A Proof of CSP Dichotomy Conjecture

Dmitriy Zhuk

Department of Mechanics and Mathematics
Lomonosov Moscow State University
Moscow, Russia
Email: zhuk@intsys.msu.ru

Abstract—Many natural combinatorial problems can be expressed as constraint satisfaction problems. This class of problems is known to be NP-complete in general, but certain restrictions on the form of the constraints can ensure tractability. The standard way to parameterize interesting subclasses of the constraint satisfaction problem is via finite constraint languages. The main problem is to classify those subclasses that are solvable in polynomial time and those that are NP-complete. It was conjectured that if a core of a constraint language has a weak near unanimity polymorphism then the corresponding constraint satisfaction problem is tractable, otherwise it is NP-complete.

In the paper we present an algorithm that solves Constraint Satisfaction Problem in polynomial time for constraint languages having a weak near unanimity polymorphism, which proves the remaining part of the conjecture.

Keywords—Constraint satisfaction problem; CSP dichotomy; computational complexity

I. INTRODUCTION

Formally, the Constraint Satisfaction Problem (CSP) is defined as a triple \((X, D, C)\), where

- \(X = \{x_1, \ldots, x_n\}\) is a set of variables,
- \(D = \{D_1, \ldots, D_n\}\) is a set of the respective domains,
- \(C = \{C_1, \ldots, C_q\}\) is a set of constraints,

where each variable \(x_i\) can take on values in the nonempty domain \(D_i\), every constraint \(C_j \in C\) is a pair \((t_j, \rho_j)\) where \(t_j\) is a tuple of variables of length \(m_j\), called the constraint scope, and \(\rho_j\) is an \(m_j\)-ary relation on the corresponding domains, called the constraint relation.

The question is whether there exists a solution to \((X, D, C)\), that is a mapping that assigns a value from \(D_i\) to every variable \(x_i\) such that for each constraints \(C_j\) the image of the constraint scope is a member of the constraint relation.

In this paper we consider only CSP over finite domains. The general CSP is known to be NP-complete [1], [2]; however, certain restrictions on the allowed form of constraints involved may ensure tractability (solvability in polynomial time) [3], [4], [5], [6], [7], [8]. Below we provide a formalization to this idea.

To simplify the presentation we assume that all the domains \(D_1, \ldots, D_n\) are subsets of a finite set \(A\). By \(R_A\) we denote the set of all finitary relations on \(A\), that is, subsets of \(A^m\) for some \(m\). Then all the constraint relations can be viewed as relations from \(R_A\).

For a set of relations \(\Gamma \subseteq R_A\) by CSP(\(\Gamma\)) we denote the Constraint Satisfaction Problem where all the constraint relations are from \(\Gamma\). The set \(\Gamma\) is called a constraint language. Another way to formalize the Constraint Satisfaction Problem is via conjunctive formulas. Every \(h\)-ary relation on \(A\) can be viewed as a predicate, that is, a mapping \(A^h \to \{0, 1\}\). Suppose \(\Gamma \subseteq R_A\), then CSP(\(\Gamma\)) is the following decision problem: given a formula

\[
\rho_1(x_{1,1}, \ldots, x_{1,n_1}) \land \cdots \land \rho_s(x_{s,1}, \ldots, x_{s,n_s})
\]

where \(\rho_i \in \Gamma\) for every \(i\); decide whether this formula is satisfiable.

It is well known that many combinatorial problems can be expressed as CSP(\(\Gamma\)) for some constraint language \(\Gamma\). Moreover, for some sets \(\Gamma\) the corresponding decision problem can be solved in polynomial time; for others it is NP-complete. It was conjectured that CSP(\(\Gamma\)) is either in P, or NP-complete [9].

Conjecture 1. Suppose \(\Gamma \subseteq R_A\) is a finite set of relations. Then CSP(\(\Gamma\)) is either solvable in polynomial time, or NP-complete.

We say that an operation \(f: A^n \to A\) preserves the relation \(\rho \in R_A\) of arity \(m\) if for any tuples \((a_{1,1}, \ldots, a_{1,m}), \ldots, (a_{n,1}, \ldots, a_{n,m}) \in \rho\) the tuple \((f(a_{1,1}, \ldots, a_{1,m}), \ldots, f(a_{1,m}, \ldots, a_{n,m}))\) is in \(\rho\). We say that an operation preserves a set of relations \(\Gamma\) if it preserves every relation in \(\Gamma\). A mapping \(f: A \to A\) is called an endomorphism of \(\Gamma\) if it preserves \(\Gamma\).

Theorem 1. [7] Suppose \(\Gamma \subseteq R_A\). If \(f\) is an endomorphism of \(\Gamma\), then CSP(\(\Gamma\)) is polynomially reducible to CSP(\(\Gamma(f)\)) and vice versa, where \(\Gamma(f)\) is a constraint language with domain \(f(\Gamma)\) defined by \(f(\Gamma) = \{f(\rho) : \rho \in \Gamma\}\).

A constraint language is a core if every endomorphism of \(\Gamma\) is a bijection. It is not hard to show that if \(f\) is an endomorphism of \(\Gamma\) with minimal range, then \(f(\Gamma)\) is a core. Another important fact is that we can add all singleton unary relations to a core constraint language without increasing the complexity of its CSP. By \(\sigma_{=a}\) we denote the unary relation \(\{a\}\).
Theorem 2. [7] Let $\Gamma \subseteq R_A$ be a core constraint language, and $\Gamma' = \Gamma \cup \{ \sigma_{=a} \mid a \in A \}$, then $\text{CSP}(\Gamma')$ is polynomially reducible to $\text{CSP}(\Gamma)$.

Therefore, to prove Conjecture 1 it is sufficient to consider only the case when $\Gamma$ contains all unary singleton relations. In other words, all the predicates $x = a$, where $a \in A$, are in the constraint language $\Gamma$.

In [10] Schaefer classified all tractable constraint languages over two-element domain. In [11] Bulatov generalized the result for three-element domain. His dichotomy theorem was formulated in terms of a $G$-set. Later, the dichotomy conjecture was formulated in several different forms (see [7]).

The result of McKenzie and Maróti [12] allows us to formulate the dichotomy conjecture in the following nice way. An operation $f$ is called a weak near-unanimity operation (WNU) if $f(x, x, \ldots, x) = x$ and $f(y, x, \ldots, x) = f(x, y, x, \ldots, x) = \cdots = f(x, x, \ldots, x, y)$. Then $\text{CSP}(\Gamma)$ can be solved in polynomial time if there exists a WNU preserving $\Gamma$; $\text{CSP}(\Gamma)$ is NP-complete otherwise.

One direction of this conjecture follows from [12].

Theorem 3. [12] Suppose $\Gamma \subseteq R_A$, $\{ \sigma_{=a} \mid a \in A \} \subseteq \Gamma$. If there exists no WNU preserving $\Gamma$, then $\text{CSP}(\Gamma)$ is NP-complete.

The dichotomy conjecture was proved for many special cases: for CSPs over undirected graphs [13], for CSPs over digraphs with no sources or sinks [14], for constraint languages containing all unary relations [15], and many other. Recently, a proof of the dichotomy conjecture was announced by Andrei Bulatov [16]. Note that Bulatov’s algorithm also works for infinite constraint languages. More information about the algebraic approach to CSP can be found in [17].

In this paper we present an algorithm that solves $\text{CSP}(\Gamma)$ in polynomial time if $\Gamma$ is preserved by a WNU, and therefore prove the dichotomy conjecture. This is a short version of the paper published online [18] with some auxiliary statements and proofs omitted.

The paper is organized as follows. In Section II we give main definitions, in Section III we explain the algorithm. In Section IV we prove a theorem that explains the main idea of the algorithm and formulate theorems that prove correctness of the algorithm. In Section V we give an example that explains how the algorithm works for a system of linear equations in $\mathbb{Z}_2$.

In the next section we give the remaining definitions. In Section VII we formulate statements we will need in the proof of main theorems (see [18] for the proof).

In the last section we prove the main theorems of this paper formulated in Section IV. First, we explain how a linear variable can be added and prove the existence of a bridge. Finally, we use simultaneous induction to prove the main theorems.

II. Definitions

A set of operations is called a clone if it is closed under composition and contains all projections. For a set of operations $M$ by $\text{Clo}(M)$ we denote the clone generated by $M$.

A WNU $w$ is called special if $x \circ (x \circ y) = x \circ y$, where $x \circ y = w(x, \ldots, x, y)$. It is not hard to show that for any WNU $w$ on a finite set there exists a special WNU $w' \in \text{Clo}(w)$.

A relation $\rho \subseteq A_1 \times \cdots \times A_n$ is called subdirect if for every $i$ the projection of $\rho$ onto the $i$-th coordinate is $A_i$. For a relation $\rho$ by $p_{r,i}, \ldots, i_s(\rho)$ we denote the projection of $\rho$ onto the coordinates $i_1, \ldots, i_s$.

A. Algebras

An algebra is a pair $A := (A; F)$, where $A$ is a finite set, called universe, and $F$ is a family of operations on $A$, called basic operations of $A$. In the paper we always assume that we have a special WNU preserving all constraint relations. Therefore, every domain $D$ can be viewed as an algebra $(D; w)$. By $\text{Clo}(A)$ we denote the clone generated by all basic operations of $A$.

An equivalence relation $\sigma$ on the universe of an algebra $A$ is called a congruence if it is preserved by every operation of the algebra. A congruence (an equivalence relation) is called proper, if it is not equal to the full relation $A \times A$. We use standard universal algebraic notions of a term operation, a subalgebra, a factor algebra, a product of algebras, see [19]. We say that a subalgebra $R = (R; F_R)$ is a subdirect subalgebra of $A \times B$ if $R$ is a subdirect relation in $A \times B$.

B. Polynomially complete algebras

An algebra is called polynomially complete (PC) if the clone generated by $F_A$ and all constants on $A$ is the clone of all operations on $A$.

C. Linear algebra

A finite algebra $(A; w_A)$ is called linear if it is isomorphic to $(\mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_n}; x_1 + \ldots + x_n)$ for prime numbers $p_1, \ldots, p_n$. It is not hard to show that for every algebra $(B; w_B)$ there exists a minimal congruence $\sigma$, called the minimal linear congruence, such that $(B; w_B)/\sigma$ is linear.

D. Absorption

Let $B = (B; F_B)$ be a subalgebra of $A = (A; F_A)$. We say that $B$ absorbs $A$ if there exists $t \in \text{Clo}(A)$ such that $t(B, B, \ldots, B, A, B, \ldots, B) \subseteq B$ for any position of $A$. In this case we also say that $B$ is an absorbing subuniverse of $A$. If the operation $t$ can be chosen binary then we say that $B$ is a binary absorbing subuniverse of $A$. 

332
E. Center

Suppose \( A = (A; w_A) \) is a finite algebra with a WNU operation. \( C \subseteq A \) is called a center if there exists an algebra \( B = (B; w_B) \) with a WNU operation of the same arity and a subdirect subalgebra \( (R; w_R) \) of \( A \times B \) such that there is no binary absorbing subuniverse in \( B \) and

\[
C = \{ a \in A \mid \forall b \in B : (a, b) \in R \}.
\]

F. CSP instance

An instance of the constraint satisfaction problem is called a CSP instance. Sometimes we use the same letter for a CSP instance and for the set of constraints of this instance. For a variable \( z \) by \( D_z \) we denote the domain of the variable \( z \).

We say that \( z_1 - C_1 - z_2 - \cdots - C_{t-1} - z_1 \) is a path in \( \Theta \) if \( z_i, z_{i+1} \) are in the scope of \( C_i \) for every \( i \). We say that a path \( z_1 - C_1 - z_2 - \cdots - C_{t-1} - z_1 \) connects \( b \) and \( c \) if there exists \( a_i \in D_{z_i} \) for every \( i \) such that \( a_1 = b, a_t = c \), and the projection of \( C_0 \) onto \( z_i, z_{i+1} \) contains the tuple \( (a_i, a_{i+1}) \).

A CSP instance is called cycle-consistent if for every \( i \) and \( a \in D_i \), any path starting and ending with \( x_i \) in \( \Theta \) connects \( a \) and \( a \).

A CSP instance \( \Theta \) is called linked if for every variable \( x_i \) appearing in a constraint of \( \Theta \) and every \( a, b \in D_i \) there exists a path in \( \Theta \) that connects \( a \) and \( b \). Suppose \( X' \subseteq X \). Then we can define a projection of \( \Theta \) onto \( X' \), that is a CSP instance where variables are elements of \( X' \) and constraints are projections of constraints of \( \Theta \) onto \( X' \). We say that an instance \( \Theta \) is fragmented if the set of variables \( X \) can be divided into 2 nonempty disjoint sets \( X_1 \) and \( X_2 \) such that the constraint scope of any constraint of \( \Theta \) either has variables only from \( X_1 \), or only from \( X_2 \).

A CSP instance \( \Theta \) is called irreducible if for any subset of constraints \( \Theta' \subseteq \Theta \) and any subset of variables \( X' \subseteq X \) the projection of \( \Theta' \) onto \( X' \) is fragmented, linked, or its solution set is subdirect.

We say that a constraint \( ((y_1, \ldots, y_l); \rho_1) \) is weaker than a constraint \( ((z_1, \ldots, z_k); \rho_2) \) if \( \rho_2(z_1, \ldots, z_k) \Rightarrow \rho_1(y_1, \ldots, y_l) \), and \( \rho_1(y_1, \ldots, y_l) \not\Rightarrow \rho_2(z_1, \ldots, z_k) \).

Let \( D'_i \subseteq D_i \) for every \( i \). A constraint \( C \) of \( \Theta \) is called crucial in \( (D'_1, \ldots, D'_n) \) if \( \Theta \) has no solutions in \( (D'_1, \ldots, D'_n) \) but the replacement of \( C \in \Theta \) by all weaker constraints gives an instance with a solution in \( (D'_1, \ldots, D'_n) \). A CSP instance \( \Theta \) is called crucial in \( (D'_1, \ldots, D'_n) \) if every constraint of \( \Theta \) is crucial in \( (D'_1, \ldots, D'_n) \).

Remark 1. Suppose \( \Theta \) has no solutions in \( (D'_1, \ldots, D'_n) \). Then we can replace constraints of \( \Theta \) by all weaker constraints until we get a CSP instance that is crucial in \( (D'_1, \ldots, D'_n) \).

III. Algorithm

A. Main part

Suppose we have a constraint language \( \Gamma_0 \) that is preserved by a WNU operation. As it was mentioned before, \( \Gamma_0 \) may also be preserved by a special WNU operation \( w \). Let \( k_0 \) be the maximal arity of the relations in \( \Gamma_0 \). By \( \Gamma \) we denote the set of all relations of arity at most \( k_0 \) that are preserved by \( w \). Obviously, \( \Gamma_0 \subseteq \Gamma \), therefore \( \text{CSP}(\Gamma_0) \) can be reduced to \( \text{CSP}(\Gamma) \).

In this section we provide an algorithm that solves \( \text{CSP}(\Gamma) \) in polynomial time. Suppose we have a CSP instance \( \Theta = (X, D, C) \), where \( X = \{x_1, \ldots, x_n\} \) is a set of variables, \( D = \{D_1, \ldots, D_n\} \) is a set of the respective domains, \( C = \{C_1, \ldots, C_q\} \) is a set of constraints. Let the arity of the WNU \( w \) be equal to \( m \).

The algorithm is recursive, the list of all possible recursive calls is given in the end of this subsection. One of the main recursive calls is the reduction of a subuniverse \( D_i \) to \( D'_i \) such that either \( \Theta \) has a solution with \( x_i \in D'_i \), or it has no solutions at all.

Step 1. Check whether \( \Theta \) is cycle-consistent. If not then we reduce a domain \( D_i \) for some \( i \) or state that there are no solutions.

Step 2. Check whether \( \Theta \) is irreducible. If not then we reduce a domain \( D_i \) for some \( i \) or state that there are no solutions.

Step 3. Replace every constraint of \( \Theta \) by all weaker constraints. Recursively calling the algorithm, check that the obtained instance has a solution with \( x_i = b \) for every \( i \in \{1, 2, \ldots, n\} \) and \( b \in D_i \). If not, reduce \( D_i \) to the projection onto \( x_i \) of the solution set of the obtained instance.

By Theorem 6 we cannot loose the only solution while doing the following two steps.

Step 4. If \( D_i \) has a binary absorbing subuniverse \( B_i \subseteq D_i \) for some \( i \), then we reduce \( D_i \) to \( B_i \).

Step 5. If \( D_i \) has a center \( C_i \subseteq D_i \) for some \( i \), then we reduce \( D_i \) to \( C_i \).

By Theorem 7 we can do the following step.

Step 6. If there exists a congruence \( \sigma \) on \( D_i \) such that the algebra \( (D_i; w)/\sigma \) is polynomially complete, then we reduce \( D_i \) to any equivalence class of \( \sigma \).

By Theorem 4, it remains to consider the case when for every domain \( D_i \) there exists a congruence \( \sigma_i \) on \( D_i \) such that \( (D_i; w)/\sigma_i \) is linear, i.e., it is isomorphic to \( (\mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_l}; x_1 + \cdots + x_m) \) for prime numbers \( p_1, \ldots, p_l \). Moreover, \( \sigma_i \) is proper if \( |D_i| > 1 \).

We denote \( D_i/\sigma_i \) by \( L_i \). We define a new CSP instance \( \Theta_L \) with domains \( L_1, \ldots, L_n \). To every con-
constraint $((x_1, \ldots, x_m); \rho) \in \Theta$ we assign a constraint $((x'_1, \ldots, x'_m); \rho')$, where $\rho' \subseteq L_1 \times \cdots \times L_m$ and $(E_1, \ldots, E_m) \in \rho' \iff (E_1 \times \cdots \times E_m) \cap \rho \neq \emptyset$. The constraints of $\Theta_2$ are all constraints that are assigned to the constraints of $\Theta$.

Since every relation on $\mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_l}$ preserved by $x_1 + \cdots + x_m$ is known to be a conjunction of linear equations, the instance $\Theta_L$ can be viewed as a system of linear equations in $\mathbb{Z}_p$ for different $p$. To simplify the explanation we include variables with different domains in one equation. Note that all essential variables of every equation have the same domain.

Our general idea is to add some linear equations to $\Theta_L$ so that for any solution of $\Theta_L$ there exists the corresponding solution of $\Theta$. We start with the empty set of equations $E_0$, which is a set of constraints on $L_1, \ldots, L_n$.

**Step 7.** Put $E_0 := \emptyset$.

**Step 8.** Solve the system of linear equations $\Theta_L \cup E$ and choose independent variables $y_1, \ldots, y_k$. If it has no solutions then $\Theta$ has no solutions. If it has just one solution, then, recursively calling the algorithm, solve the reduction of $\Theta$ to this solution. Either we get a solution of $\Theta$ or $\Theta$ has no solutions.

Then there exist $Z = \mathbb{Z}_{q_1} \times \cdots \times \mathbb{Z}_{q_k}$ and a linear mapping $\phi: Z \rightarrow L_1 \times \cdots \times L_n$ such that any solution of $\Theta_L \cup E$ can be obtained as $\phi(a_1, \ldots, a_k)$ for some $(a_1, \ldots, a_k) \in Z$.

Note that for any tuple $(a_1, \ldots, a_k) \in Z$ we can check recursively whether $\Theta$ has a solution in $\phi(a_1, \ldots, a_k)$. To do this, we just need to solve an easier CSP instance (on smaller domains). Similarly, we can check whether $\Theta$ has a solution in $\phi(a_1, \ldots, a_k)$ for every $(a_1, \ldots, a_k) \in Z$. To do this, we just need to check the existence of a solution in $\phi(0, \ldots, 0, 1, 0, \ldots, 0)$ and $\phi(0, \ldots, 0)$ for any position of 1.

**Step 9.** If $\Theta$ has a solution in $\phi(0, \ldots, 0)$, then $\Theta$ has a solution.

**Step 10.** Put $\Theta' := \Theta$. Iteratively remove from $\Theta'$ all constraints that are weaker than some other constraints of $\Theta'$.

**Step 11.** For every constraint $C \in \Theta'$

1) Let $\Omega$ be obtained from $\Theta'$ by replacing a constraint $C \in \Theta'$ by all weaker constraints without dummy variables. Remove from $\Omega$ all constraints that are weaker than some other constraints of $\Omega$.

2) If $\Omega$ has no solutions in $\phi(a_1, \ldots, a_k)$ for some $(a_1, \ldots, a_k) \in Z$, then put $\Theta' := \Omega$. Repeat Step 11.

At this moment, the CSP instance $\Theta'$ has the following property. $\Theta'$ has no solutions in $\phi(b_1, \ldots, b_k)$ for some $(b_1, \ldots, b_k) \in Z$, but if we replace any constraint $C \in \Theta'$ by all weaker constraints, then we get an instance that has a solution in $\phi(a_1, \ldots, a_k)$ for every $(a_1, \ldots, a_k) \in Z$.

Therefore, $\Theta'$ is crucial in $\phi(b_1, \ldots, b_k)$.

In the remaining steps we will find a new linear equation that can be added to $\Theta_L$. Suppose $V$ is an affine subspace of $\mathbb{Z}_p^n$ of dimension $h - 1$, thus $V$ is the solution set of a linear equation $x_1 x_2 + \cdots + c_h x_h = c_0$. Then the coefficients $c_0, c_1, \ldots, c_h$ can be learned (up to a multiplicative constant) by $(p \cdot h + 1)$ queries of the form “$(a_1, \ldots, a_h) \in V$?” as follows. First, we need at most $(h + 1)$ queries to find a tuple $(a_1, \ldots, a_h) \notin V$. Then, to find this equation it is sufficient to check for every $a$ and every $i$ whether the tuple $(a_1, \ldots, a_i-1, a, a_{i+1}, \ldots, a_h)$ satisfies this equation.

**Step 12.** Suppose $\Theta'$ is not linked. For each $i$ from 1 to $k$

1) Check that for every $(a_1, \ldots, a_i) \in \mathbb{Z}_{q_1} \times \cdots \times \mathbb{Z}_{q_i}$ there exist $(a_{i+1}, \ldots, a_k) \in \mathbb{Z}_{q_{i+1}} \times \cdots \times \mathbb{Z}_{q_k}$ and a solution of $\Theta'$ in $\phi(a_1, \ldots, a_k)$.

2) If yes, go to the next $i$.

3) If no, then find an equation $c_1 y_1 + \cdots + c_i y_i = c_0$ such that for every $(a_1, \ldots, a_i) \in \mathbb{Z}_{q_1} \times \cdots \times \mathbb{Z}_{q_i}$ satisfying $c_1 a_1 + \cdots + c_i a_i = c_0$ there exist $(a_{i+1}, \ldots, a_k) \in \mathbb{Z}_{q_{i+1}} \times \cdots \times \mathbb{Z}_{q_k}$ and a solution of $\Theta'$ in $\phi(a_1, \ldots, a_k)$.

4) Add the equation $c_1 y_1 + \cdots + c_i y_i = c_0$ to $E_0$.

5) Go to Step 8.

If $\Theta'$ is linked, then by Theorem 8 there exists a constraint $((x_1, \ldots, x_i), \rho)$ in $\Theta'$ and a subuniverse $\sigma$ of $D_1 \times \cdots \times D_i \times \mathbb{Z}_p$ such that the projection of $\sigma$ onto the first $s$ coordinates is bigger than $\rho$ but the projection of $\sigma \cap (D_1 \times \cdots \times D_i \times \{0\})$ onto the first $s$ coordinates is equal to $\rho$. Then we add a new variable $z$ with domain $\mathbb{Z}_p$ and replace $((x_1, \ldots, x_i), \rho)$ by $((x_1, \ldots, x_i, z), \sigma)$. We denote the obtained instance by $\Theta_L$. Let $L$ be the set of all tuples $(a_1, \ldots, a_k, b) \in \mathbb{Z}_{q_1} \times \cdots \times \mathbb{Z}_{q_k} \times \mathbb{Z}_p$ such that $\Theta$ has a solution with $z = b$ in $\phi(a_1, \ldots, a_k)$. We know that the projection of $L$ onto the first $n$ coordinates is a full relation. Therefore $L$ is defined by one linear equation. If this equation is $z = b$ for some $b \neq 0$, then both $\Theta'$ and $\Theta$ have no solutions. Otherwise, we put $z = 0$ in this equation and get an equation that describes all $(a_1, \ldots, a_k)$ such that $\Theta'$ has a solution in $\phi(a_1, \ldots, a_k)$. It remains to find this equation.

**Step 13.** Suppose $\Theta'$ is linked.

1) Find an equation $c_1 y_1 + \cdots + c_k y_k = c_0$ such that for every $(a_1, \ldots, a_k) \in \mathbb{Z}_{q_1} \times \cdots \times \mathbb{Z}_{q_k}$ satisfying $c_1 a_1 + \cdots + c_k a_k = c_0$ there exists a solution of $\Theta'$ in $\phi(a_1, \ldots, a_k)$.

2) If the equation was not found then $\Theta$ has no solutions.

3) Add the equation $c_1 a_1 + \cdots + c_k a_k = c_0$ to $E_0$.

4) Go to Step 8.

Note that every time we reduce our domains, we get constraint relations that are still from $\Gamma$.

We have four types of recursive calls of the algorithm:
1) we reduce one domain $D_i$, for example to a binary absorbing subuniverse or to a center (Steps 1, 4, 5, 6).
2) we solve an instance that is not linked. In this case we divide the instance into the linked parts and solve each of them independently (Steps 2, 12).
3) we replace every constraint by all weaker constraints and solve an easier CSP instance (Step 3).
4) we reduce every domain $D_i$ such that $|D_i| > 1$ (Steps 8, 9, 11, 13).

Lemma 5 states the depth of the recursive calls of type 3 is at most $|I'|$. It is easy to see that the depth of the recursive calls of type 2 and 4 is at most $|A|$.

**B. Remaining parts**

In this section we explain Steps 1, 2, and 12 of the algorithm, which were not clarified in the previous section.

**Provide cycle-consistency.** To provide cycle-consistency it is sufficient to use constraint propagation providing (2,3)-consistency. Formally, it can be done in the following way. First, for every pair of variables $(x_i, x_j)$ we consider the intersections of projections of all constraints onto these variables. The corresponding relation we denote by $\rho_{i,j}$. For every $i, j, k \in \{1, 2, \ldots, n\}$ we replace $\rho_{i,j}$ by $\rho'_{i,j}$ where $\rho'_{i,j}(x, y) = \exists z \, \rho_{i,j}(x, y) \land \rho_{i,k}(x, z) \land \rho_{k,j}(z, y)$. It is not hard to see that this replacement does not change the solution set.

We repeat this procedure while we can change some $\rho_{i,j}$. If at some moment we get a relation $\rho_{i,j}$ that is not subdirect in $D_i \times D_j$, then we can either reduce $D_i$ or $D_j$, or, if $\rho_{i,j}$ is empty, state that there are no solutions. If we cannot change any relation $\rho_{i,j}$ and every $\rho_{i,j}$ is subdirect in $D_i \times D_j$, then the original CSP instance is cycle-consistent.

**Solve the instance that is not linked.** Suppose the instance $\Theta$ is not linked and not fragmented, then it can be solved in the following way. We say that an element $d_i \in D_i$ and an element $d_j \in D_j$ are linked if there exists a path that connects $d_i$ and $d_j$. Let $P$ be the set of pairs $(i, a)$ such that $i \in \{1, 2, \ldots, n\}, a \in D_i$. Then $P$ can be divided into the linked components.

It is easy to see that it is sufficient to solve the problem for every linked component and join the results. Precisely, for a linked component by $D'_i$ we denote the set of all elements $d$ such that $(i, d)$ is in the component. It is easy to see that $\emptyset \subsetneq D'_i \neq D_i$ for every $i$. Therefore, the reduction to $(D'_1, \ldots, D'_n)$ is a CSP instance on smaller domains.

**Check irreducibility.** For every $k \in \{1, 2, \ldots, n\}$ and every maximal congruence $\sigma_k$ on $D_k$ we do the following.
1) Put $I = \{k\}$.
2) Choose a constraint $C$ having the variable $x_i$ in the scope for some $i \in I$, choose another variable $x_j$ from the scope such that $j \notin I$.
3) Denote the projection of $C$ onto $(x_i, x_j)$ by $\delta$.
4) Put $\sigma_j(x, y) = \exists x' \exists y' \, \delta(x, x') \land \delta(y, y') \land \sigma_j(x', y')$.
If $\sigma_j$ is a proper equivalence relation, then add $j$ to $I$.
5) go to the next $C, x_i$, and $x_j$ in 2).

As a result we get a set $I$ and a congruence $\sigma_i$ on $D_i$ for every $i \in I$. Put $X' = \{x_i \mid i \in I\}$. It follows from the construction that for every equivalence class $E_k$ of $\sigma_k$ and every $i \in I$ there exists a unique equivalence class $E_i$ of $\sigma_i$ such that there can be a solution with $x_k \in E_k$ and $x_i \in E_i$. Thus, for every equivalence class of $\sigma_k$ we have a reduction to the instance on smaller domains. Then for every $i$ and $a \in E_i$ we consider the corresponding reduction and check whether there exists a solution with $x_i = a$.

Thus, we can check whether the solution set of the projection of the instance onto $X'$ is subdirect or empty. If it is empty then we state that there are no solutions. If it is not subdirect, then we can reduce the corresponding domain. If it is subdirect, then we go to the next $k \in \{1, 2, \ldots, n\}$ and next maximal congruence $\sigma_k$ on $D_k$, and repeat the procedure.

**IV. Correctness of the Algorithm**

A. Rosenberg completeness theorem

The main idea of the algorithm is based on a beautiful result obtained by Ivo Rosenberg in 1970, who found all maximal clones on a finite set. Applying this result to the clone generated by a WNU together with all constant operations, we can show that every algebra with a WNU operation has a binary absorption, a center, or it is polynomially complete or linear modular some congruence.

**Theorem 4.** Suppose $A = (A; w)$ is an algebra, $w$ is a special WNU of arity $m$. Then one of the following holds:

1) there exists a binary absorbing set $B \subseteq A$,
2) there exists a center $C \subseteq A$,
3) there exists a proper congruence $\sigma$ on $A$ such that $(A; w)/\sigma$ is polynomially complete,
4) there exists a proper congruence $\sigma$ on $A$ such that $(A; w)/\sigma$ is isomorphic to $(\mathbb{Z}_2; x_1 + \cdots + x_m)$.

**Proof:** Let us prove this statement by induction on the size of $A$. If we have a binary absorbing subuniverse in $A$ then there is nothing to prove. Let $M$ be the clone generated by $w$ and all constant operations on $A$. If $M$ is the clone of all operations, then $(A; w)$ is polynomially complete. Otherwise, by Rosenberg Theorem [20], $M$ belongs to one of the following maximal clones.

1) Maximal clone of monotone operations;
2) Maximal clone of autodual operations;
3) Maximal clone defined by an equivalence relation;
4) Maximal clone of quasi-linear operations;
5) Maximal clone defined by a central relation;
6) Maximal clone defined by an $h$-universal relation.

Let us consider all the cases.

1) The minimal element of the partial order can be viewed as a center. Since there is no binary absorbing subuniverse, we have a center in $A$.  

335
2) Constants are not autodual operations. This case cannot happen.
3) Let δ be a maximal congruence on A. We consider a factor algebra (A:w)/δ and apply the inductive assumption.
   a) If A/δ has a binary absorbing subuniverse B′ ⊆ A/δ, then we can check that ∪E∈E B E is a binary absorbing subuniverse of A.
   b) If A/δ has a center C′ ⊆ A/δ, then we can check that ∪E∈E C E is a center of A.
   c) Suppose (A/δ)/σ is polynomially complete.
      Since δ is a maximal congruence, σ is an equality relation and A/δ is polynomially complete.
   d) Suppose (A/δ)/σ is isomorphic to (Zp; x1 + ... + xm). Since δ is a maximal congruence, σ is an equality relation and A/δ is isomorphic to (Zp; x1 + ... + xm).
4) By Lemma 6.4 from [21], we know that w(x1, ..., xm) = x1 + ... + xm, where + is the operation in an abelian group. We assume that A has no nontrivial congruences, otherwise we refer to case 3). Then the algebra A is simple and isomorphic to (Zp; x1 + ... + xm) for a prime number p.
5) We consider the central relation ρ. It is not hard to see that the existence of a binary absorbing subuniverse on A × ⋯ × A implies the existence of a binary absorbing subuniverse on A. Therefore, the center of ρ can be viewed as a center.
6) By Corollary 5.10 from [21] this case cannot happen.

B. Correctness of the algorithm

Lemma 5. The depth of the recursive calls of type 3 in the algorithm is less than |Γ|.

Proof: First, we introduce a partial order on the set of relations in Γ in the following way. We say that ρ1 ≤ ρ2 if one of the following conditions hold
1) the arity of ρ1 is less than the arity of ρ2.
2) the arity of ρ1 equals the arity of ρ2, pr_i(ρ1) ⊆ pr_i(ρ2) for every i, pr_j(ρ1) ≠ pr_j(ρ2) for some j.
3) the arity of ρ1 equals the arity of ρ2, pr_i(ρ1) = pr_i(ρ2) for every i, and ρ1 ⊆ ρ2.
It is easy to see that any reduction makes every relation smaller or does not change it. Since our constraint language Γ is finite, there can be at most |Γ| recursive calls of type 3.

The following three theorems will be proved in Section VIII.

Theorem 6. Suppose Θ is a cycle-consistent irreducible CSP instance, B is a binary absorbing set or a center of D_i. Then Θ has a solution if and only if Θ has a solution with x_i ∈ B.

Theorem 7. Suppose Θ is a cycle-consistent irreducible CSP instance, there does not exist a binary absorbing subuniverse or a center on D_j for every j, (D_j:w)/σ is a polynomially complete algebra, E is an equivalence class of σ. Then Θ has a solution if and only if Θ has a solution with x_i ∈ E.

Theorem 8. Suppose the following conditions hold:
1) Θ is a cycle-consistent irreducible CSP instance with domain set (D_1, ..., D_n);
2) there does not exist a binary absorbing subuniverse or a center on D_j for every j;
3) if we replace every constraint of Θ by all weaker constraints then the obtained instance has a solution with x_i = b for every i and b ∈ D_i;
4) Θ_L is Θ factorized by minimal linear congruences;
5) (D_1', ..., D_n') is a solution of Θ_L, and Θ is crucial in (D_1', ..., D_n').
Then there exists a constraint ((x_1, ..., x_n), ρ) in Θ and a subuniverse ζ of D_1' × ⋯ × D_k' × Z_p such that the projection of ζ onto the first s coordinates is bigger than ρ but the projection of ζ ∩ (D_1 × ⋯ × D_s × {0}) onto the first s coordinates is equal to ρ.

V. AN EXAMPLE IN Z_4

In this section we demonstrate the main part of the algorithm for a system of linear equations in Z_4. Suppose we have a system

\[ \begin{align*}
  x_1 + 2x_2 + x_3 + x_4 &= 0 \\
  2x_1 + x_2 + x_3 + x_4 &= 0 \\
  x_1 + x_2 &= 2 \\
  x_1 + x_2 + 2x_3 + 4x_4 &= 0
\] \]

The minimal congruence σ such that (Z_4; x_1 + ... + x_5)/σ is linear is an equivalence relation modulo 2.

We write the corresponding system of linear equations in Z_2, where x_i' = x_i mod 2.

\[ \begin{align*}
  x_1' + x_3' + x_4' &= 0 \\
  x_2' + x_3' + x_4' &= 0 \\
  x_1' + x_2' &= 0
\] \]

We choose independent variables x_1' and x_3', and write the general solution: x_1' = x_1', x_2' = x_1', x_3' = x_3', x_4' = x_1' + 3. We check that (1) doesn’t have a solution, corresponding to x_1' = x_3' = 0. Let us remove the last equation from (1).

\[ \begin{align*}
  x_1 + 2x_2 + x_3 + x_4 &= 0 \\
  2x_1 + x_2 + x_3 + x_4 &= 0 \\
  x_1 + x_2 &= 2
\] \]

We check that (3) still has no solutions corresponding to x_1' = x_3' = 0.

We check that if we remove any equation from (3), then for any a_1, a_3 ∈ Z_2 there will be a solution corresponding
to \( x'_1 = a_1 \) and \( x'_3 = a_3 \). Hence we need to add exactly one equation to describe all pairs \((a_1, a_3)\) such that (3) has a solution corresponding to \( x'_1 = a_1 \) and \( x'_3 = a_3 \). Let the equation be \( c_1 x'_1 + c_3 x'_3 = c_0 \). We need to find \( c_1, c_3, \) and \( c_0 \).

Since (3) has a solution corresponding to \( x'_1 = 1, x'_2 = 0 \), but no solutions for \( x'_1 = 0, x'_2 = 1 \), the equation is \( x'_2 = 1 \).

We add this equation to (2) and solve the new system of linear equations in \( \mathbb{Z}_2 \).

\[
\begin{align*}
x'_1 + x'_2 + x'_4 &= 0 \\
x'_2 + x'_3 + x'_4 &= 0 \\
x'_1 + x'_2 &= 0 \\
x'_4 &= 1
\end{align*}
\]

(4)

The general solution of this system is \( x'_1 = 1, x'_2 = 1, x'_3 = x'_4 = x'_3 + 1, \) where \( x'_3 \) is an independent variable. We go back to (1), and check whether it has a solution corresponding to \( x'_3 = 0 \). Thus, we find a solution \((1,1,0,1)\).

While solving the system of equations, we just solved systems of linear equations in the field \( \mathbb{Z}_2 \) and constraint satisfaction problems on 2 element set (which are also equivalent to system of equations in \( \mathbb{Z}_2 \)).

VI. THE REMAINING DEFINITIONS

A. Additional notations

We say that the \( i \)-th variable of a relation \( \rho \) is compatible with the congruence \( \sigma \) if \((a_1,\ldots,a_n)\) \( \in \rho \) and \((a_1,b_i)\) \( \in \sigma \) implies \((a_1,a_{i-1},b_i,a_{i+1},\ldots,a_n)\) \( \in \rho \). We say that a relation is compatible with \( \sigma \) if every variable of this relation is compatible with \( \sigma \).

We say that a congruence \( \sigma \) is irreducible if it cannot be represented as an intersection of other binary relations \( \delta_1, \delta_2 \) compatible with \( \sigma \). For an irreducible congruence \( \sigma \) on a set \( A \) by \( \sigma^* \) we denote the minimal binary relation \( \sigma \cong \) compatible with \( \sigma \).

For a relation \( \rho \) by \( \text{Con}(\rho, i) \) we denote the binary relation \( \sigma(y,y') \) defined by

\[
\exists x_1 \ldots \exists x_{i-1} \exists x_{i+1} \ldots \exists x_n \rho(x_1,\ldots,x_{i-1},y,x_{i+1},\ldots,x_n) \wedge \rho(x_1,\ldots,x_{i-1},y',x_{i+1},\ldots,x_n).
\]

For a constraint \( C = \rho(x_1,\ldots,x_n) \), by \( \text{Con}(C, x_i) \) we denote \( \text{Con}(\rho, i) \).

A subuniverse \( A' \) of \( A \) is called a PC subuniverse if \( A' = E_1 \cap \cdots \cap E_n \), where \( E_i \) is an equivalence class of a congruence \( \sigma_i \) such that \( A/\sigma_i \) is a PC algebra.

For an algebra \( A \) by \( \text{ConLin}(A) \) we denote the minimal linear congruence. A subuniverse of \( A \) is called a linear subuniverse if it is compatible with \( \text{ConLin}(A) \).

B. Variety of algebras

We consider the variety of all algebras \( A = (A; w) \) such that \( w \) is a special WNU operation of arity \( m \). In the paper every algebra and every domain is considered as an algebra in this variety. Every relation \( \rho \subseteq A_1 \times \cdots \times A_n \) appearing in the paper is a subalgebra of \( A_1,\ldots,A_n \) for some algebras \( A_1,\ldots,A_n \) of this variety.

C. Formulas

Every variable \( x \) appearing in the paper has its domain, which we denote by \( D_x \). A set of constraints is called a formula. Sometimes we write a formula as \( C_1 \wedge \cdots \wedge C_n \).

For example, a CSP instance can be viewed as a formula.

For a formula \( \Omega \) by \( \text{Var}(\Omega) \) we denote the set of all variables of \( \Omega \). For a formula \( \Omega \) by \( \text{Expanded}(\Omega) \) we denote the set of all formulas \( \Omega' \) such that there exists a mapping \( S : \text{Var}(\Omega') \rightarrow \text{Var}(\Omega) \) satisfying the following conditions:

1) for every constraint \( \rho(x_1,\ldots,x_n) \) of \( \Omega \) either variables \( S(x_1),\ldots,S(x_n) \) are different and the constraint \( \rho(S(x_1),\ldots,S(x_n)) \) is weaker than or equal to some constraint of \( \Omega \), or \( \rho \) is a binary reflexive relation and \( S(x_1) = S(x_2) \);

2) if a variable \( x \) appears in \( \Omega \) and \( \Omega' \) then \( S(x) = x \).

Remark 2. It is easy to check for every cycle-consistent irreducible CSP instance \( \Theta \) that any instance \( \Theta' \in \text{Expanded}(\Theta) \) is also cycle-consistent and irreducible.

For a formula \( \Theta \) and a variable \( x \) of this formula by \( \text{LinkedCon}(\Theta, x) \) we denote the congruence on the set \( D_x \) defined as follows: \((a,b)\in\text{LinkedCon}(\Theta, x)\) if there exists a path in \( \Theta \) that connects \( a \) and \( b \).

D. Critical relations and parallelogram property

We say that a relation has parallelogram property if any permutation of variables in \( \rho \) satisfies the following implication

\[
\forall \alpha_1, \beta_1, \alpha_2, \beta_2: (\alpha_1\beta_2, \beta_1\alpha_2, \beta_1\beta_2) \in \rho \Rightarrow \alpha_1\alpha_2 \in \rho.
\]

We say that the \( i \)-th variable of a relation \( \rho \) is rectangular, if for every \((a_1, b_i) \in \text{Con}(\rho, i) \) and \((a_1,\ldots,a_n) \in \rho \) we have \((a_1, a_{i-1}, b_i, a_{i+1},\ldots,a_n) \in \rho \). We say that a relation is rectangular if all of its variables are rectangular. The following facts can be easily seen: if the \( i \)-th variable of \( \rho \) is rectangular then \( \text{Con}(\rho, i) \) is a congruence; if a relation has parallelogram property then it is rectangular.

A relation \( \rho \subseteq A_1 \times \cdots \times A_n \) is called critical if it cannot be represented as an intersection of other subalgebras of \( A_1 \times \cdots \times A_n \) and it has no dummy variables.

A constraint is called critical if the constraint relation is critical.
E. Reductions

A CSP instance is called 1-consistent if every constraint of the instance is subdirect.

Suppose the domain set of the instance $\Theta$ is $D = (D_1, \ldots, D_n)$. The domain set $D' = (D'_1, \ldots, D'_n)$ is called a reduction if $D'_i$ is a subuniverse of $D_i$ for every $i$.

The reduction $D' = (D'_1, \ldots, D'_n)$ is called 1-consistent if the instance obtained after reduction of every domain is 1-consistent.

We say that $D'$ is an absorbing reduction, if $D'_i$ is a binary absorbing subuniverse of $D_i$ with a term operation $t$ for every $i$. We say that $D'$ is a central reduction, if $D'_i$ is a center of $D_i$ for every $i$. We say that $D'$ is a PC/linear reduction, if $D'_i$ is a PC/linear subuniverse of $D_i$ and $D_i$ does not have a center or binary absorbing subuniverse for every $i$.

Additionally, we say that $D'$ is a minimal central/PC/linear reduction if $D'$ is a minimal center/PC/linear subuniverse of $D_i$ for every $i$. We say that $D'$ is a minimal absorbing reduction for a term operation $t$ if $D'$ is a minimal absorbing subuniverse of $D_i$ with $t$ for every $i$.

A reduction is called nonlinear if it is an absorbing, central, or PC reduction. A reduction $D'$ is called proper if it is an absorbing, central, PC, or linear reduction such that $D' \neq D$.

We usually denote reductions by $D^{(j)}$ for some $j$ (or by $D^{(i)}$). In this case by $C^{(j)}$ we denote the constraint obtained after reduction of the constraint $C$. Similarly, by $\Theta^{(j)}$ we denote the instance obtained after reduction of $\Theta$.

For a relation $\rho$ by $\rho^{(j)}$ we denote the relation $\rho$ restricted to the corresponding domains of $D^{(j)}$. Sometimes we write $(a_1, \ldots, a_n) \in D^{(j)}$ to say that every $a_i$ belongs to the corresponding $D_i^{(j)}$.

A strategy for a CSP instance $\Theta$ with a domain set $D$ is a sequence of reductions $D^{(0)}, \ldots, D^{(s)}$, where $D^{(i)} = (D_1^{(i)}, \ldots, D_n^{(i)})$, such that $D^{(0)} = D$ and $D^{(i)}$ is a proper 1-consistent reduction of $\Theta^{(i-1)}$ for every $i \geq 1$. A strategy is called minimal if every reduction in the sequence is minimal.

F. Bridges

Suppose $\sigma_1$ and $\sigma_2$ are congruences on $D_1$ and $D_2$, correspondingly. A relation $\rho \subseteq D^2_1 \times D^2_2$ is called a bridge from $\sigma_1$ to $\sigma_2$ if the first two variables of $\rho$ are compatible with $\sigma_1$, the last two variables of $\rho$ are compatible with $\sigma_2$, $\text{pr}_1(\rho) \supseteq \sigma_1$, $\text{pr}_3(\rho) \supseteq \sigma_2$, and $(a_1, a_2, a_3, a_4) \in \rho$ implies $(a_1, a_2) \in \sigma_1 \Rightarrow (a_3, a_4) \in \sigma_2$.

Suppose $\sigma_1, \sigma_2, \sigma_3$ are irreducible congruences, we have a bridge $\rho_1$ from $\sigma_1$ to $\sigma_2$ and a bridge $\rho_2$ from $\sigma_2$ to $\sigma_3$. Then we can define a bridge from $\sigma_1$ to $\sigma_3$ by $\exists y_1 \exists y_2 \rho_1(x_1, x_2, y_1, y_2) \land \rho_2(y_1, y_2, z_1, z_2)$.

A bridge $\rho \subseteq D^4$ is called reflexive if $(a, a, a, a) \in \rho$ for every $a \in D$.

We say that two congruences $\sigma_1$ and $\sigma_2$ on a set $D$ are adjacent if there exists a reflexive bridge from $\sigma_1$ to $\sigma_2$.

Remark 3. Since we can always put $\rho(x_1, x_2, x_3, x_4) = \sigma(x_1, x_3) \land \sigma(x_2, x_4)$, any congruence is adjacent with itself.

We say that two constraints $C_1$ and $C_2$ are adjacent in a common variable $x$ if $\text{Con}(C_1, x)$ and $\text{Con}(C_2, x)$ are adjacent. A formula is called connected if every constraint in the formula is rectangular and for every two constraints there exists a path that connects them. It can be shown (see Theorem 22) that every two constraints with a common variable in a connected instance are adjacent.

Then a CSP instance, whose constraints are rectangular, can be divided into the connected components.

VII. Auxiliary Statements without Proof

A. Absorption, Center, PC Subuniverse, and Linear Subuniverse

In this subsection we formulate the common property of a binary absorption, a center, a PC subuniverse, and a linear subuniverse, that is, if we restrict all but one variables of a subdirect relation to binary absorbing subuniverses, centers, PC subuniverses, or linear subuniverses, then we restrict the remaining variable correspondingly. The proof of Lemma 9 can be found in [22], the proof of remaining lemmas are in the full proof [18].

Lemma 9. Suppose $\rho \subseteq A_1 \times \cdots \times A_n$ is a relation such that $\text{pr}_1(\rho) = A_1, C = \text{pr}_1([(C_1 \times \cdots \times C_n) \cap \rho])$, where $C_i$ is a binary absorbing subuniverse in $A_i$ with a term operation $t$ for every $i$. Then $C$ is a binary absorbing subuniverse in $A_1$ with the term operation $t$.

Lemma 10. Suppose $\rho \subseteq A_1 \times \cdots \times A_n$ is a relation such that $\text{pr}_1(\rho) = A_1, C = \text{pr}_1([(C_1 \times \cdots \times C_n) \cap \rho])$, where $C_i$ is a center in $A_i$ for every $i$. Then $C$ is a center in $A_1$.

Lemma 11. Suppose $\rho \subseteq A_1 \times \cdots \times A_n$ is a subdirect relation, there is no binary absorption and center on $A_i$ for every $i$, $C = \text{pr}_1([(C_1 \times \cdots \times C_n) \cap \rho])$, where $C_i$ is a PC subuniverse in $A_i$ for every $i$. Then $C$ is a PC subuniverse in $A_1$.

Lemma 12. Suppose $\rho \subseteq A_1 \times \cdots \times A_n$ is a relation such that $\text{pr}_1(\rho) = A_1$, there is no binary absorption on $A_1$, $C = \text{pr}_1([(C_1 \times \cdots \times C_n) \cap \rho])$, where $C_i$ is a linear subuniverse in $A_i$ for every $i$. Then $C$ is a linear subuniverse in $A_1$.

B. Properties of reductions

The next two lemmas summarize some properties of minimal reductions (see the proof in [18]).

Lemma 13. Suppose $D^{(3)}$ is a proper minimal reduction, the constraint $\rho(x_1, \ldots, x_n)$ is subdirect, $\rho^{(3)}(x_1, \ldots, x_n)$ is not empty. Then $\rho^{(3)}(x_1, \ldots, x_n)$ is subdirect.
Lemma 14. Suppose \( D^{(1)} \) is a proper minimal reduction for a cycle-consistent irreducible CSP instance \( \Theta \). \( \Theta^{(1)} \) has a solution. Then \( \Theta^{(1)} \) is cycle-consistent and irreducible.

The next theorem allows us to find the next minimal reduction whenever there exists a binary absorption, a center, or a PC subuniverse. Combining this with Theorem 4, we obtain that the difficulties with finding the next reduction can be only if \( \text{ConLin}(D_i) \) is proper for any domain \( D_i \) such that \( |D_i| > 1 \) (see the proof in [18]).

Theorem 15. Suppose \( D^{(0)}, D^{(1)}, \ldots, D^{(s)} \) is a strategy for a cycle-consistent CSP instance \( \Theta \).

- If \( D^{(s)} \) has a binary absorbing set \( B \) then there exists a 1-consistent minimal absorbing reduction \( D^{(s+1)} \) of \( \Theta^{(s)} \) with \( D^{(s+1)} \subseteq B \).
- If \( D^{(s)} \) has a center \( B \) then there exists a 1-consistent minimal central reduction \( D^{(s+1)} \) of \( \Theta^{(s)} \) with \( D^{(s+1)} \subseteq B \).
- If \( D^{(s)} \) has no binary absorption and center for every \( y \) but there exists a proper PC subuniverse \( B \) in \( D^{(s)} \) for some \( x \), then there exists a 1-consistent minimal PC reduction of \( \Theta^{(s)} \) with \( D^{(s+1)} \subseteq B \).

The next lemma shows an important property of a relation without parallelagram property.

Lemma 16. Suppose \( D^{(0)}, D^{(1)}, \ldots, D^{(s)} \) is a strategy for the constraint \( \rho(x_1, \ldots, x_n) \). \( D^{(s+1)} \) is a linear reduction, \[(b_1, \ldots, b_s, a_{t+1}, \ldots, a_n) \in \rho, \]
\[(a_1, \ldots, a_t, b_{t+1}, \ldots, b_n) \in \rho, \]
\[(b_1, \ldots, b_t, b_{t+1}, \ldots, b_n) \in \rho, \]
\[(a_1, \ldots, a_t, a_{t+1}, \ldots, a_n) \in D^{(s+1)} \].

Then there exists \((d_1, d_2, \ldots, d_n) \in \rho^{(s+1)}\).

VIII. PROOF OF THE MAIN THEOREMS

A. Adding linear variable

First, we prove a property of critical relations with a rectangular variable. Then, we prove the main property of a bridge, that is, we explain how a bridge can be used to add a new linear variable to a CSP instance.

Lemma 17. Suppose \( \rho \) is a critical subdirect relation, the \( i \)-th variable of \( \rho \) is rectangular. Then \( \text{Con}(\rho, i) \) is an irreducible congruence.

Proof: Assume the converse. To simplify notations assume that \( i = 1 \). Put \( \sigma = \text{Con}(\rho, i) \). Consider binary relations \( \delta_1, \ldots, \delta_s \) compatible with \( \sigma \) such that \( \delta_1 \cap \cdots \cap \delta_s = \sigma \). Put \( \rho_i(x_1, \ldots, x_n) = \exists x'_1 \rho(x'_1, x_2, \ldots, x_n) \land \delta_i(x_1, x'_1) \).

It is easy to see that the intersection of \( \rho_1, \ldots, \rho_s \) gives \( \rho \), which contradicts the fact that \( \rho \) is critical.

Below we formulate few statements from [21] that will help us to prove the main property of a bridge. A relation \( \rho \subseteq A^n \) is called strongly rich if for every tuple \((a_1, \ldots, a_n)\) and every \( j \in \{1, \ldots, n\} \) there exists a unique \( b \in A \) such that \((a_1, \ldots, a_{j-1}, b, a_{j+1}, \ldots, a_n) \in \rho \). We will need two statements from [21].

Theorem 18. [21] Suppose \( \rho \subseteq A^n \) is a strongly rich relation preserved by a WNU. Then there exists an abelian group \((A; +)\) and bijective mappings \( \phi_1, \phi_2, \ldots, \phi_n : A \to A \) such that \[
\rho = \{(x_1, \ldots, x_n) | \phi_1(x_1) + \phi_2(x_2) + \ldots + \phi_n(x_n) = 0\}.
\]

Lemma 19. [21] Suppose \((G; +)\) is a finite abelian group, the relation \( \sigma \subseteq G^4 \) is defined by \( \sigma = \{(a_1, a_2, a_3, a_4) | a_1 + a_2 = a_3 + a_4\} \), \( \sigma \) is preserved by a WNU \( f \). Then \( f(x_1, \ldots, x_n) = t \cdot x_1 + t \cdot x_2 + \ldots + t \cdot x_n \) for some \( t \in \{1, 2, 3, \ldots\} \).

Proof: Since the relations \( \rho \) and \( \omega \) are compatible with \( \sigma \), we consider \( A/\sigma \) instead of \( A \) and assume that \( \sigma \) is the equality relation, \( \rho \) and \( \omega \) are relations on \( A/\sigma \).

Without loss of generality we assume that \( \rho(x_1, x_2, y_1, y_2) = \rho(y_1, y_2, x_1, x_2) \) and \( (a, b, a, b) \in \rho \) for any \((a, b) \in \omega \). Otherwise, we consider the relation \( \rho' \) instead of \( \rho \), where \( \rho'(x_1, x_2, y_1, y_2) = \exists z_1 \exists z_2 \rho(x_1, x_2, z_1, z_2) \land \rho(y_1, y_2, z_1, z_2) \).

We prove by induction on the size of \( A \). Assume that for some subuniverse \( A' \subseteq A \) we have \((A' \times A') \cap (\omega \times \sigma) \neq \emptyset \). By \( \rho', \sigma' \) we denote the restriction of \( \rho, \sigma \) to \( A' \) correspondingly. By \( \omega' \) we denote a minimal relation compatible with \( \sigma' \) such that \( \sigma' \subseteq \omega' \subseteq (A' \times A') \cap \omega \). By the inductive assumption for \( \rho \cap (\omega \times \omega) \) there exists a relation \( \zeta' \subseteq A' \times A' \times \mathbb{Z}_p \) such that \((x_1, x_2, 0) \in \zeta' \Leftrightarrow (x_1, x_2) \in \sigma' \) and \( \text{pr}_{1,2}(\zeta') = \omega' \). Put \( \zeta(x_1, x_2, z) = \exists y_1 \exists y_2 \rho(x_1, x_2, y_1, y_2) \land \zeta'(y_1, y_2, z) \).

It is easy to see that \( \zeta \) satisfies the necessary conditions.

Thus, we assume that for any subuniverse \( A' \subseteq A \) we have \((A' \times A') \cap (\omega \times \sigma) = \emptyset \).

Consider a pair \((a_1, a_2) \in \omega \times \sigma \). Then \{\(a | (a_1, a) \in \omega \)\} = \{\(a | (a_1, a) \in \omega \)\} and \( (a_1, a_2) \in \omega \). Hence, any element connected in \( \omega \) to some other element is connected to all elements. Since \((a_1, a_2) \in \omega \) for every \( a \in A \setminus \{a_1, a_2\} \), if \( |A| > 2 \) then \( \omega = A \times A \).

If \( |A| = 2 \) and \( \omega \neq A \times A \) then \( \omega = \{(a, a), (a, b), (b, b)\} \).

This case cannot happen because the corresponding relation \( \rho \) is not preserved by any WNU.
Thus, we assume that $\omega = A \times A$.

Let us show that for any $a_1, a_2, a_3 \in A$ there exists a unique $a_4$ such that $(a_1, a_2, a_3, a_4) \in \rho$. For every $a \in A$ put $\lambda_a(x_1, x_2) = \exists y_2 \rho(x_1, a, x_2, y_2)$. It is easy to see that $\sigma \subseteq \lambda_a \subseteq \omega$. Therefore $\lambda_a = \omega = A \times A$ for every $a$. We consider the unary relation defined by $\delta(x) = \rho(a_1, a_2, a_3, x)$. By the above fact $\delta$ is not empty. If $\delta$ contains more than one element, then we get a contradiction with the fact that there are no proper subuniverses.

Then $\rho$ is a strongly rich relation. By Theorem 18, there exist an Abelian group $(A; +)$ and bijective mappings $\phi_1, \phi_2, \phi_3, \phi_4: A \rightarrow A$ such that

$$\rho = \{(a_1, a_2, b_1, b_2) \mid \phi_1(a_1) + \phi_2(a_2) + \phi_3(b_1) + \phi_4(b_2) = 0\}.$$

We know that $(a, a, b, b) \in \rho$ for any $a, b \in A$. $ho(x_1, x_2, y_1, y_2) = \rho(y_1, y_2, x_1, x_2)$. Then without loss of generality we can assume that $\phi_1(x) = \phi_3(x) = x$, $\phi_2(x) = \phi_4(x) = -x$.

Since $w$ is a special WNU, it follows from Lemma 19 that $w$ on $A$ is defined by $x_1 + \ldots + x_m$. Therefore, the relation $\zeta \subseteq A \times A \times A$ defined by $\zeta = \text{span}\{(b_1, b_2, b_3) \mid b_1 - b_2 + b_3 = 0\}$ is preserved by $w$. If $(A; +)$ is not simple, then there exists a subuniverse $A' \subseteq A$ contradicting our assumption. Therefore, $(A; +)$ is a simple Abelian group.

**Corollary 20.1.** Suppose $\sigma \subseteq A^2$ is an irreducible congruence, $\rho(x_1, x_2, y_1, y_2)$ is a bridge from $\sigma$ to $\sigma$ such that $\rho(x, y, y, y)$ defines a full relation. Then there exists a prime number $p$ and a relation $\zeta \subseteq A \times A \times \mathbb{Z}_p$ such that $x_1, x_2, 0) \in \zeta \iff (x_1, x_2) \in \sigma$ and $\text{pr}_{1, 2} \zeta = \sigma^*$. 

**B. Existence of a bridge**

In this subsection we explain how we get a bridge from a rectangular relation and join bridges appeared in the instance together.

**Lemma 21.** Suppose $\rho \subseteq A_1 \times \ldots \times A_n$ is a subdirect relation, the first and the last variables of $\rho$ are rectangular, there exist $(b_1, a_2, \ldots, a_n), (a_1, \ldots, a_{n-1}, b_n) \in \rho$ such that $(a_1, a_2, \ldots, a_n) \notin \rho$. Then there exists a bridge $\delta$ from $\text{Con}(\rho, 1)$ to $\text{Con}(\rho, n)$ such that $\delta(x, x, y, y)$ is equal to the projection of $\rho$ onto the first and the last variables.

**Proof:** The required bridge can be defined by

$$\delta(x_1, x_2, y_1, y_2) = \exists z_2 \ldots \exists z_{n-1} \rho(x_1, z_2, \ldots, z_{n-1}, y_1) \land \rho(x_2, z_2, \ldots, z_{n-1}, y_2).$$

**Theorem 22.** Suppose $\Theta$ is a cycle-consistent connected formula such that every constraint relation is a critical rectangular relation. Then for every constraints $C, C'$ with a common variable $x$ there exists a bridge $\delta$ from $\text{Con}(C, x)$ to $\text{Con}(C', x)$ such that $\delta(x, x, y, y)$ contains the relation $\text{LinkedCon}(\Theta, x)$.

**Proof:** Since $C$ and $C'$ are connected, there exists a path $z_0C_1z_2z_3 \ldots C_{i-1}z_{i-1}C_z$, where $z_0 = z_i = x$, $C_1 = C$, $C_i = C'$, and $C_i$ and $C_{i+1}$ are adjacent in $z_i$ for every $i$.

By Lemma 17, every relation defined by $\text{Con}(C_0, x_0)$ for some $C_0$ and $x_0$ is an irreducible congruence. Suppose $\sigma_1$ is a reflexive bridge from $\text{Con}(C_i, z_i)$ to $\text{Con}(C_{i+1}, z_i)$, $\delta_i$ is a bridge from $\text{Con}(C_i, z_{i-1})$ to $\text{Con}(C_i, z_i)$ from Lemma 21 for every $i$. Then we join all bridges together and define a new bridge $\delta(\rho_0, u_0, v_1, v_0')$ by

$$\exists u_1 \exists u_2 \exists v_1 \exists v_2 \ldots \exists u_{i-1} \exists v_{i-1} \exists u_i' \exists v_i' \delta_i(u_0, u_0', v_0, v_1, v_0').$$

Since $\Theta$ is cycle-consistent, $\delta$ is a reflexive bridge from $\text{Con}(C, x)$ to $\text{Con}(C', x)$. Thus we proved that any two constraints with a common variable are adjacent.

It is not hard to show that there exists a path in $\Theta$ starting and ending at $x$ that connects any pair of elements $(a, b) \in \text{LinkedCon}(\Theta, x)$. Since every pair of constraints with common variable are adjacent, we can assume that the above path $z_0C_1z_2z_3 \ldots C_{i-1}z_{i-1}C_z$ satisfies this property. Then it is easy to check that $\delta(x, x, y, y)$ contains $\text{LinkedCon}(\Theta, x)$.

**C. Three main statements**

In this subsection we prove that all constraints in a crucial instance have the parallelogram property, show that we can always find a linked connected component with required properties, prove that we cannot loose the only solution while applying a minimal nonlinear reduction.

We prove theorems of this subsection simultaneously by the induction on the size of the reductions (domain sets). First, we need to introduce an order on the reductions. Suppose we have two domain sets $D^{(T)}$ and $D^{(L)}$. We say that $D^{(L)} \subseteq D^{(T)}$ if for every $D^{(L)}$ one of the following conditions hold

1. there exists a variable $x$ such that $D^{(L)} = D^{(T)}$.
2. there exists a variable $x$ such that $D^{(L)} \subseteq D^{(T)}$ and there does not exist a variable $z$ such that $D^{(L)} = D^{(T)}$. It is not hard to see that the relation $\leq$ is transitive and there does not exist an infinite descending chain of reductions.

Let $D^{(L)}$ be a domain set. Assume that Theorems 24 and 25 hold if $D^{(T)} < D^{(L)}$, and Theorem 23 holds if $D^{(T)} \leq D^{(L)}$. We omit the proof of Theorem 24 (see [18]) and prove Theorem 25 for $D^{(L)} = D^{(T)}$, and Theorem 23 for $D^{(L)} = D^{(T)}$.

**Theorem 23.** Suppose $D^{(L)}, \ldots, D^{(s)}$ is a minimal strategy for a cycle-consistent irreducible CSP instance $\Theta$, the constraint $\rho(x_1, \ldots, x_n)$ is crucial in $D^{(s)}$. Then $\rho$ is a critical relation with the parallelogram property.
Proof: Since $\rho(x_1, \ldots, x_n)$ is crucial, $\rho$ is a critical relation. Let $\Theta'$ be obtained from $\Theta$ by replacement of $\rho(x_1, \ldots, x_n)$ by all weaker constraints.

Assume that $|D^s_{(k)}| = 1$ for every variable $x$. Since the reduction $D^s$ is 1-consistent, we get a solution, which contradicts the fact that $\Theta$ has no solutions in $D^s$.

If we have a binary absorption, or a center, or a proper PC subuniverse on some domain $D^s_{(k)}$, then by Theorem 15 there exists a minimal nonlinear reduction $D^{(s+1)}$ for $\Theta$. Hence, by Theorem 25 $\Theta'$ has a solution in $D^{(s+1)}$. Therefore, we can assume that if we replace any constraint of $\Theta$ by all weaker constraints then we get an instance with a solution in every 1-consistent minimal PC reduction.

By Remark 1, we weaken the instance to get an instance that is crucial in $D^{(1)}$. If the obtained instance is not linked, then we consider a linked component $\Upsilon$ having a nonempty intersection with $D^{(1)}$ and apply the inductive assumption (see details in [18]). Therefore, by Theorem 23, every constraint in the obtained instance has the parallelogram property. By Theorem 24, there exists an instance $\Theta' \in \text{Expanded}(\Theta)$ that is crucial in $D^{(1)}$ and contains a linked connected component $\Omega$.

Choose a variable $x$ appearing in a constraint $C \in \Omega$. By Lemma 17, $\text{Con}(C, x)$ is irreducible. By Theorem 22, there exists a bridge $\delta$ from $\text{Con}(C, x)$ to $\text{Con}(C, x)$ such that $\delta(x, y, z)$ is a full reduction. By Corollary 20.1, there exists a relation $\zeta \subseteq D_x \times D_x \times \mathbb{Z}_p$ such that $(x_1, x_2, 0) \in \zeta \Leftrightarrow (x_1, x_2) \in \text{Con}(C, x)$ and $\pi_{1,2}(\zeta) = \text{Con}(C, x)$. Let us replace the variable $x$ of $C$ in $\Theta'$ by $x'$ and add the constraint $\zeta(x, x', z)$. The obtained instance we denote by $\Theta''$. By the assumption, $\Theta''$ has a solution with $z = 0$, and a solution in $D^{(1)}$ with $z \neq 0$.

If $D^{(1)}$ is an absorbing or central reduction, then by Corollaries 9, 10 the restriction of all variable of $\Theta''$ to $D^{(1)}$ implies the corresponding restriction of the variable $z$. This contradicts the fact that the domain of $z$ is $\mathbb{Z}_p$.

It remains to consider the case when $D^{(1)}$ is a PC reduction. Combining our assumption for the PC case and Theorem 15, we can show that for every variable $y$ and a PC subuniverse $U$ of $D_y$ the instance $\Theta''$ has a solution with $y \in U$. Hence, by Corollary 11, the restriction of $\Theta''$ to $D^{(1)}$ implies the corresponding restriction of $z$, which contradicts the fact that the domain of $z$ is $\mathbb{Z}_p$.

D. Proof of Theorems from Section IV

Proof of Theorem 6 and Theorem 7. By Theorem 15, there exists a smaller minimal reduction. By Theorem 25, there exists a solution in this reduction.

Proof of Theorem 8. Assume the converse. We denote the reduction $(D^1, \ldots, D^n)$ by $D^{(1)}$. By Theorem 23, every constraint in $\Theta$ has the parallelogram property. By Theorem 24, there exists an instance $\Theta' \in \text{Expanded}(\Theta)$ that is crucial in $D^{(1)}$ and contains a linked connected component $\Omega$ such that the solution set of $\Omega$ is not subdirect or $\Omega^{(1)}$ has no solutions. By condition 3), if the solution set of $\Omega$ is not
subdirect then \( \Omega \) contains a constraint relation from \( \Theta \). Since \( \Theta \) is crucial in \( D^1 \), if \( \Omega^{(1)} \) has no solutions then \( \Omega \) contains a constraint relation from \( \Theta \). Let \( ((x_{i_1}, \ldots, x_{i_s}), \rho) \in \Omega \) be a constraint such that \( \rho \) is a constraint relation from \( \Theta \).

By Lemma 17, \( \text{Con}(\rho, 1) \) is an irreducible congruence. By Theorem 22, there exists a bridge \( \delta \) from \( \text{Con}(\rho, 1) \) to \( \text{Con}(\rho, 1) \) such that \( \delta(x, x, y, y, y) \) is a full relation. By Corollary 20.1, there exists a relation \( \xi \subseteq D_{i_1} \times D_{i_1} \times \mathbb{Z}^p \) such that \( (x_1, x_2, 0) \in \xi \iff (x_1, x_2) \in \text{Con}(\rho, 1) \) and \( \text{pr}_{1,2}(\xi) = \text{Con}(\rho, 1)^* \).

Put \( \xi(x_{i_1}, \ldots, x_{i_s}, z) = \exists x'_{i_1} \rho(x'_{i_1}, x_{i_2}, \ldots, x_{i_s}) \land \xi(x_{i_1}, x'_{i_1}, z) \).

REFERENCES


