Electronic Colloquium on Computational Complexity, Revision 1 of Report No. 93 (2007)

# The Complexity of the Counting Constraint Satisfaction Problem

Andrei A. Bulatov
Simon Fraser University

**Abstract**

The Counting Constraint Satisfaction Problem ($\#\mathrm{CSP}(\mathcal{H})$) over a finite relational structure $\mathcal{H}$ can be expressed as follows: given a relational structure $\mathcal{G}$ over the same vocabulary, determine the number of homomorphisms from $\mathcal{G}$ to $\mathcal{H}$. In this paper we characterize relational structures $\mathcal{H}$ for which $\#\mathrm{CSP}(\mathcal{H})$ can be solved in polynomial time and prove that for all other structures the problem is #P-complete.

## 1 Introduction

In the Counting Constraint Satisfaction Problem, $\#\mathrm{CSP}(\mathcal{H})$, over a finite relational structures $\mathcal{H}$ the objective is, given a finite relational structure $\mathcal{G}$, to compute the number of homomorphisms from $\mathcal{G}$ to $\mathcal{H}$. Various particular cases of the #CSP arise and have been extensively studied in a wide range of areas from logic and graph theory [4, 19, 29, 38, 42, 51, 57, 61, 62], to artificial intelligence [56, 58], to statistical physics [3, 17, 49]. In different areas this problem often appears in different equivalent forms: (1) the problem of finding the number of models of a conjunctive formula, (2) the problem of computing the size (number of tuples) of the evaluation $Q(D)$ of a conjunctive query (without projection) $Q$ on a database $D$ and also (3) the problem of counting the number of assignments to a set of variables subject to specified constraints.

Since the seminal papers [59, 33], the complexity of the decision counterpart of #CSP, the Constraint Satisfaction Problem or CSP for short, has been an object of intensive study. The ultimate goal of that research direction is to classify finite relational structures with respect to the complexity of the corresponding CSP. We shall refer to this research problem as the *classification problem*. A number of significant results have been obtain, see e.g. [59, 33, 5, 7, 1], but a full classification is far from being completed.

Although the classification problem for the general #CSP has been tackled for the first time very recently, a massive work has been done in the study of the complexity of various particular counting CSPs. These particular problems include classical combinatorial problems such as #CLIQUE, GRAPH RELIABILITY, ANTICHAIN, PERMANENT etc. [51, 57, 61, 62] expressible in the form of #CSP; the counting SATISFIABILITY and GENERALIZED SATISFIABILITY problems (in these problems the objective is to find the number of satisfying assignments to a propositional formula) [19, 58] which correspond to $\#\mathrm{CSP}(\mathcal{H})$ for 2-element structures $\mathcal{H}$, counting the number of solution of equations over finite semigroups [55, 48] and many others.

However, the main focus of research in this area has been #$H$-COLORING problem and its variants. In the #$H$-COLORING problem the aim is to find the number of homomorphisms from a given graph $G$ to the fixed graph $H$. Thus, it is equivalent to $\#\mathrm{CSP}(\mathcal{H})$ where $\mathcal{H}$ is a graph. Dyer and Greenhill [29] proved that, for every undirected graph $H$, its associated #$H$-COLORING problem is either in FP (we shall call such problems *tractable*) or is #P-complete. They also provided a complete characterization of the tractable problems. This result has been extended to the counting LIST #$H$-COLORING problem [25, 21], which allows additional restrictions on possible images of a node. Recently, Dyer, Goldberg, and Paterson

ISSN 1433-8092

[32, 28] obtained a similar classification for directed acyclic graphs. Furthermore, some other variants of the #$H$-COLORING problem for undirected graphs have been intensively studied during the last few years [23, 24]. Another direction in this area is the study of problems with restricted input, that is subproblems of the #$H$-COLORING problem in which the input graph $G$ must be planar [42, 60], a partial $k$-tree [22], sparse or of low degree [38, 39], etc. Finally, we should mention the approach to counting problems using approximation and randomized algorithms, see e.g. [47, 27, 26, 30].

The counting CSP admits various generalizations. In one of them, *Weghted #CSP* every tuple from relations are assigned weights that are used to compute weights of mappings from one relational structure to another, and the problem is to find the sum of the weights of all mappings [31]. A particular case of the Weighted #CSP, in which only one binary relation is allowed, is often referred to as *partition functions* [53, 34]. Partition functons are widely used in statistical phisics [3, 17, 49]. Recently, further generalizations of the counting CSPs attracted considerable attention in connection with the study of *holographic reductions*, see e.g. [18].

In [13] we started a systematic study of the classification problem for the general #CSP. The main approach chosen was the *algebraic approach* which has proved to be quite useful in the study of the decision CSP [44, 45, 5, 7, 1]. This approach uses invariance properties of predicates definable in relational structures. Invariance properties are usually expressed as *polymorphisms* of the predicates, that is (multi-ary) operations on the universe of the relational structure compatible with the predicates.

In [13], we proved that if $\#\mathrm{CSP}(\mathcal{H})$ is tractable, then $\mathcal{H}$ has a *Mal'tsev* polymorphism, that is a ternary operation $m(x, y, z)$ satisfying the identities $m(x, y, y) = m(y, y, x) = x$. Another observation was that the *congruences*, i.e. the definable equivalence relations, of $\mathcal{H}$ play a very important role. In particular, these results allowed us to come up with a simple proof of the result of [29][1]. In [14], another necessary condition for the tractability of $\#\mathrm{CSP}(\mathcal{H})$ was identified. It imposes certain restrictions onto possible congruences of $\mathcal{H}$, in terms of cardinalities of their equivalence classes.

In this paper, after giving general definitions (Sections 2.1 and 2.2) and introducing the basics of the algebraic approach (Sections 2.3, 2.4 and 2.5), we go deeper into the structure of congruence lattices of relational structures with a Mal'tsev polymorphism (Sections 3.1 and 3.3), its connections with types of prime quotients (Section 3.2), and the structure of relations with a Mal'tsev polymorphism (Section 3.4). In Section 4 we identify two more necessary conditions for tractability, again expressed in terms of properties of congruences. Then, in Section 5, several observations are made in preparation to introducing an algorithm solving the problem $\#\mathrm{CSP}(\mathcal{H})$ for every relational structure $\mathcal{H}$ satisfying all the conditions obtained. The algorithm is then described in details in Section 6. Thus, we completely solve the classification problem for the general counting CSP. Finally, in Section 7 we compare our result with a recent result of [28] classifying the complexity of the $\#H$-COLORING problem for directed acyclic graphs.

We intensively use methods and results from a number of areas of algebra: lattice theory, tame congruence theory, commutator theory and ring theory. To make the paper available for a wider audience we avoid excessive use of algebraic terminology. In spite of that, some parts of the paper, Section 4 and especially proofs, may require from the reader some familiarity with basic algebraic objects and ideas. The keen reader is referred to textbooks [16, 35, 37, 41]. The reader should be aware that to avoid yet another layer of objects we use algebraic terminology for relational structures, while in the algebraic literature the same concepts are used for "dual" objects, universal algebras.

[1] Note that the hardness results [29] remain true even for graphs of degree at most 3, and so are stronger than those in [13].

# 2 Preliminaries

## 2.1 Relational structures and homomorphisms

Our notation concerning relations and relational structures is fairly standard. Let $[n]$ denote the set $\{1, \dots, n\}$. The set of all $n$-tuples of elements from a set $H$ is denoted by $H^n$. We denote tuples of elements in boldface, for instance, $\mathbf{a}$, and their components by $\mathbf{a}[1], \mathbf{a}[2], \dots$. For a subset $I = \{i_1, \dots, i_k\} \subseteq [n]$ and an $n$-tuple $\mathbf{a}$, by $\mathrm{pr}_I \mathbf{a}$ we denote the *projection of* $\mathbf{a}$ *onto* $I$, the $k$-tuple $(\mathbf{a}[i_1], \dots, \mathbf{a}[i_k])$. For an $n$-ary relation $R \subseteq H^n$, its projection onto $I$ is defined to be $\mathrm{pr}_I R = \{\mathrm{pr}_I \mathbf{a} \mid \mathbf{a} \in R\}$. If $D_i = \mathrm{pr}_i R$ for $i \in [n]$ we say that $R$ is a *subdirect product* of $D_1, \dots, D_n$. If $D_1 = \dots = D_n = H$ then $R$ is said to be an $n$*-th* (or $n$*-ary*) *subdirect power* of $H$. For $\mathbf{a} = (\mathbf{a}[1], \dots, \mathbf{a}[n])$ and $\mathbf{b} = (\mathbf{b}[1], \dots, \mathbf{b}[m])$, $(\mathbf{a}, \mathbf{b})$ denotes the tuple $(\mathbf{a}[1], \dots, \mathbf{a}[n], \mathbf{b}[1], \dots, \mathbf{b}[m])$, while $\langle \mathbf{a}, \mathbf{b} \rangle$ denotes the pair of tuples. Sometimes we need more complicated indexing. Let $I, J \subseteq [n]$ be disjoint, $I = \{i_1, \dots, i_k\}$, $J = \{j_1, \dots, j_\ell\}$, and assume that $i_1 < \dots < i_k$ and $j_1 < \dots < j_\ell$. Let also $\mathbf{a} = (\mathbf{a}[i_1], \dots, \mathbf{a}[i_k])$ and $\mathbf{b} = (\mathbf{b}[j_1], \dots, \mathbf{b}[j_\ell])$. Then $(\mathbf{a}, \mathbf{b})$ denotes the tuple $\mathbf{c}$ whose entries are indexed by elements of the set $I \cup J$ such that $\mathbf{c}[i] = \mathbf{a}[i_t]$ if $i = i_t \in I$ and $\mathbf{c}[i] = \mathbf{b}[j_t]$ if $i = j_t \in J$.

A *vocabulary* is a finite set of relational symbols $R_1, \dots, R_n$ each of which has a fixed arity. A *relational structure* over vocabulary $R_1, \dots, R_n$ is a tuple $\mathcal{H} = (H; R_1^{\mathcal{H}}, \dots, R_n^{\mathcal{H}})$ such that $A$ is a non-empty set, called the *universe* of $\mathcal{H}$, and each $R_i^{\mathcal{H}}$ is a relation on $H$ having the same arity as the symbol $R_i$. Let $\mathcal{G}, \mathcal{H}$ be relational structures over the same vocabulary $R_1, \dots, R_n$. A *homomorphism* from $\mathcal{G}$ to $\mathcal{H}$ is a mapping $\varphi\colon G \to H$ from the universe of $\mathcal{G}$ (the *instance*) to the universe $H$ of $\mathcal{H}$ (the *template*) such that, for every relation $R^{\mathcal{G}}$ (say, $m$-ary) of $\mathcal{G}$ and every tuple $(a_1, \dots, a_m) \in R^{\mathcal{G}}$, we have $(\varphi(a_1), \dots, \varphi(a_m)) \in R^{\mathcal{H}}$.

A relation $R$ is said to be *primitive positive definable* (*pp*-) in $\mathcal{H}$, if it can be expressed using the predicates $R_i^{\mathcal{H}}$ of $\mathcal{H}$ together with the binary equality predicate on $H$ (denoted $\Delta_H$), conjunction, and existential quantification. We use $\mathsf{def}(\mathcal{H})$ to denote the set of all pp-definable relations.

**Example 2.1** Let $\mathcal{H}$ be a 3-element structure with the universe $\{a, b, c\}$ and one binary disequality relation $R$. Structure $\mathcal{H}$ can be thought of as a 3-element complete graph. Then pp-formula

$$\begin{aligned} Q(x, y, z) &= \exists t, u, v, w (R(t, x) \wedge R(t, y) \wedge R(t, z) \wedge R(u, v) \wedge R(v, w) \\ &\quad \wedge R(w, u) \wedge R(u, x) \wedge R(v, y) \wedge R(w, z)) \end{aligned}$$

defines relation

$$Q = \left( \begin{array}{cccccccccccccccccc} a & a & b & a & b & b & a & a & c & a & c & c & b & b & c & b & c & c \\ a & b & a & b & a & b & a & c & a & c & a & c & b & c & b & c & b & c \\ b & a & a & b & b & a & c & a & a & c & c & a & c & b & b & c & c & b \end{array} \right),$$

consisting of all triples containing exactly 2 different elements from $\{a, b, c\}$ (triples are written vertically).

Another useful way to represent relation $Q$ is to view it as the set of restriction of homomorphisms from the graph shown in Fig. 1 to $\mathcal{H}$ restricted onto $\{x, y, z\}$. Observe that this connection between pp-definitions and restrictions of homomorphisms is rather general.

## 2.2 Constraint Satisfaction Problem

The counting constraint satisfaction problem can be formulated in several ways (see Section 1). We use the model theoretic form of this problem.

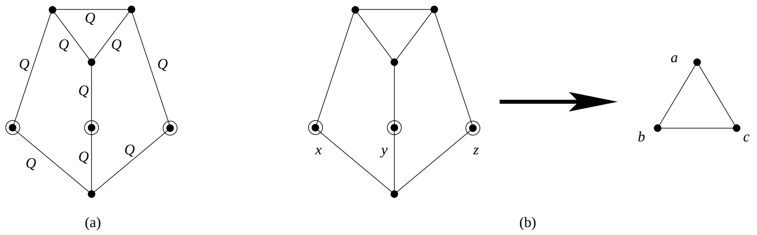

Figure 1:

**Definition 2.2** *Let $\mathfrak{H}$ be a class of relational structures. In the* counting constraint satisfaction problem associated with $\mathfrak{H}$ ($\#\mathrm{CSP}(\mathfrak{H})$)*, the objective is, given a structure $\mathcal{H} \in \mathfrak{H}$ and a structure $\mathcal{G}$, to compute the number of homomorphisms from $\mathcal{G}$ to $\mathcal{H}$. We will refer to this problem as to a* uniform *#CSP.*

*If $\mathfrak{H}$ consists of a single structure $\mathcal{H}$, then we write $\#\mathrm{CSP}(\mathcal{H})$ instead of $\mathrm{CSP}(\{\mathcal{H}\})$ and refer to such problem as a* non-uniform homomorphism problem, *because the inputs are just source structures.*

**Example 2.3 ($\#H$-Coloring, [29, 40, 50])** A graph $\mathcal{H}$ is a structure with a vocabulary consisting of one binary symbol $R$. Then $\#\mathrm{CSP}(\mathcal{H})$ is widely known as the $\#H$-Coloring Problem, in which the objective is to compute the number of homomorphisms from a given graph into $\mathcal{H}$.

**Example 2.4 (#3-SAT, [19, 20, 61, 62])** An instance of the #3-SAT problem is specified by giving a propositional logic formula in CNF each clause of which contains 3 literals, and asking how many assignments satisfy it. Therefore, #3-SAT is equivalent to $\#\mathrm{CSP}(\mathcal{S}_3)$, where $\mathcal{S}_3$ is the 2-element relational structure with the universe $\{0,1\}$ and the vocabulary $R_1, \ldots, R_8$. Predicates $R_1^{\mathcal{S}_3}, \ldots, R_8^{\mathcal{S}_3}$ are the 8 predicates expressible by 3-clauses.

**Example 2.5 (Systems of linear equations)** Let $F$ be a finite field and #Linear Equations$(F)$ is the problem of finding the number of solutions to a system of linear equations over $F$. It is not hard to see that #Linear Equations$(F)$ is equivalent to $\#\mathrm{CSP}(\mathfrak{L})$, where $\mathfrak{L}$ is the class of relational structures with the universe $F$ and the relations corresponding to hyperplanes of finite-dimensional vector spaces over $F$.

In fact, #Linear Equations$(F)$ cannot be straightforwardly reduced to $\#\mathrm{CSP}(\mathfrak{L})$ in polynomial time. The reason is that the representation of relations by linear equations is much more concise than that by a list of tuples, see discussion after Example 2.6. However, in this case some reduction exists. It is carried out by first reducing a system of linear equations to a system of equations each of which contains at most 3 variables; clearly, some new variables should be introduced at this step. Then such a system is straightforwardly reduced to $\#\mathrm{CSP}(\mathcal{L}_3)$, where $\mathcal{L}_3$ is the the relational structure from $\mathfrak{L}$ containing all ternary relations expressible by linear equations.

**Example 2.6 (Equations over semigroups, [55, 48])** Let $S$ be a finite semigroup, that is, a set with a binary associative operation. An equation over $S$ is an expression of the form $x_1 \cdot x_2 \cdot \ldots \cdot x_m = y_1 \cdot y_2 \cdot \ldots \cdot y_m$ where $\cdot$ is the semigroup operation, and $x_i, y_j$ are either indeterminates or constants. Then $\#\mathrm{EQN}_S^*$ stands for the problem of counting the number of solutions to a system of semigroup equations.

The problem $\#\mathrm{EQN}_S^*$ is equivalent to the problem $\#\mathrm{CSP}(\mathfrak{S})$ where $\mathfrak{S}$ is the class of structures with universe $S$ and relations expressible as the set of solutions of a semigroup equation.

In the last two examples, as well as for many other uniform problems, there is a minor ambiguity concerning a representation of the input. We always assume that in uniform problems the relations of the template are represented explicitly, by a list of tuples of the relation. In Examples 2.5, 2.6 such a representation is not the most natural one. However, the class of relations admitting a succinct representation is rather limited (see, e.g. [43]), and thus such representations are unsuitable for the study of the general problem. Moreover, changing representation does not affect the complexity of non-uniform problems.

Every counting CSP belongs to the class #P. However, the exact complexity of $\#\mathrm{CSP}(\mathcal{H})$ strongly depends on the structure $\mathcal{H}$. We say that a relational structure $\mathcal{H}$ is *#-tractable* if $\#\mathrm{CSP}(\mathcal{H})$ is solvable in polynomial time; $\mathcal{H}$ is *#P-complete* if $\#\mathrm{CSP}(\mathcal{H})$ is #P-complete. Note that all reductions used in this paper are Turing reductions. The research problem we deal with in this paper is the following one.

**Problem 1 (classification problem)** *Characterize #-tractable and #P-complete relational structures.*

**Example 2.7** (1) Dyer and Greenhill [29] proved that if $H$ is an undirected graph then $\#H$-COLORING can be solved in polynomial time if and only if every connected component of $H$ is either a complete bipartite graph, or a complete graph with all loops present, or a single vertex. Otherwise the problem is #P-complete.

(2) A 2-element relational structure $\mathcal{H}$ is #-tractable if and only if every predicate of $\mathcal{H}$ can be represented by a system of linear equations over the 2-element field [19, 20]. Otherwise, $\mathcal{H}$ is #P-complete.

(3) $\#\mathrm{CSP}(\mathcal{L}_3)$ is solvable in polynomial time.

(4) The problem $\#\mathrm{EQN}^*_S$ is solvable in polynomial time if and only if $S$ is a direct product of a uniformly inflated Abelian group, inflated left-zero semigroup, and an inflated right-zero semigroup. Otherwise $\#\mathrm{EQN}^*_S$ is #P-complete. For details see [48].

## 2.3 Polymorphisms, Algebras and Complexity

Any operation on a set $H$ can be extended in a standard way to an operation on tuples over $H$, as follows. For any ($m$-ary) operation $f$, and any collection of tuples $\mathbf{a}_1, \ldots, \mathbf{a}_m \in H^n$, define $f(\mathbf{a}_1, \ldots, \mathbf{a}_m)$ to be $(f(\mathbf{a}_1[1], \ldots, \mathbf{a}_m[1]), \ldots, f(\mathbf{a}_1[n], \ldots, \mathbf{a}_m[n]))$, that is, $f$ acts on $H^n$ component-wise. Then $f$ *preserves* an $n$-ary relation $R$ (or $R$ is *invariant* under $f$, or $f$ is a *polymorphism of* $R$) if for any $\mathbf{a}_1, \ldots, \mathbf{a}_m \in R$ the tuple $f(\mathbf{a}_1, \ldots, \mathbf{a}_m)$ belongs to $R$. For a given set of operations, $C$, the set of all relations invariant under every operation from $C$ is denoted by $\mathsf{Inv}(C)$. For a relational structure $\mathcal{H}$ we use $\mathsf{Pol}(\mathcal{H})$ to denote the set of all operations preserving every relation of $\mathcal{H}$.

**Example 2.8** Let $R$ be the solution space of a system of linear equations over a field $F$. Then the operation $m(x, y, z) = x - y + z$ is a polymorphism of $R$. Indeed, let $A \cdot \mathbf{x} = \mathbf{b}$ be the system defining $R$, and $\mathbf{x}, \mathbf{y}, \mathbf{z} \in R$. Then

$$A \cdot m(\mathbf{x}, \mathbf{y}, \mathbf{z}) = A \cdot (\mathbf{x} - \mathbf{y} + \mathbf{z}) = A \cdot \mathbf{x} - A \cdot \mathbf{y} + A \cdot \mathbf{z} = \mathbf{b}.$$

In fact, the converse can also be shown: if $R$ is invariant under $m$ then it is the solution space of a certain system of linear equations.

The following proposition links together polymorphisms and pp-definability of relations.

**Proposition 2.9 ([36, 2, 46])** *Let $\mathcal{H}$ be a finite structure, and let $R \subseteq H^n$ be a non-empty relation. Then $R$ is preserved by all polymorphisms of $\mathcal{H}$ if and only if $R$ is pp-definable in $\mathcal{H}$.*

The connection between polymorphisms and the complexity of counting CSPs is provided by the following result.

**Proposition 2.10 ([13])** *Let $\mathcal{H}_1$ and $\mathcal{H}_2$ be relational structures with the same universe. If* $\mathsf{Pol}(\mathcal{H}_1) \subseteq \mathsf{Pol}(\mathcal{H}_2)$ *then $\#\mathrm{CSP}(\mathcal{H}_2)$ is polynomial time reducible to $\#\mathrm{CSP}(\mathcal{H}_1)$.*

Theorem 2.10 amounts to say that all the information about the complexity of $\#\mathrm{CSP}(\mathcal{H})$ can be extracted from the family of polymorphisms of $\mathcal{H}$. Sets of polymorphisms often provide a more convenient and concise way of describing a class of constraint satisfaction problems. For example, in [13], we used polymorphisms to identify some conditions necessary for the #-tractability of a relational structure. A ternary operation $m(x, y, z)$ on a set $H$ is said to be *Mal'tsev* if $m(x, y, y) = m(y, y, x) = x$ for all $x, y \in H$.

**Proposition 2.11 ([13])** *If $\mathcal{H}$ is a relational structure which is invariant under no Mal'tsev operation then $\mathcal{H}$ is #P-complete.*

Notice that if $\mathcal{H}$ has a Mal'tsev polymorphism then the decision CSP corresponding to $\mathcal{H}$ can be solved in polynomial time [6, 12].

**Example 2.12** Mal'tsev operation $m(x, y, z)$ is a polymorphism of graph $H_1$ shown in Fig. 2, where $m$ is given by

$$m(i_1j_1, i_2j_2, i_3j_3) = ij,$$

$i = i_1$ $[j = j_1]$ unless $i_1 = i_2$ $[j_1 = j_2]$, in this case $i = i_3$ $[j = j_3]$.

Graph $H_2$ has no Mal'tsev polymorphisms. Indeed, if some $f(x, y, z)$ is a Mal'tsev operation, then

$$f\left(\begin{pmatrix} a \\ c \end{pmatrix}, \begin{pmatrix} a \\ d \end{pmatrix}, \begin{pmatrix} b \\ d \end{pmatrix}\right) = \begin{pmatrix} b \\ d \end{pmatrix} \notin E(H_2).$$

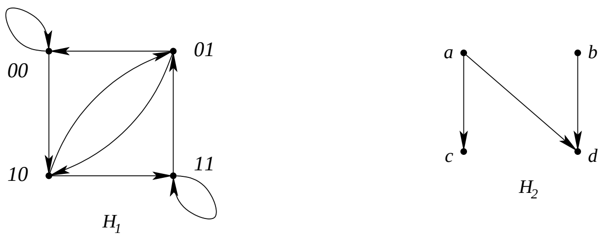

Figure 2:

In our algebraic definitions we follow [16, 54]. For algebraic notions and results concerning the decision CSP the reader is referred to [9, 15].

A (*universal*) *algebra* is an ordered pair $\mathbb{A} = (A, F)$ where $A$ is a non-empty set and $F$ is a family of finitary operations on $A$. The set $A$ is called the *universe* of $\mathbb{A}$, operations from $F$ are called *basic*. An algebra with a finite universe is referred to as a *finite algebra*, while the set of basic operations needs not to be finite.

Any relational structure $\mathcal{H}$ with universe $H$ can be converted into an algebra $\mathsf{Alg}(\mathcal{H}) = (H; \mathsf{Pol}(\mathcal{H}))$. Conversely, every algebra $\mathbb{A} = (A; F)$ corresponds to a class of structures $\mathsf{Str}(\mathbb{A})$ with universe $A$ and relations from $\mathsf{Inv}(F)$. Using this correspondence we can define #-tractable algebras. An algebra $\mathbb{A}$ is said to be *#-tractable* if every structure $\mathcal{H} \in \mathsf{Str}(\mathbb{A})$ is #-tractable; it is said to be *#P-complete* if some $\mathcal{H} \in \mathsf{Str}(\mathbb{A})$ is #P-complete.

We shall express the complexity of $\#\mathrm{CSP}(\mathcal{H})$ in terms of $\mathsf{Alg}(\mathcal{H})$. For example, if an algebra has a Mal'tsev operation, it is called a *Mal'tsev algebra*. Proposition 2.11 implies that if $\#\mathrm{CSP}(\mathcal{H})$ is tractable then $\mathsf{Alg}(\mathcal{H})$ is Mal'tsev.

## 2.4 Subalgebras and congruences

We shall use various constructions on algebras, but two of these constructions, subalgebras and congruences, can be defined for relational structures, and are very useful and illustrative in this context.

A *subalgebra* of a structure $\mathcal{H} = (H; R_1^{\mathcal{H}}, \ldots, R_k^{\mathcal{H}})$ is a unary relation pp-definable in $\mathcal{H}$, and a *congruence* of $\mathcal{H}$ is an equivalence relation pp-definable in $\mathcal{H}$. For a subset $B \subseteq H$, the substructure of $\mathcal{H}$ *induced* by $B$ is defined to be $\mathcal{H}\big|_B = (B; R_1^{\mathcal{H}}\big|_B, \ldots, R_k^{\mathcal{H}}\big|_B)$, where $R_i\big|_B = R_i \cap B^{m_i}$, $R_i$ is $m_i$-ary. For an equivalence relation $\alpha$ and $a \in H$, the class of $\alpha$ containing $\alpha$ is denoted by $a^\alpha$ and the set of all classes of $\alpha$ by $H/_\alpha$. The *quotient structure* $\mathcal{H}/_\alpha$ is defined to be $\mathcal{H}/_\alpha = (H/_\alpha; R_1^{\mathcal{H}}/_\alpha, \ldots, R_k^{\mathcal{H}}/_\alpha)$, where $R_i/_\alpha = \{(a_1^\alpha, \ldots, a_{m_i}^\alpha) \mid (a_1, \ldots, a_{m_i}) \in R_i\}$.

**Example 2.13** Let $\mathcal{H} = (V, E)$ be a digraph without sources and sinks, i.e. the in-degree and out-degree of each vertex is non-zero. We define two binary relations, $\xi_{\mathcal{H}}$ and $\zeta_{\mathcal{H}}$, on the vertex set $H$ of $\mathcal{H}$: $\langle a, b\rangle \in \xi_{\mathcal{H}}$ if and only if $a, b$ have a common out-neighbour and $\langle a, b\rangle \in \zeta_{\mathcal{H}}$ if and only if $a, b$ have a common in-neighbour; in other words, $\xi_{\mathcal{H}} = \{\langle a, b\rangle \mid (a, c), (b, c) \in E$ for a certain $c \in H\}$, $\zeta_{\mathcal{H}} = \{\langle a, b\rangle \mid (c, a), (c, b) \in E$ for a certain $c \in H\}$. Relations $\xi_{\mathcal{H}}$ and $\zeta_{\mathcal{H}}$ are pp-definable in $\mathcal{H}$, as the following pp-formulas show

$$\xi_{\mathcal{H}}(x, y) = \exists z(E(x, z) \wedge E(y, z)), \qquad \zeta_{\mathcal{H}}(x, y) = \exists z(E(z, x) \wedge E(z, y)).$$

In general, $\xi_{\mathcal{H}}, \zeta_{\mathcal{H}}$ are reflexive and symmetric relations. However, if $\mathcal{H}$ has a Mal'tsev polymorphism $m$, they are also transitive. Indeed, suppose that $\langle a, b\rangle \in \xi_{\mathcal{H}}$, $d \in H$ is their common out-neighbour, and $c$ is an out-neighbour of $a$. If $c$ is not an out-neighbour of $b$, then $\mathcal{H}$ contains $H_2$ (see Fig. 2) as a subgraph and $(b, c)$ is not an edge, which contradicts the assumption that $\mathcal{H}$ has a Mal'tsev polymorphism. Therefore, the out-neighbourhoods of $a, b$ are equal whenever $\langle a, b\rangle \in \xi_{\mathcal{H}}$, that implies transitivity. Thus, $\xi_{\mathcal{H}}, \zeta_{\mathcal{H}}$ are congruences of $\mathcal{H}$.

For the graph $H_3$ shown in Fig. 3, the $\xi_{\mathcal{H}_3}$-classes are $\{a, b, c\}, \{d, e\}$, and the $\zeta_{\mathcal{H}_3}$-classes are $\{a, b, e\}, \{c, d\}$.

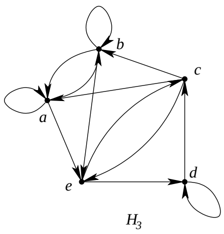

Figure 3:

**Proposition 2.14 ([13])** *Let $\mathcal{H}$ be a relational structure, $B$ and $\alpha$ its subalgebra and congruence respectively.*

*(1) If $\mathcal{H}$ is #-tractable then so are $\mathcal{H}\big|_B$ and $\mathcal{H}/_\alpha$.*

*(2) If $\mathcal{H}\big|_B$ or $\mathcal{H}/_\alpha$ is #P-complete then $\mathcal{H}$ is #P-complete.*

In a similar way we define congruences of relations. Let $R \in \mathsf{def}(\mathcal{H})$ be an $n$-ary relation. It can be viewed as a subalgebra of $n$th direct power of $\mathcal{H}$. A *congruence on* $R$ is a $2n$-ary relation $Q \in \mathsf{def}(\mathcal{H})$ such that $\mathrm{pr}_{\{1,\ldots,n\}}Q = \mathrm{pr}_{\{n+1,\ldots,2n\}}Q = R$, and, if $Q$ is treated as a binary relation on $R$, it is an equivalence relation. An important example of a congruence on $R$ is the following. Let $\alpha \in \mathsf{Con}(\mathcal{H})$ and denote by $\alpha^n$ the relation on $R$ given by $\langle \mathbf{a}, \mathbf{b} \rangle \in \alpha^n$ if and only if $\langle \mathbf{a}[i], \mathbf{b}[i] \rangle \in \alpha$ for all $i \in [n]$. As the following pp-definition shows, $\alpha^n$ is a congruence of $R$

$$\alpha^n(x_1, \ldots, x_n; y_1, \ldots, y_n) = R(x_1, \ldots, x_n) \wedge R(y_1, \ldots, y_n) \wedge \bigwedge_{i=1}^{n} \alpha(x_i, y_i).$$

**Example 2.15** Let us reconsider relation $Q$ on the 3-element set $\{a, b, c\}$, whose pp-definition is given in Example 2.1. We show that the binary relation $T$ on $Q$ that relates triples with the same set of entries is a congruence of $Q$. This can be done in two ways: we may verify that the following pp-formula defines exactly that (6-ary on $\{a, b, c\}$) relation

$$\begin{aligned} T(x, y, z, x', y', z') = \exists t, u, v, w, u', v', w'(&R(t, x) \wedge R(t, y) \wedge R(t, z) \wedge R(u, v) \\ &\wedge R(v, w) \wedge R(w, u) \wedge R(u, x) \wedge R(v, y) \wedge R(w, z) \wedge R(t, x') \wedge R(t, y') \wedge R(t, z') \\ &\wedge R(u', v') \wedge R(v', w') \wedge R(w', u') \wedge R(u', x') \wedge R(v', y') \wedge R(w', z'), \end{aligned}$$

or we may observe that the $T$ is formed by restrictions of homomorphisms from the graph shown in Fig. 4 to $\mathcal{H}$ onto $\{x, y, z, x', y', z'\}$.

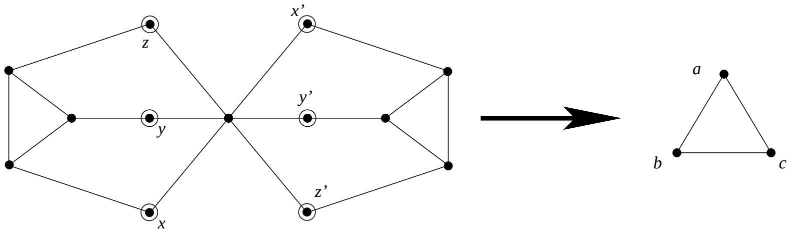

Figure 4:

The existence of a Mal'tsev polymorphism provides a necessary condition for the #-tractability of a relational structure. However, it is not a sufficient condition, as Example 2.17 below shows. In the Section 4 we prove two more necessary conditions. A particular case of one of them is that proved in [14].

Let $\alpha, \beta$ be congruences of a $\mathcal{H}$, where $\alpha, \beta$ are incomparable, that is, neither $\alpha \subseteq \beta$, nor $\beta \subseteq \alpha$. Let $A_1, \ldots, A_k$ and $B_1, \ldots, B_\ell$ be the $\alpha$- and $\beta$-classes respectively (see Fig. 5). Then $M(\alpha, \beta)$ denotes the $k \times \ell$-matrix $(m_{ij})$, where $m_{ij} = |A_i \cap B_j|$.

**Proposition 2.16 ([8])** *Let $\mathcal{H}$ be a relational structure, and let $\alpha, \beta$ be incomparable congruences of $\mathcal{H}$. If $\mathsf{rank}(M(\alpha, \beta)) > k$, where $k$ is the number of classes of the smallest congruence containing both $\alpha$ and $\beta$, then $\#\mathrm{CSP}(\mathcal{H})$ is #P-complete.*

Classes of the smallest congruence $\gamma$ containing both $\alpha$ and $\beta$ can be easily represented in terms of matrix $M(\alpha, \beta)$: This matrix (as well as any other square matrix) after suitable synchronized permutations of rows and columns can be partitioned into a collection of square cells sitting on the diagonal, so that all entries outside the cells equal zero. The finest partition of this kind gives the classes of $\gamma$.

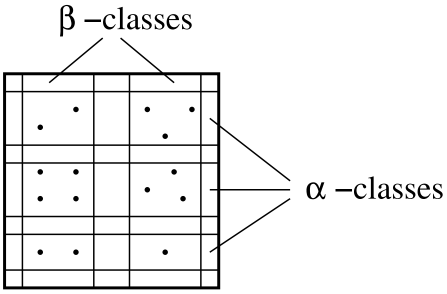

Figure 5:

**Example 2.17** Let $\mathcal{H}$ be the graph $H_3$ shown in Fig. 3, $\alpha = \xi_{H_3}$ and $\beta = \zeta_{H_3}$. We have $A_1 = \{a, b, c\}, A_2 = \{e, d\}$, $B_1 = \{a, b, e\}, B_2 = \{c, d\}$ and

$$M(\alpha, \beta) = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}.$$

By Proposition 2.16, the problem $\#\mathrm{CSP}(H_3)$ is #P-complete.

## 2.5 Varieties and Complexity

It will be convenient for us to jump back and forth between model-theoretic and algebraic views to the CSP. The language of relational structures is more convenient when describing algorithms. On the other hand, standard algebraic constructions allow us to strengthen necessary conditions for #-tractability, and eventually formulate a criterion for #-tractability.

**Definition 2.18** (1) *Let $\mathbb{A} = (A; F)$ be an algebra. The $k$-th* direct power *of $\mathbb{A}$ is the algebra $\mathbb{A}^k = (A^k; F)$ where we treat each* (*say, $n$-ary*) *operation $f \in F$ as acting on $A^k$ component-wise.*

(2) *Let $\mathbb{A} = (A; F)$ be an algebra, and let $B$ be a subset of $A$ such that, for any* (*say, $n$-ary*) *$f \in F$, and for any $b_1, \ldots, b_n \in B$, we have $f(b_1, \ldots, b_n) \in B$. Then the algebra $\mathbb{B} = (B; F\rfloor_B)$, where $F\rfloor_B$ consists of restrictions of operations $f \in F$ onto $B$, is called a* subalgebra *of $\mathbb{A}$.*

*Note that a set $B$ is a subalgebra of a structure $\mathcal{H}$ if and only if $B$ is the universe of a subalgebra of* $\mathsf{Alg}(\mathcal{H})$.

(3) *Let $\mathbb{A}_1 = (A_1; F_1)$ and $\mathbb{A}_2 = (A_2; F_2)$ such that $F_1 = \{f_i^1 \mid i \in I\}$, $F_2 = \{f_i^2 \mid i \in I\}$, and $f_i^1, f_i^2$ are of the same arity $n_i$, $i \in I$. A mapping $\varphi : A_1 \to A_2$ is called a* homomorphism *from $\mathbb{A}_1$ to $\mathbb{A}_2$ if $\varphi f_i^1(a_1, \ldots, a_{n_i}) = f_i^2(\varphi(a_1), \ldots, \varphi(a_{n_i}))$ holds for all $i \in I$ and all $a_1, \ldots, a_{n_i} \in A_1$. If the mapping $\varphi$ is onto then $\mathbb{A}_2$ is said to be a* homomorphic image *of $\mathbb{A}_1$.*

A common way of constructing homomorphic images is through congruences and quotient algebras. A *congruence* of an algebra $\mathbb{A} = (A; F)$ is an equivalence relation on $A$ invariant under all operations from $F$. Let $\theta$ be a congruence of $\mathbb{A}$. The algebra $\mathbb{A}/_\theta = (A/_\theta; F/_\theta)$, where $F/_\theta = \{f/_\theta \mid f \in F\}$ and $f/_\theta$ is given by $f/_\theta(a_1^\theta, \ldots, a_n^\theta) = (f(a_1, \ldots, a_n))^\theta$ is called a *quotient algebra*. Observe that an equivalence relation is a congruence of a structure $\mathcal{H}$ if and only if it is a congruence of $\mathsf{Alg}(\mathcal{H})$.

**Theorem 2.19 ([13])** *Let $\mathbb{A} = (A; F)$ be a finite algebra. Then*

(1) *if $\mathbb{A}$ is #-tractable then so is every subalgebra, homomorphic image, and direct power of $\mathbb{A}$.*

(2) *if $\mathbb{A}$ has a #P-complete subalgebra, homomorphic image, or direct power, then $\mathbb{A}$ is #P-complete.*

For an algebra $\mathbb{A}$ the class of algebras that are homomorphic images of subalgebras of direct powers of $\mathbb{A}$ is called the *variety* generated by $\mathbb{A}$, and is denoted by $\mathsf{var}(\mathbb{A})$. An operation $f$ on the universe of an algebra $\mathbb{A} = (A; F)$ that preserves all relations invariant under $F$ is called a *term* operation of $\mathbb{A}$. Every term operation of $\mathbb{A}$ can be obtained from operations of $F$ by means of superposition.

An operation $f$ on a set $A$ is said to be *idempotent* if the equality $f(x, \dots, x) = x$ holds for all $x \in A$. Algebras whose basic operations are idempotent possess many useful properties. The *full idempotent reduct* of an algebra $\mathbb{A} = (A; F)$ is the algebra $\mathsf{Id}(\mathbb{A}) = (A; F_{\rm id})$ where $F_{\rm id}$ consists of all idempotent term operations of $\mathbb{A}$. There is another way to characterize $F_{\rm id}$. If $\mathbb{A} = \mathsf{Alg}(\mathcal{H})$ for a certain relational structure $\mathcal{H}$, then $\mathsf{Id}(\mathbb{A}) = \mathsf{Alg}(\mathcal{H}_{\rm id})$, where $\mathcal{H}_{\rm id}$ is an expansion of $\mathcal{H}$ by unary relations $K_h$, $h \in \mathcal{H}$, and $K_h$ is interpreted as the *constant relation* $\{(h)\}$, containing only one tuple, namely $(h)$. We will need the following simple observation about relational structures with idempotent polymorphisms.

**Lemma 2.20** *Let $\mathcal{H}$ be a relational structure whose polymorphisms are idempotent, $R \in \mathsf{def}(\mathcal{H})$ an $n$-ary relation, $\alpha$ a congruence of $R$, and $B$ an $\alpha$-class. Then $B$ is a relation pp-definable in $\mathcal{H}$.*

Indeed, let $\mathbf{a} \in B$. Since every polymorphism of $\mathcal{H}$ is idempotent, the constant relations $K_{\mathbf{a}[i]}$, $i \in [n]$, are pp-definable in $\mathcal{H}$. Then

$$\begin{aligned} B(x_1, \dots, x_n) \;\; = \;\; & \exists y_1, \dots, y_n (R(x_1, \dots, x_n) \wedge \alpha(x_1, \dots, x_n; y_1, \dots, y_n) \\ & \wedge K_{\mathbf{a}[1]}(y_1) \wedge \dots \wedge K_{\mathbf{a}[n]}(y_n)). \end{aligned}$$

The following theorem shows the connection between complexity and full idempotent reducts.

**Theorem 2.21 ([13])** *(1) A finite algebra $\mathbb{A}$ is #-tractable* [*#P-complete*] *if and only if so is $\mathsf{Id}(\mathbb{A})$.*
*(2) A relational structure $\mathcal{H}$ is #-tractable* [*#P-complete*] *if and only if so is $\mathcal{H}_{\rm id}$.*

If $\mathbb{A}$ is an idempotent algebra and the condition of Proposition 2.16 is true for every pair of congruences of $\mathbb{A}$ then $\mathbb{A}$ is said to be *congruence singular*. If every finite algebra in a variety is congruence singular then the variety is called congruence singular. We call a relational structure $\mathcal{H}$ congruence singular if $\mathsf{Alg}(\mathcal{H})$ generates a congruence singular variety. By Proposition 2.16 and Theorems 2.19, 2.21, every structure $\mathcal{H}$ that is not #P-complete is congruence singular. The main result of the paper is that this condition is sufficient for #-tractability.

**Theorem 2.22** *A relational structure $\mathcal{H}$* [*an algebra $\mathbb{A}$*], *is #-tractable if and only if $\mathcal{H}_{\rm id}$ is congruence singular* [*$\mathsf{Id}(\mathbb{A})$ generates a congruence singular variety*].

Observe that the condition of having a Mal'tsev polymorphism (term operation) is not included into the criterion. As we shall see later (Lemma 3.3) every congruence singular structure has a Mal'tsev polymorphism.

We complete this section with a more combinatorial characterization of congruence singular relational structures. Let $\mathcal{H}$ be a relational structure, $R$ a relation pp-definable in $\mathcal{H}$, and $\alpha, \beta, \delta$ congruences of $R$ such that $\delta \le \alpha, \beta$. By $M(R; \alpha, \beta; \delta)$ we denote the matrix $M(\alpha, \beta)$ computed for $R$ in the quotient structure $\mathcal{H}/_{\delta}$. More precisely, let $A_1, \dots, A_k$ and $B_1, \dots, B_\ell$ be the $\alpha$- and $\beta$-classes respectively. Then $M(R; \alpha, \beta; \delta)$ is the $k \times \ell$-matrix $(m_{ij})$ where $m_{ij}$ equals the number of $\delta$-classes in $A_i \cap B_j$.

**Lemma 2.23** *A relational structure $\mathcal{H}$ is congruence singular if and only if for any relation $R$ pp-definable in $\mathcal{H}$ and any congruences $\delta, \alpha, \beta$ of $R$ such that $\delta \le \alpha, \beta$, the rank of the matrix $M(R; \alpha, \beta; \delta)$ equals the number of classes in the smallest congruence containing both $\alpha$ and $\beta$.*

**Proof:** Let $\mathbb{A} = \mathsf{Alg}(\mathcal{H})$. We show that for any finite algebra $\mathbb{B}$ from the variety generated by $\mathbb{A}$ and congruences $\alpha, \beta$ of $\mathbb{B}$ there are a relation $R$ pp-definable in $\mathcal{H}$ and congruences $\delta, \alpha', \beta'$ of $R$ with $\delta \leq \alpha, \beta$ such that $M(\alpha, \beta) = M(R; \alpha', \beta'; \delta)$; and, conversely, for any $R, \delta, \alpha', \beta'$, there are $\mathbb{B}$ and $\alpha, \beta$ satisfying the above equality.

Take $\mathbb{B}$, $\alpha$, and $\beta$. By the HSP-Theorem (see, e.g., [16]) $\mathbb{B}$ is a homomorphic image of a subalgebra of (say, $k$-th) direct power of $\mathbb{A}$. Let $\mathbb{C}$ denote the subalgebra of the direct power, and let $\mathbb{B}$ be a homomorphic image of $\mathbb{C}$, let $\varphi$ be the homomorphism, and let $\gamma$ be the corresponding congruence of $\mathbb{C}$, that is $\langle a, b\rangle \in \gamma$ if and only if $\varphi(a) = \varphi(b)$. The universe $C$ of $\mathbb{C}$ can be viewed as a subset of $H^k$ — recall that $H$ is the universe of $\mathbb{A}$ — invariant under all polymorphisms of $\mathcal{H}$. Thus $C$ is a $k$-ary relation pp-definable in $\mathcal{H}$. We choose $R = C$. Then the term operations of $\mathbb{C}$ are the polymorphisms of $\mathcal{H}$ acting on $R$ component-wise. Furthermore, $\gamma$ is an equivalence relation on $C$ invariant under all operations of $\mathbb{C}$, and therefore under all polymorphisms of $\mathcal{H}$. Hence $\gamma$ is a congruence of $R$, and we set $\delta = \gamma$. Finally, define $\alpha'$, $\beta'$ as follows: $\alpha' = \{\langle \mathbf{a}, \mathbf{b}\rangle \in R^2 \mid \langle \varphi(\mathbf{a}), \varphi(\mathbf{b})\rangle \in \alpha\}$, and $\beta' = \{\langle \mathbf{a}, \mathbf{b}\rangle \in R^2 \mid \langle \varphi(\mathbf{a}), \varphi(\mathbf{b})\rangle \in \beta\}$. Every $\alpha'$- or $\beta'$-class $D$ corresponds to the $\alpha$-, respectively, $\beta$-class $\varphi(D) = \{\varphi(a) \mid a \in D\}$, and this correspondence is one-to-one. The $\delta$-classes inside $D$ are also in a one-to-one correspondence with the elements of $\varphi(D)$. This implies the equality of the matrices.

Now take a $k$-ary relation $R$ pp-definable in $\mathcal{H}$ and congruences $\delta, \alpha', \beta'$ of $R$. First we set $\mathbb{C} = (R; \{f^{\mathbb{C}} \mid f \in \mathsf{Pol}(\mathcal{H})\}$, where $f^{\mathbb{C}}$ acts on $k$-tuples from $R$ component-wise. Since $R$ is invariant under all polymorphisms of $\mathcal{H}$ these operations are well-defined. Algebra $\mathbb{B}$ can be defined as the quotient algebra $\mathbb{C}/_{\delta}$, and congruences $\alpha, \beta$ as follows: $\alpha = \{\langle \mathbf{a}^{\delta}, \mathbf{b}^{\delta}\rangle \mid \langle \mathbf{a}, \mathbf{b}\rangle \in \alpha'\}$ and $\beta = \{\langle \mathbf{a}^{\delta}, \mathbf{b}^{\delta}\rangle \mid \langle \mathbf{a}, \mathbf{b}\rangle \in \beta'\}$. As before, we have one-to one correspondences between $\alpha$-, $\beta$- and $\alpha'$-, $\beta'$- classes, as well as, between $\delta$-classes and elements of $\mathbb{B}$, that implies the result. □

# 3 Congruence lattices and the structure of relations

## 3.1 Lattices and congruence lattices

In this section we look closer at the family of congruences of a relational structure $\mathcal{H}$. All definitions and results given here were originally introduced for algebras. As our algorithms are described in terms of relational structures, we reformulate them in terms of structures, replacing congruences of algebras with congruences of structures, and term operations of an algebra with polymorphisms of a structure. However, the notions we arrive to for a structure $\mathcal{H}$ are exactly the same as those defined for the algebra $\mathsf{Alg}(\mathcal{H})$.

The set of all congruences of structure $\mathcal{H}$ is denoted by $\mathsf{Con}(\mathcal{H})$. Let $\alpha, \beta \in \mathsf{Con}(\mathcal{H})$. The intersection of $\alpha$ and $\beta$ is again a congruence of $\mathcal{H}$ and is denoted $\alpha \wedge \beta$. As is well known, the smallest equivalence relation containing both $\alpha$ and $\beta$ is the transitive closure of $\alpha \cup \beta$. It can be shown that this equivalence relation is a congruence of $\mathcal{H}$, denoted by $\alpha \vee \beta$. The set $\mathsf{Con}(\mathcal{H})$ together with the operations $\wedge$ (*meet*) and $\vee$ (*join*) is called the *congruence lattice* of $\mathcal{H}$. The set $\mathsf{Con}(\mathcal{H})$ is naturally ordered with respect to inclusion. The least element of $\mathsf{Con}(\mathcal{H})$ is the equality relation, denoted by $\Delta$, and the greatest element is the total relation, denoted by $\bigtriangledown$.

If $R$ is a relation pp-definable in $\mathcal{H}$, then $\mathsf{Con}(R)$ denotes the set of all congruences on $R$. This set depends on $\mathcal{H}$ as well as on $R$, but usually $\mathcal{H}$ is clear from the context. The set $\mathsf{Con}(R)$ is also a lattice.

Lattices can also be introduced in an abstract way, as a set along with operations $\wedge$ and $\vee$ satisfying certain conditions, see [37]. The structure of a lattice allows one to define a partial order $\leq$ on $L$: $a \leq b$ if and only if $a \wedge b = a$, or, equivalently, $a \leq b$ if and only if $a \vee b = b$. Note that $a \wedge b$ and $a \vee b$ are the greatest lower and the least upper bound of $a, b$, respectively, in terms of this order.

We will deal with lattices of several particular types. A lattice $L$ is said to be (a) *modular* if, for any $a, b, c \in L$ such that $b \leq a$, the equality $a \wedge (b \vee c) = b \vee (a \wedge c)$ holds; (b) *meet semi-distributive* if, for any $a, b, c \in L$ such that $a \wedge b = a \wedge c$, the equality $a \wedge b = a \wedge (b \vee c)$ holds; (c) *distributive* if for any $a, b, c \in L$, the equality $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$ holds. Modular and distributive lattices are very well studied, see, e.g., [37, Ch. II, IV].

A lattice $L$ is modular if and only if it contains no *pentagon*, Fig. 6(a), as a sublattice. Note that this does not mean that $L$ does not contain this configuration in terms of order: It must also be the case that $a \wedge c = b \wedge c = d$ and $a \vee c = b \vee c = e$, see e.g., [37, Theorem 2, Ch. II]. Similarly, $L$ is distributive if and only if it contains no pentagons or diamond, see Fig. 6(b), as a sublattice. It is also not hard to check that a diamond is not a meet semi-distributive lattice. Thus we obtain the following

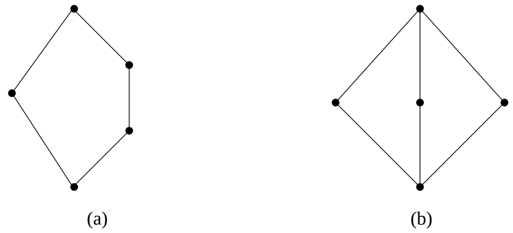

Figure 6: Pentagon (a) and diamond (b)

**Observation 3.1** *Every modular semi-distributive lattice is distributive.*

One particularly useful property of modular lattices is the following. A pair $a, b$ of elements from a lattice $L$ is called a *prime quotient*, denoted $a \prec b$, if $a \leq b$ and there is no $c \in L$ such that $a \leq c \leq b$ and $c \neq a, b$. Suppose $a \leq b$. A sequence $a = c_0 \prec c_1 \prec \ldots \prec c_k = b$ is called a *maximal chain* from $a$ to $b$. Observe that such a chain is maximal in the sense that there are no other elements between the $c_i$. Number $k$ is called the *length* of the chain.

**Proposition 3.2 (The Jordan-Hölder Chain Condition, [37], Th. 1, Ch. II.2)** *For any two elements $a \leq b$ of a modular lattice, all maximal chains from $a$ to $b$ have the same length.*

For elements $a, b$ of a lattice $L$ such that $a \leq b$, the *interval* $[a, b]$ is the set of all $c$ with $a \leq c \leq b$. Intervals $[a, b]$ and $[c, d]$ are said to be *perspective* if $b \vee c = d$, $b \wedge c = a$ or $a \vee d = b$, $a \wedge d = c$ (see Fig. 8(a)). Thus perspectivity is a binary relation on the set of intervals of $L$. Two intervals that belong to the transitive closure of this relation are said to be *projective* to each other.

## 3.2 Congruence lattices and types of prime quotients

If $\mathcal{H}$ has a Mal'tsev polymorphism, the set $\mathsf{Con}(\mathcal{H})$ cannot be just an arbitrary collection of equivalence relations. In particular, any two members $\alpha, \beta$ of $\mathsf{Con}(\mathcal{H})$ must be *permutable*, that is $\alpha \circ \beta = \beta \circ \alpha$. This means that, for any $\alpha$-class $A$ and any $\beta$-class $B$ belonging the same $\alpha \vee \beta$-class, $A \cap B$ is non-empty (see Fig. 7). As is easily seen, congruences $\alpha, \beta$ are permutable if and only if $\alpha \circ \beta = \beta \circ \alpha = \alpha \vee \beta$.

**Lemma 3.3** *If a relational structure $\mathcal{H}$ is congruence singular* [*an algebra $\mathbb{A}$ generates a congruence singular variety*], *then it has a Mal'tsev polymorphism* [*a Mal'tsev term operation*].

*Therefore for any relation $R$ pp-definable in $\mathcal{H}$ its congruence lattice $\mathsf{Con}(R)$ is modular.*

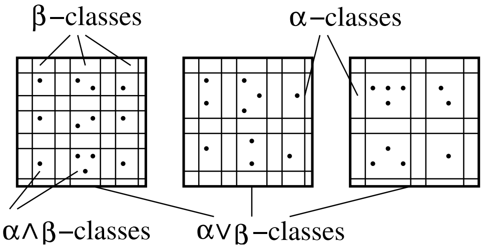

Figure 7:

**Proof:** By the well known result of Mal'tsev [16], Theorem 12.1, an algebra $\mathbb{A}$ has a Mal'tsev term operation if and only if any two congruences of any algebra in the variety generated by $\mathbb{A}$ are permutable. Therefore it suffices to prove that if the variety generated by $\mathsf{Alg}(\mathcal{H})$ for a structure $\mathcal{H}$ is congruence singular then it is congruence permutable.

Suppose $\mathcal{H}$ is congruence singular, $\mathbb{B} \in \mathsf{var}(\mathsf{Alg}(\mathcal{H}))$, and $\alpha, \beta \in \mathsf{Con}(\mathbb{B})$. If $\alpha \subseteq \beta$ or $\beta \subseteq \alpha$ then they are obviously permutable. If the congruences are incomparable then $\mathsf{rank}(M(\alpha,\beta)) = k$ where $k$ is the number of $\alpha \vee \beta$-classes. It is convenient to represent $\alpha \vee \beta$-classes as cells of matrix $M(\alpha,\beta)$. The equality $\mathsf{rank}(M(\alpha,\beta)) = k$ implies, in particular, that all entries in a cell are non-zero. Therefore, for any $a, b$ from the same $\alpha \vee \beta$-class, say, $a$ belongs to $\alpha$-class $A_1$ and $\beta$-class $B_1$, and $b$ belongs to $\alpha$-class $A_2$ and $\beta$-class $B_2$, we have $A_1 \cap B_2 \neq \varnothing$ and $A_2 \cap B_1 \neq \varnothing$, as the corresponding entries of $M(\alpha,\beta)$ must be non-zero. Then $\langle a, b\rangle \in \alpha \circ \beta$, as any $c \in A_1 \cap B_2$ witnesses, and $\langle a, b\rangle \in \beta \circ \alpha$, as any $d \in A_2 \cap B_1$ witnesses. Thus $\alpha \circ \beta = \beta \circ \alpha = \alpha \vee \beta$.

The second part of the lemma follows from the observation that $\mathsf{Con}(R)$ is the congruence lattice of certain algebra in the variety generated by $\mathsf{Alg}(\mathcal{H})$ and the fact that the congruence lattice of a congruence permutable algebra is modular. □

A pair of congruences $\langle \alpha, \beta\rangle$ is said to be a *prime quotient* if they form a prime quotient in the congruence lattice.

We shall use some notions and results of tame congruence theory [41]. Tame congruence theory is a tool to study a local structure of universal algebras and relational structures through certain properties of prime quotients of the congruence lattice. In general, this theory identifies five possible types of such quotients defined in a fairly sophisticated way. Fortunately, in our case of relational structures with a Mal'tsev polymorphism, only two of those types can occur, and the definition of these possible types can be significantly simplified.

A prime quotient $\alpha \prec \beta$ is said to be of the *affine* type, if, for any $\beta$-class $B$, there is a module $M_B$ with the base set $B/_{\alpha}$ over a ring $R_B$ such that for any $f(x_1, \ldots, x_n, y_1, \ldots, y_m) \in \mathsf{Pol}(\mathcal{H})$ and $a_1, \ldots, a_m \in H$, if the operation $g(x_1, \ldots, x_n) = f(x_1, \ldots, x_n, a_1, \ldots, a_m)$ preserves $B$, then it can be represented as an operation of the module $M_B$:

$$(g|_B(x_1, \ldots, x_n))/_{\alpha} = c_1x_1 + \ldots + c_nx_n + a.$$

In all other cases, $\alpha \prec \beta$ has the *Boolean* type.

**Example 3.4** Let $\mathcal{L}_2$ be a 2-element relational structure whose relational symbols are interpreted as solution spaces of systems of linear equations. Then $\mathcal{L}_2$ has only two congruences: $\Delta_2$, the equality relation, and

$\nabla_2$, the total binary relation. As Example 2.8 shows, the prime quotient $\Delta_2 \prec \nabla_2$ is of the affine type. Thus, the affine type corresponds to some kind of "linearity" in a broad sense.

Prime quotients $\alpha_1 \prec \beta_1$ and $\alpha_2 \prec \beta_2$ are said to be perspective [projective] if the intervals $[\alpha_1, \beta_1]$ and $[\alpha_2, \beta_2]$ are perspective [projective] in $\mathsf{Con}(\mathcal{H})$.

**Lemma 3.5 ([41], Lemma 6.2)** *If $\alpha_1 \prec \beta_1$ and $\alpha_2 \prec \beta_2$ are projective quotients in $\mathsf{Con}(\mathcal{H})$, then they have the same type.*

## 3.3 Congruence lattices of relational structures with a Mal'tsev polymorphism

We will often distinguish two cases: when the congruence lattice of our relational structure omits the affine type, and when the affine type occurs in this lattice. Note that, since by Lemma 3.3 we need to consider only structures with a Mal'tsev polymorphism, all congruence lattices we consider are modular

### 3.3.1 Distributive lattices and structures omitting the affine type

If $\mathcal{H}$ omits the affine type then, by Theorem 9.15 of [41], $\mathsf{Con}(\mathcal{H})$ is meet semi-distributive, and by Observation 3.1 it is distributive. We will need several properties of distributive lattices. An element $a$ of a lattice $L$ is said to be *join-irreducible* if for any $b, c \in L$ such that $a = b \vee c$ either $b = a$ or $c = a$ (see Fig, 8(b)). By $[a)$ we denote the *principal ideal generated* by $a$, i.e. the set of all elements $b \in L$ with $b \leq a$ (see Fig 8(d)).

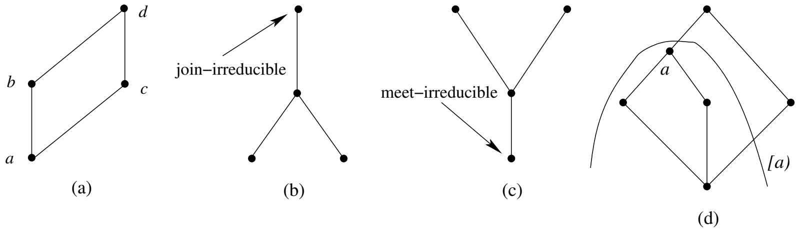

Figure 8: Perspective intervals (a), join-irreducible (b) and meet-irreducible (c) elements, and principal ideal (d)

**Proposition 3.6 ([37], Theorem 9, Corollary 11, Ch. II.1)** *For any finite distributive lattice $L$ there is a finite set, $M$, and a injective mapping $\mathcal{J}\colon L \longrightarrow 2^M$ (the set of all subsets) such that $\mathcal{J}(a \vee b) = \mathcal{J}(a) \cup \mathcal{J}(b)$ and $\mathcal{J}(a \wedge b) = \mathcal{J}(a) \cap \mathcal{J}(b)$.*

*Set $M$ can be chosen to be $J(L)$, the set of all join irreducible elements of $L$, and $\mathcal{J}(a)$ to be $J(L) \cap [a)$.*

**Example 3.7** The lattice shown in Fig. 9(a) is distributive. Its representation as a lattice of subsets is also shown.

**Proposition 3.8 ([37], Corollary 14, Ch. II.1)** *Every maximal chain of a finite distributive lattice $L$ has length $|J(L)|$.*

Let $L$ be a distributive lattice with $\Delta$ and $\bigtriangledown$, the least and greatest elements, respectively, and let $\mathcal{J}$ its set representation as described in Proposition 3.6.

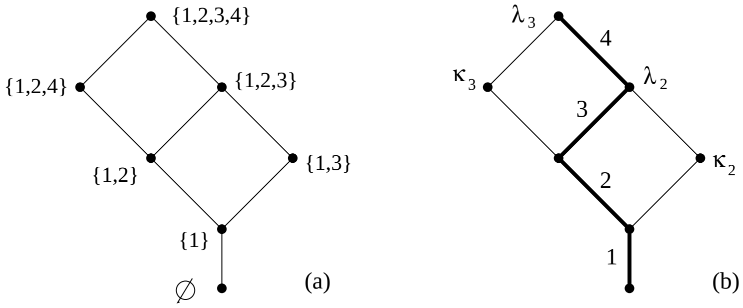

Figure 9:

**Corollary 3.9** *For any prime quotient $a \prec b$ in $L$, $|\mathcal{J}(b) - \mathcal{J}(a)| = 1$.*

**Proof:** Take a maximal chain in $[a)$ that starts at $\Delta$ and ends at $a$. Then continue it by $a \prec b$ and by a maximal chain from $b$ to $\bigtriangledown$. The resulting chain is a maximal chain in $L$ and therefore has length $|J(L)|$. Since $\mathcal{J}(\Delta) = \varnothing$ and $\mathcal{J}(\bigtriangledown) = J(L)$, the difference of set representations of consecutive elements of the chain is 1-element. □

**Lemma 3.10** *An interval $[a, b]$ is projective to interval $[c, d]$ if and only if $\mathcal{J}(b) - \mathcal{J}(a) = \mathcal{J}(d) - \mathcal{J}(c)$.*

**Proof:** Assume we have $a = b \wedge c$, $d = b \vee c$. Then $\mathcal{J}(d) = \mathcal{J}(c) \cup \mathcal{J}(b) = \mathcal{J}(a) \cup (\mathcal{J}(b) - \mathcal{J}(a)) \cup \mathcal{J}(c) = \mathcal{J}(c) \cup (\mathcal{J}(b) - \mathcal{J}(a))$, and $\mathcal{J}(b) - \mathcal{J}(a)$ and $\mathcal{J}(c)$ are disjoint.

Conversely, let $[a, b]$, $[c, d]$ be intervals such that $\mathcal{J}(b) - \mathcal{J}(a) = \mathcal{J}(d) - \mathcal{J}(c)$. Let $\mathcal{J}(b) - \mathcal{J}(a) = K$. Set $c' = a \vee c$ and $d' = b \vee c$. Clearly, $\mathcal{J}(d') = \mathcal{J}(c') \cup K$, so $b \wedge c' = a, b \vee c' = d'$ and $c' \wedge d = c$, $c' \vee d = d'$. Intervals $[a, b]$ and $[c, d]$ are projective. □

**Lemma 3.11** *Let $L$ be a distributive lattice and let $C$ be a maximal chain $a_0 \prec a_1 \prec \ldots \prec a_k$, where $a_0, a_k$ are the least and greatest elements of $L$, respectively. Then for any prime quotient $a \prec b$ in $L$ there is a unique $\omega \in [k]$ such that $a \prec b$ is projective to $a_{\omega-1} \prec a_\omega$. Moreover, $\mathcal{J}(b) - \mathcal{J}(a) = \mathcal{J}(a_\omega) - \mathcal{J}(a_{\omega-1})$.*

**Proof:** Let $a \prec b$ be a prime quotient and $\omega \in [k]$ such that $\mathcal{J}(b) - \mathcal{J}(a) = \mathcal{J}(a_\omega) - \mathcal{J}(a_{\omega-1})$. By Lemma 3.10 intervals $[a, b]$ and $[a_{\omega-1}, a_\omega]$ are projective. Since $\mathcal{J}(a_\omega) - \mathcal{J}(a_{\omega-1}) \neq \mathcal{J}(a_{\omega'}) - \mathcal{J}(a_{\omega'-1})$ whenever $\omega \neq \omega'$, the result follows by Lemma 3.10. □

It will be convenient for us to use another representation of elements of a distributive lattice $L$. Take a maximal chain $C$ in $L$, say, $a_0 \prec a_1 \prec \ldots \prec a_k$, where $a_0, a_k$ are the least and greatest elements of $L$, respectively, and let $M = \{1, \ldots, k\}$ be the set of its prime quotients, where $\omega \in M$ denotes the quotient $a_{\omega-1} \prec a_\omega$. An element $a \in L$ corresponds to the set $\mathcal{M}(a)$ of quotients from $M$ that are projective to quotients of the form $c \prec d \leq a$. As the following lemma shows this alternative representation is equivalent to $\mathcal{J}$.

**Lemma 3.12** *There is a one-to-one correspondence $\varphi$ between the set $J(L)$ of join irreducible elements of lattice $L$ and set $M$ such that, for any $a \in L$, an element $b \in J(L)$ satisfies the inequality $b \leq a$ if and only if there is a prime quotient $c \prec d \leq a$ projective to $\varphi(b)$. Thus, $\mathcal{M}(a) = \{\varphi(b) \mid b \in \mathcal{J}(a)\}$.*

**Proof:** For a join-irreducible element $b \in J(L)$ let $b'$ denote the only element in $L$ such that $b' \prec b$. Clearly, $\mathcal{J}(b) - \mathcal{J}(b') = \{b\}$, therefore by Lemma 3.10 all such quotients are not projective to each other. We set $\varphi(b) = \omega$ where $\omega$ is the unique prime quotient in $M$ such that $b' \prec b$ is projective to $a_{\omega-1} \prec a_\omega$. If $b \in \mathcal{J}(a)$ then clearly $\varphi(b) \in \mathcal{M}(a)$. It remains to show the converse, that is for any prime quotient $c \prec d \leq a$ there is $b \in J(L)$ with $b \leq a$ such that $c \prec d$ is projective to $b' \prec b$.

Let $\mathcal{J}(a) = \{b_1, \dots, b_\ell\}$. Then for any element $c \leq a$ we have $\mathcal{J}(c) \subseteq \{b_1, \dots, b_\ell\}$. For any prime quotient $c \prec d \leq a$ if $\mathcal{J}(d) - \mathcal{J}(c) = \{b_i\}$, then $\mathcal{J}(d) - \mathcal{J}(c) = \mathcal{J}(b_i) - \mathcal{J}(b'_i)$, and, therefore, by Lemma 3.10, the quotients $c \prec d$ and $b'_i \prec b_i$ are projective. □

For a relational structure $\mathcal{H}$ and its congruence lattice $\mathsf{Con}(\mathcal{H})$ we use the following notation. Let $C$ be a maximal chain $\Delta_H = \theta_0 \prec \theta_1 \prec \dots \prec \theta_\ell = \bigtriangledown_H$. The set $M$ is defined to be the set of the prime quotients of this chain. Slightly abusing the notation the quotient $\theta_{\omega-1} \prec \theta_\omega$ will be denoted by $\omega$. A congruence $\theta \in \mathsf{Con}(\mathcal{H})$ corresponds to the set $\mathcal{M}(\theta)$ of quotients from $M$ that are projective to quotients of the form $\gamma \prec \beta \leq \theta$. The bottom end of a prime quotient $\omega \in M$ will be denoted by $\omega_-$, and the top one by $\omega_+$.

The following proposition comprises properties of $\mathsf{Con}(\mathcal{H})$ that follow easily from the representation of this lattice as a lattice of subsets.

**Proposition 3.13** *(1) Every prime quotient in $\mathsf{Con}(\mathcal{H})$ is projective to one and only one of the intervals of $C$.*

*(2) For any $\omega \in M$, $\mathcal{M}(\omega_+) = \{1, \dots, \omega\}$.*

*(3) Mapping $\mathcal{M}$ is a representation of $\mathsf{Con}(\mathcal{H})$ by subsets of $M$.*

*(4) For any $\omega \in M$, that is, any prime quotient in $C$, there is the greatest prime quotient $\kappa_\omega \prec \lambda_\omega$ projective to $\omega$; that is, for any $\alpha \prec \beta$ projective to $\omega$ we have $\alpha \leq \kappa_\omega$ and $\beta \leq \lambda_\omega$.*

*(5) For any $\omega \in M$, the congruence $\kappa_\omega$ is* meet-irreducible, *that is, if $\kappa_\omega = \alpha \wedge \beta$ than $\kappa_\omega = \alpha$ or $\kappa_\omega = \beta$ (see Fig. 8(c)).*

**Proof:** Items (1)–(3) follow straightforwardly from Lemmas 3.11 and 3.12. In part (2) Lemma 3.11 is applied to the interval $[\Delta_H, \omega_+]$.

(4) Let $\kappa_\omega$ be the join of all $\alpha \in \mathsf{Con}(\mathcal{H})$ such that $\omega \notin \mathcal{M}(\alpha)$. By parts (2) and (3) of the proposition $\omega \notin \mathcal{M}(\kappa_\omega)$. Then set $\lambda_\omega = \kappa_\omega \vee \omega_+$. Since $\omega \notin \mathcal{M}(\omega_-)$, we have $\omega_- \leq \kappa_\omega$ and $\mathcal{M}(\lambda_\omega) = \mathcal{M}(\kappa_\omega) \cup \mathcal{M}(\omega_-) \cup \{\omega\} = \mathcal{M}(\kappa_\omega) \cup \{\omega\}$.

Let $\alpha \prec \beta$ be a prime quotient projective to $\omega$, that is $\mathcal{M}(\beta) - \mathcal{M}(\alpha) = \{\omega\}$. Then $\omega \notin \mathcal{M}(\alpha)$, so $\alpha \leq \kappa_\omega$. As $\mathcal{M}(\beta) - \mathcal{M}(\alpha) = \mathcal{M}(\lambda_\omega) - \mathcal{M}(\kappa_\omega)$, we have $\beta \leq \lambda_\omega$, and by Lemma 3.10 $\alpha \prec \beta$ and $\kappa_\omega \prec \lambda_\omega$ are projective.

(5) Suppose $\kappa_\omega = \alpha \wedge \beta$. Then $\omega \notin \mathcal{M}(\alpha)$ or $\omega \notin \mathcal{M}(\beta)$. By the choice of $\kappa_\omega$, either $\alpha \leq \kappa_\omega$ or $\beta \leq \kappa_\omega$. □

### 3.3.2 Relational structures admitting the affine type

Let us again consider the congruence lattice $\mathsf{Con}(\mathcal{H})$. A congruence $\beta$ is said to be *solvable* over $\alpha$ if there are $\alpha = \theta_1 \prec \dots \prec \theta_k = \beta$ such that all the prime quotients $\theta_i \prec \theta_{i+1}$ have the affine type. Then $\overset{s}{\sim}$ denotes the binary relation on $\mathsf{Con}(\mathcal{H})$ defined as follows: $\alpha \overset{s}{\sim} \beta$ if and only if $\alpha \vee \beta$ is solvable over $\alpha \wedge \beta$.

**Proposition 3.14** *(1) $\overset{s}{\sim}$ is an equivalence relation and, moreover, a* congruence *of $\mathsf{Con}(\mathcal{H})$; that is, for any $\alpha_1, \alpha_2, \beta_1, \beta_2 \in \mathsf{Con}(\mathcal{H})$ such that $\alpha_1 \overset{s}{\sim} \alpha_2, \beta_1 \overset{s}{\sim} \beta_2$, we have $(\alpha_1 \vee \beta_1) \overset{s}{\sim} (\alpha_2 \vee \beta_2), (\alpha_1 \wedge \beta_1) \overset{s}{\sim} (\alpha_2 \wedge \beta_2)$.*

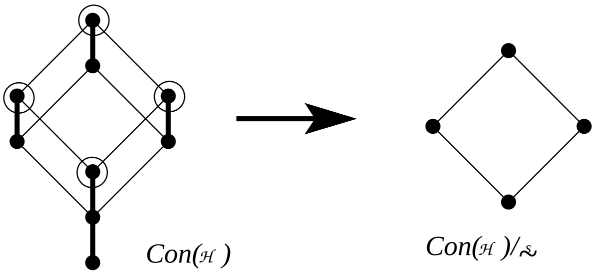

Figure 10: Congruence lattice and its quotient lattice modulo $\overset{s}{\sim}$. Prime quotients of the affine type are shown by thick lines; the greatest elements in the classes of $\overset{s}{\sim}$ are encircled

*(2) Every class $S$ of $\overset{s}{\sim}$ has the greatest $\alpha_S$ and the least $\beta_S$ elements (with respect to $\le$), and equals the interval $[\beta_S, \alpha_S]$. Every prime quotient inside $S$ has the affine type.*

*(3) The quotient lattice $\mathcal{L}_{\mathcal{H}} = \mathsf{Con}(\mathcal{H})/_{\overset{s}{\sim}}$ is distributive (see Fig. 10).*

**Proof:** (1) is Lemma 7.4 of [41].

(2) The first part follows from the well known fact that every class of any congruence of a finite lattice is an interval, and therefore every class has the least and the greatest elements. Let $\alpha \prec \beta$ be a prime quotient in $S$. We have $\alpha \overset{s}{\sim} \beta$, that is $\alpha = \alpha \wedge \beta$ and $\alpha \vee \beta = \beta$ are connected with a chain of prime quotients of the affine type. However, $\mathsf{Con}(\mathcal{H})$ is modular, hence $\alpha \prec \beta$ is the only such chain.

(3) Theorem 7.7(2) from [41] claims that $\mathcal{L}_{\mathcal{H}}$ is meet semi-distributive. Since $\mathsf{Con}(\mathcal{H})$ is modular, so is $\mathcal{L}_{\mathcal{H}}$, and by Observation 3.1 $\mathcal{L}_{\mathcal{H}}$ is distributive. □

The $\overset{s}{\sim}$-class containing congruence $\alpha$ will be denoted by $\alpha^{\sim}$.

Proposition 3.14(3) implies that $\mathcal{L}_{\mathcal{H}}$ can be represented as a lattice of subsets of a finite set $M$. Similar to Subsection 3.3.1, $M$ can be chosen to be the set of prime quotients of a maximal chain $C$ in $\mathcal{L}_{\mathcal{H}}$. Note that the endpoints of $\omega \in M$ are sets $S_1, S_2$ of congruences from $\mathsf{Con}(\mathcal{H})$ ($S_1$ corresponds to the bottom end of $\omega$). By $\omega_-$ we denote the greatest element of $S_1$, and by $\omega_+$ the least element of $S_2$ such that $\omega_- \le \omega_+$. Let $\beta \prec \gamma$ be the greatest quotient in $\mathcal{L}_{\mathcal{H}}$ projective to $\omega$. Again, $\beta$ and $\gamma$ are sets $T_1, T_2$ of congruences from $\mathsf{Con}(\mathcal{H})$ ($T_1$ corresponds to $\beta$). By $\kappa_\omega$ we denote the greatest element of $T_1$, and $\lambda_\omega$ the least element in $T_2$ such that $\kappa_\omega \le \lambda_\omega$ (see Fig. 11).

**Proposition 3.15** *(1) Intervals $[\omega_-, \omega_+]$ and $[\kappa_\omega, \lambda_\omega]$ are prime quotients.*

*(2) Prime quotient $\omega_- \prec \omega_+$ is projective to $\kappa_\omega \prec \lambda_\omega$.*

*(3) Prime quotients $\omega_- \prec \omega_+$ and $\kappa_\omega \prec \lambda_\omega$ have the Boolean type.*

*(4) Congruence $\kappa_\omega$ is meet-irreducible.*

**Proof:** (1) Let $\omega_- \le \alpha \le \omega_+$. Since $(\omega_-)^{\sim} \prec (\omega_+)^{\sim}$, congruence $\alpha$ belongs to one of the two $\overset{s}{\sim}$-classes. It cannot be the case that $\alpha \in (\omega_-)^{\sim}$ and $\alpha \ne \omega_-$, because $\omega_-$ is the greatest element in $(\omega_-)^{\sim}$. If $\alpha \in (\omega_+)^{\sim}$ then $\alpha = \omega_+$, as $\omega_- \le \alpha$ and $\omega_+$ is the least element in $(\omega_+)^{\sim}$ with this property.

For $\kappa_\omega$ and $\lambda_\omega$ the argument is the same.

(2) Since $(\omega_-)^{\sim} \le (\kappa_\omega)^{\sim}$ and $\kappa_\omega$ is the greatest element in $(\kappa_\omega)^{\sim}$, it follows that $\omega_- \le \kappa_\omega$. Then $(\kappa_\omega \wedge \omega_+)^{\sim} = (\kappa_\omega)^{\sim} \wedge (\omega_+)^{\sim} = (\omega_-)^{\sim}$, hence, as $\omega_-$ is the greatest element in $(\omega_-)^{\sim}$,we obtain $\omega_- \le \kappa_\omega \wedge \omega_+ \le \omega_-$, that is, $\kappa_\omega \wedge \omega_+ = \omega_-$. Next, $(\kappa_\omega \vee \omega_+)^{\sim} = (\kappa_\omega)^{\sim} \vee (\omega_+)^{\sim} = (\lambda_\omega)^{\sim}$. Since $\kappa_\omega \le \kappa_\omega \vee \omega_+$, it follows that $\kappa_\omega \vee \omega_+ \ge \lambda_\omega$. Thus intervals $[\omega_-, \omega_+]$ and $[\kappa_\omega, \kappa_\omega \vee \omega_+]$ are projective. By the Isomorphism

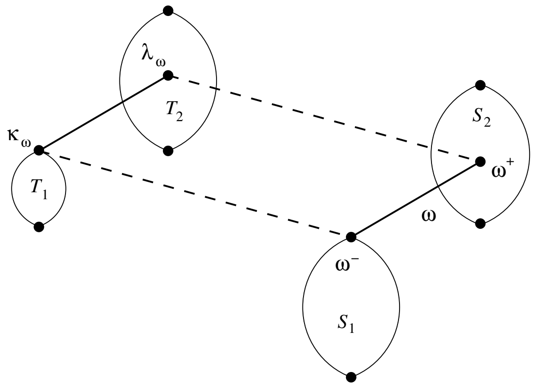

Figure 11: Congruence lattice and congruences $\kappa_\omega, \lambda_\omega$. Solid lines represent prime intervals of the Boolean type, ovals represent $\overset{s}{\sim}$-classes

Theorem for modular lattices, see Theorem 2, Chapter IV of [37], they are isomorphic. Hence, as $\omega_- \prec \omega_+$ is a prime quotient, $[\kappa_\omega, \kappa_\omega \vee \omega_+]$ is also a prime quotient, which implies $\kappa_\omega \vee \omega_+ = \lambda_\omega$.

(3) If $\omega_- \prec \omega_+$ or $\kappa_\omega \prec \lambda_\omega$ had the affine type, the $\overset{s}{\sim}$-classes $(\omega_-)^\sim$ and $(\omega_+)^\sim$, or $(\kappa_\omega)^\sim$ and $(\lambda_\omega)^\sim$, respectively, would be equal. A contradiction with the assumptions made.

(4) Suppose $\kappa_\omega = \alpha \wedge \beta$, then $\alpha^\sim \wedge \beta^\sim = (\kappa_\omega)^\sim$. By Proposition 3.13 $(\kappa_\omega)^\sim$ is meet-irreducible, therefore $\alpha^\sim = \kappa_\omega^\sim$ or $\beta^\sim = \kappa_\omega^\sim$. If, say, $\alpha^\sim = (\kappa_\omega)^\sim$ then $\alpha = \kappa_\omega$. □

## 3.4 Structure of relations invariant under a Mal'tsev operation

### 3.4.1 Basic properties

The following proposition contains some basic properties of relations invariant under a Mal'tsev operation, which will be constantly used.

**Proposition 3.16** *Let $\mathcal{H}$ be a structure with a Mal'tsev polymorphism $m$ and let $R$ be an $n$-ary relation pp-definable in $\mathcal{H}$. Then for any $I \subseteq [n]$ the following properties hold*
*(1) $R$ is* rectangular, *that is if* $\mathbf{a}, \mathbf{b} \in \mathrm{pr}_I R, \mathbf{c}, \mathbf{d} \in \mathrm{pr}_{[n]-I} R$ *and* $(\mathbf{a}, \mathbf{c}), (\mathbf{a}, \mathbf{d}), (\mathbf{b}, \mathbf{c}) \in R$, *then* $(\mathbf{b}, \mathbf{d}) \in R$.
*(2) The relation $\theta_I = \{\langle \mathbf{a}, \mathbf{b} \rangle \in (\mathrm{pr}_I R)^2 \mid$ there is $\mathbf{d} \in \mathrm{pr}_{[n]-I} R$ such that $(\mathbf{a}, \mathbf{d}), (\mathbf{b}, \mathbf{d}) \in R\}$ is a congruence of* $\mathrm{pr}_I R$.
*(3) There is a one-to-one correspondence $\pi$ between $\theta_I$- and $\theta_{[n]-I}$-classes such that $R$ is a disjoint union of sets of the form $B \times C$, where $B$ and $C$ are a $\theta_I$- and $\theta_{[n]-I}$-class, respectively, related by $\pi$.*

**Proof:** (1) It suffices to observe that

$$m\left(\begin{pmatrix} \mathbf{a} \\ \mathbf{d} \end{pmatrix}, \begin{pmatrix} \mathbf{a} \\ \mathbf{c} \end{pmatrix}, \begin{pmatrix} \mathbf{b} \\ \mathbf{c} \end{pmatrix}\right) = \begin{pmatrix} \mathbf{b} \\ \mathbf{d} \end{pmatrix}.$$

(2) It is straightforward that $\theta_I$ is reflexive and symmetric. If $\langle \mathbf{a}, \mathbf{b} \rangle, \langle \mathbf{b}, \mathbf{c} \rangle \in \theta_I$, say, $(\mathbf{a}, \mathbf{d}), (\mathbf{b}, \mathbf{d}) \in R$ and $(\mathbf{b}, \mathbf{e}), (\mathbf{c}, \mathbf{e}) \in R$, then by rectangularity $(\mathbf{a}, \mathbf{e}) \in R$ implying $\langle \mathbf{a}, \mathbf{c} \rangle \in \theta_I$. Finally, if, say, $I = \{1, \ldots, k\}$ and $[n] - I = \{k+1, \ldots, n\}$ then $\theta_I$ is defined by the pp-formula

$$\begin{aligned} \theta_I(x_1, \ldots, x_k, y_1, \ldots, y_k) \quad = \quad & \exists x_{k+1}, \ldots, x_n (R(x_1, \ldots, x_k, x_{k+1}, \ldots, x_n) \\ & \wedge R(y_1, \ldots, y_k, x_{k+1}, \ldots, x_n)). \end{aligned}$$

(3) Let $B$ be a $\theta_I$-class and $C$ a $\theta_{[n]-I}$-class such that $(\mathbf{a},\mathbf{b}) \in R$ for some $\mathbf{a} \in B$, $\mathbf{b} \in C$. Then for any $\mathbf{c} \in C$ there is $\mathbf{d} \in \mathrm{pr}_I R$ with $(\mathbf{d},\mathbf{b}), (\mathbf{d},\mathbf{c}) \in R$. By rectangularity we get $(\mathbf{a},\mathbf{c}) \in R$. Repeating the same argument for tuples from $B$ we conclude $B \times C \subseteq R$. Finally, if for some $\mathbf{a} \in B$ there is $\mathbf{b} \in \mathrm{pr}_{[n]-I} R - C$ with $(\mathbf{a},\mathbf{b}) \in R$ then, as $(\mathbf{a},\mathbf{c}) \in R$ for any $\mathbf{c} \in C$, we have $\langle \mathbf{b},\mathbf{c}\rangle \in \theta_{[n]-I}$, contradicting the assumption $\mathbf{b} \in \mathrm{pr}_{[n]-I} R - C$. □

Binary relations invariant with respect to a Mal'tsev operation have particularly simple form. Let $B_1, B_2$ be subalgebras of $\mathcal{H}$ and let $\alpha_1 \in \mathsf{Con}(B_1)$, $\alpha_2 \in \mathsf{Con}(B_2)$ be such that $|B_1/_{\alpha_1}| = |B_2/_{\alpha_2}|$. Let also $\varphi$ be a one-to-one mapping from $B_1/_{\alpha_1}$ to $B_2/_{\alpha_2}$. The *thick mapping* corresponding to $\varphi$ is the binary relation $R = \{(a,b) \in B_1 \times B_2 \mid \varphi(a^{\alpha_1}) = b^{\alpha_2}\}$. Any congruence $\alpha$ is the thick mapping corresponding to the identity mapping on $H/_{\alpha}$. Proposition 3.16(3) implies the following

**Corollary 3.17** *Let $\mathcal{H}$ be a relational structure with a Mal'tsev polymorphism. Then every binary relation $R$ pp-definable in $\mathcal{H}$ is a thick mapping.*

Indeed, let $R$ be a subdirect product of $B_1$ and $B_2$, and let $\alpha_1 = \theta_{\{1\}}$, $\alpha_2 = \theta_{\{2\}}$. Then by Proposition 3.16(3) there is a one-to-one correspondence $\varphi$ between $\alpha_1$- and $\alpha_2$-classes such that $R$ is a disjoint union of sets of the form $B \times \varphi(B)$, $B$ is an $\alpha_1$-class. Thus $R$ is the thick mapping corresponding to $\varphi$.

We shall use thick mappings throughout the paper. Somewhat related to thick mappings is the following relation on the set of coordinate positions of a relation. Let $R$ be a $k$-ary subdirect power of $H$. By $\alpha^*$ we denote a relation on the set $[k]$ defined as follows: $i, j$ are *not* in $\alpha^*$ if there are $\mathbf{a},\mathbf{b} \in R$ such that $\langle \mathbf{a}[i], \mathbf{b}[i]\rangle \in \alpha$, but $\langle \mathbf{a}[j], \mathbf{b}[j]\rangle \notin \alpha$, or $\langle \mathbf{a}[j], \mathbf{b}[j]\rangle \in \alpha$, but $\langle \mathbf{a}[i], \mathbf{b}[i]\rangle \notin \alpha$.

### 3.4.2 The Boolean type and rectangularity properties

Let $\mathbb{A}$ be a finite algebra. Algebra $\mathbb{A}$ is called *subdirectly irreducible* if there is a congruence $\mu$, the *monolith* of $\mathbb{A}$, such that $\Delta_A \prec \mu$ and for any congruence $\gamma \neq \Delta_A$ we have $\mu \leq \gamma$. Similarly, we call a relational structure $\mathcal{H}$ subdirectly irreducible if $\mathsf{Con}(\mathcal{H})$ has a monolith, that is a congruence $\mu$ satisfying the conditions above.

Let $R \in \mathsf{def}(\mathcal{H})$, where $\mathcal{H}$ is a subdirectly irreducible structure with a Mal'tsev polymorphism, be an $k$-ary subdirect power of $\mathcal{H}$. The equivalence relation $\mu^*$ is defined in the same way as before. Note that if $\langle i,j\rangle \in \mu^*$ then $\mathrm{pr}_{i,j} R$ is the graph of a bijective mapping $\psi$, that is, $\mathrm{pr}_{i,j} R = \{(a, \psi(a)) \mid a \in H\}$. If the prime quotient $\Delta_H \prec \mu$ has the Boolean type, Lemma 2.7 from [11] characterizes $\mu^*$-classes in terms of so-called *coherent sets*. It shows that in this case $\mu^*$-classes are the coherent sets. Then Lemma 2.6 of [11] can be restated as follows.

**Lemma 3.18 (Lemma 2.6, [11])** *Let $R$ be an $n$-ary subdirect power of $\mathcal{H}$ and the structure $\mathcal{H}$ is subdirectly irreducible. Let also $\mu$ be its monolith, let prime quotient $\Delta_H \prec \mu$ have the Boolean type, and let $I_1, \dots, I_\ell$ be the $\mu^*$-classes (or, equivalently, the coherent sets). Let also $B_1, \dots, B_n$ be $\mu$-classes such that $R \cap (B_1 \times \dots \times B_n) \neq \varnothing$, and*

$$R_{I_j} = \mathrm{pr}_{I_j} R \cap \prod_{i \in I_j} B_i.$$

*Then $R \cap (B_1 \times \dots \times B_n) = R_{I_1} \times \dots \times R_{I_\ell}$.*

Recall that for a congruence $\alpha \in \mathsf{Con}(\mathcal{H})$, we denote by $\alpha^n$ the congruence of $R$ consisting of pairs $\langle \mathbf{a},\mathbf{b}\rangle$ of tuples such that $\langle \mathbf{a}[i], \mathbf{b}[i]\rangle \in \alpha$ for all $i \in [n]$.

**Corollary 3.19** *Let $\mathcal{H}$ be a structure with a Mal'tsev polymorphism, let $M$ be a maximal chain in $\mathsf{Con}(\mathcal{H})$, let $R$ be an $n$-ary subdirect power of $\mathcal{H}$ and $\omega \in M$. Let also $B_1, \dots, B_n$ be some classes of $\lambda_\omega$ and $I_1, \dots, I_\ell$ the classes of $\kappa^*_\omega$. Let also $R' = R/_{\kappa^n_\omega}$, where $R/_{\kappa^n_\omega} = \{((\mathbf{a}[1])^{\kappa_\omega}, \dots, (\mathbf{a}[n])^{\kappa_\omega}) \mid \mathbf{a} \in R\}$, and $B'_i = B_i/_{\kappa_\omega}$ for $i \in [n]$. Then either $R \cap (B_1 \times \dots \times B_n) = \varnothing$, or*

$$R' \cap (B'_1 \times \dots \times B'_n) = R'_{I_1} \times \dots \times R'_{I_\ell},$$

*where $R'_{I_j} = \mathrm{pr}_{I_j} R' \cap \prod_{i \in I_j} B'_i$.*

**Proof:** Relation $R'$ can be treated as a subdirect power of $\mathcal{H}/_{\kappa_\omega}$. Since $\kappa_\omega$ is meet-irreducible by Proposition 3.15(4), the congruence lattice of structure $\mathcal{H}/_{\kappa_\omega}$ has a monolith, $\lambda_\omega$, and therefore is subdirectly irreducible. Now the result follows straightforwardly from Proposition 3.15(3) and Lemma 3.18. □

**Remark 3.20** *(1) Let $I_j = \{i_{j1}, \dots, i_{jk_j}\}$. Every $R'_{I_j}$ can be represented as the set $\{(a, \psi_{ji_{j2}}(a), \dots, \psi_{ji_{jk_j}}(a)) \mid a \in B'_{i_{j1}}\}$, where $(\mathrm{pr}_{i_{j1}, i_{jm}} R') \cap (B'_{i_{j1}} \times B'_{i_{jm}})$ is the graph of mapping $\psi_{ji_{jm}}$.*

*(2) Another way to state Corollary 3.19 is the following. Let $i_1, \dots, i_\ell$ be representatives of the $\kappa^*_\omega$-classes. Then for any choice of $\kappa_\omega$-classes $a'_{i_m} \in B'_{i_m}$, $m \in [\ell]$, there is $\mathbf{a} \in R$ such that $\mathbf{a}[i_m] \in a'_{i_m}$ for all $m \in [\ell]$.*

# 4 Necessary condition for tractability

In this section we prove two more necessary conditions for #-tractability. Both of them follow from Proposition 2.16, but they allow us to design an algorithm for #CSP.

If the algebra corresponding to a structure $\mathcal{H}$ does not omit the affine type, then we have a stronger necessary condition for the tractability of $\#\mathrm{CSP}(\mathcal{H})$.

**Proposition 4.1** *If $\mathcal{H}$ is congruence singular then for any congruences $\delta \leq \alpha < \beta \in \mathsf{Con}(\mathcal{H})$ such that $\alpha \overset{s}{\sim} \beta$, any $n$-ary relation $R \in \mathsf{def}(\mathcal{H})$, and any sequences $A_1, \dots, A_n$ and $B_1, \dots, B_n$ of $\alpha$-classes such that $A_i, B_i$ belong to the same $\beta$-class for each $i \in [n]$, if $R_1 = R \cap (A_1 \times \dots \times A_n) \neq \varnothing$ and $R_2 = R \cap (B_1 \times \dots \times B_n) \neq \varnothing$, then $|R_1/_{\delta^n}| = |R_2/_{\delta^n}|$.*

Suppose that Proposition 4.1 is proved in the case $\alpha \prec \beta$, that is, the following lemma is true (we prove it later).

**Lemma 4.2** *If $\mathcal{H}$ is congruence singular then for any congruences $\delta \leq \alpha \prec \beta \in \mathsf{Con}(\mathcal{H})$ such that $\alpha \prec \beta$ has the affine type, any $n$-ary relation $R \in \mathsf{def}(\mathcal{H})$, and any sequences $A_1, \dots, A_n$ and $B_1, \dots, B_n$ of $\alpha$-classes such that $A_i, B_i$ belong to the same $\beta$-class for all $i \in [n]$, if $R_1 = R \cap (A_1 \times \dots \times A_n) \neq \varnothing$ and $R_2 = R \cap (B_1 \times \dots \times B_n) \neq \varnothing$, then $|R_1/_{\delta^n}| = |R_2/_{\delta^n}|$.*

Then the general case follows.

**Proof:** [of Proposition 4.1] We proceed by induction on the length of a maximal chain $\alpha = \alpha_1 \prec \dots \prec \alpha_k = \beta$. Lemma 4.2 provides the base case of induction. Suppose that the proposition is proved for $\delta \leq \alpha < \gamma$ where $\gamma \prec \beta$. That is for any sequences $A'_1, \dots, A'_n$ and $B'_1, \dots, B'_n$ of $\alpha$-classes such that $A_i, B_i$ belong to the same $\gamma$-class for each $i \in [n]$, if $R'_1 = R \cap (A'_1 \times \dots \times A'_n) \neq \varnothing$ and $R'_2 = R \cap (B'_1 \times \dots \times B'_n) \neq \varnothing$, then $|R'_1/_{\delta^n}| = |R'_2/_{\delta^n}|$.

Let $A''_i, B''_i$ be the $\gamma$-classes containing $A_i, B_i$, respectively, and $R''_1 = R \cap (A''_1 \times \ldots \times A''_n)$, $R''_2 = R \cap (B''_1 \times \ldots \times B''_n)$. Since $\gamma \prec \beta$ and this prime quotient has the affine type, we can apply Lemma 4.2 to the triple of congruences $\delta \le \gamma \prec \beta$ to obtain $|R''_1/_{\delta^n}| = |R''_2/_{\delta^n}|$. Then we apply Lemma 4.2 to the triple of congruences $\alpha \le \gamma \prec \beta$, and obtain the equality $|R''_1/_{\alpha^n}| = |R''_2/_{\alpha^n}|$; denote this number by $N$. By the induction hypothesis, every $\alpha^n$-class inside $R''_1$ (and inside $R''_2$) contains the same number of $\delta^n$-classes. Therefore $|R''_1/_{\delta^n}| = N \cdot |R_1/_{\delta^n}|$ and $|R''_2/_{\delta^n}| = N \cdot |R_2/_{\delta^n}|$. Equality $|R_1/_{\delta^n}| = |R_2/_{\delta^n}|$ follows. □

To prove Lemma 4.2 we make use of some basics of commutator theory in congruence modular varieties (see [35]). As usual we introduce all required notions for relational structures rather than for algebras. Let $\mathcal{H}$ be a relational structure with a Mal'tsev polymorphism $m$, $R \in \mathsf{def}(\mathcal{H})$ a $k$-ary relation, and $\alpha, \beta, \gamma$ congruences of $R$. Congruence $\alpha$ *centralizes* $\beta$ *modulo* $\gamma$, denoted $C(\alpha, \beta; \gamma)$, if, for any ($n$-ary) polymorphism $f$ of $\mathcal{H}$, any $\langle \mathbf{u}, \mathbf{v} \rangle \in \alpha$ and any $\langle \mathbf{a}_1, \mathbf{b}_1 \rangle, \ldots, \langle \mathbf{a}_{n-1}, \mathbf{b}_{n-1} \rangle \in \beta$,

$$\begin{aligned} &\langle f(\mathbf{u}, \mathbf{a}_1, \ldots, \mathbf{a}_{n-1}), f(\mathbf{u}, \mathbf{b}_1, \ldots, \mathbf{b}_{n-1}) \rangle \in \gamma \\ \iff \quad &\langle f(\mathbf{v}, \mathbf{a}_1, \ldots, \mathbf{a}_{n-1}), f(\mathbf{v}, \mathbf{b}_1, \ldots, \mathbf{b}_{n-1}) \rangle \in \gamma. \end{aligned}$$

The smallest congruence $\gamma$ such that $C(\alpha, \beta; \gamma)$ is called the *commutator* of $\alpha, \beta$, denoted $[\alpha, \beta]$.

**Example 4.3** Let $\mathcal{H}$ be a 3-element structure with the universe $H = \{0, 1, 2\}$ and 4-ary relation $R$ that contains the tuples listed below (written vertically)

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

(these are the tuples $(a, b, c, d)$ satisfying the equality $a + b \equiv c + d \pmod 2$), and also tuples obtained from them by replacing some of the 1's with 2. Consider unary relation $H$. Set $\beta = \bigtriangledown_H$, and set $\alpha$ to be the congruence with classes $A^0 = \{0\}$ and $A^1 = \{1, 2\}$. Observe that $\alpha$ is a congruence, since it is given by the following pp-formula

$$\alpha(x, y) = \exists z R(x, y, z, z).$$

It is not hard to show that the polymorphisms of $\mathcal{H}$ are the operations $f(x_1, \ldots, x_n)$ satisfying the following condition: there is an operation $g(y_1, \ldots, y_n)$ on $\{0, 1\}$ such that (a) $g(y_1, \ldots, y_n) = e_1 y_1 + \ldots + e_n y_n + e \pmod 2$, and (b) if $x_i \in A^{y_i}$ for $i \in [n]$ then $f(x_1, \ldots, x_n) \in A^{g(y_1, \ldots, y_n)}$.

We show that $[\beta, \beta] \le \alpha$. Let $f(x_1, \ldots, x_n)$ be a polymorphism of $\mathcal{H}$ and $g(y_1, \ldots, y_n) = e_1 y_1 + \ldots + e_n y_n + e$ the corresponding linear operation on $\{0, 1\}$. Let also $u, v, a_1, \ldots, a_{n-1}, b_1, \ldots, b_{n-1} \in H$ be such that $\langle u, v \rangle \in \beta$ and $\langle a_i, b_i \rangle \in \beta$ (as $\beta$ is the total relation, these are just any elements of $H$). Let $u \in A^{u'}, v \in A^{v'}$ and $a_i \in A^{a'_i}, b_i \in A^{b'_i}$ for $i \in [n-1]$. If $\langle f(u, a_1, \ldots, a_{n-1}), f(u, b_1, \ldots, b_{n-1}) \rangle \in \alpha$ then $g(u', a'_1, \ldots, a'_{n-1}) = g(u', b'_1, \ldots, b'_{n-1})$. Using the linearity of $g$ we have $e_2 a'_1 + \ldots + e_n a'_{n-1} + e = e_2 b'_1 + \ldots + e_n b'_{n-1} + e \pmod 2$. Therefore $g(v', a'_1, \ldots, a'_{n-1}) = g(v', b'_1, \ldots, b'_{n-1})$, and so $\langle f(v, a_1, \ldots, a_{n-1}), f(v, b_1, \ldots, b_{n-1}) \rangle \in \alpha$. The converse implication is similar.

The next propesition follows from Proposition 4.3 and Theorem 4.9 of [35], Theorem 7.2 of [41]

**Proposition 4.4** *Let $\mathcal{H}$ be a relational structure with a Mal'tsev polymorphism, $R \in \mathsf{def}(\mathcal{H})$ a ($k$-ary) relation, and $\alpha, \beta$ congruences of $R$. Then*

*(1)* $[\alpha, \beta] = [\beta, \alpha]$*;*
*(2) if* $\alpha \prec \beta$*, then this prime quotient has the affine type if and only if* $[\beta, \beta] \leq \alpha$*;*
*(3) if* $\alpha \leq \beta$ *and* $[\beta, \beta] \leq \alpha$*, there is a congruence* $\theta$ *of* $\beta$ *(where* $\beta$ *is considered as a* $2k$*-ary relation from* $\mathsf{def}(\mathcal{H})$*) such that the set* $\{(\mathbf{a}, \mathbf{b}) \mid \langle \mathbf{a}, \mathbf{b}\rangle \in \alpha\}$ *is a class of* $\theta$*.*

Now we are in a position to prove Lemma 4.2.

**Proof:** [of Lemma 4.2] By switching to the quotient structure $\mathcal{H}/_\delta$ we may assume that $\delta$ is the equality relation. To prove Lemma 4.2 we consider several congruences of $R$, including $\alpha^n$ and $\beta^n$. As we are concerned about $\alpha$-classes within some $\beta$-classes, we can restrict $R$ to a single $\beta^n$-class. By Lemma 2.20 every $\beta^n$ class of $R$ is a relation pp-definable in $\mathcal{H}$, so let $R'$ be an arbitrary such class.

CLAIM 1. $[\beta^n, \beta^n] \leq \alpha^n$.

Let $f$ be a ($k$-ary) polymorphism of $\mathcal{H}$, and let $\langle \mathbf{u}, \mathbf{v}\rangle \in \beta^n$ and $\langle \mathbf{a}_1, \mathbf{b}_1\rangle, \dots, \langle \mathbf{a}_{k-1}, \mathbf{b}_{k-1}\rangle \in \beta^n$ where $\mathbf{u}, \mathbf{v}, \mathbf{a}_i, \mathbf{b}_i \in R'$ for $i \in [k-1]$. If $\langle f(\mathbf{u}, \mathbf{a}_1, \dots, \mathbf{a}_{k-1}), f(\mathbf{u}, \mathbf{b}_1, \dots, \mathbf{b}_{k-1})\rangle \in \alpha^n$ then $\langle f(\mathbf{u}[i], \mathbf{a}_1[i], \dots, \mathbf{a}_{k-1}[i]), f(\mathbf{u}[i], \mathbf{b}_1[i], \dots, \mathbf{b}_{k-1}[i])\rangle \in \alpha$ for each $i \in [n]$. Since $C(\beta, \beta; \alpha)$, this implies $\langle f(\mathbf{v}[i], \mathbf{a}_1[i], \dots, \mathbf{a}_{k-1}[i]), f(\mathbf{v}[i], \mathbf{b}_1[i], \dots, \mathbf{b}_{k-1}[i])\rangle \in \alpha$ for each index $i \in [n]$. Thus $\langle f(\mathbf{v}, \mathbf{a}_1, \dots, \mathbf{a}_{k-1}), f(\mathbf{v}, \mathbf{b}_1, \dots, \mathbf{b}_{k-1})\rangle \in \alpha^n$.

Every $\alpha^n$-class of $R'$ has the form $R' \cap (A_1 \times \dots \times A_n)$ for certain $\alpha$-classes $A_1, \dots, A_n$. Let $C_1, \dots, C_k$ be the $\alpha^n$-classes of $R'$, and $|C_i| = \ell_i$. We have to prove that $\ell_i = \ell_j$ for any $i, j \in [k]$.

We treat the congruence $\beta^n$ restricted onto $R'$ as a $2n$-ary relation pp-definable in $\mathcal{H}$; let us denote it by $Q$. By the choice of $R'$ we have $Q = R'^2$. Proposition 4.4(3) implies that there is a congruence $\gamma$ of $Q$ such that the set $D$ of pairs of the form $(\mathbf{a}, \mathbf{b})$, $\mathbf{a}, \mathbf{b} \in R'$ and $\langle \mathbf{a}, \mathbf{b}\rangle \in \alpha^n$, is a $\gamma$-class. Let $\gamma' = \gamma \vee \alpha^{2n}$.

CLAIM 2. (1) Every class $E$ of $\gamma'$ is the union $(C_1 \times C_{\varphi_E(1)}) \cup \dots \cup (C_k \times C_{\varphi_E(k)})$ for a certain bijective mapping $\varphi_E : [k] \to [k]$.
(2) The set $D$ is a class of $\gamma'$; and for this class $\varphi_D$ is the identity mapping.

Note that for any tuples $\mathbf{a}, \mathbf{b}, \mathbf{c}, \mathbf{d} \in R$ such that $\mathbf{a}, \mathbf{c} \in C_i$ and $\mathbf{b}, \mathbf{d} \in C_j$ we have $\langle (\mathbf{a}, \mathbf{b}), (\mathbf{c}, \mathbf{d})\rangle \in \alpha^{2n}$.

We start with (2). Clearly, $D$ has the required form of a union for the identity mapping $\varphi_D$. Since $D$ is a class of $\gamma$ and a union of $\alpha^{2n}$-classes, it is a class of $\gamma \vee \alpha^{2n} = \gamma'$.

(1) It suffices to prove three claims: (a) for any $C_i, C_j$, if $(C_i \times C_j) \cap E \neq \varnothing$ then $C_i \times C_j \subseteq E$; (b) if $(\mathbf{a}, \mathbf{b}), (\mathbf{c}, \mathbf{d}) \in E$ and $\langle \mathbf{a}, \mathbf{c}\rangle \in \alpha^n$, then $\langle \mathbf{b}, \mathbf{d}\rangle \in \alpha^n$; and (c) for any $C_i$ there is $C_j$ such that $(C_i \times C_j) \cap E \neq \varnothing$.

Property (a) follows from the inclusion $\alpha^{2n} \leq \gamma'$.

To prove (b) suppose that there are $(\mathbf{a}, \mathbf{b}), (\mathbf{c}, \mathbf{d}) \in E$ such that $\langle \mathbf{a}, \mathbf{c}\rangle \in \alpha^n$, but $\langle \mathbf{b}, \mathbf{d}\rangle \notin \alpha^n$. As $\alpha^{2n} \leq \gamma'$, we may assume $\mathbf{a} = \mathbf{c}$. Since $\gamma'$ is a congruence on $Q$, and therefore is reflexive, $(\mathbf{a}, \mathbf{a}, \mathbf{a}, \mathbf{a}), (\mathbf{b}, \mathbf{b}, \mathbf{d}, \mathbf{d})$, $(\mathbf{a}, \mathbf{b}, \mathbf{a}, \mathbf{b}) \in \gamma'$, considering $\gamma'$ as a 4-ary relation on $R'$. Then we have

$$m\begin{pmatrix} \mathbf{a} & \mathbf{a} & \mathbf{b} \\ \mathbf{a} & \mathbf{b} & \mathbf{b} \\ \mathbf{a} & \mathbf{a} & \mathbf{d} \\ \mathbf{a} & \mathbf{d} & \mathbf{d} \end{pmatrix} = \begin{pmatrix} \mathbf{b} \\ \mathbf{a} \\ \mathbf{d} \\ \mathbf{a} \end{pmatrix} \in \gamma' \quad \text{and} \quad m\begin{pmatrix} \mathbf{a} & \mathbf{a} & \mathbf{b} \\ \mathbf{b} & \mathbf{a} & \mathbf{a} \\ \mathbf{a} & \mathbf{a} & \mathbf{d} \\ \mathbf{b} & \mathbf{a} & \mathbf{a} \end{pmatrix} = \begin{pmatrix} \mathbf{b} \\ \mathbf{b} \\ \mathbf{d} \\ \mathbf{b} \end{pmatrix} \in \gamma',$$

which implies that $(\mathbf{b}, \mathbf{d}) \in D$, and therefore $\langle \mathbf{b}, \mathbf{d}\rangle \in \alpha^n$, a contradiction.

To prove (c) suppose that, for some $C_i$ and for any $C_j$, $(C_i \times C_j) \cap E = \varnothing$. Take $\mathbf{a} \in C_i$ and $(\mathbf{b}, \mathbf{c}) \in E$. Then $(\mathbf{b}, \mathbf{c}, \mathbf{b}, \mathbf{c}), (\mathbf{b}, \mathbf{b}, \mathbf{b}, \mathbf{b}), (\mathbf{a}, \mathbf{a}, \mathbf{b}, \mathbf{b}) \in \gamma'$ (the last tuple belongs to $\gamma'$ because $(\mathbf{a}, \mathbf{a}), (\mathbf{b}, \mathbf{b}) \in D$). We have

$$m\begin{pmatrix} \mathbf{b} & \mathbf{b} & \mathbf{a}\\ \mathbf{c} & \mathbf{b} & \mathbf{a}\\ \mathbf{b} & \mathbf{b} & \mathbf{b}\\ \mathbf{c} & \mathbf{b} & \mathbf{b}\end{pmatrix} = \begin{pmatrix}\mathbf{a}\\ \mathbf{d}\\ \mathbf{b}\\ \mathbf{c}\end{pmatrix} \in \gamma,$$

where $\mathbf{d} = m(\mathbf{c}, \mathbf{b}, \mathbf{a})$. Thus $(\mathbf{a}, \mathbf{d}) \in E$, a contradiction

Suppose that $\ell_i \neq \ell_j$ for some $i, j \in [k]$; clearly if such $i, j$ exist we can choose $i = 1$. Without loss of generality we also assume $\ell_1 < \ell_j$. We present a pair of congruences of $R'$ that violate the condition of Proposition 2.16. One of them is $\gamma'$ the other one is $\beta'$ defined to be the congruence $\alpha^n \times \beta^n$. In other words, $\langle(\mathbf{a}, \mathbf{b}), (\mathbf{c}, \mathbf{d})\rangle \in \beta'$ if and only if $\langle \mathbf{a}, \mathbf{c}\rangle \in \alpha^n$. It is not hard to see that $\gamma' \vee \beta' = \beta^n \times \beta^n$ and $\gamma' \wedge \beta' = \alpha^n \times \alpha^n$. Indeed, $\alpha^{2n} \leq \gamma' \wedge \beta'$. If $\langle(\mathbf{a}, \mathbf{b}), (\mathbf{c}, \mathbf{d})\rangle \in \gamma' \wedge \beta'$ then $\langle \mathbf{a}, \mathbf{c}\rangle \in \alpha^n$, since $\langle(\mathbf{a}, \mathbf{b}), (\mathbf{c}, \mathbf{d})\rangle \in \beta'$, and by Claim 2 this implies $\langle \mathbf{b}, \mathbf{d}\rangle \in \alpha^n$. Thus $\gamma' \wedge \beta' \leq \alpha^n \times \alpha^n$. Let $(\mathbf{a}, \mathbf{b}), (\mathbf{c}, \mathbf{d}) \in R'$. As $\beta^{2n}$ is the total binary relation on $R'$ these pairs are in the same $\beta^{2n}$-class. By Claim 2 there is $\mathbf{e} \in R'$ such that $\langle(\mathbf{a}, \mathbf{b}), (\mathbf{c}, \mathbf{e})\rangle \in \gamma'$. Since $\langle(\mathbf{c}, \mathbf{e}), (\mathbf{c}, \mathbf{d})\rangle \in \beta'$ we have $\langle(\mathbf{a}, \mathbf{b}), (\mathbf{c}, \mathbf{d})\rangle \in \gamma' \circ \beta' \subseteq \gamma' \vee \beta'$.

Every class of $\alpha^n \times \alpha^n$ is the Cartesian product of two classes $C_i, C_j$ of $\alpha^n$. Therefore, its cardinality equals $\ell_i\ell_j$. Thus, the row of the matrix $M(\gamma', \beta')$ corresponding to a $\gamma'$-class $E$ looks as follows

$$\begin{pmatrix} \ell_1\ell_{\varphi_E(1)} & \ell_2\ell_{\varphi_E(2)} & \cdots & \ell_k\ell_{\varphi_E(k)} \end{pmatrix}.$$

The row corresponding to the class $D$ is

$$\begin{pmatrix} \ell_1^2 & \ell_2^2 & \cdots & \ell_k^2 \end{pmatrix}.$$

As $Q = R'^2$, there is a $\gamma'$-class $E$ such that $C_1 \times C_j \subseteq E$ (recall that $\ell_1 < \ell_j$). Since $\mathcal{H}$ is congruence singular, the rows of $M(\gamma', \beta')$ corresponding to classes $D$ and $E$ are proportional, that is

$$\frac{\ell_1}{\ell_{\varphi_E(1)}} = \frac{\ell_2}{\ell_{\varphi_E(2)}} = \ldots = \frac{\ell_k}{\ell_{\varphi_E(k)}}.$$

Let $j_1 = 1$, $j_2 = \varphi_E(1) = j$, and $j_t = \varphi_E(j_{t-1})$ for $t > 2$. Let also $m > 1$ be the minimal number such that $j_m = 1$. We prove $\ell_{j_t} > \ell_{j_{t-1}}$ that leads to a contradiction, as it would imply that $\ell_1 < \ell_{j_m} = \ell_1$. By the assumption made $\ell_{j_1} = \ell_1 < \ell_j = \ell_{j_2}$, which gives us the base case. From the equalities above we have $\ell_{j_t}^2 = \ell_{j_{t-1}}\ell_{j_{t+1}}$. Therefore if $\ell_{j_{t-1}} < \ell_t$ then $\ell_t < \ell_{j_{t+1}}$, which proves the induction step. □

**Example 4.3 (continued)** Reconsider the relational structure $\mathcal{H}$ from Example 4.3. By Proposition 4.1 the problem #CSP($\mathcal{H}$) is #P-complete. Indeed, consider congruences $\alpha$ and $\beta = \bigtriangledown_H$ of $H$. We showed that $[\beta, \beta] \leq \alpha$, therefore by Proposition 4.4, prime quotient $\alpha \prec \beta$ has the affine type. Setting $\delta = \Delta_H$ we see that $\alpha$-classes $A^0$ and $A^1$ contain different number of elements.

The constrution used in the proof of Proposition 4.1 in this case looks as follows. Congruence $\beta$ is the binary relation $H^2$. Congruence $\gamma'$ of $\beta$ such that $D = \{(0,0), (1,1), (1,2), (2,1), (2,2)\}$ is its class can be chosen to be the congruence with classes $D$ and $E = \{(0,1), (0,2), (1,0), (2,0)\}$; and it is easy to see that we can use $R$ defined in Example 4.3 for that. Finally, the classes of $\beta' = \alpha \times \beta$ are $\{(0,0), (0,1), (0,2)\}$ and $\{(1,0), (1,1), (1,2), (2,0), (2,1), (2,2)\}$. Therefore

$$M(R; \gamma', \beta'; \Delta_H) = \begin{pmatrix} 1 & 4\\ 2 & 2\end{pmatrix},$$

and its rank equals 2.

We will also need another corollary from Proposition 2.16. Let $T$ be a $k$-dimensional array, that is a collection of numbers $T[i_1,\dots,i_k]$ indexed by tuples $(i_1,\dots,i_k)$, where $1\le i_k\le m_k$. Array $T$ has rank 1, denoted $\mathsf{rank}(T)=1$, if for each $\ell\in[k]$, and any $i_1,\dots,i_{\ell-1},i_{\ell+1},\dots,i_k,j_1,\dots,j_{\ell-1},j_{\ell+1},\dots,j_k$ with $i_u,j_u\in[m_u]$, we have

$$\frac{T[i_1,\dots,i_{\ell-1},1,i_{\ell+1},\dots,i_k]}{T[j_1,\dots,j_{\ell-1},1,j_{\ell+1},\dots,j_k]}=\dots=\frac{T[i_1,\dots,i_{\ell-1},m_\ell,i_{\ell+1},\dots,i_k]}{T[j_1,\dots,j_{\ell-1},m_\ell,j_{\ell+1},\dots,j_k]}. \tag{1}$$

Observe that if $k=2$, and thus $T$ is a matrix, $T$ has rank 1 in the sense introduced above if and only if $T$ has the row- (column-) rank 1.

**Lemma 4.5** *Array $T$ has rank 1 if and only if for each $\ell\in[k]$ there are numbers $t^\ell_1,\dots,t^\ell_{m_k}$ such that*

$$T[i_1,\dots,i_k]=t^1_{i_1}\cdot\ldots\cdot t^k_{i_k}.$$

**Proof:** If numbers $t^\ell_1,\dots,t^\ell_{m_k}$ with the required properties exist then equalities (1) are trivially true. To prove the converse we observe that (1) implies that for any $i_1,\dots,i_k$ and $\ell\in[k]$

$$T[i_1,\dots,i_k]=T[i_1,\dots,i_{\ell-1},1,i_{\ell+1},\dots,i_k]\cdot\frac{T[1,\dots,1,i_\ell,1,\dots,1]}{T[1,\dots,1]}.$$

Therefore

$$T[i_1,\dots,i_k]=T[i_1,1,\dots,1]\cdot\prod_{\ell=2}^{k}\frac{T[1,\dots,1,i_\ell,1,\dots,1]}{T[1,\dots,1]}.$$

Choosing $t^1_i=T[i,1,\dots,1]$ for $i\in[m_i]$ and $t^j_i=\frac{T[1,\dots,1,i,1,\dots,1]}{T[1,\dots,1]}$ for $2\le j\le k$ and $i\in[m_j]$ we obtain the result. □

Now let $R$ be a relation pp-definable in a structure $\mathcal{H}$ with a Mal'tsev polymorphism, and let $\gamma_1,\dots,\gamma_k$ be congruences on $R$ such that for each $i\in[k]$

$$\gamma_i\vee(\gamma_1\wedge\ldots\wedge\gamma_{i-1}\wedge\gamma_{i+1}\wedge\ldots\wedge\gamma_k)=\gamma_1\vee\ldots\vee\gamma_k \tag{2}$$

Let also $C$ be a class of $\gamma=\gamma_1\vee\ldots\vee\gamma_k$, and let $A^i_1,\dots,A^i_{m_i}$ be the classes of $\gamma_i$ from $C$. Condition (2) means that for any $j_1,\dots,j_k$ the set $A^1_{j_1}\cap\ldots\cap A^k_{j_k}$ is a nonempty class of $\beta=\gamma_1\wedge\ldots\wedge\gamma_k$. Indeed, let $\ell$ be the smallest number such that for certain $j_1,\dots,j_\ell$ the set $A^1_{j_1}\cap\ldots\cap A^\ell_{j_\ell}=\varnothing$. Then for any $\mathbf{a},\mathbf{b}\in C$ we have

$$\langle\mathbf{a},\mathbf{b}\rangle\in\gamma_\ell\vee(\gamma_1\wedge\ldots\wedge\gamma_{\ell-1}\wedge\gamma_{\ell+1}\wedge\ldots\wedge\gamma_k)\le\gamma_\ell\vee(\gamma_1\wedge\ldots\wedge\gamma_{\ell-1}).$$

Moreover, as congruences of $R$ are permutable, $\langle\mathbf{a},\mathbf{b}\rangle\in\gamma_\ell\circ(\gamma_1\wedge\ldots\wedge\gamma_{\ell-1})$. Suppose $\mathbf{a}\in A^\ell_j$ and $\mathbf{b}$ belongs to a class $A^1_{j_1}\cap\ldots\cap A^{\ell-1}_{j_{\ell-1}}$ of $\gamma_1\wedge\ldots\wedge\gamma_{\ell-1}$. Then there exists $\mathbf{c}$ such that $\mathbf{c}\in A^\ell_j$ and $\mathbf{c}\in A^1_{j_1}\cap\ldots\cap A^{\ell-1}_{j_{\ell-1}}$, a contradiction. It is also clear that any two classes of this form are different. We consider a $k$-dimensional array $M(C;\gamma_1,\dots,\gamma_k)$, where

$$M(C;\gamma_1,\dots,\gamma_k)[i_1,\dots,i_k]=|A^1_{i_1}\cap\ldots\cap A^k_{i_k}|.$$

**Proposition 4.6** *Let $\gamma_1,\dots,\gamma_k$ be congruences of a structure $\mathcal{H}$ that has a Mal'tsev polymorphism, let them satisfy condition (2), and let $C$ be a class of $\gamma_1\vee\ldots\vee\gamma_k$. Then, if $\mathcal{H}$ is congruence singular then* $\mathsf{rank}(M(C;\gamma_1,\dots,\gamma_k))=1$.

**Proof:** We consider congruences $\gamma_i$ and $\beta_i = \gamma_1 \wedge \ldots \wedge \gamma_{i-1} \wedge \gamma_{i+1} \wedge \ldots \wedge \gamma_k$. To simplify the notation we assume $i = k$. If $\mathcal{H}$ is congruence singular, then $\mathsf{rank}(M(C; \gamma_k, \beta_k; \Delta_H)) = 1$. Let $A_1^j, \ldots, A_{m_j}^j$ be the classes of $\gamma_j$ from $C$. The classes of $\beta_k$ have the form $A_{i_1}^1 \cap \ldots \cap A_{i_{k-1}}^{k-1}$, the classes of $\gamma_k \wedge \beta_k$ are the classes of $\gamma_1 \wedge \ldots \wedge \gamma_k$. Therefore every row of $M(C; \beta_k, \gamma_k; \Delta_H)$ is equal to

$$(M(C; \gamma_1, \ldots, \gamma_k)[i_1, \ldots, i_{k-1}, 1], \ldots, M(C; \gamma_1, \ldots, \gamma_k)[i_1, \ldots, i_{k-1}, m_k])$$

for some $i_1, \ldots, i_{k-1}$. Since $\mathsf{rank}(M(C; \gamma_k, \beta_k)) = 1$, we get

$$\frac{M(C; \gamma_1, \ldots, \gamma_k)[i_1, \ldots, i_{k-1}, 1]}{M(C; \gamma_1, \ldots, \gamma_k)[j_1, \ldots, j_{k-1}, 1]} = \ldots = \frac{M(C; \gamma_1, \ldots, \gamma_k)[i_1, \ldots, i_{k-1}, m_k]}{M(C; \gamma_1, \ldots, \gamma_k)[j_1, \ldots, j_{k-1}, m_k]},$$

for any $j_1, \ldots, j_{k-1}, j_s \in [m_s]$. The proposition is proved. □

An important example of a collection of congruences satisfying condition (2) is the following (we prove it in Section 5.3). Let $\omega \in M$, and let $I_1, \ldots, I_k$ be the classes of $\kappa_\omega^*$. Congruence $\gamma_j$ is given by: $\langle \mathbf{a}, \mathbf{b} \rangle \in \gamma_j$ if and only if $\langle \mathbf{a}[i], \mathbf{b}[i] \rangle \in \omega_-$ for $i \in I_j$ and $\langle \mathbf{a}[i], \mathbf{b}[i] \rangle \in \omega_+$ otherwise.

# 5 Algorithms: prerequisites

## 5.1 Decision CSPs over structures with a Mal'tsev polymorphism.

If a relational structure $\mathcal{H}$ has a Mal'tsev polymorphism, then the decision CSP with the template $\mathcal{H}$ can be solved in polynomial time [6, 12]. Here we shall use the algorithm presented in [12], and we call it MAL'TSEV. This algorithm builds a sort of a succinct (polynomial size) representation for the set of all solutions.

Let $n$ be a positive integer, let $H$ be a finite set, let $\mathbf{a}, \mathbf{b}$ be $n$-tuples and let $(i, a, b)$ be any element in $[n] \times H^2$. We say that pair $\langle \mathbf{a}, \mathbf{b} \rangle$ *witnesses* $(i, a, b)$ if $\mathrm{pr}_{[i-1]}\mathbf{a} = \mathrm{pr}_{[i-1]}\mathbf{b}$, $\mathbf{a}[i] = a$, and $\mathbf{b}[i] = b$. We also say that $\mathbf{a}$ and $\mathbf{b}$ witness $(i, a, b)$ meaning that $\langle \mathbf{a}, \mathbf{b} \rangle$ witnesses $(i, a, b)$.

Let $R$ be any $n$-ary relation on $H$. The *signature* of $R$, $\mathsf{Sig}_R \subseteq [n] \times H^2$, is defined to be the set containing all triples $(i, a, b) \in [n] \times H^2$ witnessed by tuples in $R$, that is

$$\mathsf{Sig}_R = \{(i, a, b) \in [n] \times H^2 \mid \text{ there are } \mathbf{a}, \mathbf{b} \in R \text{ such that } \langle \mathbf{a}, \mathbf{b} \rangle \text{ witnesses } (i, a, b)\}.$$

Note that in our notation $(i, a, b) \in \mathsf{Sig}_R$ if and only if $\langle a, b \rangle$ belongs to the relation $\theta_i$ computed for the relation $\mathrm{pr}_{[i]}R$ (see Section 3.4.1). In particular, as $\mathcal{H}$ has a Mal'tsev polymorphism, relation $\mathrm{pr}_{[i]}R$ is rectangular, and hence for any $(i, a, b) \in \mathsf{Sig}_R$ and any $\mathbf{a} \in \mathrm{pr}_{[i]}R$ with $\mathbf{a}[i] = a$, the tuple $\mathbf{b}$ such that $\mathrm{pr}_{[i-1]}\mathbf{b} = \mathrm{pr}_{[i-1]}\mathbf{a}$ and $\mathbf{b}[i] = b$ also belongs to $\mathrm{pr}_{[i]}R$.

A subset $R'$ of $R$ is called a *representation* of $R$ if $\mathsf{Sig}_{R'} = \mathsf{Sig}_R$. If furthermore, $|R'| \leq 2|\mathsf{Sig}_R|$ then $R$ is called a *compact* representation of $R$. Observe that every relation $R$ has compact representations.

Let $\mathcal{H}$ be a relational structure and $R' \subseteq H^n$ for some $n$. By $\langle R' \rangle_{\mathcal{H}}$ we denote the relation *generated* by $R'$, that is, the smallest relation $R$ pp-definable in $\mathcal{H}$ and such that $R' \subseteq R$. Alternatively, $\langle R' \rangle_{\mathcal{H}}$ can be constructed from $R'$ by adding every tuple $\mathbf{a}$ that can be obtained as $f(\mathbf{a}_1, \ldots, \mathbf{a}_n)$ where $f$ is an ($n$-ary) polymorphism of $\mathcal{H}$ and $\mathbf{a}_1, \ldots, \mathbf{a}_n \in R'$. Since $\mathcal{H}$ is usually clear from the context we shall omit this subscript. The key lemma proved in [12] states that if $R$ is a relation pp-definable in a relational structure with a Mal'tsev polymorphism, and $R'$ is a representation of $R$, then $\langle R' \rangle = R$. Given an instance $\mathcal{G}$ of the constraint satisfaction problem $\mathrm{CSP}(\mathcal{H})$, $m = |\mathcal{G}|$, the set of all solutions $\Phi(\mathcal{G}, \mathcal{H})$ to this problem can be thought of as an $m$-ary relation pp-definable in $\mathcal{H}$. The algorithm presented in [12] finds a compact representation of this set.

We will need to know the unary and binary projections of the relation $\Phi(\mathcal{G},\mathcal{H})$, that is, sets of the form $\Phi_g = \{\varphi(g) \mid \varphi \in \Phi(\mathcal{G},\mathcal{H})\}$ for $g \in \mathcal{G}$, and $\Phi_{g,h} = \{(\varphi(g),\varphi(h)) \mid \varphi \in \Phi(\mathcal{G},\mathcal{H})\}$ for $g,h \in \mathcal{G}$. Let $R'$ be a compact representation of $\Phi(\mathcal{G},\mathcal{H})$. If $a \in \Phi_g$ then $(g,a,a) \in \mathsf{Sig}_{\Phi(\mathcal{G},\mathcal{H})}$, so $\Phi_g = \mathrm{pr}_{\{g\}}R'$. It is also not hard to see (see also [12]) that $\Phi_{g,h}$ is equal to $\langle \mathrm{pr}_{g,h}R' \rangle$. Therefore, we may assume that we have a precomputed table that for each subset of $\mathcal{H} \times \mathcal{H}$ gives the binary relation it generates. Then every time we need to find $\Phi_{g,h}$ using a compact representation $R'$, we just find the corresponding projection of $R'$ and look up the table.

If there are no complexity restrictions imposed, as in the case of precomputation, the relation generated by some set $Q \subseteq \mathcal{H}^n$ can be computed by employing the standard methods. Let $Q = \{\mathbf{a}_1,\dots,\mathbf{a}_m\}$. First, find all $m$-ary polymorphisms of $\mathcal{H}$. This can be done using the *indicator problem* [46]. Next, include into $\langle Q \rangle$ all tuples that can be represented as $f(\mathbf{a}_1,\dots,\mathbf{a}_m)$ for an $m$-ary polymorphism $f$.

## 5.2 Reduction to subdirect powers.

In general, for an instance $\mathcal{G}$ of $\#\mathrm{CSP}(\mathcal{H})$ the sets $\Phi_g$, $g \in \mathcal{G}$, are subalgebras of $\mathcal{H}$ that are not necessarily equal to $\mathcal{H}$. For us, however, it is much more convenient to deal with the case when $\Phi(\mathcal{G},\mathcal{H})$ is a subdirect power of $\mathcal{H}$, that is $\Phi_g = \mathcal{H}$ for all $g \in \mathcal{G}$. We show how to transform the problem so that $\Phi_g$ is $\mathcal{H}$ for all $g \in \mathcal{G}$. To do this we borrow some methods from the multi-sorted CSP, see, e.g. [10].

Let $D_1,\dots,D_\ell$ be the subalgebras of $\mathcal{H}$ (including $H$ itself). We define a relational structure $\chi(\mathcal{H})$ as follows. The universe of $\chi(\mathcal{H})$ is $D = D_1 \times \ldots \times D_\ell$; the $i$th component of an element $\overline{a} \in D$ is denoted by $\overline{a}[i]$. For any ($n$-ary) relation $R$ pp-definable in $\mathcal{H}$ and such that $\mathrm{pr}_j R = D_{i_j}$, we set $(\overline{a}_1,\dots,\overline{a}_n) \in \chi(R)$ if and only if $(\overline{a}_1[i_1],\dots,\overline{a}_n[i_n]) \in R$. In particular, each unary relation of $\chi(\mathcal{H})$ corresponding to a relation of $\mathcal{H}$ contains all elements of $D$ and, therefore, can be thrown out. For any coordinate position $i$ of any non-unary relation $R$, the set $\mathrm{pr}_i\chi(R)$ equals $D$. Finally, to define $\chi(\mathcal{H})$ formally, for each relational symbol $R$, we interpret it as $R^{\chi(\mathcal{H})} = \chi(R)$.

**Lemma 5.1** *If $\mathcal{H}$ is congruence singular then $\chi(\mathcal{H})$ is also congruence singular.*

**Proof:** Let $R$ be an $n$-ary relation over $D$. It naturally defines an $\ell n$-ary relation $\mathsf{fla}(R)$ over $H$ that we call *flattening* of $R$:

$$\begin{aligned}\mathsf{fla}(R) \;=\; & \{\mathsf{fla}(\mathbf{a}) \in H^{\ell n} \mid \text{there is } \mathbf{a} \in R \text{ such that} \\ & (\mathsf{fla}(\mathbf{a})[\ell(j-1)+1],\dots,\mathsf{fla}(\mathbf{a})[\ell j]) = \mathbf{a}[j] \text{ for each } j \in [n]\}.\end{aligned}$$

As is easily seen, $\mathsf{fla}$ is a one-to-one mapping between the set of $n$-tuples and the set of $\ell n$-tuples, and also between $n$-ary and $\ell n$-ary relations.

CLAIM 1. $|\mathsf{fla}(R)| = |R|$.

CLAIM 2. If $R$ is pp-definable in $\chi(\mathcal{H})$ then $\mathsf{fla}(R)$ is pp-definable in $\mathcal{H}$.

The following convention for indexing variables of predicates will be helpful. If $R$ is $n$-ary and $R(x_1,\dots,x_n)$ is the corresponding predicate, we use $\mathsf{fla}(R)(x_1^1,\dots,x_1^\ell,\dots,x_n^1,\dots,x_n^\ell)$ for the predicate corresponding to $\mathsf{fla}(R)$.

First, we prove the claim for a relation $R = \chi(R')$ where $R'$ is a relation from $\mathcal{H}$. Suppose that $\mathrm{pr}_j R' = D_{i_j}$ for $j \in [n]$. It is not hard to see that

$$\mathsf{fla}(R)(x_1^1, \dots, x_1^\ell, \dots, x_n^1, \dots, x_n^\ell) = R'(x_1^{i_1}, \dots, x_n^{i_n}) \wedge \bigwedge_{j=1}^{n} \bigwedge_{i=1}^{\ell} D_i(x_j^i).$$

Now we proceed by induction on the structure of a pp-definition of $R$. If $R = R_1 \wedge R_2$ then $\mathsf{fla}(R) = \mathsf{fla}(R_1) \wedge \mathsf{fla}(R_2)$. If $R(x_1, \dots, x_n) = \exists y R'(x_1, \dots, x_n, y)$ then

$$\mathsf{fla}(R)(x_1^1, \dots, x_1^\ell, \dots, x_n^1, \dots, x_n^\ell) = \exists y^1, \dots, y^\ell$$
$$\mathsf{fla}(R')(x_1^1, \dots, x_1^\ell, \dots, x_n^1, \dots, x_n^\ell, y^1, \dots, y^\ell) \wedge \bigwedge_{i=1}^{\ell} D_i(y^i)).$$

CLAIM 3. Let $R \in \mathsf{def}(\chi(\mathcal{H}))$ be an $n$-ary relation, $\alpha, \beta$ its congruences. Then (a) for any binary relation $\theta$ on $R$ and any $\mathbf{a}, \mathbf{b} \in R$, $\langle \mathbf{a}, \mathbf{b} \rangle \in \theta$ if and only if $\langle \mathsf{fla}(\mathbf{a}), \mathsf{fla}(\mathbf{b}) \rangle \in \mathsf{fla}(\theta)$; (b) relations $\mathsf{fla}(\alpha), \mathsf{fla}(\beta)$ are congruences of $\mathsf{fla}(R)$, (c) equalities $\mathsf{fla}(\alpha \wedge \beta) = \mathsf{fla}(\alpha) \wedge \mathsf{fla}(\beta)$, $\mathsf{fla}(\alpha \vee \beta) = \mathsf{fla}(\alpha) \vee \mathsf{fla}(\beta)$ hold, and (d) the number of $\alpha$- [$\beta$-] classes equals to that of $\mathsf{fla}(\alpha)$ [respectively, $\mathsf{fla}(\beta)$], and $|B| = |\mathsf{fla}(B)|$ for each $\alpha$- [$\beta$-] class $B$.

(a) follows from the observation that $\mathsf{fla}(\mathbf{a}, \mathbf{b}) = (\mathsf{fla}(\mathbf{a}), \mathsf{fla}(\mathbf{b}))$ for any $\mathbf{a}, \mathbf{b} \in R$.

(b) To prove it use part (a) along with Claim 2.

(c) Note that if $\mathsf{fla}(\mathbf{a}) = \mathsf{fla}(\mathbf{b})$ then $\mathbf{a} = \mathbf{b}$. Hence, $\mathsf{fla}(\alpha \wedge \beta) = \mathsf{fla}(\alpha \cap \beta) = \mathsf{fla}(\alpha) \cap \mathsf{fla}(\beta) = \mathsf{fla}(\alpha) \wedge \mathsf{fla}(\beta)$. To prove $\mathsf{fla}(\alpha \vee \beta) = \mathsf{fla}(\alpha) \vee \mathsf{fla}(\beta)$ we can use (a) to show that transitive closure is preserved by $\mathsf{fla}$, that implies the result.

(d) For any $\alpha$-class $B$ by Claim 1 we have $|B| = |\mathsf{fla}(B)|$. Using (a) we can also find a one-to-one correspondence between $\alpha$- and $\mathsf{fla}(\alpha)$-classes [respectively, $\beta$- and $\mathsf{fla}(\beta)$-classes].

Finally, let $\alpha, \beta$, and $\delta$ with $\delta \le \alpha, \beta$ be congruences of $R$, and let $A_1, \dots, A_m$ and $B_1, \dots, B_k$ be the $\alpha$- and $\beta$-classes respectively. Then $\mathsf{fla}(A_1), \dots, \mathsf{fla}(A_m)$ and $\mathsf{fla}(B_1), \dots, \mathsf{fla}(B_\ell)$ are the $\mathsf{fla}(\alpha)$- and $\mathsf{fla}(\beta)$-classes, respectively. Moreover, the number of $\delta$-classes in each $\alpha \wedge \beta$-class $B$ is equal to that of $\mathsf{fla}(\delta)$-classes in $\mathsf{fla}(B)$, and the number of $\alpha \vee \beta$-classes is equal to the number of $\mathsf{fla}(\alpha) \vee \mathsf{fla}(\beta)$-classes. Therefore $M(R; \alpha, \beta; \delta) = M(\mathsf{fla}(R); \mathsf{fla}(\alpha), \mathsf{fla}(\beta); \mathsf{fla}(\delta))$. □

It is sometimes useful to replace relational structure $\mathcal{H}$ with its *expansion*. Let $\mathcal{H}$ be a relational structure with vocabulary $\tau$ and universe $H$. Structure $\mathcal{H}'$ is said to be an expansion of $\mathcal{H}$ if it has the same universe $H$, and vocabulary $\tau' \supseteq \tau$, where every symbol from $\tau$ is interpreted in $\mathcal{H}'$ in the same way as in $\mathcal{H}$. An expansion of a structure can be thought of as throwing in some extra relations. If all the added relations are pp-definable in $\mathcal{H}$ then $\#\mathrm{CSP}(\mathcal{H}')$ is polynomial time reducible to $\#\mathrm{CSP}(\mathcal{H})$. Therefore expanding a structure by adding pp-definable relations does not change the complexity of the problem. By taking an expansion of $\mathcal{H}$ if necessary, we shall assume that along with every ($n$-ary) relational symbol $R$ and any $D_{i_1}, \dots, D_{i_n}$ the vocabulary of $\mathcal{H}$ contains a symbol $R'$ such that $R'^{\mathcal{H}} = R \cap (D_{i_1} \times \dots \times D_{i_n})$.

For an instance $\mathcal{G}$ of $\#\mathrm{CSP}(\mathcal{H})$, the algorithm in Fig. 12 constructs an instance $\mathcal{G}'$ of $\#\mathrm{CSP}(\chi(\mathcal{H}))$. The following lemma completes the reduction.

**Lemma 5.2** *Let $\mathcal{G}$ is an instance of $\#\mathrm{CSP}(\mathcal{H})$ and $\mathcal{G}'$ an instance of $\#\mathrm{CSP}(\chi(\mathcal{H}))$ constructed by algorithm* `Subdirect`. *Let also $\Phi_g = \mathrm{pr}_g \Phi(\mathcal{G}, \mathcal{H})$ for $g \in \mathcal{G}$. Then $\Phi(\mathcal{G}', \chi(\mathcal{H}))$ is a subdirect power of $\chi(\mathcal{H})$*

```
Algorithm Subdirect
INPUT: an instance $\mathcal{G}$ of $\#\mathrm{CSP}(\mathcal{H})$
OUTPUT: an instance $\mathcal{G}'$ of $\#\mathrm{CSP}(\chi(\mathcal{H}))$ with the same universe as $\mathcal{G}$

Step 1      find a compact representation of $\Phi(\mathcal{G},\mathcal{H})$ using MAL'TSEV
Step 2      for each $g \in \mathcal{G}$ find $\Phi_g$
Step 3      for each ($n$-ary) relational symbol $R$ do
Step 3.1        for each tuple $(g_1,\dots,g_n) \in R^{\mathcal{G}}$ do
Step 3.1.1          let $R'$ be the relational symbol such that $R'^{\mathcal{H}} = R^{\mathcal{H}} \cap (\Phi_{g_1} \times \ldots \times \Phi_{g_n})$
Step 3.1.2          include $(g_1,\dots,g_n)$ into $R'^{\mathcal{G}'}$
                endfor
            endfor
Step 4      output $\mathcal{G}'$
```

Figure 12:

*and*

$$|\Phi(\mathcal{G}',\chi(\mathcal{H}))| = |\Phi(\mathcal{G},\mathcal{H})| \cdot \prod_{g\in G} \frac{|D|}{|\Phi_g|}.$$

*Moreover,* `Subdirect` *is polynomial time.*

**Proof:** Let $\varphi \in \Phi(\mathcal{G},\mathcal{H})$ be a homomorphism from $\mathcal{G}$ to $\mathcal{H}$. Let a set of mappings $\chi(\varphi)$ from $\mathcal{G}'$ to $\chi(\mathcal{H})$ be given by

$$\chi(\varphi) = \{\psi : \mathcal{G}' \to \chi(\mathcal{H}) \mid \text{for any } g \in \mathcal{G}' \text{ if } \Phi_g = D_i \text{ and } \psi(g) = \overline{a} \text{ then } \overline{a}[i] = \varphi(g)\}.$$

(Note that $\mathcal{G}$ and $\mathcal{G}'$ have a common universe.) We show that every $\psi \in \chi(\varphi)$ is a homomorphism from $\mathcal{G}'$ to $\chi(\mathcal{H})$. Let $R'$ be a relational symbol and $(g_1,\dots,g_n) \in R'^{\mathcal{G}'}$. Tuple $(g_1,\dots,g_n)$ comes to $R'^{\mathcal{G}'}$ on Step 3.1.2 from some $R^{\mathcal{G}}$ such that $R'^{\mathcal{H}} = R^{\mathcal{H}} \cap (\Phi_{g_1} \times \ldots \times \Phi_{g_n})$. Therefore $(\varphi(g_1),\dots,\varphi(g_n)) \in R'^{\mathcal{H}}$. Since $\mathrm{pr}_i R'^{\mathcal{H}} = \Phi_{g_i}$ for $i \in [n]$, we also have $(\psi(g_1),\dots,\psi(g_n)) \in \chi(R'^{\mathcal{H}})$. Thus $\psi$ is a homomorphism.

For any $g \in \mathcal{G}'$ and any $a \in \Phi_g$ there is $\varphi \in \Phi(\mathcal{G},\mathcal{H})$ such that $\varphi(g) = a$, hence, for any $\psi \in \chi(\varphi)$ we have $\psi(g)[i] = a$. Since for any $a_j \in D_j$, $j \in [\ell] - \{i\}$, there exists $\psi \in \chi(\varphi)$ with $\psi(g)[j] = a_j$, this implies that $\Phi(\mathcal{G}',\chi(\mathcal{H}))$ is a subdirect power of $\chi(\mathcal{H})$.

Let $\varphi \in \Phi(\mathcal{G}',\chi(\mathcal{H}))$ be a homomorphism from $\mathcal{G}'$ to $\chi(\mathcal{H})$. Let us define a mapping $\chi^{-1}(\varphi)$ from $\mathcal{G}$ to $\mathcal{H}$ as follows. For $g \in \mathcal{G}$ if $\varphi(g) = \overline{a}$ and $\Phi_g = D_i$ then set $\chi^{-1}(\varphi)(g) = \overline{a}[i]$. By the construction of $\chi(\mathcal{H})$ and $\mathcal{G}'$, if we change the value $\overline{a} = \varphi(g)$ for some $g \in \mathcal{G}$ with $\Phi_g = D_i$ to any $\overline{b}$ such that $\overline{b}[i] = \overline{a}[i]$, then the resulting mapping $\varphi'$ is still a homomorphism from $\mathcal{G}'$ to $\chi(\mathcal{H})$ and $\chi^{-1}(\varphi') = \chi^{-1}(\varphi)$. For a fixed $g$ this can be done in $\frac{|D|}{|\Psi_g|}$ ways. Conversely, for any homomorphism $\psi \in \Phi(\mathcal{G},\mathcal{H})$, any mapping $\varphi\colon \mathcal{G}' \to \chi(\mathcal{H})$ such that $\chi^{-1}(\varphi) = \psi$ is a homomorphism of $\mathcal{G}'$ to $\chi(\mathcal{H})$. Therefore for each homomorphism $\psi \in \Phi(\mathcal{G},\mathcal{H})$ there are $\prod_{g\in G} \frac{|D|}{|\Phi_g|}$ homomorphisms $\varphi \in \Phi(\mathcal{G}',\chi(\mathcal{H}))$ such that $\chi^{-1} = \psi$. The result follows.

Finally, since Step 3 makes only one pass over every tuple of relations in $\mathcal{G}$, this step can be done in linear time. Thus the time complexity of the algorithm is dominated by Step 1, which is polynomial time, as so is algorithm MAL'TSEV. □

### 5.3 Structure of Mal'tsev instances

Let $\mathcal{G}$ be a $\#\mathrm{CSP}(\mathcal{H})$ instance and $|\mathcal{G}| = m$. In this section we study certain structural properties of the set of homomorphisms $\Phi(\mathcal{G}, \mathcal{H})$ from $\mathcal{G}$ to $\mathcal{H}$. It will be convenient to assume that the universe $G$ of $\mathcal{G}$ equals $[m]$. Set $\Phi(\mathcal{G}, \mathcal{H})$ can be thought of as an $m$-ary relation pp-definable in $\mathcal{H}$. By the results of the previous subsection we may assume that $R = \Phi(\mathcal{G}, \mathcal{H})$ is a subdirect power of $\mathcal{H}$. Recall that for a congruence $\theta \in \mathsf{Con}(\mathcal{H})$ by $\theta^m$ we denote the congruence of $R$ such that $\langle \mathbf{a}, \mathbf{b} \rangle \in \theta^m$ if and only if $\langle \mathbf{a}[g], \mathbf{b}[g] \rangle \in \theta$ for all $g \in \mathcal{G}$. For congruences $\beta \le \gamma \in \mathsf{Con}(\mathcal{H})$ and a mapping $\tau \colon \mathcal{G} \to \mathcal{H}/_{\beta}$, by $\tau^\gamma$ we denote a mapping from $\mathcal{G}$ to $\mathcal{H}/_{\gamma}$ given by $\tau^\gamma(g) = \tau(g)^\gamma$.

Let $M$ be the set of prime quotients of a maximal chain in $\mathcal{L} = \mathsf{Con}(\mathcal{H})/_{\stackrel{s}{\sim}}$. As before we assume $M = \{1, \ldots, \ell\}$. Let also $\omega \in M$. Take $\tau$, an element of $R/_{\omega_+^m}$. It can be thought of as a mapping from $\mathcal{G}$ to $\mathcal{H}/_{\omega_+}$. This mapping is always a homomorphism from $\mathcal{G}$ to $\mathcal{H}/_{\omega_+}$, but not every such homomorphism belongs to $R/_{\omega_+^m}$. Indeed, if $\omega = \ell$ and $\omega_+$ is the total relation, a homomorphism from any $\mathcal{G}$ to $\mathcal{H}/_{\omega_+}$, a 1-element structure, always exists, however, $R$ can be empty. By $\Phi(\mathcal{G}, \mathcal{H}; \tau)$ we denote the set of elements $\varrho$ from $R$, that is, homomorphisms from $\mathcal{G}$ to $\mathcal{H}$, such that $\varrho^{\omega_+} = \tau$.

We study the structure of $\Phi(\mathcal{G}, \mathcal{H}; \tau)$ up to $\omega_-$. More precisely, let $E_1, \ldots, E_r$ be the $\omega_-^*$-classes and $h_1, \ldots, h_r$ representatives of these classes. For any homomorphism $\varrho \in \Phi(\mathcal{G}, \mathcal{H}; \tau)$ and any $h \in E_i$, the value $\varrho(h)^{\omega_-}$ is completely determined by the value $\varrho(h_i)$, so we may focus on possible values of such homomorphisms on $h_1, \ldots, h_r$. Our goal is to show that these values are in some sense independent, meaning that for any collection $a_1 \in \tau(h_1)/_{\omega_-}, \ldots, a_r \in \tau(h_r)/_{\omega_-}$ (recall that $\tau(h_i)$ is a $\omega_+$-class) there is $\varrho \in \Phi(\mathcal{G}, \mathcal{H}; \tau)$ such that $\varrho(h_i)^{\omega_-} = a_i$. Unfortunately, this statement is false in general, however, in the end of this section we prove a result sufficiently close to this one. Note also that $\Phi(\mathcal{G}, \mathcal{H}; \tau)$ is considered as a part of $\Phi(\mathcal{G}, \mathcal{H})$. Although, it is possible to restrict the original instance so that its solutions are only members of $\Phi(\mathcal{G}, \mathcal{H}; \tau)$, it leads to several complications. The most important of them is that elements of $\mathcal{G}$ would have different domains, and those domains would have different congruence lattices that may significantly differ from $\mathsf{Con}(\mathcal{H})$ or any part of it.

First we consider a similar problem for another prime quotient, $\kappa_\omega \prec \lambda_\omega$. This will help us because, since $\kappa_\omega \wedge \omega_+ = \omega_-$, values $\varrho(h_i)^{\kappa_\omega}$ and $\tau(h_i)$ determine $\varrho(h_i)^{\omega_-}$. We prove that the required property is true in this case. Let $A_1, \ldots, A_k$ be the $\kappa_\omega^*$-classes and $g_1, \ldots, g_k$ representatives of these classes. By $C_1^u, \ldots, C_{s_u}^u$ we denote the $\kappa_\omega$-classes from $\tau(g_u)^{\lambda_\omega}$, $u \in [\ell]$.

**Lemma 5.3** *For any choice of $i_u \in [s_u]$, $u \in [k]$, there is a homomorphism $\varrho \in R$ such that for each $u \in [k]$*

$$\varrho(g_u)^{\kappa_\omega} = C_{i_u}.$$

**Proof:** If we set $B_g$ to be the $\lambda_\omega$-class containing $\tau(g)$ then $\tau$ witnesses that $R \cap (B_1 \times \ldots \times B_m) \neq \varnothing$. Let $R' = R/_{\kappa_\omega^m}$ and $B'_g = B_g/_{\kappa_\omega}$ for $g \in G$. Then, by Corollary 3.19, we have

$$R' \cap (B'_1 \times \ldots \times B'_m) = R'_{A_1} \times \ldots \times R'_{A_k},$$

where $R'_{A_u} = \mathrm{pr}_{A_u} R' \cap \prod_{g \in A_u} B'_g$ The result follows. □

If $\kappa_\omega^m \vee (\omega_+)^m$ were equal to $\lambda_\omega^m$ this would mean that $\Phi(\mathcal{G}, \mathcal{H}; \tau)$ intersects with every $\kappa_\omega^m$-class, and since $\kappa_\omega \wedge \omega_+ = \omega_-$, this non-empty intersection would provide a homomorphism with prescribed values modulo $\omega_-$. However in general $\kappa_\omega^m \vee (\omega_+)^m \neq \lambda_\omega^m$, so it is important to find $\kappa_\omega^m \vee (\omega_+)^m$. To do that we describe the interval $[\kappa_\omega^m, \lambda_\omega^m]$ in the congruence lattice $\mathsf{Con}(R)$. It will be more convenient to think of elements of $R$ as of tuples rather than mappings.

**Lemma 5.4** *Every prime quotient in the interval $[\kappa^m_\omega, \lambda^m_\omega]$ of the congruence lattice $\mathsf{Con}(R)$ has the Boolean type, the interval $[\kappa^m_\omega, \lambda^m_\omega]$ is a distributive lattice isomorphic to the lattice $2^{[k]}$ of subsets of a $k$-element set, where $k$ is the number of $\kappa^*_\omega$-classes, and every congruence in this interval can be represented as $\eta_J$, $J \subseteq [k]$, given by: $\langle \mathbf{a}, \mathbf{b}\rangle \in \eta_J$ if and only if $\langle \mathbf{a}[g_u], \mathbf{b}[g_u]\rangle \in \kappa_\omega$ whenever $u \in [k] - J$ and $\langle \mathbf{a}[g_u], \mathbf{b}[g_u]\rangle \in \lambda_\omega$ when $u \in J$.*

**Proof:** Replacing $R$ with $R/_{\kappa^m_\omega}$ we may assume that $\kappa_\omega = \Delta_H$. Thus if tuples $\mathbf{a}, \mathbf{b} \in R$ are such that $\mathbf{a}[g_u] = \mathbf{b}[g_u]$ for all $u \in [k]$, then $\mathbf{a} = \mathbf{b}$. Therefore, it suffices to consider relation $R' = \mathrm{pr}_{\{g_1,\dots,g_k\}} R$. We study intervals of the form $[\eta_J, \eta_{J\cup\{v\}}]$ for $J \subseteq [k]$ and $v \in [k] - J$. Any such interval is non-trivial, meaning $\eta_J < \eta_{J\cup\{v\}}$. Indeed, by Lemma 5.3, for any $J \subseteq [k]$ and $v \in [k] - J$ there are tuples $\mathbf{a}, \mathbf{b} \in R$ such that $\mathbf{a}[g_v] \neq \mathbf{b}[g_v]$, but $\mathbf{a}[g_u] = \mathbf{b}[g_u]$ for all $u \in [k] - \{v\}$. By the same reason $\Delta^k_H < \eta_{\{v\}}$ for any $v \in [k]$.

First, we show that every such interval is a prime quotient. Note that interval $[\eta_J, \eta_{J\cup\{v\}}]$ is prospective to $[\Delta^k_H, \eta_{\{v\}}]$. Indeed, if $\langle \mathbf{a}, \mathbf{b}\rangle \in \eta_J$ then $\mathbf{a}[g_u] = \mathbf{b}[g_u]$ for $u \in [k] - J$, and if $\langle \mathbf{a}, \mathbf{b}\rangle \in \eta_{\{v\}}$ then $\mathbf{a}[g_u] = \mathbf{b}[g_u]$ for all $u \neq v$, implying $\eta_J \wedge \eta_{\{v\}} = \Delta^k_H$. If $\langle \mathbf{a}, \mathbf{b}\rangle \in \eta_{J\cup\{v\}}$, then by Lemma 5.3 there is a tuple $\mathbf{c}$ such that $\mathbf{a}[g_u] = \mathbf{c}[g_u]$ for all $u \neq v$ and $\mathbf{c}[g_u] = \mathbf{b}[g_u]$ for all $u \in [k]-J$. Hence $\eta_J \vee \eta_{\{v\}} = \eta_{J\cup\{v\}}$. It suffices to show that the intervals of the form $\Delta^k_H < \eta_{\{v\}}$ are prime quotients. To simplify the notation we assume $v = 1$.

Let $\Delta^k_H < \alpha \leq \eta_{\{1\}}$. For any $\langle \mathbf{a}, \mathbf{b}\rangle \in \alpha$ and any $u \neq 1$, $\mathbf{a}[g_u] = \mathbf{b}[g_u]$. This means that $\alpha$ is determined by the relation

$$\begin{aligned}\beta \;=\; & \{\langle a, b\rangle \in H^2 \mid \text{ there are } \mathbf{a}, \mathbf{b} \in R' \text{ such that } \langle \mathbf{a}, \mathbf{b}\rangle \in \alpha,\ \mathbf{a}[g_1] = a,\ \mathbf{b}[g_1] = b, \\ & \quad \text{and } \mathbf{a}[g_u] = \mathbf{b}[g_u] \text{ for all } u \neq 1\}.\end{aligned}$$

Relation $\beta$ is a congruence of $\mathcal{H}$ and $\Delta_H < \beta \leq \lambda_\omega$. As $\Delta_H \prec \lambda_\omega$, we get $\beta = \lambda_\omega$, and the rectangularity of $R$ implies $\alpha = \eta_{\{1\}}$.

Let us now check that quotient $\Delta^k_H \prec \eta_{\{1\}}$ has the Boolean type. By Proposition 3.15(3) $\Delta_H \prec \lambda_\omega$ has the Boolean type, which means that there is a polymorphism of $f(x_1, \dots, x_n)$ of $\mathcal{H}$ and elements $c, d, a_1, \dots, a_{n-1}, b_1, \dots, b_{n-1}$ such that $\langle c, d\rangle \in \lambda_\omega$, $\langle a_i, b_i\rangle \in \lambda_\omega$ for $i \in [n-1]$, and $f(c, a_1, \dots, a_{n-1}) = f(c, b_1, \dots, b_{n-1})$ but $f(d, a_1, \dots, a_{n-1}) \neq f(d, b_1, \dots, b_{n-1})$. By Lemma 5.3 there are $\mathbf{c}, \mathbf{d}$ and $\mathbf{a}_i, \mathbf{b}_i$, $i \in [n-1]$, from $R'$ such that $\mathbf{c}[g_1] = c$, $\mathbf{d}[g_1] = d$, $\mathbf{a}_i[g_1] = a_i$, $\mathbf{b}_i[g_1] = b_i$, and $\mathbf{c}[g_u] = \mathbf{d}[g_u]$, $\mathbf{a}_i[g_u] = \mathbf{b}_i[g_u]$ for $i \in [n-1]$ and $u \in [k] - \{1\}$. Observe that $\langle \mathbf{c}, \mathbf{d}\rangle, \langle \mathbf{a}_1, \mathbf{b}_1\rangle, \dots, \langle \mathbf{a}_{n-1}, \mathbf{b}_{n-1}\rangle \in \eta_{\{1\}}$. Then we have $f(\mathbf{c}, \mathbf{a}_1, \dots, \mathbf{a}_{n-1}) = f(\mathbf{c}, \mathbf{b}_1, \dots, \mathbf{b}_{n-1})$ but $f(\mathbf{d}, \mathbf{a}_1, \dots, \mathbf{a}_{n-1}) \neq f(\mathbf{d}, \mathbf{b}_1, \dots, \mathbf{b}_{n-1})$, that implies that $\eta_{\{1\}}$ does not centralize itself modulo $\Delta^k_H$, and so $\Delta_H \prec \eta_{\{1\}}$ has the Boolean type.

We have proved that any interval of the form $[\eta_J, \eta_{J\cup\{v\}}]$ is a prime quotient, and, by Lemma 3.5, it has the Boolean type. Next we show that every prime quotient $\alpha \prec \beta$ with $\Delta^k_H \leq \alpha \prec \beta \leq \lambda^k_\omega$ is projective to one of such intervals, and therefore has the Boolean type. Suppose the contrary, and let $\beta \leq \lambda^k_\omega$ be a maximal congruence such that, for some $\alpha \prec \beta$, $[\alpha, \beta]$ is projective to $[\eta_J, \eta_{J\cup\{v\}}]$ for no $J \subseteq [k]$, and $v \in [k] - J$. Let $J$ be a maximal set such that $\eta_J \leq \alpha$, and $v$ any member of $[k] - J$. Then $\eta_J \prec \eta_{J\cup\{v\}}$. Since $\alpha \wedge \eta_{J\cup\{v\}} = \eta_J$, if $\eta_{J\cup\{v\}} \leq \beta$ the interval $[\alpha, \beta]$ is prospective to $[\eta_J, \eta_{J\cup\{v\}}]$, a contradiction with the assumption made. Otherwise, by the modularity of $\mathsf{Con}(R)$, $[\alpha, \beta]$ is prospective to $[\alpha \vee \eta_{J\cup\{v\}}, \beta \vee \eta_{J\cup\{v\}}]$, a contradiction with the maximality of $\beta$. Thus, every prime quotient from interval $[\Delta^k_H, \lambda^k_\omega]$ has the Boolean type.

Finally, by Lemma 6.6 of [41], this implies that this interval does not contain a diamond, and, as $\mathsf{Con}(R)$ is modular, $[\Delta^k_H, \lambda^k_\omega]$ is distributive. Since the congruences $\eta_{\{1\}}, \dots, \eta_{\{\ell\}}$ are join-irreducible elements of this lattice, and $\eta_1 \vee \ldots \vee \eta_\ell = \lambda_\omega^m$, every element $\theta$ of this interval can be represented in the form

$$\theta = \bigvee_{u \in J} \eta_u = \eta_J$$

for some $J \subseteq [k]$. □

Now we obtain a result similar to Lemma 5.3 for homomorphisms modulo $\omega_-$. Note that $\omega_-^*$-classes cannot be used, because, in general, they have nothing in common with $\kappa_\omega^*$-classes. Indeed, a pair $\langle g, g' \rangle$ belongs to $\alpha^*$ for some congruence $\alpha$ if, for any mappings $\varrho_1, \varrho_2$, $\langle \varrho_1(g), \varrho_2(g) \rangle \in \alpha$ if and only if $\langle \varrho_1(g'), \varrho_2(g') \rangle \in \alpha$. For different congruences $\alpha$ such conditions are incomparable. However, if some homomorphism $\tau \in R/_{\omega_+^m}$ is fixed, this argument does not work anymore. Since $\kappa_\omega \wedge \omega_+ = \omega_-$, homomorphism $\tau$ and a choice of values for $g_1, \ldots, g_k$ (provided they are taken from $\tau(g_u)^{\lambda_\omega}$) determine a mapping $\varrho : \mathcal{G} \to \mathcal{H}/_{\omega_-}$. For any $g \in \mathcal{G}$, the values of $g_1, \ldots, g_k$ determine the $\kappa_\omega$-class $\varrho(g)$ belongs to, and $\tau(g)$ determines the $\omega_+$-class of $\varrho(g)$. Therefore every homomorphism from $\Phi(\mathcal{G}, \mathcal{H}; \tau)$ up to $\omega_-$ can be defined by a certain choice of values for $g_1, \ldots, g_k$. The difficulty is that some choices do not define any homomorphism. The next lemma shows which combinations of values for $g_1, \ldots, g_k$ correspond to elements of $\Phi(\mathcal{G}, \mathcal{H}; \tau)$.

**Lemma 5.5** *There is $J_\omega \subseteq [k]$ such that for any $\tau \in R/_{\omega_+^m}$ (we use notation for $\kappa_\omega$-classes introduced before Lemma 5.3), there are $i_u$ with $i_u \in [s_u]$, $u \in [k] - J_\omega$, satisfying the following conditions. For any homomorphism $\varrho \in R/_{\omega_-^m}$ with $\varrho^{\omega_+} = \tau$ the collection of $i_u$, $u \in [k] - J_\omega$, can be completed by $i_u$ with $i_u \in [s_u]$ for $u \in J_\omega$ such that $\varrho(g_u) \in \tau(g_u) \cap C_{i_u}^u$ for $u \in [k]$; and, for any $g \in A_u$, $u \in [k]$, we have $\varrho(g) = \pi(g) \cap C$, where $C$ is the $\kappa_\omega$-class corresponding to the choice of $C_{i_u}^u$ for $g_u$.*

*Conversely, for any choice of $C_{i_u}^u$, $u \in J$, the mapping $\varrho$ defined in this way is an element of $R/_{\omega_-^m}$, and $\varrho^{\omega_+} = \tau$.*

**Proof:** Observe that in the congruence lattice $\mathsf{Con}(R)$ we have $\kappa_\omega^m \wedge \omega_+^m = \omega_-^m$ and $\kappa_\omega^m \le \kappa_\omega^m \vee \omega_+^m \le \lambda_\omega^m$. By Lemma 5.4, $\kappa_\omega^m \vee \omega_+^m = \eta_{J_\omega}$ for some $J_\omega \subseteq [k]$. This means that there are fixed $i_u$, $u \in [k] - J_\omega$, with $i_u \in [s_u]$, such that for any $\varrho \in R/_{(\omega_-)^m}$, with $\varrho^{\omega_+} = \tau$, we have $\varrho(g_u) \in C_{i_u}^u$ for $u \in [k] - J_\omega$.

Take $\varrho \in R/_{\omega_-^m}$ with $\varrho^{\omega_+} = \tau$. Clearly, $\varrho^{\kappa_\omega}$ belongs to $\tau^{\lambda_\omega}/_{\kappa_\omega^m}$, and by what we showed above $\varrho(g_u) \in C_{i_u}^u$ for $u \in [k] - J_\omega$. The first part of the lemma follows.

To prove the converse statement, let us denote the $\eta_{J_\omega}$-class containing $\tau$ by $D$. Since $\kappa_\omega^m$ and $\omega_+^m$ permute, for any $\kappa_\omega^m$-class $C \subseteq D$ and any $\omega_+^m$-class $C'$, the intersection $C \cap C'$ is nonempty. Therefore, for any $\varphi \in R/_{\kappa_\omega^m}$ such that $\varphi(g_u) = C_{i_u}^u$ for $u \in [k] - J_\omega$, there is $\varrho \in R/_{\omega_-^m}$ such that $\varrho^{\kappa_\omega} = \varphi$ and $\varrho^{\omega_+} = \tau$; that is $\varrho(g) = \varphi(g) \cap \tau(g)$. The lemma is proved. □

We complete this section by presenting a collection of congruences related to $\omega_-, \omega_+$ and satisfying condition (2). Let $A_1, \ldots, A_k$ be the $\kappa_\omega^*$-classes, and let $J_\omega \subseteq [k]$ be the set defined in Lemma 5.5 for $\omega \in M$. Congruences $\gamma_u$, $u \in J_\omega$, are defined as follows: $\langle \mathbf{a}, \mathbf{b} \rangle \in \gamma_u$ if and only if $\langle \mathbf{a}[i], \mathbf{b}[i] \rangle \in \omega_-$ for $i \in A_u \cup \bigcup_{v \in [k] - J_\omega} A_v$, and $\langle \mathbf{a}[i], \mathbf{b}[i] \rangle \in \omega_+$ otherwise. (Here again we treat elements of $R$ as tuples.)

**Lemma 5.6** *Congruences $\gamma_u$, $u \in J_\omega$, satisfy condition (2).*

**Proof:** Again we use notation introduced before Lemma 5.3. Without loss of generality we assume $J_\omega = \{1, \dots, q\}$. First, observe that $\gamma_1 \wedge \dots \wedge \gamma_q = \omega_-^m$. Let $\beta_u = \gamma_u \vee \kappa_\omega^m$, that is, $\langle \mathbf{a}, \mathbf{b} \rangle \in \beta_u$ if and only if $\langle \mathbf{a}[i], \mathbf{b}[i] \rangle \in \kappa_\omega$ for $i \in A_u \cup \bigcup_{v \in [k]-J} A_v$ and $\langle \mathbf{a}[i], \mathbf{b}[i] \rangle \in \lambda_\omega$ otherwise. Let also $\theta = \gamma_1 \vee \dots \vee \gamma_q$. It is not hard to see that $\beta_1 \wedge \dots \wedge \beta_q = \kappa_\omega^m$ and $\beta_i \vee \beta_j = \eta_{J_\omega}$ for any $i, j \in [q]$. Since lattice $\mathsf{Con}(R)$ is modular, intervals $[\omega_-^m, \theta]$ and $[\kappa_\omega^m, \eta_J]$ are isomorphic, where an isomorphism can be defined by $\varphi(x) = x \vee \kappa_\omega^m$, see [37] Cha. IV, Theorem 2. Again by modularity equalities $\theta \vee \kappa_\omega^m = \omega_+^m \vee \kappa_\omega^m = \eta_{J_\omega}$ and $\theta \wedge \kappa_\omega^m = \omega_+^m \wedge \kappa_\omega^m = \omega_-^m$ imply $\theta = \omega_+^m$. Therefore we may consider $\beta_1, \dots, \beta_q$ instead of $\gamma_1, \dots, \gamma_q$, where we also may assume that $\kappa_\omega = \Delta_H$. To simplify the notation we prove condition (2) for $i = 1$.

By Lemma 5.5, $\langle \mathbf{a}, \mathbf{b} \rangle \in \beta_1$ if and only if $\mathrm{pr}_{A_1 \cup A_{q+1} \cup \dots \cup A_k} \mathbf{a} = \mathrm{pr}_{A_1 \cup A_{q+1} \cup \dots \cup A_k} \mathbf{b}$, tuples $\mathrm{pr}_{A_2 \cup \dots \cup A_q} \mathbf{a}$, $\mathrm{pr}_{A_2 \cup \dots \cup A_q} \mathbf{b}$ belong to $\mathrm{pr}_{A_2 \cup \dots \cup A_q} R$, and $\langle \mathbf{a}[g], \mathbf{b}[g] \rangle \in \lambda_\omega$ for $g \in A_2 \cup \dots \cup A_q$. Similarly, $\langle \mathbf{a}, \mathbf{b} \rangle \in \beta_2 \wedge \dots \wedge \beta_q$ if and only if $\mathrm{pr}_{A_1} \mathbf{a}, \mathrm{pr}_{A_1} \mathbf{b} \in \mathrm{pr}_{A_1} R$, $\langle \mathbf{a}[g], \mathbf{b}[g] \rangle \in \lambda_\omega$ for $g \in A_1$, and $\mathrm{pr}_{A_2 \cup \dots \cup A_k} \mathbf{a} = \mathrm{pr}_{A_2 \cup \dots A_k} \mathbf{b} \in \mathrm{pr}_{A_2 \cup \dots \cup A_k} R$. Take $\mathbf{a}, \mathbf{b} \in R$ such that $\langle \mathbf{a}, \mathbf{b} \rangle \in \lambda_\omega^m$ and $\mathbf{a}[g] = \mathbf{b}[g]$ for $g \in A_{q+1} \cup \dots \cup A_k$, and define $\mathbf{c}$ to be the tuple with $\mathbf{c}[g] = \mathbf{a}[g]$ for $g \in A_1$ and $\mathbf{c}[g] = \mathbf{b}[g]$ for $g \in A_2 \cup \dots \cup A_k$. By Lemma 5.5, $\mathbf{c} \in R$ and $\langle \mathbf{a}, \mathbf{c} \rangle \in \beta_1$, $\langle \mathbf{c}, \mathbf{b} \rangle \in \beta_2 \wedge \dots \wedge \beta_q$. Thus $\langle \mathbf{c}, \mathbf{b} \rangle \in \beta_1 \vee (\beta_2 \wedge \dots \wedge \beta_q)$. □

# 6 Algorithm: computing the number of solutions

In this section we use the results proved in the previous sections to design an algorithm solving counting CSPs for congruence singular structures.

Suppose that $\mathcal{H}$ is congruence singular. Let $\mathcal{G}$ be an instance of $\#\mathrm{CSP}(\mathcal{H})$; assume that the universe $G$ of $\mathcal{G}$ is $[m]$. As before $M = \{1, \dots, \ell\}$ is the set of prime quotients of a maximal chain in the lattice $\mathsf{Con}(\mathcal{H})/_{\overset{s}{\sim}}$. If $\ell_+ \neq \bigtriangledown_H$ or $1_- \neq \Delta_H$ then we add extra elements $(\ell+1)_-$ or $0_+$ to the set of congruences $\omega_-, \omega_+, \omega \in M$, see Fig 13. Otherwise we assume $(\ell+1)_- = \ell_+$ and $0_+ = 1_-$, respectively. In $\mathsf{Con}(\mathcal{H})$ the chain corresponds to a number of prime quotients of the form $\omega_- \prec \omega_+$ that have the Boolean type, and intervals $[\omega_+, (\omega+1)_-]$ such that every prime quotient from this interval has the affine type, see Fig. 13.

A mapping $\tau\colon \mathcal{G} \to \mathcal{H}/_\theta$ for $\theta \in \mathsf{Con}(\mathcal{H})$ will be called a *mapping of level* $\theta$. Recall that for a mapping $\tau$ of level $\theta$, by $\Phi(\mathcal{G}, \mathcal{H}; \tau)$ we denote the set of all homomorphisms $\varrho \in \Phi(\mathcal{G}, \mathcal{H})$ with $\varrho^\theta = \tau$. The overall idea of the algorithm is to compute recursively numbers of the form $|\Phi(\mathcal{G}, \mathcal{H}; \tau)|$ for instance $\mathcal{G}$ and mappings $\tau$ of level $\omega_-$ or $\omega_+$, $\omega \in M$. If $\tau$ is a mapping of level $(\ell+1)_-$ then $|\Phi(\mathcal{G}, \mathcal{H}, \tau)| = |\Phi(\mathcal{G}, \mathcal{H})|$, and if $\tau$ is a mapping of level $0_+$ then $|\Phi(\mathcal{G}, \mathcal{H}, \tau)| = 1$. For $\omega \in M$ and a mapping $\tau$ from $\mathcal{G}$ to $\mathcal{H}/_{\omega_+}$ or to $\mathcal{H}/_{\omega_-}$, we show how to reduce computing the number $|\Phi(\mathcal{G}, \mathcal{H}, \tau)|$ to computing numbers $|\Phi(\mathcal{G}, \mathcal{H}, \varrho)|$ for certain $\varrho$, mappings from $\mathcal{G}$ to $\mathcal{H}/_{\omega_-}$ or to $\mathcal{H}/_{(\omega-1)_+}$, respectively. The two cases, $\tau\colon \mathcal{G} \to \mathcal{H}/_{\omega_+}$ and $\tau\colon \mathcal{G} \to \mathcal{H}/_{\omega_-}$ will be considered in the next two subsections.

## 6.1 Prime quotients of the Boolean type

Let $A_1, \dots, A_k$ be the $\kappa_\omega^*$-classes and $g_1, \dots, g_k$ their representatives. Let $\tau$ be a mapping from $\Phi(\mathcal{G}, \mathcal{H})/_{\omega_+^m}$, that is $\tau(g)$ is a $\omega_+$-class for $g \in \mathcal{G}$. By $J_\omega$ we denote the subset of $[k]$ identified in Lemma 5.5. Without loss of generality we assume $J_\omega = [q]$. Let $C_u^1, \dots, C_{s_u}^u$ be the $\kappa_\omega$-classes from $\tau(g_u)^{\lambda_\omega}$, the $\lambda_\omega$-class containing elements from $\tau(g_u)$, for $u \in [k]$. Recall that by definition $g \in A_u$ if and only if for any $\varrho, \varrho' \in \Phi(\mathcal{G}, \mathcal{H})$ if $\langle \varrho(g_u), \varrho'(g_u) \rangle \in \kappa_\omega$ then $\langle \varrho(g), \varrho'(g) \rangle \in \kappa_\omega$ and vice versa. Therefore, for any $g \in A_u$, $u \in [k]$, and for any $\varrho \in \Phi(\mathcal{G}, \mathcal{H}; \tau)$ the value $\varrho(g)^{\omega_-}$ is determined by $\varrho(g_u)^{\omega_-}$, and that $\varrho(g)^{\omega_-} = \varrho(g)^{\kappa_\omega} \cap \tau(g)$. In other words, there is a one-to-one mapping $\varphi_g$ from the set $\{C_u^1, \dots, C_{s_u}^u\}$ to the set of $\kappa_\omega$-classes of $\tau(g)^{\lambda_\omega}$ such

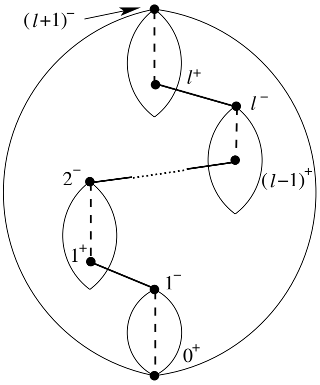

Figure 13: The congruence lattice of $\mathcal{H}$, a maximal chain in $\mathsf{Con}(\mathcal{H})/\overset{s}{\sim}$, the corresponding prime quotients, and $\overset{s}{\sim}$-classes. Prime quotients $\omega_- \prec \omega_+$ are shown by solid lines, $\overset{s}{\sim}$-classes by ovals, dashed lines represent chains of the affine type (not to be mistaken with the dotted line).

that $\varrho(g)^{\omega_-} = \varphi_g(\varrho(g_u)^{\kappa_\omega}) \cap \tau(g)$. Let $i_u$, $u \in [k] - J_\omega$ and $i_u \in [s_u]$, be the $\kappa_\omega$-classes corresponding to $\tau$ as in Lemma 5.5.

**Proposition 6.1** *(1) For any $q$-tuple $\mathbf{r}$ such that $\mathbf{r}[u] \in [s_u]$, the mapping $\varrho_\mathbf{r}\colon \mathcal{G} \to \mathcal{H}/_{\omega_-}$, where for each $u \in [k]$*

$$\varrho_\mathbf{r}(g_u) = \begin{cases} C^u_{\mathbf{r}[u]} \cap \tau(g_u), & \text{if } u \in J_\omega \\ C^u_{i_u} \cap \tau(g_u), & \text{otherwise}, \end{cases}$$

*and for each $g \in A_u$, $u \in [q]$, $\varrho_\mathbf{r}(g)^{\omega_-} = \varphi_g(\varrho_\mathbf{r}(g_u)^{\kappa_\omega}) \cap \tau(g)$, belongs to $R/_{(\omega_-)^m}$.*

*(2) $|\Phi(\mathcal{G},\mathcal{H},\tau)| = \sum_\mathbf{r} |\Phi(\mathcal{G},\mathcal{H},\varrho_\mathbf{r})|$.*

*(3) Sets $\Phi(\mathcal{G},\mathcal{H},\varrho_\mathbf{r})$ are the classes of congruence $(\omega_-)^m$ of the relation $\Phi(\mathcal{G},\mathcal{H},\tau)$.*

**Proof:** (1) follows straightforwardly from Lemma 5.5.

(2) Every homomorphism $\varrho$ from $\Phi(\mathcal{G},\mathcal{H};\tau)$ belongs to a certain set $\Phi(\mathcal{G},\mathcal{H},\varrho_\mathbf{r})$, namely, the one with $\mathbf{r}[u] = j_u$ where $\varrho(g_u) \in C^u_{j_u}$ for $u \in [q]$. On the other hand all sets of this form are disjoint.

(3) Since $\kappa_\omega \wedge \omega_+ = \omega_-$, all elements from $\Phi(\mathcal{G},\mathcal{H},\varrho_\mathbf{r})$ are $(\omega_-)^m$-related. If $\varrho \in \Phi(\mathcal{G},\mathcal{H},\varrho_\mathbf{r})$ and $\varrho' \in \Phi(\mathcal{G},\mathcal{H},\varrho_{\mathbf{r}'})$ where $\mathbf{r}[u] \neq \mathbf{r}'[u]$ then $\langle \varrho(g_u), \varrho'(g_u)\rangle \notin \omega_-$, and therefore $\langle \varrho, \varrho'\rangle \notin (\omega_-)^m$. □

We use the congruences $\gamma_1, \ldots, \gamma_q$ introduced in Section 5.3: $\langle \varrho, \varrho'\rangle \in \gamma_u$ if and only if $\langle \varrho(g), \varrho'(g)\rangle \in \omega_-$ if $g \in A_u$ or $g \in A_{q+1} \cup \ldots \cup A_k$, and $\langle \varrho(g), \varrho'(g)\rangle \in \omega_+$ otherwise. By Lemma 5.6 congruences $\gamma_1, \ldots, \gamma_q$ satisfy condition (2), and $(\omega_-)^m = \gamma_1 \wedge \ldots \wedge \gamma_q$.

Recall that $\tau$ can be treated as a $\omega_+^m$-class and that $M(\tau, \gamma_1, \ldots, \gamma_q)$ denotes the $q$-dimensional $s_1 \times \ldots \times s_q$-array such that its entry indexed by $\mathbf{r}$ is equal to $|\Phi(\mathcal{G},\mathcal{H},\varrho_\mathbf{r})|$. By Proposition 4.6, $M(\tau, \gamma_1, \ldots, \gamma_q)$ has rank 1, that is, there are numbers $t^u_1, \ldots, t^u_{s_u}$, for $u \in [q]$, such that

$$|\Phi(\mathcal{G},\mathcal{H},\varrho_\mathbf{r})| = t^1_{\mathbf{r}[1]} \cdot \ldots \cdot t^q_{\mathbf{r}[q]}.$$

If numbers $t^i_j$ are known, we have

$$\begin{aligned}\Phi(\mathcal{G},\mathcal{H},\tau) = \sum_{\mathbf{r}} \Phi(\mathcal{G},\mathcal{H},\varrho_{\mathbf{r}}) &= \sum_{\mathbf{r}} t^1_{\mathbf{r}[1]} \cdot \ldots \cdot t^q_{\mathbf{r}[q]} \\ &= t^1_1 \left( \sum_{\mathbf{r}[2],\ldots,\mathbf{r}[q]} t^2_{\mathbf{r}[2]} \cdot \ldots \cdot t^q_{\mathbf{r}[q]} \right) + \ldots + t^1_{s_1} \left( \sum_{\mathbf{r}[2],\ldots,\mathbf{r}[q]} t^2_{\mathbf{r}[2]} \cdot \ldots \cdot t^q_{\mathbf{r}[q]} \right) \\ &= \ldots = \prod_{j=1}^{q} \sum_{i=1}^{s_j} t^j_i,\end{aligned}$$

that can be computed easily.

To find the numbers $t^i_j$ we use the approach from the proof of Lemma 4.5. Fix a tuple $\mathbf{r}$, say, $\mathbf{r} = (1,\ldots,1)$. By $\mathbf{r}^i_j$ we denote the tuple, all entries of which are equal to the corresponding entries of $\mathbf{r}$, except for the $i$-th entry that is equal to $j$. Then set

$$t^1_j = |\Phi(\mathcal{G},\mathcal{H},\varrho_{\mathbf{r}^1_j})| \quad \text{and} \quad t^i_j = \frac{|\Phi(\mathcal{G},\mathcal{H},\varrho_{\mathbf{r}^i_j})|}{|\Phi(\mathcal{G},\mathcal{H},\varrho_{\mathbf{r}})|} \qquad \text{for } i \in \{2,\ldots,q\}.$$

Thus, we have reduced computing the number $|\Phi(\mathcal{G},\mathcal{H},\tau)|$, mapping $\tau$ is of level $\omega_+$, to computing numbers of the form $|\Phi(\mathcal{G},\mathcal{H},\varrho_{\mathbf{r}^i_j})|$, where $\varrho_{\mathbf{r}^i_j}$ is of level $\omega_-$.

### 6.2 Quotients of the affine type

Let $\tau \in \Phi(\mathcal{G},\mathcal{H})/_{(\omega+1)^m_-}$ for some $\omega \in M - \{\ell\}$. Congruence $(\omega+1)_-$ is solvable over $\omega_+$, and we make use of the following implication of Proposition 4.1.

**Corollary 6.2** *(1) Let $\varrho_1, \varrho_2 \in \Phi(\mathcal{G},\mathcal{H},\tau)/_{\omega^m_+}$. Then $|\Phi(\mathcal{G},\mathcal{H},\varrho_1)| = |\Phi(\mathcal{G},\mathcal{H},\varrho_2)|$.*

*(2) For any $\varrho \in \Phi(\mathcal{G},\mathcal{H},\tau)/_{\omega^m_+}$,*

$$|\Phi(\mathcal{G},\mathcal{H},\tau)| = |\Phi(\mathcal{G},\mathcal{H},\varrho)| \cdot |\Phi(\mathcal{G},\mathcal{H},\tau)/_{\omega^m_+}|.$$

Thus, to reduce computing $|\Phi(\mathcal{G},\mathcal{H},\tau)|$, where $\tau$ is of level $(\omega+1)_-$, to computing $|\Phi(\mathcal{G},\mathcal{H},\varrho)|$, where $\varrho$ is of level $\omega_+$, it suffices to find the number $|\Phi(\mathcal{G},\mathcal{H},\varrho)/_{\omega^m_+}|$.

We consider first the case when $\omega_+$ is the equality relation, that is $\omega = 0$. In this case the required number can be found using the signature $\mathsf{Sig}_R$ of the relation $R = \Phi(\mathcal{G},\mathcal{H},\tau)$ in a very simple way through the following lemma. Observe that it does not apply to the case when $1_- = \Delta_H$.

**Lemma 6.3** *Let $\mathsf{Sig}_R$ be the signature of $\Phi(\mathcal{G},\mathcal{H},\tau)$, and $\alpha_g$ be the relation $\{\langle a,b\rangle \mid (g,a,b) \in \mathsf{Sig}_R\}$. Then*

*(1) $\alpha_g$ is a congruence of $\tau(g)$;*

*(2) all $\alpha_g$ classes have the same cardinality, denoted by $v_g$;*

*(3) $|\Phi(\mathcal{G},\mathcal{H},\tau)| = v_1 \cdot \ldots \cdot v_m$.*

**Proof:** (1) Relation $\alpha_g$ is pp-definable in $\mathcal{H}$ as the following formula shows

$$\begin{aligned}\alpha_g(x,y) \quad = \quad & \exists z_1,\dots,z_{g-1},z_{g+1},\dots,z_m,u_{g+1},\dots,u_m \\ & (R(z_1,\dots,z_{g-1},x,z_{g+1},\dots,z_m) \wedge R(z_1,\dots,z_{g-1},y,u_{g+1},\dots,u_m)).\end{aligned}$$

Due to rectangularity of $R$ this relation is an equivalence relation.

(2) follows straightforwardly from Proposition 4.1, as $\alpha_g \le \omega_-$, and so $\omega_- \overset{s}{\sim} \alpha_g$.

(3) As every element of $\mathrm{pr}_{[m-1]}\Phi(\mathcal{G},\mathcal{H},\tau)$ can be extended to an element of $\Phi(\mathcal{G},\mathcal{H},\tau)$ by any member of a certain $\alpha_m$-class, the number of such extensions equals $v_m$, and we have

$$|\Phi(\mathcal{G},\mathcal{H},\tau)| = |\mathrm{pr}_{[m-1]}\Phi(\mathcal{G},\mathcal{H},\tau)| \cdot v_m.$$

Continuing this way we get $|\Phi(\mathcal{G},\mathcal{H},\tau)| = v_1 \cdot \ldots \cdot v_m$. □

To find the signature of $\Phi(\mathcal{G},\mathcal{H},\tau)$ we can use algorithm MAL'TSEV applied to the instance modified in the following way. We shall assume that for each subalgebra $B$ of $\mathcal{H}$ the vocabulary of $\mathcal{H}$ contains a unary relational symbol $R_B$ such that $R_B^{\mathcal{H}} = B$. Let $g_1,\dots,g_k \in \mathcal{G}$, and let $B_1,\dots,B_k$ be subalgebras of $\mathcal{H}$. By $\mathcal{G} \cup \{\langle g_1,B_1\rangle,\dots,\langle g_k,B_k\rangle\}$ we denote the relational structure with the same universe as $\mathcal{G}$, and such that the interpretation of every relational symbol $R \notin \{R_{B_1},\dots,R_{B_k}\}$ equals $R^{\mathcal{G}}$ while the interpretation of $R_B$ equals $R_B^{\mathcal{G}} \cup \{g_i \mid B_i = B\}$. Thus, the elements $g_1,\dots,g_k$ are forced to be mapped to $B_1,\dots,B_k$ respectively. It is not hard to check that $\Phi(\mathcal{G},\mathcal{H},\tau)$ is the set of solutions for the instance $\mathcal{G} \cup \{\langle g,\tau(g)\rangle \mid g \in [m]\}$.

Observe that if we know the signature of relation $\Phi(\mathcal{G},\mathcal{H},\tau)/_{\omega_+^m}$, which is a relation over $\mathcal{H}/_{\omega_+}$, we still can use Lemma 6.3 to find the cardinality of $|\Phi(\mathcal{G},\mathcal{H},\tau)/_{\omega_+^m}|$. In order to do that we just have to replace $\mathcal{H}$ with $\mathcal{H}/_{\omega_+}$. Therefore the problem we are facing now is how to find the signature of this relation. Unfortunately, it is not clear at all how to obtain this signature using the signature or a compact representation of $\Phi(\mathcal{G},\mathcal{H},\tau)$, nor we can use algorithm MAL'TSEV to compute the signature of $\Phi(\mathcal{G},\mathcal{H}/_{\omega_+},\tau)$, since in general $\Phi(\mathcal{G},\mathcal{H}/_{\omega_+},\tau) \neq \Phi(\mathcal{G},\mathcal{H},\tau)/_{\omega_+^m}$. Instead, to compute each member of the required signature we find a compact representation of a certain modified problem using algorithm MAL'TSEV.

More specifically, we first find the *$\omega_+$-signature* of the relation $\Phi(\mathcal{G},\mathcal{H},\tau)$. Let $n$ be a positive integer, let $H$ be a finite set, let $\theta$ be an equivalence relation on $H$, let $\mathbf{a}$, $\mathbf{b}$ be $n$-tuples, and let $(i,a,b)$ be any element in $[n]\times H^2$. We say that $\langle \mathbf{a},\mathbf{b}\rangle$ *$\theta$-witnesses* $(i,a,b)$ if $(\mathbf{a}[j],\mathbf{b}[j]) \in \theta$ for each $j<i$, $\mathbf{a}[i]=a$, and $\mathbf{b}[i]=b$. Let $R$ be an $n$-ary relation on $H$. The *$\theta$-signature* of $R$, $\theta\mathsf{Sig}_R \subseteq [n]\times H^2$, is defined to be the set containing all those $(i,a,b) \in [n]\times H^2$ $\theta$-witnessed by tuples in $R$, that is

$$\theta\mathsf{Sig}_R = \{(i,a,b) \in [n]\times H^2 \mid \text{ there are } \mathbf{a},\mathbf{b} \in R \text{ such that } \langle \mathbf{a},\mathbf{b}\rangle\ \theta\text{-witnesses } (i,a,b)\}.$$

**Lemma 6.4** *Let $\tau \in \Phi(\mathcal{G},\mathcal{H})/_{(\omega+1)_-^m}$.*

*(1) Algorithm $\omega$-SIGNATURE (see Fig. 14) finds the $\omega_+$-signature $\omega_+\mathsf{Sig}_R$ of $R = \Phi(\mathcal{G},\mathcal{H},\tau)$.*

*(2) The signature of $\Phi(\mathcal{G},\mathcal{H},\pi)/_{\omega_+^m}$ can then be found by replacing each $(g,a,b) \in \omega_+\mathsf{Sig}_R$ by $(g,a^{\omega_+},b^{\omega_+})$*

**Proof:** (1) For any $g \in [m]$, a triple $(g,a,b)$ is added to $S$ only if there are $\varrho,\varrho' \in \Phi(\mathcal{G},\mathcal{H},\tau)$ such that $\varrho(g)=a$, $\varrho'(g)=b$, and $\langle\varrho(h),\varrho'(h)\rangle \in \omega_+$ for every $h<g$. Therefore, $S \subseteq \omega_+\mathsf{Sig}_R$. If $(g,a,b) \in \omega_+\mathsf{Sig}_R$ then $a \in \mathrm{pr}_g R$. Hence there is $\varrho \in R'$ such that $\varrho(g)=a$. Suppose that $\langle \varrho',\varrho''\rangle$

```
Algorithm $\omega$-Signature
INPUT: an instance $\mathcal{G}$ of $\#\mathrm{CSP}(\mathcal{H})$, $\omega \in M$, and $\tau \in \Phi(\mathcal{G},\mathcal{H})/_{(\omega+1)^m_-}$
OUTPUT: a $\omega_+$-signature of $\Phi(\mathcal{G},\mathcal{H},\tau)$
Step 1      find a compact representation $R'$ of $\Phi(\mathcal{G},\mathcal{H},\tau)$ using MAL'TSEV
Step 2      set $S := \varnothing$ (the $\omega_+$-signature of $\Phi(\mathcal{G},\mathcal{H},\tau)$)
Step 3      for each $(g,a,b) \in [m] \times H^2$ do
Step 3.1        if there is $\varrho \in R'$ such that $\varrho(g) = a$ then do
Step 3.1.1          find a compact representation $R''$ of $\Phi(\mathcal{G}',\mathcal{H},\tau)$ where
                $\mathcal{G}' = \mathcal{G} \cup \{\langle 1, \varrho(1)^{\omega+}\rangle, \ldots, \langle g-1, \varrho(g-1)^{\omega+}\rangle\}$
Step 3.1.2          if $b \in \mathrm{pr}_g R''$ then $S := S \cup \{(g,a,b)\}$
                endif
            endfor
Step 5      return $S$
```

Figure 14:

```
Algorithm Counting
INPUT: an instance $\mathcal{G}$ of $\#\mathrm{CSP}(\mathcal{H})$ such that $\Phi(\mathcal{G},\mathcal{H})$ is a subdirect power of $\mathcal{H}$
OUTPUT: the number of homomorphisms from $\mathcal{G}$ to $\mathcal{H}$, i.e. $|\Phi(\mathcal{G},\mathcal{H})|$
Step 1      let $\tau$ be a (unique) mapping from $\mathcal{G}$ to $\mathcal{H}/_{\bigtriangledown_H}$;
            return Counting-mapping($\mathcal{G}, (\ell+1)_-, \tau$)
```

Figure 15:

$\omega_+$-witnesses the triple $(g,a,b)$. We have to show that there is $\varrho'''$ such that the pair $\langle \varrho, \varrho'''\rangle$ $\omega_+$-witnesses $(g,a,b)$. It is straightforward that $\varrho'''$ can be chosen to be $m(\varrho,\varrho',\varrho'')$, where $m$ is a Mal'tsev polymorphism of $\mathcal{H}$.

(2) By the definition, $(g,a',b')$ belongs to the signature of $\Phi(\mathcal{G},\mathcal{H},\tau)/_{\omega_+^m}$ if and only if there are $\varrho,\varrho' \in \Phi(\mathcal{G},\mathcal{H},\tau)$ such that $\varrho(g)^{\omega+} = a'$, $\varrho'(g)^{\omega+} = b'$, and $\langle \varrho(h), \varrho'(h)\rangle \in \omega_+$ for all $h < g$. These conditions mean that the pair $\langle \varrho, \varrho'\rangle$ $\omega_+$-witnesses that $(g, \varrho(g), \varrho'(g)) \in \omega_+\mathsf{Sig}R$. □

## 6.3 The algorithm

We summarize results of the previous two subsections and present an algorithm solving $\#\mathrm{CSP}(\mathcal{H})$ for a congruence singular structure $\mathcal{H}$, see Fig. 15, 16. The first of the presented algorithms just initiates a recursive process, while the second one implements the method discussed in the two previous subsections. We assume that all information about $\mathcal{H}$ required for the algorithm is known. This includes, for instance, congruences, types of prime quotients, subalgebras generated by certain sets, etc. As usual, $M$ denotes the set of prime quotients of a maximal chain in $\mathsf{Con}(\mathcal{H})/_{\overset{s}{\sim}}$.

**Comments on the algorithm** Classes of $\kappa^*_\omega$ can be computed on Step 2.1 by exploring a compact representation $Q$ of $\Phi(\mathcal{G},\mathcal{H})$; such representation can be found by means of the algorithm MAL'TSEV. Equivalence relation $\kappa^*_\omega$ is defined by binary projections of $\Phi(\mathcal{G},\mathcal{H})$, that are relations generated by $\mathrm{pr}_{g,h}Q$ for $g,h \in [m]$. Set $J_\omega$ contains those $\kappa^*_\omega$-classes $A_u$, for which projection $\mathrm{pr}_{g_u}\Phi(\mathcal{G},\mathcal{H},\tau)$ equals $\tau(g_u)$. Again, one can find a compact representation of $\Phi(\mathcal{G},\mathcal{H},\tau)$ by applying algorithm MAL'TSEV to the problem $\mathcal{G} \cup \{\langle g, \tau(g)\rangle \mid g \in [m]\}$. Finally, to find a solution $\varrho \in \Phi(\mathcal{G},\mathcal{H},\tau)/_{\omega^*_+}$ on Step 3.1 it suffices to compute a compact representation of $\Phi(\mathcal{G},\mathcal{H},\tau)$ in the same way as before, and then for any member of the representation find the corresponding quotient mapping.

**Complexity** Observe that the depth of recursion of the algorithm is at most $2\ell$ and does not depend on the input. On each step considering a prime quotient of the Boolean case the problem of finding the number $|\Phi(\mathcal{G},\mathcal{H},\tau)|$ reduces to finding $s_1 + \ldots + s_k$ numbers of the form $|\Phi(\mathcal{G},\mathcal{H},\varrho)|$, where $\varrho\colon \mathcal{G} \to \mathcal{H}/_{\omega_-}$. Since $k \le m$ and each $s_u$ does not exceed $|\mathcal{H}|$, every step of this kind requires solving at most $|\mathcal{H}|m$ smaller problems. On each step considering an interval of the affine type computing $|\Phi(\mathcal{G},\mathcal{H},\tau)|$ reduces to solving a problem of the form $|\Phi(\mathcal{G},\mathcal{H},\varrho)|$, $\varrho\colon \mathcal{G} \to \mathcal{H}/_{\omega_+}$ and finding the $\omega_+$-signature of $\Phi(\mathcal{G},\mathcal{H},\tau)$. To find the $\omega_+$-signature the algorithm runs MAL'TSEV at most $m \cdot |\mathcal{H}|^2$ times. If the time complexity of algorithm MAL'TSEV is $p(m)$, then the overall time complexity of our algorithm is $(|\mathcal{H}|^3 m^2 \cdot p(m))^\ell$.

## 7 #$H$-COLORING

Theorem 2.22 provides a complete classification of #P-complete and polynomial time solvable #$H$-COLORING problems. However, it is difficult to express the criterion stated in the theorem in terms of (di)graphs. By [29], an (undirected) graph $H$ gives rise to a polynomial time solvable #$H$-COLORING problem if and only if every connected component of $H$ is either trivial, or a complete bipartite graph, or a complete graph with loops at all vertices. In [13], we observed that an undirected graph satisfies this condition if and only if it is invariant under a Mal'tsev operation.

In this section we compare the classification result from [32, 28] for directed acyclic graphs (DAGs for short) with Theorem 2.22. We show that every congruence singular DAG satisfies the *Lovász-goodness* condition introduced in [32, 28]. The two conditions must be equivalent, however, the converse implication probably uses some nontrivial properties of pp-definitions in DAGs and remains an open problem. Note that similar difficulties arise when we try to translate other general results on constraint satisfaction problems for (di)graphs.

A DAG $H = (V, E)$ is called *layered* if $V$ can be partitioned into subsets $V_1, \ldots, V_\ell$ such that for any $(v, w) \in E$ we have $v \in V_i$, $w \in V_{i+1}$ for a certain $i < \ell$. Let $v \in V_i$, $w \in V_j$, $i < j$. Then $H_{v*}$ denotes the subgraph of $H$ induced by the vertices $u$ such that there is a directed path from $v$ to $u$; similarly, $H_{*w}$ denotes the subgraph of $H$ induced by the vertices $u$ such that there is a directed path from $u$ to $w$; and $H_{vw} = H_{v*} \cap H_{*w}$. The vertex set of the graph $H_{xy}H_{x'y'}$, where $H_{xy} = (V', E')$ and $H_{x'y'} = (V'', E'')$, is the set $((V' \cap V_i) \times (V'' \cap V_i)) \cup \ldots \cup ((V' \cap V_j) \times (V'' \cap V_j))$, a pair $((v, v'), (w, w'))$ is an edge if and only if $(v, w) \in E'$ and $(v', w') \in E''$. It is proved in [28] that $H_{xy}H_{x'y'}$ for $x, x' \in V_i$ and $y, y' \in V_j$ has only one connected component that spans all layers from $i$ to $j$. If such main connected components of graphs $H_{xy}H_{x'y'}$ and $H_{zt}H_{z't'}$, $z, z' \in V_i$, $t, t' \in V_j$, are isomorphic then we write $H_{xy}H_{x'y'} \equiv H_{zt}H_{z't'}$. Finally a layered graph is said to be *Lovász-good* if for any $i, j$, $1 \le i < j \le \ell$, and any $x, x' \in V_i$, $y, y' \in V_j$ we have $H_{xy}H_{x'y'} \equiv H_{xy'}H_{x'y}$.

The key lemma for this result is a special case of the result of [52] that we state in our notation.

**Lemma 7.1** *If $|\Phi(G, H_1)| = |\Phi(G, H_2)|$ for all graphs $G$ then graphs $H_1, H_2$ are isomorphic.*

We show that if $H$ is congruence singular then $|\Phi(G, H_{xy}H_{x'y'})| = |\Phi(G, H_{xy'}H_{x'y})|$ for any $x, x' \in V_i$, $y, y' \in V_j$, where $1 \leq i < j \leq \ell$, and any graph $G$. This implies that $H_{xy}H_{x'y'}$ and $H_{xy'}H_{x'y}$ are isomorphic, and so $H_{xy}H_{x'y'} \equiv H_{xy'}H_{x'y}$. We use an observation made in [28] that $|\Phi(G, H_1H_2)| = |\Phi(G, H_1)| \cdot |\Phi(G, H_2)|$. If $G = (W, F)$ is not layered then $|\Phi(G, H_{xy}H_{x'y'})| = |\Phi(G, H_{xy'}H_{x'y})| = 0$. Let $W_1, W_2$ denote the set of vertices on the highest and on the lowest layers of $G$, respectively. As we know, $\Phi(G, H)$ is a relation pp-definable in $H$. Now, let $\eta_1, \eta_2$ be congruences of $\Phi(G, H)$ such that $\langle \varphi, \varphi' \rangle \in \eta_i$, $i = 1, 2$, iff $\varphi(v) = \varphi'(v)$ for all $v \in W_i$. It is not hard to see that sets of the form $H_{u*}$ are classes of $\eta_1$, sets of the form $H_{*w}$ are classes of $\eta_2$, and sets of the form $H_{uw}$ are classes of $\eta_1 \wedge \eta_2$ (although there are classes of those congruences not representable in the form $H_{u*}$, $H_{*w}$, or $H_{uw}$). Since $H$ is congruence singular, we have $\mathsf{rank}(M(\eta_1, \eta_2)) = k$ where $k$ is the number of classes in $\eta_1 \vee \eta_2$. Hence

$$\begin{vmatrix} |\Phi(G, H_{xy})| & |\Phi(G, H_{xy'})| \\ |\Phi(G, H_{x'y})| & |\Phi(G, H_{x'y'})| \end{vmatrix} = 0,$$

or $\Phi(G, H_{xy}), \Phi(G, H_{x'y'})$ or $\Phi(G, H_{xy'}), \Phi(G, H_{x'y})$ are in different classes of $\eta_1 \vee \eta_2$. In the latter case either $|\Phi(G, H_{x'y})| = |\Phi(G, H_{xy'})| = 0$ or $|\Phi(G, H_{xy})| = |\Phi(G, H_{x'y'})| = 0$. The result follows.

Observe that in this argument congruence singularity is used in a very restricted way: only projection congruences of somewhat restricted type are used.

## 8 Concluding remarks and open problems

The result obtained in the paper is rather general. It includes as particular case the results of [19, 29, 21, 32, 28, 48]. However, those results are stated in terms of particular problems, and deriving them from Theorem 2.22 requires extra research.

**Problem 2** *Characterize congruence singular digraphs.*

We also should note that in some cases, e.g., [29], the #P-completeness results obtained for particular problems are stronger than those which follow from our result. For instance, #P-complete #$H$-COLORING problems in the case of undirected graphs remain #P-complete even when restricted to inputs of bounded degree.

**Problem 3** *Let $\mathcal{H}$ be a relational structure that is not congruence singular. Does the problem $\#\mathrm{CSP}(\mathcal{H})$ remains #P-complete when restricted to the class of structures of bounded degree? a class of structures with other natural restrictions?*

A major question left unanswered is how to check if a given relational structure is congruence singular. This problem may turn out to be even undecidable.

**Problem 4** *Give an algorithm for or prove that the following computational problem is undecidable: Given a relational structure check whether or not it is congruence singular.*

## References

[1] L. Barto, M. Kozik and T. Niven. Graphs, polymorphisms and the complexity of homomorphism problems. In *STOC*. 789–796. 2008.

[2] V. Bodnarchuk, L. Kaluzhnin, V. Kotov and B. Romov. Galois theory for post algebras. I. *Kibernetika 3*, 1–10. 1969.

[3] G. Brightwell and P. Winkler. Graph homomorphisms and phase transitions. *Journal of Combinatorial Theory, Ser. B 77*, 221–262. 1999.

[4] R. Bubley, M. E. Dyer, C. Greenhill and M. Jerrum. On approximately counting colourings of small degree graphs. *SIAM Journal of Computing 29*, 387–400. 1999.

[5] A. A. Bulatov. A dichotomy theorem for constraints on a three-element set. In *FOCS*. IEEE Computer Society, Vancouver, Canada, 649–658. 2002.

[6] A. A. Bulatov. Mal'tsev constraints are tractable. Tech. Rep. PRG-RR-02-05, Computing Laboratory, University of Oxford, Oxford, UK. 2002.

[7] A. A. Bulatov. Tractable conservative constraint satisfaction problems. In *LICS*. 321–330. 2003.

[8] A. A. Bulatov and M. Grohe. The complexity of partition functions. In *ICALP*. 294–306. 2004.

[9] A. A. Bulatov and P. Jeavons. Algebraic approach to multi-sorted constraints. Tech. Rep. PRG-RR-01-18, Computing Laboratory, University of Oxford, Oxford, UK. 2001.

[10] A. A. Bulatov and P. Jeavons. An algebraic approach to multi-sorted constraits. In *CP*. 197–202. 2003.

[11] A. A. Bulatov. Three-element Mal'tsev algebras. *Acta Sci. Math. (Szeged) 72*, 519–550. 2006.

[12] A. A. Bulatov and V. Dalmau. A simple algorithm for Mal'tsev constraints. *SIAM J. Comput. 36,* 1, 16–27. 2006.

[13] A. A. Bulatov and V. Dalmau. Towards a dichotomy theorem for the counting constraint satisfaction problem. *Information and Computation 205,* 5, 651–678. 2007.

[14] A. A. Bulatov and M. Grohe. The complexity of partition functions. *Theoretical Computer Science 348,* 2-3, 148–186. 2005.

[15] A. A. Bulatov, P. Jeavons and A. A. Krokhin. Classifying the complexity of constraints using finite algebras. *SIAM Journal on Computing 34,* 3, 720–742. 2005.

[16] S. Burris and H. Sankappanavar. *A course in universal algebra*. Graduate Texts in Mathematics, vol. 78. Springer-Verlag, New York-Berlin. 1981.

[17] R. Burton and J. Steif. Nonuniqueness of measures of maximal entropy for subshifts of finite type. *Ergodic Theory and Dynamical Systems 14*, 213–236. 1994.

[18] J. Cai, P. Lu and M. Xia. Holographic algorithms by Fibonacci gates and holographic reductions for hardness. In *FOCS*. 644–653. 2008.

[19] N. Creignou and M. Hermann. Complexity of generalized satisfiability counting problems. *Information and Computation 125,* 1, 1–12. 1996.

[20] N. Creignou, S. Khanna and M. Sudan. *Complexity Classifications of Boolean Constraint Satisfaction Problems*. SIAM Monographs on Discrete Mathematics and Applications, vol. 7. 2001.

[21] J. Diaz, M. Serna and D. Thilikos. Counting list $H$-colorings and variants. Tech. Rep. LSI-01-27-R, Departament LSI, Universitat Politècnica de Catalunya. 2001.

[22] J. Diaz, M. Serna and D. Thilikos. Counting $H$-colorings of partial $k$-trees. *Theoretical Computer Science 281*, 291–309. 2002.

[23] J. Diaz, M. Serna and D. Thilikos. *DIMACS/DIMATIA Workshop on Graphs, Morphism and Statistical Physics*. DIMACS Series in Discrete Mathematics and Theoretical Computer Science Chapter. Recent results on parameterized $H$-coloring. American Mathematical Society. 2004.

[24] J. Diaz, M. Serna and D. Thilikos. The restrictive $H$-coloring. *Discrete Applied Mathematics 145*, 2, 297–305. 2005.

[25] Q. Donner. On the number of list $H$-colorings. *J. Graph Theory 16*, 3, 239–245.

[26] M. E. Dyer, A. Frieze and M. Jerrum. 2002. On counting independent sets in sparse graphs. *SIAM Journal on Computing 31*, 1527–1541. 1992.

[27] M. E. Dyer, L. A. Goldberg, C. Greenhill and M. Jerrum. On the relative complexity of approximate counting problems. In *APPROX*. LNCS, vol. 1913. Springer-Verlag, 108–119. 2000.

[28] M. E. Dyer, L. A. Goldberg and M. Paterson. On counting homomorphisms to directed acyclic graphs. In *ICALP*. 38–49. 2006.

[29] M. E. Dyer and C. Greenhill. The complexity of counting graph homomorphisms. *Random Structures and Algorithms 17*, 260–289. 2000.

[30] M. E. Dyer, L. A. Goldberg and M. Jerrum. An approximation trichotomy for boolean #CSP. *CoRR abs/0710.4272*. 2007.

[31] M. E. Dyer, L. A. Goldberg and M. Jerrum. The complexity of weighted boolean #CSP. *CoRR abs/0704.3683*. 2007.

[32] M. E. Dyer, L. A. Goldberg and M. Paterson. On counting homomorphisms to directed acyclic graphs. Tech. Rep. TR05-121, ECCC. 2005.

[33] T. Feder and M. 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.

[34] M. Freedman., L. Lovász and A. Schrijver. Reflection positivity, rank connectivity, and homomorphism of graphs. *J. Amer. Math. Soc. 20*, 1, 37–51. 2007.

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

[36] D. Geiger. Closed systems of function and predicates. *Pacific Journal of Mathematics*, 95–100. 1968.

[37] G. Grätzer. *General Lattice Theory*. Birkhäuser Verlag, Basel.

[38] C. Greenhill. 2000. The complexity of counting colourings and independent sets in sparse graphs and hypergraphs. *Computational Complexity 9*, 52–73. 1998.

[39] P. Hell and J. Nešetřil. Counting list homomorphisms for graphs with bounded degrees. In *Graphs, Morphisms and Statistical Physics*. DIMACS Series in Discrete Mathematics and Theoretical Computer Science 63, 105–112. 2004.

[40] P. Hell and J. Nešetřil. On the complexity of $H$-Coloring. *Journal of Combinatorial Theory, Ser.B 48,* 92–110. 1990.

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

[42] H. Hunt III, M. Marathe, V. Radhakrishnan and R. Stearns. The complexity of planar counting problems. *SIAM Journal on Computing 27*, 1142–1167. 1998.

[43] P. Idziak, P. Markovic, R. McKenzie, M. Valeriote and R. Willard. Tractability and learnability arising from algebras with few subpowers. In *LICS*, 213–224. 2007.

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

[45] P. Jeavons, D. Cohen and M. Cooper. Constraints, consistency and closure. *Artificial Intelligence 101,* 1-2, 251–265. 1998.

[46] P. Jeavons, D. Cohen and M. Gyssens. How to determine the expressive power of constraints. *Constraints 4,* 113–131. 1999.

[47] M. Jerrum and A. Sinclair. The Markov chain Monte Carlo method: an approach to approximate counting and integration. In *Approximation Algorithms for NP-hard Problems*. PSW, 482–520. 1996.

[48] O. Klíma, B. Larose and P. Tesson. Systems of equations over finite semigroups and the #CSP dichotomy conjecture. In *MFCS*. 584–595. 2006.

[49] J. Lebowitz and G. Gallavotti. Phase transitions in binary lattice gases. *Journal of Math. Physics 12,* 1129–1133. 1971.

[50] L. Levin. Universal enumeration problems. *Problems on Information Transmission 9*, 265–266. 1973.

[51] N. Linial. Hard enumeration problems in geometry and combinatorics. *SIAM Journal on Algebraic and Discrete Methods 7,* 2, 331–335. 1986.

[52] L. Lovász. Operations with structures. *Acta. Math. Acad. Sci. Hung. 18,* 321–328. 1967.

[53] L. Lovász. The rank of connection matrices and the dimension of graph algebras. *European Journal of Combinatorics 27,* 6, 962–970. 2006.

[54] R. McKenzie, G. McNulty and W. Taylor. *Algebras, Lattices and Varieties*. Vol. I. Wadsworth and Brooks, California. 1987.

[55] G. Nordh and P. Jonsson. The complexity of counting solutions to systems of equations over finite semigroups. In *COCOON*. 370–379. 2004.

[56] P. Orponen. Dempster's rule of combination is #-complete. *Artificial Intelligence 44,* 245–253. 1990.

[57] J. Provan and M. Ball. The complexity of counting cuts and of computing the probability that a graph is connected. *SIAM Journal on Computing 12,* 4, 777–788. 1983.

[58] D. Roth. On the hardness of approximate reasonning. *Artificial Intelligence 82*, 273–302. 1996.

[59] T. Schaefer. The complexity of satisfiability problems. In *STOC*. 216–226. 1978.

[60] S. Vadhan. The complexity of counting in sparse, regular and planar graphs. *SIAM Journal on Computing 31,* 2, 398–427. 2001.

[61] L. Valiant. The complexity of computing the permanent. *Theoretical Computing Science 8*, 189–201. 1979.

[62] L. Valiant. The complexity of enumeration and reliability problems. *SIAM Journal on Computing 8,* 3, 410–421. 1979.

```
Algorithm Counting-mapping
INPUT:    an instance $\mathcal{G}$ of #CSP($\mathcal{H}$) such that $\Phi(\mathcal{G},\mathcal{H})$ is a subdirect power of $\mathcal{H}$,
          a congruence $\theta \in \{0_+, 1_-, 1_+, \dots, \ell_+, (\ell+1)_-\}$, and a mapping $\tau$ of level $\theta$
OUTPUT: the number $|\Phi(\mathcal{G},\mathcal{H},\tau)|$
Step 1      if $\theta = 0_+$ then return 1
Step 2      if $\theta = \omega_+$ for some $\omega \in M$ the do
Step 2.1      find the $\kappa^*_\omega$-classes $A_1,\dots,A_k$ and choose their representatives $g_1,\dots,g_k$,
              set $J_\omega = \{u_1,\dots,u_q\} \subseteq [k]$ as in Proposition 6.1, let $C^u_1,\dots,C^u_{s_u}$ be $\kappa_\omega$-classes
              belonging to $\tau(g_u)^{\lambda_\omega}$ for $u \in J$
Step 2.2      set $\mathbf{r}_0[1] := 1,\dots,\mathbf{r}_0[q] := 1$
Step 2.3      set $t :=$Counting-mapping$(\mathcal{G},\omega_-,\varrho_{\mathbf{r}_0})$
Step 2.4      for $v = 1$ to $s_{u_1}$ do
Step 2.4.1      set $\mathbf{r}[1] := v$ and $\mathbf{r}[2] := 1,\dots,\mathbf{r}[q] := 1$
Step 2.4.2      $t^1_v :=$Counting-mapping$(\mathcal{G},\omega_-,\varrho_{\mathbf{r}})$
              endfor
Step 2.5      for $u = 2$ to $q$ do
Step 2.5.1      for $v = 1$ to $s_u$ do
Step 2.5.1.1      set $\mathbf{r}[1] := 1,\dots,\mathbf{r}[u-1] := 1$, $\mathbf{r}[u] := v$, and $\mathbf{r}[u+1] := 1,\dots,\mathbf{r}[q] := 1$
Step 2.5.1.2      set $t^u_v :=$Counting-mapping$(\mathcal{G},\omega_-,\varrho_{\mathbf{r}})$
Step 2.5.1.3      set $t^u_v := \dfrac{t^u_v}{t}$
                endfor
              endfor
Step 2.6      return $\left(\prod_{u=1}^{q}\sum_{v=1}^{s_u} t^u_v\right)$
            endif
Step 3      else if $\theta = (\omega+1)_-$ do
Step 3.1      find $\varrho \in \Phi(\mathcal{G},\mathcal{H},\tau)/_{\omega^m_+}$
Step 3.2      set $t_0 :=$Counting-mapping$(\mathcal{G},\omega_+,\varrho)$
Step 3.3      set $S :=\theta$-Signature$(\mathcal{G},\tau,\omega_+)$
Step 3.4      set $v_g$ to be the size of $\eta_g$-classes, $\eta_g = \{\langle a^{\omega_+}, b^{\omega_+}\rangle \mid (g,a,b) \in S\}$
Step 3.5      return $\left(t_0 \cdot \prod_{g=1}^{m} v_g\right)$
            endif
```

Figure 16: