $K^i(\mathbf{a})$.

5.3 Constructing a basis

In this section we describe an algorithm that builds a standard basis of the solution space of a given problem instance $\mathcal{P}$. The algorithm produces a plan for $\mathcal{P}$, as is described in Section 5.1, and then finds the basis inductively starting from the trivial problem instance $\mathcal{P}^k$. We denote the solution space of $\mathcal{P}^l$ by $\mathcal{S}^l$. There are two cases when finding a basis of $\mathcal{P}^l$. The first one, when the lth step is of type **3**, is easy because of Lemma 1. In this case, for each tuple $\mathbf{a}$ from the basis of $\mathcal{S}^{l+1}$, the algorithm finds a representative $\mathbf{b}$ from $\mathcal{S}^l$ such that $\mathbf{b}\!\uparrow^{l+1} = \mathbf{a}$, and for each element of $\mathbb{A}_{v^l}^l$, add a tuple to this set of representatives. Second case, when lth step is of type **2**, is more complicated. In this case the algorithm finds a basis of the solution space for each block $C_1, \ldots, C_s$ of the monolith $\mu_{v^l}^l$ of $\mathbb{A}_{v^l}^l$ separately. For this it takes a basis B_{C_p} of $\mathcal{S}_{C_p} = \{\mathbf{a} \in \mathcal{S}^{l+1}\colon \mathbf{a} = \mathbf{b}\!\uparrow^{l+1}, \mathbf{b}[v^l] \in C_p\}$, $1 \leq p \leq s$, which was found in the previous $(l+1)$th step; and for each $1 \leq t \leq q$, and each $\mathbf{a} \in B_{C_p}$ finds a vector $\mathbf{a}_t \in \mathbb{A}^l$ such that $\mathbf{a}_t\big|_{s_t^l} \in \varrho_t^l$ and $\mathbf{a}_t\!\uparrow^{l+1} = \mathbf{a}$. The set $\{\mathbf{a}_t\colon \mathbf{a} \in B_{C_p}\}$ is denoted by $B_{C_p,t}$. Then the algorithm takes an arbitrary vector $\mathbf{a} \in B_{C_p,t}$, sets $a = \mathbf{a}[v^l]$, and set $D'_{p,t}$ to be the set of elements from $a/_{\mu_{v_l}^l}$ if $v^l \notin s_t^l$ or ϱ_t^l is v^l-rectangular modulo $\mu_{v^l}^l$, or $\{a\}$ otherwise, extended by components of $\mathbf{a}$ to vectors from $\mathbb{A}^l$. Finally, the algorithm finds a basis of intersection of subalgebras generated by basises $B_{C_p,t} \cup D'_{p,t}$, $1 \leq t \leq q$.

During this process the problem instance may be tightened, that forces rearranging the plan, because 3-minimality may be destroyed, or the graph G^l changed. The formal description of the algorithm follows.

INPUT. $\mathcal{P} = (V; \{\mathbb{A}_v : v \in V\}; \{C_1, \ldots, C_q\})$ where $\mathbb{A}_v$ are Mal'tsev with a Mal'tsev term $\mathbf{d}$, $C_t = (s_t, \varrho_t)$.

OUTPUT. A standard basis B of the solution space, or "NO" if the problem has no solution.

ALGORITHM.

Step 1 Let $\theta_{v,1}, \ldots, \theta_{v,t_v}$ be meet-irreducible congruences of $\mathbb{A}_v$, $v \in V$, such that $\theta_{v,1} \cap \ldots \cap \theta_{v,t_v} = \underline{0}_v$. **For each** $v \in V$ **set** $\mathbb{A}^1_{(v,1)} = \mathbb{A}_v/_{\theta_{v,1}}, \ldots, \mathbb{A}^1_{(v,t_v)} = \mathbb{A}_v/_{\theta_{v,t_v}}$. Then $\mathbb{A}_v$ is a subdirect product of $\mathbb{A}^1_{(v,1)}, \ldots, \mathbb{A}^1_{(v,t_v)}$. **If** $\mathbb{A}_v$ is subdirectly irreducible, **then set** $t_v = 1$ and $\mathbb{A}^1_{(v,1)} = \mathbb{A}_v$.

Step 2 **Set**

$W^1 = \bigcup_{v \in V} \{(v, j) \colon 1 \le j \le t_v\}$.

$C'^1_t = (s'^1_t, \varrho'^1_t)$, for each $1 \le t \le q$, where

$$\begin{aligned} s'^1_t &= \bigcup_{v \in s_t} \{(v, j) \colon 1 \le j \le t_v\}; \\ \varrho'^1_t &= \{(\mathbf{a}[v]/_{\theta_{v,1}}, \ldots, \mathbf{a}[v]/_{\theta_{v,t_v}})_{v \in s_t} \colon (\mathbf{a}[v])_{v \in s_t} \in \varrho_t\}. \end{aligned}$$

$\mathcal{P}'^1 = (W^1; \{\mathbb{A}^1_v \colon v \in W^1\}, C'^1_1, \ldots, C'^1_q)$.

Step 3 **Establish 3-minimality**.

Step 4 **Find** the digraph $G^1 = G(\mathcal{P}'^1) = (W^1, E^1)$ where $(v, w) \in E^1$ if and only if $\mathcal{S}'^1_{\{v,w\}}$ is the graph of a mapping $\varphi_{v,w} \colon \mathbb{A}^1_v \mapsto \mathbb{A}^1_w$.

Step 5 **Choose** a representative from each strongly connected component of G^1; let V^1 denote the set of the representatives. **Set** $\mathcal{P}^1 = (V^1; \{\mathbb{A}^1_v \colon v \in V^1\}; C^l_1, \ldots, C^l_q\}$ that is obtained from $\mathcal{P}'^1$ as follows. For each $C'^1_t = (s'^1_t, \varrho'^1_i)$ we **replace** each variable $v \in s'^1_i = (v_1, \ldots, v_m)$ with v', replace ϱ'^1_i with the relation $\{(\varphi^{-1}_{v'_1,v_1}(\mathbf{a}[v_1]), \ldots, \varphi^{-1}_{v'_m,v_m}(\mathbf{a}[v_m])) \colon \mathbf{a} \in \varrho'^{l+1}_i\}$, and then **remove** all repetitions of entries from the obtained constraint scope and corresponding coordinate positions of the obtained relation.

Step 6 **Apply** the procedure of planning to $\mathcal{P}^1$.

Step 7 **If** $\mathcal{P}^k$ has an empty constraint, **Output** 'NO'. Otherwise, as all the algebras $\mathbb{A}^k_v$ are trivial, the problem instance $\mathcal{P}^k$ has the only solution. **Set** $B = B^k$ to be the set consisting of this solution.

Step 8 **For each** $1 \le l < k$ **do** the following.

Step 8.1 Suppose we have a basis $\overline{B} = \overline{B}^k \cup \ldots \cup \overline{B}^{l+1}$ of the solution space $\mathcal{S}^{l+1}$. **If** lth step is of type **3**, **then do**

Step 8.1.1 **For each** $\mathbf{a} \in \overline{B}$ **choose** an element a such that $a\!\!\upharpoonright^{l+1} = \mathbf{a}|_{v^l\upharpoonright^{l+1}}$, **and set** $\mathbf{a}'$ to be such that

$$\mathbf{a}'[w] = \begin{cases} \mathbf{a}[w], & \text{if } w \neq v^l,\ w \in V^{l+1}; \\ a, & \text{if } w = v^l; \\ \varphi_{w',w}(\mathbf{a}'[w']), & \text{otherwise, } w' \text{ is the variable of } V^{l+1} \\ & \text{from the same strongly connected} \\ & \text{component } G^{l+1} \text{ as } w. \end{cases}$$

Then set $B^j = \{\mathbf{a}' : \mathbf{a} \in \overline{B}^j\}$ for $l < j \leq k$.

Step 8.1.2 Let $C_1, \ldots, C_s$ be the $\mu^l_{v^l}$-blocks. **For each** C_p **choose** $\mathbf{a}_p \in \mathcal{S}^{l+1}$ such that $\mathbf{a}_p|_{v\upharpoonright^{l+1}} = C_p\!\!\upharpoonright^{l+1}$.
/* See Section 6.5. */
Set B^l_p to be the set of all tuples $\mathbf{b} \in \mathbb{A}^l$ such that

$$\mathbf{b}[w] = \begin{cases} \mathbf{a}_p[w], & \text{if } w \neq v^l,\ w \in V^{l+1}; \\ b \in C_p, & \text{if } w = v^l; \\ \varphi_{w',w}(\mathbf{b}[w']), & \text{otherwise, } w' \text{ is the variable of } V^{l+1} \\ & \text{from the same strongly connected} \\ & \text{component of } G^{l+1} \text{ as } w, \end{cases}$$

and $B^l = B^l_1 \cup \ldots \cup B^l_s$.

Step 8.2 **If** lth step is of type **2 then do**

Step 8.2.1 Let $C_1, \ldots, C_s$ be the $\mu^l_{v^l}$-blocks of $\mathbb{A}^l_{v^l}$, and $\mathcal{S}_{C_p}$, $1 \leq p \leq s$, be the set $\{\mathbf{a} \in \mathcal{S}^{l+1} \colon \mathbf{a} = \mathbf{b}\!\!\upharpoonright^{l+1},\ \mathbf{b}[v^l] \in C_p\}$. **For each** $1 \leq p \leq s$ **take** a basis B_{C_p} of $\mathcal{S}_{C_p}$.
/* B_{C_p} is already found in step $l+1$ */

Step 8.2.2 **For each** $1 \leq t \leq q$, **each** $1 \leq p \leq s$, and **each** $\mathbf{a} \in B_{C_p}$ **choose** $\mathbf{a}_t \in \mathbb{A}^l$ such that
$\mathbf{a}_t\!\!\upharpoonright^{l+1} = \mathbf{a}$,
$\mathbf{a}_t|_{s^l_t} \in \varrho^l_t$.
/* Such a vector $\mathbf{a}_t$ exists, because $\mathbf{a}|_{s^{l+1}_t} \in \varrho^{l+1}_t = \varrho^l_t\!\!\upharpoonright^{l+1}$. */
Set $B_{C_p,t} = \{\mathbf{a}_t \colon \mathbf{a} \in B_{C_p}\}$.

Step 8.2.3 **For each** $1 \leq p \leq s$ **fix** a tuple $\mathbf{a}^p \in B_{C_p}$, the corresponding tuples $\mathbf{a}^p_1, \ldots, \mathbf{a}^p_s$ from $B_{C_p,1}, \ldots, B_{C_p,s}$ respectively; **and for each** $1 \leq t \leq q$, **set** $D_{p,t}$ to be $\mathbf{a}^p_t[v^l]/_{\mu^l_{v^l}}$ if $v^l \notin s^l_t$ or ϱ^l_t is v^l-rectangular modulo $\mu^l_{v^l}$, and $\{\mathbf{a}^p_t[v^l]\}$ otherwise.

Step 8.2.4 **Set** $D'_{p,t} = \{\mathbf{b} \in \mathbb{A}^l \colon \mathbf{b}[v^l] \in D_{p,t},\ \mathbf{b}|_{V^l - \{v^l\}} = \mathbf{a}^p_t|_{V^l - \{v^l\}}\}$.

Step 8.2.5 **For each** $1 \le p \le s$ **solve** the system of equations

$$
\begin{array}{rl}
\multicolumn{2}{l}{\mathbf{b}^k_{p,1} + K^{k-1}(x)\cdot B^{k-1}_{C_p,1} + \ldots + K^{l+1}(x)\cdot B^{l+1}_{C_p,1} + y^1_1\mathbf{b}^1_1 + \ldots + y^{n_1}_1\mathbf{b}^{n_1}_1} \\
= & \mathbf{b}^k_{p,2} + K^{k-1}(x)\cdot B^{k-1}_{C_p,2} + \ldots + K^{l+1}(x)\cdot B^{l+1}_{C_p,2} + y^1_2\mathbf{b}^1_2 + \ldots + y^{n_2}_2\mathbf{b}^{n_2}_2 \\
\vdots & \\
\multicolumn{2}{l}{\mathbf{b}^k_{p,1} + K^{k-1}(x)\cdot B^{k-1}_{C_p,1} + \ldots + K^{l+1}(x)\cdot B^{l+1}_{C_p,1} + y^1_1\mathbf{b}^1_1 + \ldots + y^{n_1}_1\mathbf{b}^{n_1}_1} \\
= & \mathbf{b}^k_{p,q} + K^{k-1}(x)\cdot B^{k-1}_{C_p,q} + \ldots + K^{l+1}(x)\cdot B^{l+1}_{C_p,q} + y^1_q\mathbf{b}^1_q + \ldots + y^{n_q}_q\mathbf{b}^{n_q}_q
\end{array} \tag{1}
$$

where $B_{C_p,t} = \{\mathbf{b}^k_{p,t}\} \cup B^{k-1}_{C_p,t} \cup \ldots \cup B^{l+1}_{C_p,t}$, $D_{p,t} = \{\mathbf{b}^1_t, \ldots, \mathbf{b}^{n_t}_t\}$. The solution space of the system is denoted by $\mathcal{S}'_p$, and its standard basis by E_p. Let also $\mathcal{S}' = \bigcup_{1\le p\le s} \mathcal{S}'_p$.
/* Since each E_p is a standard basis, we have $E_p = E^k_p \cup \ldots \cup E^l_p$. For an algorithm solving the system see Section 6.2.*/

Step 8.2.6 **If** all E_p are empty, **then Output**("NO") **and Stop**.

Step 8.2.7 **Otherwise**, transform the sets $E_1, \ldots, E_p$ to a standard basis.
/* See Section 6.6 */

Step 8.3 **For each** $i \in \{k, \ldots, l-1\}$, **each** $v \in V^i$, **and** a subalgebra $\mathbb{B}$ of $\mathbb{A}^i_v$ **find** a standard basis of the set $\mathcal{S}_{\mathbb{B}} = \{\mathbf{a} \in \mathcal{S}^l{\uparrow}^i \colon \mathbf{a}[v] \in \mathbb{B}\}$ if $i \ne l-1$, and of the set $\mathcal{S}'_{\mathbb{B}} = \{\mathbf{a} \in \mathcal{S}^l : \mathbf{a}|_{v\uparrow^l} \in \mathbb{B}{\uparrow}^l\}$ otherwise.
/* See Section 6.4 */

Step 8.4 **For each** tuple **a from each** constraint relation ϱ^l_t **find** a basis of the set $\{\mathbf{b} \in \mathcal{S}^l \colon \mathbf{b}|_{s^l_t} = \mathbf{a}\}$. For this **do**

Step 8.4.1 Let $s^l_t = \{v_1, \ldots, v_n\}$. **Set** $D^0 = B$.

Step 8.4.2 **For each** $1 \le j \le n$ **find** a standard basis of the set $\{\mathbf{b} \in \langle D^{j-1}\rangle : \mathbf{b}[v_j] = \mathbf{a}[v_j]$.
/* See Section 6.4. */

Step 8.4.3 **Set** $D = D^n$.

Step 8.4.4 **If** the basis D is empty, then remove **a** from ϱ^l_t, and all **b** from ϱ^i_t, $1 \le i < l$, such that $\mathbf{b}{\uparrow}^l = \mathbf{a}$.

Step 8.5 Denote by $\mathcal{P}^{1\prime}$ the problem instance obtained from $\mathcal{P}^1$ in the previous step. **If** there is 3-element subset $W \subseteq V^1$ such that the sets of partial solutions to $\mathcal{P}^{1\prime}$, and $\mathcal{P}^1$ for W are different, then **establish** 3-minimality of $\mathcal{P}^{1\prime}$, denote the obtained problem instance by $\mathcal{P}^1$ **and Goto** Step 3.

Step 8.6 **Otherwise, build** the graph $G(\mathcal{P}^{l\prime})$ where $\mathcal{P}^{l\prime}$ is the problem instance obtained from $\mathcal{P}^l$ in Step 8.4. **If** $G(\mathcal{P}^{l\prime}) \ne G(\mathcal{P}^l)$ **then set** $\mathcal{P}^1$ to be $\mathcal{P}^{1\prime}$, **and Goto** Step 3.

6 Subroutines and comments to the algorithm

6.1 Solutions of the system (1) and of the problem instance

6.1.1 Near-standard decomposition

In this section we need an extended version of the standard basis decomposition.

Suppose that $B = B^l \cup \ldots \cup B^k$ is a basis of $\mathcal{S}^l$, $K(x)$ is an arbitrary tuple of integers, but $K^k(x) = (1)$, and $\sum_{i=1}^m \alpha_i = 0$ for all $K_p^j(\mathbf{x}) = (\alpha_1, \ldots, \alpha_m)$. Define an element $\mathbf{b}$ of $\mathbb{A}^l$ through the following rules.

- $\mathbf{b}^k = \mathbf{a}$ where $B^k = \{\mathbf{a}\}$.
- For $l \le j < k$ suppose that $\mathbf{b}^{j+1}$ is already defined.
- Let $B_1^j, \ldots, B_s^j$ be parts of the basis B^j, $\mathbf{b}_0 = \mathbf{b}^{j+1}$, $\mathbf{b}_{p-1}$ already defined, and $B_p^j = \{\mathbf{a}_1, \ldots, \mathbf{a}_m\}$, $K_p^j(x) = (\alpha_1, \ldots, \alpha_m)$.

  In the term $\mathbf{d}(x, y, z)$ we call the positions x, z **even**, and the position y **odd**. Set

  $$\mathbf{b}_p = \mathbf{d}(\ldots \mathbf{d}(\mathbf{d}(\mathbf{b}_{p-1}, \mathbf{a}_{i_1}), \mathbf{a}_{i_2}, \mathbf{a}_{i_4}) \ldots)$$

  where the numbers of occurrences of $\mathbf{a}_i$ in even and odd positions are β_i, γ_i respectively, and $\beta_i - \gamma_i = \alpha_i$ for $i \in \{1, \ldots, m\}$. (Therefore, $\mathbf{b}_p$ is not uniquely defined.) Set $\mathbf{b}^j = \mathbf{b}_s$.

Finally, $\mathbf{b} = \mathbf{b}^l$.

Lemma 3 *An element has a near-standard B-decomposition if and only if it has the standard B-decomposition.*

Indeed, if $\mathbf{b}$ has a near-standard B-decomposition, then $\mathbf{b}$ belongs to the algebra generated by B. Therefore, $\mathbf{b}$ has the standard B-decomposition.

6.1.2 Correspondence between the solutions of the linear system and of the problem instance

In this section we, first, show how to link the solutions of a linear system of the form (1) and the solutions of the problem instance, and second, how to reduce the system (1) to a linear system over certain Abelian group.

Suppose that lth step is of type **2**, and for pth $\mu_{v^l}^l$-class C_p there appear the system

$$\begin{aligned}
&\mathbf{b}_{p,1}^k + K^{k-1}(x) \cdot B_{C_p,1}^{k-1} + \ldots + K^{l+1}(x) \cdot B_{C_p,1}^{l+1} + y_1^1 \mathbf{b}_1^1 + \ldots + y_1^{n_1} \mathbf{b}_1^{n_1} \\
&\quad = \ \mathbf{b}_{p,2}^k + K^{k-1}(x) \cdot B_{C_p,2}^{k-1} + \ldots + K^{l+1}(x) \cdot B_{C_p,2}^{l+1} + y_2^1 \mathbf{b}_2^1 + \ldots + y_2^{n_2} \mathbf{b}_2^{n_2} \\
&\quad \vdots \\
&\mathbf{b}_{p,1}^k + K^{k-1}(x) \cdot B_{C_p,1}^{k-1} + \ldots + K^{l+1}(x) \cdot B_{C_p,1}^{l+1} + y_1^1 \mathbf{b}_1^1 + \ldots + y_1^{n_1} \mathbf{b}_1^{n_1} \\
&\quad = \ \mathbf{b}_{p,q}^k + K^{k-1}(x) \cdot B_{C_p,q}^{k-1} + \ldots + K^{l+1}(x) \cdot B_{C_p,q}^{l+1} + y_q^1 \mathbf{b}_q^1 + \ldots + y_q^{n_q} \mathbf{b}_q^{n_q}
\end{aligned} \tag{2}$$

where $B_{C_p,t} = \{\mathbf{b}^k_{p,t}\} \cup B^{k-1}_{C_p,t} \cup \ldots \cup B^{l+1}_{C_p,t}$ is such that $B_{C_p,t}{\uparrow}^{l+1}$ is a basis of $\mathcal{S}_{C_p}$, and for each $\mathbf{a} \in B_{C_p,t}$, $\mathbf{a}|_{s^l_t} \in \varrho^l_t$; $\{\mathbf{b}^1_t, \ldots, \mathbf{b}^{n_t}_t\}$ is the basis $D'_{p,t}$.

Lemma 4 *A tuple* $\mathbf{c} \in \mathbb{A}^l$ *is a solution to* $\mathcal{P}^l$ *if and only if there are* $(K^{k-1}(x), \ldots, K^{l+1}(x), y^1_1, \ldots, y^{n_1}_1, \ldots, y^{n_q}_q)$ *such that, for any* $1 \leq t \leq q$, $(K^{k-1}(x), \ldots, K^{l+1}(x), y^1_t, \ldots, y^{n_t}_t)$ *are near-standard coordinates, and* $\mathbf{c}$ *can be represented in the form*

$$\mathbf{b}^k_{p,t} + K^{k-1}(x) \cdot B^{k-1}_{C_p,t} + \ldots + K^{l+1}(x) \cdot B^{l+1}_{C_p,t} + y^1_1 \mathbf{b}^1_1 + \ldots + y^{n_1}_1 \mathbf{b}^{n_1}_1$$

where p *is such that* $\mathbf{c}[v^l] \in C_p$.

Proof. Let $\mathbf{c} \in \mathcal{S}^l$, and $\mathbf{c}[v^l] \in C_p$. Then, for any $1 \leq t \leq q$, $\mathbf{c}{\uparrow}^{l+1} \in \mathcal{S}_{C_p}$ can be decomposed

$$\mathbf{c}{\uparrow}^{l+1} = \mathbf{b}^k_{p,t} + K^{k-1}(\mathbf{c}) \cdot B^{k-1}_{C_p,t}{\uparrow}^{l+1} + \ldots + K^{l+1}(\mathbf{c}) \cdot B^{l+1}_{C_p,t}{\uparrow}^{l+1}$$

where $K^k(\mathbf{c}), \ldots, K^{l+1}(\mathbf{c})$ does not depend on t. For each $1 \leq t \leq q$, set

$$\mathbf{a}_t = (\mathbf{b}^k_{p,t} + K^{k-1}(\mathbf{c}) \cdot B^{k-1}_{C_p,t} + \ldots + K^{l+1}(\mathbf{c}) \cdot B^{l+1}_{C_p,t})$$

Notice that $\mathbf{a}_t[w] = \mathbf{c}[w]$ for all variables $w \neq v^l$. If $D'_{p,t} = \{\mathbf{b}^1_t, \ldots, \mathbf{b}^{n_t}_t\}$ is such that $\{\mathbf{b}^1_t[v^l], \ldots, \mathbf{b}^{n_t}_t[v^l]\} = C_p$ (see p. 20) then

$$\mathbf{c} = \mathbf{d}(\mathbf{a}, \mathbf{b}^i_t, \mathbf{b}^j_t)$$

where $\mathbf{b}^i_t[v^j] = \mathbf{a}[v^j]$, $\mathbf{b}^j_t[v^j] = \mathbf{c}[v^j]$. Therefore, there are $y^1_t, \ldots, y^{n_t}_t$ such that

$$\mathbf{c} = \mathbf{b}^k_{p,t} + K^{k-1}(\mathbf{c}) \cdot B^{k-1}_{C_p,t} + \ldots + K^{l+1}(\mathbf{c}) \cdot B^{l+1}_{C_p,t} + y^1_t \mathbf{b}^1_t + \ldots + y^{n_t}_t \mathbf{b}^{n_t}_t.$$

In fact, $y^i_t = -1$, $y^j_t = 1$, and $y^m_t = 0$ otherwise. If $|D'_{p,t}| = 1$ then $\mathbf{c}|_{s^l_t} = \mathbf{a}$ and $y^1_t = 0$.

Conversely, if the conditions of the lemma hold then, for every $\leq t \leq q$, the tuple $\mathbf{c}|_{s^l_t}$ can be represented in the form

$$\mathbf{b}^k_{p,t}|_{s^l_t} + K^{k-1}(x) \cdot B^{k-1}_{C_p,t}|_{s^l_t} + \ldots + K^{l+1}(x) \cdot B^{l+1}_{C_p,t}|_{s^l_t} + y^1_1 \mathbf{b}^1_1|_{s^l_t} + \ldots + y^{n_1}_1 \mathbf{b}^{n_1}_1|_{s^l_t}.$$

Every tuple involved in this representation belongs to ϱ^l_t, hence, $\mathbf{c}|_{s^l_t}$ also belongs to ϱ^l_t, and so $\mathbf{c}$ is a solution to $\mathcal{P}^l$. $\square$

Lemma 4 implies that a tuple $\mathbf{c}$ is a solution to $\mathcal{P}^l$ if and only if its near-standard coordinates in basises $B_{C_p,t}$, $1 \leq t \leq q$, form a solution to (2).

For every variable $w \in V^l$, $w \neq v^l$, each equation of (2) holds for any $K^{k-1}(x), \ldots, K^{l+1}(x)$, $y^1_1, \ldots, y^{n_q}_q$ whenever they are near-standard coordinates. Indeed, we have $\mathbf{c}_{t_1}[w] = \mathbf{c}_{t_2}[w]$, for any $\mathbf{c} \in B_{C_p}$, $t_1, t_2 \in \{1, \ldots, q\}$, and $w \neq v^l$. Therefore

$$\begin{aligned}&(\mathbf{b}^k_{p,t_1} + K^{k-1}(x) \cdot B^{k-1}_{p,t_1} + \ldots + K^{l+1}(x) \cdot B^{l+1}_{p,t_1})[w] \\ = \quad &(\mathbf{b}_{p,t_2} + K^{k-1}(x) \cdot B^{k-1}_{p,t_2} + \ldots + K^{l+1}(x) \cdot B^{l+1}_{p,t_2})[w];\end{aligned}$$

let us denote this element by $\mathbf{b}[w]$. Then, we have $\mathbf{b}_1^1[w] = \ldots = \mathbf{b}_1^{n_1}[w] = \mathbf{b}_2^1[w] = \ldots = \mathbf{b}_q^{n_q}[w] = \mathbf{z}[w]$. So, for each $t \in \{1, \ldots, q\}$, the expression in the right (left for $t = 1$) side is equal to

$$\mathbf{b}[w] + y_t^1\mathbf{z}[w] + \ldots + y_t^{n_t}\mathbf{z}[w] = \mathbf{d}(\ldots(\mathbf{d}(\mathbf{b}[w], \mathbf{z}[w], \mathbf{z}[w]), \ldots), \mathbf{z}[w]\mathbf{z}[w]) = \mathbf{b}[w].$$

Further, for any t and $\mathbf{a} \in B_{C_p,t} \cup D'_{p,t}$, the element $\mathbf{a}[v^l]$ belongs to C_p. Let $B_{C_p,t} = \{\mathbf{a}_t^1, \ldots, \mathbf{a}_t^m\}$, $D'_{p,t} = \{\mathbf{b}_t^1, \ldots, \mathbf{b}_t^{n_t}\}$, and $a_t^i = \mathbf{a}_t^i[v^l]$, $b_t^j = \mathbf{b}_t^j[v^l]$. Let also $(K^{k-1}(x), \ldots, K^{l+1}(x)) = (x_2, \ldots, x_{m-1})$. Since lth step is of type **2**, the Mal'tsev operation $\mathbf{d}$ on C_p is of the form $\mathbf{d}(x, y, z) = x - y + z$ where $+, -$ are operations of an Abelian group $\mathbb{Q} = (C_p; \mathbf{d}(x, a, y), \mathbf{d}(a, x, a), a)$, and $a \in C_p$ is an arbitrary element. Then each equation of (2) can be rewritten as

$$\begin{aligned}
& (a_1^1 + x_2a_1^2 + \ldots + x_ma_1^m + y_1^1b_1^1 + \ldots + y_1^{n_1}b_1^{n_1} \\
= \;& (a_t^1 + x_2a_t^2 + \ldots + x_ma_t^m + y_t^1b_t^1 + \ldots + y_t^{n_t}b_t^{n_t}.
\end{aligned} \tag{3}$$

Finally, one may derive from (3) the linear system

$$\begin{aligned}
& x_2(a_1^2 - a_2^2) + \ldots + x_m(a_1^m - a_2^m) + y_1^1b_1^1 + \ldots + y_1^{n_1}b_1^{n_1} \\
+ \;& y_2^1b_2^1 + \ldots + y_2^{n_2}b_2^{n_2} = a_2^1 - a_1^1, \\
& \vdots \\
& x_1(a_1^2 - a_q^2) + \ldots + x_m(a_1^m - a_q^m) + y_1^1b_1^1 + \ldots + y_1^{n_1}b_1^{n_1} \\
+ \;& y_q^1b_q^1 + \ldots + y_q^{n_q}b_q^{n_q} = a_q^1 - a_1^1.
\end{aligned} \tag{4}$$

6.1.3 How to choose a basis of the solution space of the linear system

Every solution $(x_2, \ldots, x_m, y_1^1, \ldots, y_q^{n_q})$ to the system (4) such that, for any $1 \le t \le q$, $(x_2, \ldots, x_m, y_t^1, \ldots, y_t^{n_t})$ are near-standard coordinates corresponds to a solution of $\mathcal{P}^l$ represented as

$$\mathbf{a}_1^1 + x_2 \cdot \mathbf{a}_1^2 + \ldots + x_m \cdot \mathbf{a}_1^m + y_1^1 \cdot \mathbf{b}_1^1 + \ldots y_1^{n^1} \cdot \mathbf{b}_1^{n_1}.$$

We therefore have to find a set of solutions to (4) corresponding vectors of which form a standard basis the solution space. The set of those tuples whose near-standard coordinates satisfy the system (2) will be denoted by $\mathcal{S}_L$.

Notice that due to Lemma 4, the set of vectors from $\mathbb{A}^l$ corresponding to the solution space of (1) is a subalgebra of $\mathbb{A}^l$.

INPUT A system L of the form (1), and a set $B \subseteq \prod_{v \in V^l} \mathbb{A}_v^l$ such that $B{\upharpoonright}^{l+1}$ is a basis of $\mathcal{S}^{l+1}$ and $\mathbf{a}|_{s_1^l} \in \varrho_1^l$ for all $\mathbf{a} \in B$.

OUTPUT A standard basis $\widetilde{B}$ of the set $\mathcal{S}_L$ of elements whose (standard) coordinates satisfy the system L.

ALGORITHM

Step 1 **Construct** the linear system L' of the form (4).

Step 2 **For each** $l \leq j < k$, **and** $1 \leq t \leq s$ where $B_1^j, \ldots, B_s^j$ are the parts of the basis corresponding to jth step, **add** to L' the equation

$$x_1 + \ldots + x_m = 0$$

where $K_t^j(x) = (x_1, \ldots, x_m)$. The obtained system is denoted by L''.

Step 3 **Find** a basis D of the set of solutions of the system L''. This set is a coset in a direct power of $\mathbb{Q}$. **If** the system is inconsistent, **then** $\widetilde{B} = \varnothing$ **and Stop**.

Step 4 **Set** $\widetilde{B}^k = \{\mathbf{a}\}$ where

$$\mathbf{a} = K^k \cdot B^k + \ldots + K^l \cdot B^l,$$

and K is an arbitrary tuple from D.

Step 5 **For each** $l < j < k$ **do**

Step 5.1 **Denote** by Π the coset spanned on the set

$$\{(K^k, \ldots, K^{j+1}) : K \in D\}$$

Step 5.2 Let $B^j = B_1^j \cup \ldots \cup B_{s'}^j$, and $C'_1, \ldots, C'_{s'}$ be the $\mu^j_{v^j}$-blocks. **For each** $1 \leq p' \leq s'$ **do**

Step 5.2.1 Let $B_{C'_{p'}}$ be a basis of $\mathcal{S}_{C'_{p'}}$ that is the subspace of $\mathcal{S}^l{\uparrow}^j$ which consists of elements $\mathbf{a}$ with $\mathbf{a}[v^j] \in C'_{p'}$.
/* This basis is already known */
Let also $D_{p'}$ be a set of tuples $\{(K^k(\mathbf{a}), \ldots, K^{j+1}(\mathbf{a})) : \mathbf{a} \in B_{C'_{p'}}\}$ where $K(\mathbf{a})$ is the coordinates of $\mathbf{a}$ in B.

Step 5.2.2 **Find** a basis $\overline{D}_{p'}$ of the intersection of Π and the coset spanned on $D_{p'}$.
/* That is of the set of those partial solutions of L'' whose corresponding vectors lie in $\mathcal{S}_{C'_{p'}}$. */

Step 5.2.3 **If** $\overline{D}_{p'} = \varnothing$, **then set** $\widetilde{B}^j_{p'} = \varnothing$.

Step 5.2.4 **Otherwise choose** $(K_0^k, \ldots, K_0^{j+1}) \in \overline{D}_{p'}$ **and find** the set $\overline{\overline{D}}_{p'}$ of those tuples $K = (K^k, \ldots, K^{j+1}, K^j)$ from the space of partial solutions of L'' which are of the form

$$K^k = K_0^k, \ldots, K^{j+1} = K_0^{j+1}, K_r^j = (0, \ldots, 0) \text{ for all } r \neq p',$$

and $K_{p'}^j = (x_1, \ldots, x_n)$ is such that $x_1 = 0$ if $n = 1$, and there is $1 \leq r \leq n$ such that

$$x_i = \begin{cases} 1, & \text{if } i = r, \\ -1, & \text{if } i = r', \\ 0, & \text{otherwise,} \end{cases}$$

in the case when $n > 1$ where r' is such that

$$(K^k \cdot B^k + \ldots + K^{j+1} \cdot B^{j+1})[v^j] = \mathbf{b}^{r'}[v^j]$$

and $B_{p'}^j = \{\mathbf{b}^1, \ldots, \mathbf{b}^n\}$.

Step 5.2.5 **Set** $\widetilde{B}^j_{p'} = \{K^k \cdot B^k + \ldots + K^l \cdot B^l : K \in \overline{\overline{D}}_{p'}\}$.
/* Here K is near-standard. */

Step 5.3 **Set** $\widetilde{B}^j = \widetilde{B}^j_1 \cup \ldots \cup \widetilde{B}^j_{s'}$.

Step 6 Choose $\mathbf{a} \in \widetilde{B}^k \cup \ldots \cup \widetilde{B}^{l+1}$, **and find** a basis D^l of the subspace of the solution space of L'' that consists of elements $\mathbf{b}$ with $K^k(\mathbf{b}) = K^k(\mathbf{a}), \ldots, K^{l+1}(\mathbf{b}) = K^{l+1}(\mathbf{a})$. **Set** $E = \{K^k \cdot B^k + \ldots + K^l \cdot B^l : K \in D^l\}$. The set $\{a \in \mathbb{A}^l_{v_l} : a = \mathbf{a}[v^l],\ \mathbf{a} \in E\}$ is a subset M of C_p. **Set** $\widetilde{B}^l = \{\mathbf{b} : \mathbf{b}[v^l] \in M,\ \mathbf{b}|_{V^l - \{v^l\}} = \mathbf{b}|_{V^l - \{v^l\}}\}$.

Step 7 Set $\widetilde{B} = \widetilde{B}^k \cup \ldots \cup \widetilde{B}^l$.

To conclude this subsection we have to show that the set $\widetilde{B}$ is really a standard basis of $\mathcal{S}_L$.

Lemma 5 *The set $\widetilde{B}$ obtained by the algorithm from this subsection is a standard basis of the solution space, $\mathcal{S}_L$, of the system L.*

Proof. By the definition, for each element $\mathbf{a} \in \mathcal{S}_L$, the standard coordinates $K(\mathbf{a})$ give rise to a solution of L. Since standard coordinates satisfy the equations added in Step 2, solution spaces of L' and L'' determines the same set of vectors. Moreover, as is shown in Section 6.1.2, the systems L and L' are equivalent. Therefore denoting the set of vectors corresponding to solutions of L'' by $\mathcal{S}_{L''}$, we have $\mathcal{S}_L = \mathcal{S}_{L''}$.

Then we show that, for each $k \geq j \geq l$, the set $(\widetilde{B}^k \cup \ldots \cup \widetilde{B}^j)\!\uparrow^j$ is a standard basis of $\mathcal{S}_L\!\uparrow^j$. This trivially holds for $j = k$, and we have the induction base. So, suppose that the required property holds for $j + 1$.

For each $\mu^j_{v^j}$-block $C_{p'}$, the set $\widetilde{B}^j_{p'}$ may be chosen as arbitrary set such that $\widetilde{B}^j_{p'}\!\uparrow^j$ is of the form $\{\mathbf{a}_b : b \in C_{p'},\ b$ is the v^jth component of a vector from $\mathcal{S}_L\!\uparrow^j\}$ where

$$\mathbf{a}_b[w] = \begin{cases} b, & \text{if } w = v^j, \\ \mathbf{a}[w], & \text{otherwise,} \end{cases}$$

and $\mathbf{a}[w]$, $w \in V^j - \{v^j\}$ are certain fixed elements. However, it is easily seen from Steps 5.2.3, 5.2.4 that $\widetilde{B}^j_{p'}$, in fact, is of the required form. □

6.2 Solving equations over an Abelian group

In Section 5.2 we reduce the problem of solving of a system (2) to the problem of finding a basis of the solution space of a linear system over a finite Abelian group $\mathbb{Q}$. This system can be easily transformed to a problem from number theory.

Let

$$\begin{aligned} x_1\mathbf{a}_{11} + \ldots + x_n\mathbf{a}_{1n} &= \mathbf{b}_1 \\ &\vdots \\ x_1\mathbf{a}_{m1} + \ldots + x_n\mathbf{a}_{mn} &= \mathbf{b}_m \end{aligned}$$

be the given system. The group $\mathbb{Q}$ can be represented as a direct sum of cyclic groups $\mathbb{Q} = \sum_{i=1}^{r} \mathbb{G}_i$. Fix generating elements $g_1, \ldots, g_r$ of $\mathbb{G}_1, \ldots, \mathbb{G}_r$ respectively. We may assume that summands are subgroups of $\mathbb{Q}$ and therefore treat $g_1, \ldots, g_r$ as elements of $\mathbb{Q}$. Every element $\mathbf{g}$ of $\mathbb{Q}$ can be represented as $\alpha^1 g_1 + \ldots + \alpha^r g_r$ where $\alpha^1, \ldots, \alpha^r$ are residues modulo $s = \operatorname{lcm}\{|\mathbb{G}_1|, \ldots, |\mathbb{G}_r|\}$. We will write this fact as follows: $\mathbf{g} = (\alpha^1, \ldots, \alpha^r)$.

Set $\mathbf{a}_{ij} = (\alpha_{ij}^1, \ldots, \alpha_{ij}^r)$, $\mathbf{b}_i = (\beta_i^1, \ldots, \beta_i^r)$, $i \in \{1, \ldots, m\}$, $j \in \{1, \ldots, n\}$. Then the system can be rewritten in the form

$$\begin{aligned}
x_1\alpha_{11}^1 + \ldots + x_n\alpha_{1n}^1 &= \beta_1^1 \\
&\vdots \\
x_1\alpha_{11}^r + \ldots + x_n\alpha_{1n}^r &= \beta_1^r \\
x_1\alpha_{21}^1 + \ldots + x_n\alpha_{2n}^1 &= \beta_2^1 \\
&\vdots \\
x_1\alpha_{m1}^r + \ldots + x_n\alpha_{mn}^r &= \beta_m^r
\end{aligned}$$

The solution of this system is a coset of the group $(\mathbb{Z}_s)^n$. A generating set and shifting element for this coset can be found in time $O(n^3(mr)^3 \log s)$, $r = O(\log s)$, by known algorithm of number theory (see, e.g. [22]). The required generating set of the original linear system is now easily recoverable.

6.3 Finding a basis of a subalgebra

6.3.1 The algorithm

Input. A basis B of the solution space $\mathcal{S}^l$ of $\mathcal{P}^l$, subalgebra $\mathbb{B}$ of $u \in J\mathbb{A}_u^i$, $l-1 \le i \le k$, $J \subseteq V^i$.

Output. A standard basis $\overline{B}$ of $\mathcal{S}_{\mathbb{B}} = \{\mathbf{a} \in \mathcal{S}^l{\uparrow}^i \colon \mathbf{a}|_J \in \mathbb{B}\}$.

Algorithm.

Step 1 **For each** $\mathbf{c} \in \mathbb{B}$ **do**

/* Find a basis of that subset of $\mathcal{S}_{\mathbb{B}}$ which consists of elements $\mathbf{a}$ with $\mathbf{a}|_J = \mathbf{c}$. */

Step 1.1 **Set** $J^m = J{\uparrow}^m$ for $i \le m \le k$.

Step 1.2 **Set** $\mathbf{c}_m = \mathbf{c}{\uparrow}^m$ for $i \le m \le k$.

Step 1.3 Set $\mathcal{S}_{\mathbf{c}} = \{\mathbf{a} \in \mathcal{S}^l{\uparrow}^i \colon \mathbf{a}|_J = \mathbf{c}\}$. Set $\mathcal{T}_{\mathbf{c}}^m = \{\mathbf{a} \in \mathcal{S}^l{\uparrow}^m \colon \mathbf{a}|_{J^m} = \mathbf{c}_m\}$ if $m > i$, and $\mathcal{T}_{\mathbf{c}}^m = \mathcal{S}_{\mathbf{c}}$ if $m = i$.

Step 1.4 **Set** $D_{\mathbf{c}}^k = B^k{\uparrow}^k$.

Step 1.5 **For each** $i \le m < k$ **do**

Step 1.5.1 Suppose we have found a basis $\overline{D}_{\mathbf{c}}$ of $\mathcal{T}_{\mathbf{c}}^{m+1}$. **For each** $\mathbf{a} \in \overline{D}_{\mathbf{c}}$ **choose** a tuple $\mathbf{a}' \in \mathcal{S}^l{\uparrow}^m$ such that $\mathbf{a}'{\uparrow}^{m+1} = \mathbf{a}$.

/* The tuple $\mathbf{a}'$ can be found as follows. Let $K^k(\mathbf{a}), \ldots, K^{m+1}(\mathbf{a})$ be the coordinates of $\mathbf{a}$ in the basis $B\!\uparrow^{m+1}$. Then set

$$\mathbf{a}' = K^k(\mathbf{a}) \cdot B^k\!\!\uparrow^m + \ldots + K^{m+1}(\mathbf{a}) \cdot B^{m+1}\!\!\uparrow^m . \quad */$$

The set of all chosen tuples is denoted by $\widetilde{D}_{\mathbf{c}}$.

Step 1.5.2 CASE 1. mth step is of type **3**.

Step 1.5.3 SUBCASE 1A. $v^m \notin J^m$.
Let $C_1, \ldots, C_s$ be the $\mu^m_{v^m}$-blocks. **For each** $1 \le p \le s$ **find** $\mathbf{a}^p \in \mathcal{T}^m_c$ such that $\mathbf{a}^p[v^m] \in C_p$.
/* See Section 6.4. Actually, for some C_p such a vector may do not exist. */
Then **set**

$$D_c = \widetilde{D}_{\mathbf{c}} \cup E_1 \cup \ldots \cup E_s$$

where **if** $\mathbf{a}_p$ with the required properties exists, **then** $E_p = \{\mathbf{a}_b : b \in C_p\}$ with

$$\mathbf{a}_b[w] = \begin{cases} b, & \text{if } w = v^m; \\ \mathbf{a}^p[w], & \text{otherwise;} \end{cases}$$

otherwise, set $E_p = \varnothing$.
/* By Lemma 1, $D_c \subseteq \mathcal{S}^l\!\uparrow^m$. */

Step 1.5.4 SUBCASE 1B. $v^m \in J^m$.
Set $D_{\mathbf{c}} = \{\mathbf{a}' : \mathbf{a} \in \widetilde{D}_{\mathbf{c}}\}$ where

$$\mathbf{a}'[w] = \begin{cases} \mathbf{c}_m[v^m], & \text{if } w = v^m; \\ \mathbf{a}[w], & \text{otherwise.} \end{cases}$$

/* By Lemma 1 each $\mathbf{a}'$ belongs to $\mathcal{T}^m_{\mathbf{c}}$. */

Step 1.5.5 CASE 2. mth step is of type **2**.

Step 1.5.6 SUBCASE 2A. $v^m \notin J^m$.
Let $C_1, \ldots, C_s$ be those $\mu^m_{v^m}$-blocks for which $C_p \cap \widetilde{D}_{\mathbf{c}}|_{\{v^m\}} \neq \varnothing$. **For each** $1 \le p \le s$, **choose** $\mathbf{a}_p \in \widetilde{D}_{\mathbf{c}}$ such that $\mathbf{a}_p[v^m] \in C_p$
/* See Section 6.4. */
and set

$$D^m = D^m_1 \cup \ldots \cup D^m_s$$

with

$$D^m_p = \{\mathbf{a}'^{\,1}_p, \ldots, \mathbf{a}'^{\,k_p}_p\}$$

where

$$\mathbf{a}'^{\,j}_p = \mathbf{d}(\mathbf{a}_p, \mathbf{a}^1_p, \mathbf{a}^j_p),$$

and $\{\mathbf{a}^1_p, \ldots, \mathbf{a}^{k_p}_p\} = B^m_p$ is the part of the basis B_{C_p} of $\mathcal{S}_{C_p}$, and $\mathbf{a}^1_p[v^m] = \mathbf{a}_p[v^m]$.

/* Since $m \le i$, a basis of $\mathcal{S}_{C_p}$ is already found, see Step 8.3 of the algorithm from Section 5.3. */

/* Since, for any $\mathbf{a} \in D^m_p$, $\mathbf{a}\big|_{J^m} = \mathbf{a}_p\big|_{J^m} = \mathbf{c}_m$, we have $D^m_p \subseteq \mathcal{T}^m_c$ for all p. */

Step 1.5.7 SUBCASE 2B. $v^m \in J^m$.

Let C_p be that $\mu^m_{v^m}$-block which contains $\mathbf{c}_m[v]$.

Step 1.5.7.1 **Find** $\mathbf{a} \in \mathcal{S}^m$ such that $\mathbf{a}\big|_{J^m} = \mathbf{c}_m\big|_{J^m}$.

/* See Section 6.4. $\prod_{v\in J_m} \mathbb{A}^m_v$ is a homomorphic image of $\prod_{u\in J} \mathbb{A}^i_u$, and therefore, a 'small' algebra for which all the required information is known. */

Step 1.5.7.2 **Set** E_p to be $\{\mathbf{a}'^1, \ldots, \mathbf{a}'^n\}$ where

$$\mathbf{a}'^j = \mathbf{d}(\mathbf{a}, \mathbf{a}^1_p, \mathbf{a}^j_p).$$

and $\{\mathbf{a}^1_p, \ldots, \mathbf{a}^n_p\} = B^m_{C_p}$.

/* Since $m \le i$, a basis of $\mathcal{S}_{C_p}$ is already found, see Step 8.3 of the algorithm from Section 5.3. */

Step 1.5.7.3 **Solve** the equation

$$K^k(x)\cdot \widetilde{D}^k_{\mathbf{c}}[v^m] + \ldots + K^{m+1}(x)\cdot \widetilde{D}^{m+1}_c[v^m] + y_1\mathbf{a}'^1[v^m] + \ldots + y_n\mathbf{a}'^n[v^m] = \mathbf{c}_m[v^m] \quad (5)$$

where $\widetilde{D}_{\mathbf{c}} = \widetilde{D}^k_{\mathbf{c}} \cup \ldots \cup \widetilde{D}^{m+1}_{\mathbf{c}}$. Let $D_{\mathbf{c}}$ be a standard basis of its solution space.

/* See Section 6.3.2. */

Step 2 **Transform** the sets $D_{\mathbf{c}}$, $\mathbf{c} \in \mathbb{B}$, to a standard basis $\overline{B}$.

/* See Section 6.6 */

6.3.2 Solving an equation of the form (5)

Denote $\mathbf{c}_m[v^m]$ by c, $\mathbf{a}'^i[v^m]$ by a'_i for $\mathbf{a}'^i \in E_p$. As well as in Section 6.1.2, (5) can be reduced to a linear equation

$$x_2b_2 + \ldots + x_rb_r + y_1a'_1 + \ldots + y_na'_n = c - b_1$$

where $\{b_1\} = \widetilde{D}^k_{\mathbf{c}}[v^m]$, $\{\mathbf{b}_2, \ldots, \mathbf{b}_r\} = \widetilde{D}^{k-1}_{\mathbf{c}} \cup \ldots \cup \widetilde{D}^{m+1}_{\mathbf{c}}$. Then the equation can be solved analogously the linear system from Section 6.1.3. Notice also that when finding a standard basis of the solution space of the linear system the algorithm from Section 6.1.3 uses basises of sets of the form $\mathcal{S}_{\mathbb{C}}$. However, it does not cause a confusion, because $\mathbb{C}$ is always a subalgebra of $\mathbb{A}^j_v$ for certain $v \in V^j$ where $j > i$; and therefore a basis of $\mathcal{S}_{\mathbb{C}}$ is already found.

6.3.3 Soundness

Lemma 6 *The set $\overline{B}$ generated by the algorithm in this section for given number $l-1 \le i \le k$, a set $J \subseteq V^i$, and a subalgebra $\mathbb{B}$ of $\prod_{u\in J} \mathbb{A}^i_u$ is a standard basis, of $\mathcal{S}_{\mathbb{B}}$.*

Proof. We actually have to prove that $D_{\mathbf{c}}$ is a standard basis of $\mathcal{S}_{\mathbf{c}}$ for each $\mathbf{c} \in \mathbb{B}$. For this it is enough to prove that the set $D_{\mathbf{c}}$ generated in mth step of the algorithm is a standard basis of $\mathcal{T}^m_{\mathbf{c}}$. If $m = k$, this holds trivially, and we have the induction base.

Suppose that in $(m+1)$th step the algorithm has found a standard basis $\overline{D}_{\mathbf{c}}$ of $\mathcal{T}^{m+1}_{\mathbf{c}}$. There are two cases.

Case 1. mth step is of type **3**.
If $v^m \notin J^m$, then $\widetilde{D}_{\mathbf{c}} \subseteq \mathcal{T}^m_{\mathbf{c}}$, because for each $\mathbf{a} \in \overline{D}_{\mathbf{c}}$ and the corresponding vector $\mathbf{a}' \in \widetilde{D}_{\mathbf{c}}$, we have $\mathbf{a} = \mathbf{a}'{\uparrow}^{m+1}$ and $\mathbf{a}\big|_{J^{+1}m} = \mathbf{c}_{m+1}$ uniquely determines $\mathbf{a}\big|_{J^m}$, therefore, $\mathbf{a}\big|_{J^m} = \mathbf{c}_m$. Furthermore, $D^m_{\mathbf{c}} \subseteq \mathcal{T}^m_{\mathbf{c}}$ by Lemma 1; and Lemma 2 implies that $D_{\mathbf{c}}$ is a standard basis.

If $v^m \in J^m$, then $D_{\mathbf{c}} \subseteq \mathcal{S}^m$ by Lemma 1, and $D_{\mathbf{c}} \subseteq \mathcal{T}^m_{\mathbf{c}}$ by the choice of $D_{\mathbf{c}}$. Since for any $\mathbf{a}, \mathbf{b} \in \mathcal{T}^m_{\mathbf{c}}$ we have $\mathbf{a} = \mathbf{b}$ whenever $\mathbf{a}{\uparrow}^{m+1} = \mathbf{b}{\uparrow}^{m+1}$, the set $D_{\mathbf{c}}$ is a standard basis.

Case 2. mth step is of type **2**.
If $v^m \notin J^m$, then $D_{\mathbf{c}} \subseteq \mathcal{T}^m_{\mathbf{c}}$, and $D_{\mathbf{c}}$ is a standard basis by Lemma 2. If $v^m \notin J^m$, then the lemma follows from Lemma 5. □

6.4 Finding a representative of a subalgebra

We are given by elements $\mathbf{a}_1, \ldots, \mathbf{a}_n$ of $\prod_{v \in V^l} \mathbb{A}^l_v$, $J \subseteq V^l$, $\mathbf{a} \in \mathbb{B} = \prod_{u \in J} \mathbb{A}^l_u$, and are going to find an element $\mathbf{b}$ from the algebra generated by $\mathbf{a}_1, \ldots, \mathbf{a}_n$ and such that $\mathbf{b}\big|_J = \mathbf{a}$.

Notice that it can be checked in linear time, whether a belongs to the subalgebra of $\mathbb{B}$ generated by $\mathbf{a}_1\big|_J, \ldots, \mathbf{a}_n\big|_J$. Moreover, in the case when $\mathbf{a}$ belongs to the subalgebra, a representing term $f(\mathbf{a}_1\big|_J, \ldots, \mathbf{a}_n\big|_J) = a$ can also be found in linear time. Therefore, the required element may be taken as $\mathbf{b} = f(\mathbf{a}_1, \ldots, \mathbf{a}_n)$.

If $\mathbf{a}_1, \ldots, \mathbf{a}_n$ themselves form a subalgebra then bb can be chosen to be one of them.

6.5 Decomposing on a basis

Input. A basis B of the solution space $\mathcal{S}^l$, a tuple $\mathbf{a} \in \prod_{v \in V^l} \mathbb{A}^l_v$.

Output. $K(\mathbf{a})$ if $\mathbf{a} \in \mathcal{S}^l$, 'NO' otherwise.

Algorithm.

Step 1 Let $B^k = \{\mathbf{z}\}$.

Step 2 **For** $k - 1 \geq m \geq l$ **do**

Step 2.1 **Set** $\mathbf{b} = \mathbf{z}{\uparrow}^m + K^{k-1}(\mathbf{a}) \cdot B^{k-1}{\uparrow}^m + \ldots + K^{m+1}(\mathbf{a}) \cdot B^{m+1}{\uparrow}^m$.

Step 2.2 Let $C_1, \ldots, C_s$ be $\mu^m_{v^m}$-blocks.
If $\mathbf{a}{\uparrow}^m [v^m] \notin \{\mathbf{c}[v^m] \colon \mathbf{c} \in B^m{\uparrow}^m\}$ **then Output** 'NO' **and Stop, otherwise** let $\mathbf{a}{\uparrow}^m [v^m] \in C_p$.

Step 2.3 **If** $|B^m_p| = 1$ **and** $\mathbf{a}{\uparrow}^m \neq \mathbf{b}$ **then then Output** 'NO' **and Stop**.

Step 2.4 **If** $|B_p^m| > 1$ **then set** $K_i^m(\mathbf{a}) = (0,\ldots,0)$ **for all** $i \neq p$ **and** $K_p^m(\mathbf{a}) = (x_1,\ldots,x_m)$ where $C_p = \{a_1,\ldots,a_m\}$,

$$x_i = \begin{cases} 1, & \text{if } a_i = \mathbf{a}{\uparrow}^m\ [v^m] \\ -1, & \text{if } a_i = \mathbf{b}{\uparrow}^m\ [v^m] \\ 0, & \text{otherwise.} \end{cases}$$

If $\mathbf{a}{\uparrow}^m\ [v^m] = \mathbf{b}[v^m]$ **then** $K_p^m(\mathbf{a}) = (0,\ldots,0)$.

Soundness of this algorithm follows immediately from definition of a standard basis.

6.6 Transformation of a basis

The algorithm presented in this subsection is applied in two situations: Step 8.2.8 of the algorithm from Section 5.3, and Step 2 of the algorithm from Section 6.3. In the first case the basises $E_1,\ldots,E_s$ satisfy the condition $\{\mathbf{a}[v]: \mathbf{a} \in E\} = \mathbb{A}_v^l$, $E = E_1 \cup \ldots \cup E_s$ while in the second case a basis of $\mathcal{S}^l$ is known.

INPUT. Standard basises $E_1,\ldots,E_s$ of some subalgebras of $\mathbb{A}^l$.

OUTPUT. A standard basis B of the subalgebra generated by $E_1 \cup \ldots \cup E_s$.

ALGORITHM.

Step 1 **Set** $B^k = E_1^k$.

Step 2 **For each** $l \leq j < k$ **do**

Step 2.1 Suppose that $B^k,\ldots,B^{j+1}$ are already found.

Step 2.2 **Set** $\overline{E}^j = \bigcup_{1\leq p\leq s} E_p^j$, and let $C_1,\ldots,C_s$ be μ_{vj}^j-classes.

Step 2.3 **For each** $1 \leq p \leq s$ **do**

Step 2.3.1 Let E_p' denote the set $\{\mathbf{a} \in \overline{E}^j: \mathbf{a}{\uparrow}^j\ [v^j] \in C_p\}$, and let $E_p' = \{\mathbf{a}_1,\ldots,\mathbf{a}_t\}$. Each $\mathbf{a}_i{\uparrow}^{j+1}$ is $(B^k \cup \ldots \cup B^{k+1}){\uparrow}^{j+1}$-decomposable; let $\mathbf{a}_i{\uparrow}^{j+1} = f_i(\mathbf{b}_1{\uparrow}^{j+1}, \ldots, \mathbf{b}_r{\uparrow}^{j+1})$ where $B^k \cup \ldots \cup B^{k+1} = \{\mathbf{b}_1,\ldots,\mathbf{b}_r\}$.
/* For an algorithm finding the standard basis decomposition see Section 6.5. */
For any $1 \leq i \leq t$, **set** $\mathbf{a}_i' = f_i(\mathbf{b}_1{\uparrow}^j,\ldots,\mathbf{b}_r{\uparrow}^j)$, $\mathbf{a}_i'' = f_i(\mathbf{b}_1,\ldots,\mathbf{b}_r)$.

Step 2.3.2 **If**, for any $i \in \underline{t}$, $\mathbf{a}_i{\uparrow}^j = \mathbf{a}_i'$, then **set** $B_p^j = \{\mathbf{b}\}$ where $\mathbf{b}$ is an arbitrary tuple from B^{j+1} such that $\mathbf{b}{\uparrow}^j\ [v_j] \in C_p$.
/* Such a tuple exists by the definition of a basis. */

Step 2.3.3 **Otherwise**, suppose that for certain i $\mathbf{a}_i[v^j]{\uparrow}^j \neq \mathbf{a}_i'[v^j]$; without loss of generality we may assume $i = 1$.
/* This means that $\mathcal{S}^j$ is v^j-rectangular modulo μ_{vj}^j. */
Let C be the subalgebra of $\mathbb{A}_{vj}^j$ generated by $\{\mathbf{a}_1{\uparrow}^j\ [v^j],\ldots,\mathbf{a}_t{\uparrow}^j\ [v^j]\}$.

Step 2.3.4 **If**, for any $v \in V^l$, $\{\mathbf{a}[v] \colon \mathbf{a} \in E\} = \mathbb{A}^l_v$ **then do** the following. Denote $a = \mathbf{a}_1{\uparrow^j}\ [v^j]$, $a' = \mathbf{a}'_1{\uparrow^j}\ [v^j]$. By Proposition 2, for any $c \in C$, there are a term operation $f_c(x, y_1, \ldots, y_m)$ and $e_1, \ldots, e_m \in \mathbb{A}^j_{v^j}$ such that $f_c(a, e_1, \ldots, e_m) = a, f_c(a', e_1, \ldots, e_m) = c$. Since $e_1, \ldots, e_m$ belong to the set $\{\mathbf{b}{\uparrow^j}\ [v^j] \colon \mathbf{b} \in E\}$, there are $\mathbf{e}_1, \ldots, \mathbf{e}_m \in E$ such that $\mathbf{e}_i[v^j] = e_i$.
Set

$$
\begin{aligned}
\mathbf{b}_1 = \begin{pmatrix} a \\ \mathbf{b}' \end{pmatrix} &= f_c(\mathbf{a}_1{\uparrow^j}, \mathbf{e}_1{\uparrow^j}, \ldots, \mathbf{e}_m{\uparrow^j}) = \\
& f_c\left(\begin{pmatrix} a \\ \overline{\mathbf{a}}_1 \end{pmatrix}, \begin{pmatrix} e_1 \\ \mathbf{e}'_1 \end{pmatrix}, \ldots, \begin{pmatrix} e_m \\ \mathbf{e}'_m \end{pmatrix}\right); \\
\mathbf{b}_2 = \begin{pmatrix} c \\ \mathbf{b}' \end{pmatrix} &= f_c(\mathbf{a}'_1{\uparrow^j}, \mathbf{e}_1{\uparrow^j}, \ldots, \mathbf{e}_m{\uparrow^j}) = \\
& f_c\left(\begin{pmatrix} a' \\ \overline{\mathbf{a}}_1 \end{pmatrix}, \begin{pmatrix} e_1 \\ \mathbf{e}'_1 \end{pmatrix}, \ldots, \begin{pmatrix} e_m \\ \mathbf{e}'_m \end{pmatrix}\right); \\
\mathbf{b}''_1 &= f_c(\mathbf{a}_1, \mathbf{e}_1, \ldots, \mathbf{e}_m); \\
\mathbf{b}''_2 &= f_c(\mathbf{a}'_1, \mathbf{e}_1, \ldots, \mathbf{e}_m).
\end{aligned}
$$

Finally, **set**

$$
\begin{aligned}
\mathbf{a}_c &= \begin{pmatrix} c \\ \overline{\mathbf{a}}_1 \end{pmatrix} = \mathbf{d}(\mathbf{a}_1{\uparrow^j}, \mathbf{b}_1, \mathbf{b}_2) = \mathbf{d}\left(\begin{pmatrix} a \\ \overline{\mathbf{a}}_1 \end{pmatrix}, \begin{pmatrix} a \\ \mathbf{b}' \end{pmatrix}, \begin{pmatrix} c \\ \mathbf{b}' \end{pmatrix}\right), \\
\mathbf{a}''_c &= \mathbf{d}(\mathbf{a}_1, \mathbf{b}''_1, \mathbf{b}''_2).
\end{aligned}
$$

Set $B^j_p = \{\mathbf{a}''_c \colon c \in C_p\}$.

Step 2.3.5 **If** a standard basis $\overline{B}$ of $\mathcal{S}^l$ is known **then do** the following. For each $c \in C$ **set** $\mathbf{c}_c = \mathbf{d}(\mathbf{a}_1, \overline{\mathbf{b}}_b, \overline{\mathbf{b}}_c)$ where $\overline{\mathbf{b}}_b, \overline{\mathbf{b}}_c \in \overline{B}^j_p$ are such that $\mathbf{b}_b{\uparrow^j}\ [v^j] = \mathbf{a}_1{\uparrow^j}\ [v^j]$, $\mathbf{b}_c{\uparrow^j}\ [v^j] = c$. Then **set** $B^j_p = \{\mathbf{c}_c \colon c \in C\}$.

Step 3 **Set** $B = B^k \cup \ldots \cup B^l$.

6.7 Soundness and time complexity

The algorithm described above generates, for given problem instance $\mathcal{P} \in \mathrm{CSP}(\mathbb{A})$, a certain set $B \subseteq \mathbb{A}^{|V|}$. What we have to prove is that B is a standard basis of the solution space of $\mathcal{P}$.

Proposition 3 *The set B generated by the algorithm described in Sections 5,6 for a problem instance $\mathcal{P} \in \mathrm{CSP}(\mathbb{A})$ is a standard basis of the solution space, $\mathcal{S}$, of $\mathcal{P}$.*

Proof. We consider the algorithm constructing a basis described in Section 5.3. Soundness of its subroutines is verified in Sections 6.1.3, 6.3.3. Clearly, it is enough to prove that the set $B^k \cup \ldots \cup B^l$ obtained in lth step is a standard basis of $\mathcal{S}^l$, the solution space of $\mathcal{P}^l$, for any $1 \leq l \leq k$. Notice first, that the procedure of planning does not change the solution space of the original problem, because establishing 3-minimality does not. This means, in particular, that if $\mathcal{P}$ has a solution, then $\mathcal{P}^k$ has a solution. In the latter case B^k is obviously a standard basis of $\mathcal{S}^k$. Otherwise, if $\mathcal{P}^k$ is inconsistent, the algorithm output 'NO' as required.

If $\mathcal{P}^{l+1}$ is inconsistent, then so is $\mathcal{P}^l$. So, suppose that the set $\overline{B}^k \cup \ldots \cup \overline{B}^{l+1}$ obtained in $l+1$th step is a standard basis of $\mathcal{S}^{l+1}$, and prove that $B^k \cup \ldots \cup B^l$ obtained in lth step is a standard basis of $\mathcal{S}^l$.

CASE 1. lth step is of type **3**.
By Lemma 1, for any $\mathbf{a}$ from the set $B^k \cup \ldots \cup B^l$, and any $1 \leq t \leq q$, we have $\mathbf{a}|_{s_t^l} \in \varrho_t^l$. This means $B^k \cup \ldots \cup B^l \subseteq \mathcal{S}^l$.

Conversely, if $\mathbf{a} \in \mathcal{S}^l$ then $\mathbf{a}{\uparrow}^{l+1} \in \mathcal{S}^{l+1}$. Hence $\mathbf{a}{\uparrow}^{l+1}$ can be $(B^k \cup \ldots \cup B^{l+1}){\uparrow}^{l+1}$-decomposed. Let $K'(\mathbf{a}{\uparrow}^{l+1})$ be its coordinates. Denoting $\mathbf{b} = K'(\mathbf{a}{\uparrow}^{l+1}) \cdot (B^k \cup \ldots \cup B^{l+1})$ we have $\mathbf{b}[w] = \mathbf{a}[w]$ whenever $w \neq v^l$, and $(a,b) \in \mu^l_{v^l}$, $a = \mathbf{a}[v^l], b = \mathbf{b}[v^l]$. Let C_p be the $\mu^l_{v^l}$-block containing a, b. Then $\mathbf{a} = \mathbf{d}(\mathbf{b}, \mathbf{a}_b, \mathbf{a}_a)$ for $\mathbf{a}_b, \mathbf{a}_a \in B^l_p$.

CASE 2. lth step is of type **2**.
In this case we just have to verify, that for each $1 \leq p \leq s$, the set E_p is a standard basis of $\mathcal{S}'_p$. However, this follows straightforwardly from Lemmas 4, 5, 6. □

Then we estimate the time complexity of the algorithm. Let $n = |V|$, m be the total number of tuples in the constraint relations, r the maximal arity of the relations, and $P = |\mathbb{A}|$ (note that P is a constant). So the size of the problem instance is $n \log n + mr \log P$.

Notice first, that in spite of the number of variables in the problem instance may increase during the procedure of planning, this number does not exceed Cn where C is a certain constant depending only on the original algebra. Therefore the number of steps in one procedure of planning $k \leq Cn|\mathbb{A}| = CnP$. Furthermore each invoking of the procedure of planning but first one is caused by removing at least one tuple from one of the constraint relations. Therefore, this procedure and Steps 7,8 of the algorithm from Section 5.3 are applied at most $m+1$ times. Since each step of the procedure of planning requires cubic time (actually, establishing of 3-minimality contributes the most complexity), what is much less than the complexity of Steps 7,8, we may neglect the complexity of the procedure of planning.

On each step the algorithm from Section 5.3 does the following:
1) solve a system of equation (if a step is of type **3**, it is relatively easy and can be neglected);
2) check all tuples from the constraint relation if they are parts of a solution;
3) find basises for all subalgebras of certain kind.

1) The number of elements in a part of a standard basis corresponding to lth step does not exceed P, hence the total number of elements in a basis is less than $P \cdot CnP \leq CnP^2$. Therefore the linear system obtained in Step 8, and then transformed in Section 6.1.2 has at most CnP^2 variables, $qCn \log P$ equations (here $Cn \log p$ is the maximal number of cyclic summands of $\mathbb{Q}$), and can be solved in time $O(qn^3)$. In the algorithm from Section 6.1.3 this system has to be solved with various restrictions at most once for each

part of a standard basis, that is CnP times. Thus, the resulting complexity of solving the system is $O(qn^4)$.

3) For each variable there is a constant number, D, of subalgebras whose basis is to be found. The number D depends only on the original algebra $\mathbb{A}$. Therefore in each step the algorithm constructs basises for at most DCn subalgebras. To obtain a basis of a subalgebra the algorithm from Section 6.3 runs over at most P its elements and at most Cn steps of the procedure of planning. For each step the algorithm solves a linear equation, that contributes, similarly (1), the time $O(qn^4)$. So, the total complexity of finding basises of subalgebras is $O(qn^6)$.

2) The algorithm checks m tuples of length at most r each. For this it applies mr times the procedure of finding a basis of a one-element subalgebra. Thus, the complexity of this procedure is $O(qn^6mr)$.

Finally, the estimation for the total time is $O(qn^7m^2r)$.

References

[1] J.F. Allen. *Natural Language Understanding.* Benjamin Cummihgs, 1994.

[2] A.A. Bulatov. Three-element mal'tsev algebras. Accepted to Acta Sci. Math.

[3] A.A. Bulatov and P. Jeavons. Algebraic structures in combinatorial problems. Technical Report MATH-AL-4-2001, Technische universität Dresden, Dresden, Germany, 2001.

[4] A.A. Bulatov and P.G. Jeavons. Algebraic approach to multi-sorted constraints. Technical Report PRG-RR-01-18, Computing Laboratory, University of Oxford, Oxford, UK, 2001. Submitted to Theoretical Computer Science.

[5] A.A. Bulatov, A.A. Krokhin, and P.G. Jeavons. Classifying complexity of constraints using finite algebras. Submitted to SIAM Journal of Computing.

[6] A.A. Bulatov, A.A. Krokhin, and P.G. Jeavons. Constraint satisfaction problems and finite algebras. In *Proceedings of 27th International Colloquium on Automata, Languages and Programming—ICALP'00*, volume 1853 of *Lecture Notes in Computer Science*, pages 272–282. Springer-Verlag, 2000.

[7] P.M. Cohn. *Universal Algebra.* Harper & Row, 1965.

[8] R. Dechter and A. Dechter. Structure-driven algorithms for truth maintenance. *Artificial Intelligence*, 82(1-2):1–20, 1996.

[9] R. Dechter and J. Pearl. Network-based heuristics for constraint satisfaction problems. *Artificial Intelligence*, 34(1):1–38, 1988.

[10] H.B. Enderton. *A mathematical introduction to logic.* Harcourt/Academic Press, 2001.

[11] T. Feder. Constraint satisfaction on finite groups with near subgroups. Submitted to SIAM Journal of Computing.

[12] T. Feder and M.Y. Vardi. The computational structure of monotone monadic SNP and constraint satisfaction: A study through datalog and group theory. *SIAM Journal of Computing*, 28:57–104, 1998.

[13] R. Freese and R. McKenzie. *Commutator theory for congruence modular varieties*, volume 125 of *London Math. Soc. Lecture Notes.* London, 1987.

[14] M. Garey and D.S. Johnson. *Computers and Intractability: A Guide to the Theory of NP-Completeness.* Freeman, San Francisco, CA., 1979.

[15] G. Gottlob, L. Leone, and F. Scarcello. Hypertree decompositions and tractable queries. In *Proceedings of PODS'98*, 1999.

[16] G. Gottlob, L. Leone, and F. Scarcello. A comparison of structural CSP decomposition methods. *Artificial Intelligence*, 124(2):243–282, 2000.

[17] M. Grohe, T. Schwentick, and L. Segoufin. When is the evaluation of conjunctive queries tractable? In *Proceedings of the 33rd Annual ACM Simposium on Theory of Computing*, pages 657–666, Hersonissos, Crete, Greece, July 2001. ACM Press.

[18] M. Gyssens, P.G. Jeavons, and D.A. Cohen. Decomposing constraint satisfaction problems using database techniques. *Artificial Intelligence*, 66(1):57–89, 1994.

[19] A. G. Hamilton. *Logic for mathematicians.* Cambridge University Press, 1988.

[20] C. Herrman. Affine algebras in congruence-modular varieties. *Acta Sci. Math. (Szeged)*, 41:119–125, 1971.

[21] D. Hobby and R.N. McKenzie. *The Structure of Finite Algebras*, volume 76 of *Contemporary Mathematics.* American Mathematical Society, Providence, R.I., 1988.

[22] T.H. Jackson. *Number Theory.* Routledge and Kegan Paul, 1975.

[23] P.G. Jeavons. On the algebraic structure of combinatorial problems. *Theoretical Computer Science*, 200:185–204, 1998.

[24] P.G. Jeavons, D.A. Cohen, and M.C. Cooper. Constraints, consistency and closure. *Artificial Intelligence*, 101(1-2):251–265, 1998.

[25] P.G. Jeavons, D.A. Cohen, and M. Gyssens. A unifying framework for tractable constraints. In *Proceedings 1st International Conference on Constraint Programming—CP'95 (Cassis, France, September 1995)*, volume 976 of *Lecture Notes in Computer Science*, pages 276–291. Springer-Verlag, 1995.

[26] P.G. Jeavons, D.A. Cohen, and M. Gyssens. Closure properties of constraints. *Journal of the ACM*, 44:527–548, 1997.

[27] P.G. Jeavons, D.A. Cohen, and J.K. Pearson. Constraints and universal algebra. *Annals of Mathematics and Artificial Intelligence*, 24:51–67, 1998.

[28] Ph.G. Kolaitis and M.Y. Vardi. Conjunctive-query containment and constraint satisfaction. *J. Comput. Syst. Sci.*, 61:302–332, 2000.

[29] P.B. Ladkin and R.D. Maddux. On binary constraint problems. *Journal of the ACM*, 41:435–469, 1994.

[30] A.K. Mackworth. Consistency in networks of relations. *Artificial Intelligence*, 8:99–118, 1977.

[31] A.K. Mackworth. Constraint satisfaction. In S.C. Shapiro, editor, *Encyclopedia of Artificial Intelligence*, volume 1, pages 285–293. Wiley Interscience, 1992.

[32] A.K. Mackworth and E.C. Freuder. The complexity of constraint satisfaction revisited. *Artificial Intelligence*, 59:57–62, 1993.

[33] R.N. McKenzie, G.F. McNulty, and W.F. Taylor. *Algebras, Lattices and Varieties*, volume I. Wadsworth and Brooks, California, 1987.

[34] U. Montanari. Networks of constraints: Fundamental properties and applications to picture processing. *Information Sciences*, 7:95–132, 1974.

[35] B.A. Nadel. Constraint satisfaction in Prolog: Complexity and theory-based heuristics. *Information Sciences*, 83(3-4):113–131, 1995.

[36] B.A. Nadel and J. Lin. Automobile transmission design as a constraint satisfaction problem: Modeling the kinematik level. *Artificial Intelligence for Engineering Design, Anaysis and Manufacturing (AI EDAM)*, 5(3):137–171, 1991.

[37] T.J. Schaefer. The complexity of satisfiability problems. In *Proceedings 10th ACM Symposium on Theory of Computing (STOC'78)*, pages 216–226, 1978.

[38] E. Schwalb and L. Vila. Temporal constraints: a survey. *Constraints*, 3(2-3):129–149, 1998.

[39] E. Tsang. *Foundations of Constraint Satisfaction.* Academic Press, London, 1993.

[40] M.Y. Vardi. Constraint satisfaction and database theory: a tutorial. In *Proceedings of 19th ACM Symposium on Priciples of Database Systems (PODS'00)*, 2000.