Proof complexity of CSP

Azza Gaysin

Department of Algebra, Charles University in Prague

ICMS, Mathematical Approaches to Lower Bounds: Complexity of Proofs and Computation, online, 8 July 2022

Presentation Plan

1. Constraint satisfaction problem (CSP) + Universal algebra notions;
2. Outline of Zhuk's algorithm;
3. Formalization of Zhuk's algorithm in V^1;
4. Results.

Constraint satisfaction problem (CSP) + Universal algebra notions

Definition 1 (CSP over finite domains).

The *Constraint Satisfaction Problem* is a problem of deciding whether there exists an assignment to a set of variables that satisfies some specified constraints. An *instance of CSP problem* over finite domains is defined as a triple $\Theta = (X, D, C)$, where

- $X = \{x_0, ..., x_{n-1}\}$ is a finite set of variables,
- $D = \{D_0, ..., D_{n-1}\}$ is a set of non-empty finite domains,
- $C = \{C_0, ..., C_{m-1}\}$ is a set of constraints, each $C_j = (\vec{x}_j, \rho_j)$ with a tuple of variables of some length m_j, $\vec{x}_j$, called *the constraint scope*, and an m_j-ary relation on the product of the corresponding domains, called the *constraint relation* ρ_j.

A *constraint language* $\mathbf{R}$ is a set of relations on finite domain. CSP($\mathbf{R}$) is a subclass of CSP defined by the property that any constraint relation in any instance of CSP($\mathbf{R}$) must belong to $\mathbf{R}$.

Constraint satisfaction problem (CSP) + Universal algebra notions

Definition 2 (CSP, equivalent definition).

Let $\mathcal{A} = (A, R_1^A, ..., R_k^A)$ be a relational structure over a vocabulary R_1,..., R_n. The *Constraint Satisfaction Problem* associated with $\mathcal{A}$, denoted by CSP($\mathcal{A}$), is the question: given a structure $\mathcal{X} = (X, R_1^X, ..., R_k^X)$ over the same vocabulary whether there exists a homomorphism from $\mathcal{X}$ to $\mathcal{A}$.

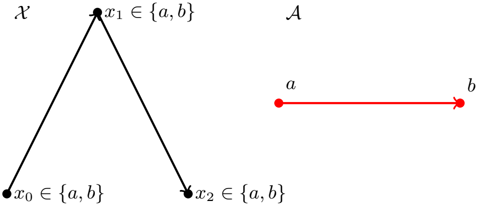

Figure 1: Equivalence of the CSP definitions

Constraint satisfaction problem (CSP) + Universal algebra notions

We say that an m-ary operation $f : A^m \to A$ *preservers* an n-ary relation $\rho \in A^n$ (or f is a *polymorphism* of ρ, or ρ is *invariant* under f) if $f(\bar{a_1}, ..., \bar{a_m}) \in \rho$ for all choices of $\bar{a_1}, ..., \bar{a_m} \in \rho$. We will denote the set of all operations preserving ρ by $Pol(\rho)$.

$$f \begin{pmatrix} a_{11} & a_{12} & ... & a_{1m} \\ a_{21} & a_{22} & ... & a_{2m} \\ ... & ... & ... & ... \\ a_{n1} & a_{n2} & ... & a_{nm} \end{pmatrix} \in \rho$$

Theorem 1.

For any relational structure $\mathcal{A} = (A, R_1, R_2, ...)$ *there exists an algebra* $\mathbb{A} = (A, F_1, F_2, ...)$*, such that* $Clone(\mathbb{A}) = Pol(\mathcal{A})$*.*

Constraint satisfaction problem (CSP) + Universal algebra notions

Definition 3 (Weak-near unanimity).

An operation Ω on a set A is called the *weak-near unanimity operation* (WNU) if it satisfies $\Omega(y, x, x, ..., x) = \Omega(x, y, x..., x) = ... = \Omega(x, x, ..., x, y)$ for all $x, y \in A$. Furthermore, Ω is called *idempotent* if $\Omega(x, ..., x) = x$ for all $x \in A$, and is called *special* if for all $x, y \in A$ $\Omega(x, ..., x, \Omega(x, ..., x, y)) = \Omega(x, ..., x, y)$.

Theorem 2 (CSP Dichotomy Theorem).

Suppose $\mathbf{R}$ is a finite set of relations on A. Then CSP($\mathbf{R}$) can be solved in polynomial time if there exists a WNU operation Ω on A preserving $\mathbf{R}$; CSP($\mathbf{R}$) is NP-complete otherwise. [1] [2]

Theorem 3.

For any constraint language $\mathbf{R}$ there is constraint language $\mathbf{R}'$ such that

- *all relations in $\mathbf{R}'$ are at most binary and*
- *$\mathbf{R}$ and $\mathbf{R}'$ pp-constructs each other.*

There is a clear procedure how to construct $\mathbf{R}'$.

[1] D. Zhuk, A proof of the csp dichotomy conjecture, J. ACM, 67(5),August 2020

[2] A. A. Bulatov, A dichotomy theorem for nonuniform CSPs. In 2017 IEEE 58th Annual Symposium on Foundations of Computer Science (FOCS), pages 319–330, 2017

Constraint satisfaction problem (CSP) + Universal algebra notions

Definition 4 (Binary absorption).

If $\mathbb{B} = (B, F_{\mathbb{B}})$ is a subalgebra of $\mathbb{A} = (A, F_{\mathbb{A}})$, then B *binary absorbs* $\mathbb{A}$ if there exists a binary term operation $f \in Clone(F_{\mathbb{A}})$ such that $f(a, b) \in B$ and $f(b, a) \in B$ for any $a \in A$ and $b \in B$.

Definition 5 (Center).

If $\mathbb{A} = (A, \Omega_{\mathbb{A}})$ is a finite algebra with a special WNU operation, then $C \subseteq A$ is a *center* if there exists an algebra $\mathbb{B} = (B, \Omega_{\mathbb{B}})$ with a special WNU operation of the same arity and a subdirect subalgebra $\mathbb{D} = (D, \Omega_{\mathbb{D}})$ of $\mathbb{A} \times \mathbb{B}$ such that there is no non-trivial binary absorbing subuniverse in $\mathbb{B}$ and $C = \{a \in A | \forall b \in B : (a, b) \in D\}$.

Definition 6 (Polynomially complete algebra).

We call an algebra $\mathbb{A} = (A, F_{\mathbb{A}})$ *polynomially complete* if the clone generated by $F_{\mathbb{A}}$ and all constants on A is the clone of all operations on A, i.e. we can generate any operation on A using $F_{\mathbb{A}}$, constant operations, projections and superpositions.

Constraint satisfaction problem (CSP) + Universal algebra notions

Definition 7 (Linear algebra).

An idempotent finite algebra $\mathbb{A} = (A, \Omega_{\mathbb{A}})$, where $\Omega_{\mathbb{A}}$ is an m-ary idempotent special WNU operation, is called *linear* if it is isomorphic to $(\mathbb{Z}_{p_1} \times ... \times \mathbb{Z}_{p_s}, x_1 + ... + x_m)$ for prime numbers $p_1, ..., p_s$.

Lemma 1 (Affine subspaces).

Suppose that relation $\rho \subseteq (\mathbb{Z}_{p_1})^{n_1} \times ... \times (\mathbb{Z}_{p_k})^{n_k}$ is preserved by $x_1 + ... + x_m$, where $p_1, ..., p_k$ are distinct prime numbers dividing $m-1$ and $\mathbb{Z}_{p_i} = (\mathbb{Z}_{p_i}, x_1 + ... + x_m)$ for every i. Then $\rho = L_1 \times ... \times L_k$, where each L_i is an affine subspace of $(\mathbb{Z}_{p_i})^{n_i}$.

Constraint satisfaction problem (CSP) + Universal algebra notions

Theorem 4.

Suppose $\mathbb{A} := (A, \Omega)$ is a finite algebra, where Ω is a special idempotent WNU of arity m. Then at least one of the following conditions holds:

1. *there exists a non-trivial binary absorbing subuniverse $B \subsetneq A$,*
2. *there exists a non-trivial center $C \subsetneq A$,*
3. *there exists a proper congruence σ on A such that $(A, \Omega)/\sigma$ is polynomially complete,*
4. *there exists a proper congruence σ on A such that $(A, \Omega)/\sigma$ is isomorphic to $(\mathbb{Z}_p, x_1 + \ldots + x_m)$ for some p.*[3]

[3] Dmitriy Zhuk. A proof of the csp dichotomy conjecture. J. ACM, 67(5):1–78, August 2020

Outline of Zhuk's algorithm

Zhuk's algorithm solves CSP in polynomial time for constraint languages having a WNU polymorphism:

- Consider a CSP instance of CSP($\mathbf{R}$), where $\mathbf{R}$ is preserved by special WNU operation Ω, $\Theta = (X, D, C)$.
- We say that a constraint C_1 is *weaker or equivalent* to a constraint C_2 if the scope of C_1 is a subset of the scope of C_2 and C_2 implies C_1. We say that C_1 is *weaker* than C_2 if C_1 is weaker or equivalent to C_2, but C_1 does not imply C_2.
- Before the linear part it reduces domains based on consistency properties and strong subsets.
- During the linear part it makes an instance weaker (replacing constraints by weaker constraints), restricts domains to linear congruences classes and searches for additional linear equations.
- The algorithm is deeply recursive: any time when it reduces/restricts some domain it starts all from the beginning.

Outline of Zhuk's algorithm

- Check if the instance is "nice" (different types of consistency of the instance: cycle-consistency, irreducibility, subdirect solution set of a weaker instance). If not, reduce domains until the instance is "nice" or there is no solution (some domain is empty).
- Check whether some domains have a non-trivial binary absorbing subuniverse or a non-trivial center. If they do, reduce the domain to the subuniverse or to the center.
- Check whether there is a proper congruence on a domain such that its factor algebra is polynomially complete. If there is such a congruence, then reduce the domain to some equivalence class of the congruence.
- If the algorithm cannot reduce any domain of CSP instance Θ further, it means that on every domain D_i of size greater than 1 there exists a congruence σ_i such that $(D_i, \Omega)/\sigma_i$ is isomorphic to some $(\mathbb{Z}_{p_1} \times ... \times \mathbb{Z}_{p_k}, x_1 + ... + x_m)$. Apply the linear case of the algorithm.

- Define a new CSP instance Θ_L with domains $D_1/\sigma_1, ..., D_n/\sigma_n$, which we will call factorized CSP instance. Every relation on $\mathbb{Z}_{p_1} \times ... \times \mathbb{Z}_{p_r}$ preserved by $\Omega(x_1, ..., x_m) = x_1 + ... + x_m$ is a conjunction of linear equations (due to Lemma 1).

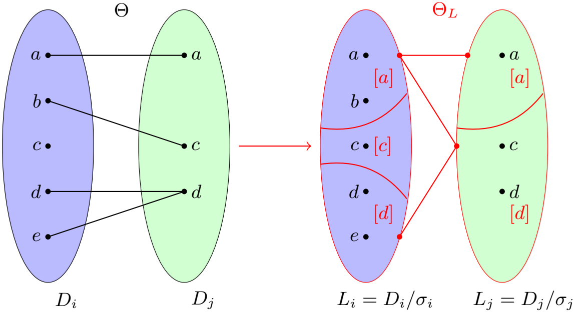

Figure 2: Factorization of the initial instance.

Outline of Zhuk's algorithm

- Compare two sets: S_Θ/Σ and S_{Θ_L}. If Θ_L has no solution, then so does Θ, if $S_\Theta/\Sigma = S_{\Theta_L}$, then we are done, if $S_\Theta/\Sigma \subsetneq S_{\Theta_L}$, then move on.
- Repeat further steps iteratively. Start with the initial instance Θ. Every iteration make the instance Θ weaker and check whether the solution set to this weaker instance, factorized by congruences, contains S_{Θ_L} (using recursion).
- At every iteration at the end there is some weaker instance Θ' such that there is a solution $s \in S_{\Theta_L}$ and $s \notin S_{\Theta'}/\Sigma$, but if we replace any other constraint in Θ' with all weaker constraints, every solution to Θ_L will be in $S_{\Theta'}/\Sigma$.
- Find the solution set to instance Θ' factorized by congruences by finding new equations additional to the set S_{Θ_L}.
- Consider the factorized instance Θ_L and instance Θ', which is weaker than Θ, and now compare two solution sets: S_Θ/Σ and $S_{\Theta'}/\Sigma \cap S_{\Theta_L}$. If $S_\Theta/\Sigma \subsetneq S_{\Theta'}/\Sigma \cap S_{\Theta_L}$, then repeat iteration.

Outline of Zhuk's algorithm

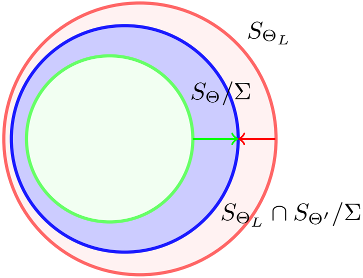

Figure 3: Solution sets.

Setting:

- Second-sorted theory ($x, y, z, \ldots$ of the first kind are called *number variables*, $X, Y, Z, \ldots$ of the second kind are called *set variables*);
- Sets code functions and relations using pairing function $\langle x, y\rangle$: $\langle x, y\rangle = \frac{(x+y)(x+y+1)}{2} + y$, for any set Z, $m \geq 2$: $Z(x_1, \ldots, x_m) =_{def} Z(\langle x_1, \ldots, x_m\rangle)$;
- Fixed algebra $\mathbb{A} = (A, \Omega)$ (size of A, arity m, all strong subsets are known) and fixed $\mathcal{A} = (A, \mathbf{R}_A)$;
- Only finite set of relations $\mathbf{R}_A$ of arity at most 2, invariant under Ω. $\mathbf{R}_A = (\mathbf{R}_A^1, \mathbf{R}_A^2)$, where

$$\mathbf{R}_A^1(j, a, a) \iff E_j^1(a) \wedge \mathbf{R}_A^2(i, a, b) \iff E_i^2(a, b).$$

  Thus, any relation on A is either of the form $x_i \in D_i$, or an edge between domains $E^{ij}(a, b)$.

Formalization of Zhuk's algorithm in V^1

Definition 8.

A *directed input graph* is a pair $\mathcal{X} = (V_\mathcal{X}, E_\mathcal{X})$ with $V_\mathcal{X}(i)$ for all $i < |V_\mathcal{X}| = n$ and $E_\mathcal{X}$ being a binary relation on $V_\mathcal{X}$. A *target digraph with domains* is an $(n+2)$-tuple of sets $\mathcal{A}' = (V_{\mathcal{A}'}, E_{\mathcal{A}'}, D_0, ..., D_{n-1})$, where:

- $|V_{\mathcal{A}'}| \leq \langle n, k\rangle$, where k is size of the algebra,
- each D_i is the subset of length k,
- $V_{\mathcal{A}'}(i, a) \iff D_i(a)$, which means that $a \in D_i$,
- $|E_{\mathcal{A}'}| < \langle\langle n, k\rangle, \langle n, k\rangle\rangle$, $E_{\mathcal{A}'}(i, a, j, b)$ means that there is an edge (a, b) from D_i to D_j, and is such that:

$$E_{\mathcal{A}'}(u, v) \to \exists i, j < n\, \exists a, b < k\;\, u = \langle i, a\rangle \wedge v = \langle j, b\rangle \wedge \\ D_i(a) \wedge D_j(b). \tag{1}$$

Basically, by $E_{\mathcal{A}'}(i, a, j, b)$ we code the binary relation $E^{ij}_{\mathcal{A}'}$.

Formalization of Zhuk's algorithm in V^1

Definition 9 (Theory V^1).

1. Two-sorted theory;
2. Accepts bounded comprehension axiom $\Sigma_0^{1,b}$-CA: $\forall x \exists X \leq x \, \forall y < x \, y \in X \equiv \phi(y)$;
3. Accepts the IND scheme for all $\Sigma_1^{1,b}$-formulas.

V^1 is isomorphic to S_2^1 (corresponds to polynomial time reasoning).

Theorem 5 (V^1 Translation).

Suppose that $\phi(\bar{x}, \bar{X})$ is a $\Sigma_0^{1,b}$-formula such that

$$V^1 \vdash \forall \bar{x} \forall \bar{X} \phi(\bar{x}, \bar{X}).$$

Then the formulas $\langle \phi \rangle_{\langle \bar{m}, \bar{n} \rangle}$ have polynomial size extended Frege proofs and these proofs can be constructed by a p-time algorithm.[4]

[4] Jan Krajicek. Bounded Arithmetic, Propositional Logic and Complexity Theory. Encyclopedia of Mathematics and its Applications. Cambridge University Press, 1995

Formalization of Zhuk's algorithm in V^1

- We augmented theory V^1 with three universal algebra $\Sigma_1^{1,b}$-axioms: for any cycle-consistent irreducible CSP instance $\Theta = (X, D, C)$
  1. if B is a nontrivial binary absorbing subuniverse of D_i, then Θ has a solution only if Θ has a solution with $x_i \in B$;
  2. if C is a nontrivial center of D_i, then Θ has a solution only if Θ has a solution with $x_i \in C$;
  3. if there does not exist a nontrivial binary absorbing subuniverse or a nontrivial center on D_j for every j, $(D_i, \Omega)/\sigma_i$ is a polynomially complete algebra, and E is an equivalence class of σ, then Θ has a solution only if Θ has a solution with $x_i \in E$.

  For this it was needed to formalize in V^1 UA-notions such as WNU operation, Taylor algebra, polymorphism, subdirect relation, binary absorbing, central, PC subuniverses, belonging to the clone, etc.
- For the linear part of the algorithm it was needed to formalize in V^1 finite abelian groups, matrices and matrix operation, graphs and graphs homomorphisms, congruences and factor-algebras.

Results

- CSP($\mathcal{A}$): for any $\mathcal{X}$, the question is whether it can be homomorphically mapped into $\mathcal{A}$. For unsatisfiable instances $\mathcal{X}$, $\neg HOM(\mathcal{X}, \mathcal{A})$ can be encoded by a propositional tautology, the size of $\neg HOM(\mathcal{X}, \mathcal{A})$ is polynomial in the sizes of $\mathcal{X}$ and $\mathcal{A}$.
- When CSP($\mathcal{A}$) is p-time decidable: for which proof systems $\neg HOM(\mathcal{X}, \mathcal{A})$ are not hard tautologies?

Lemma 2.

V^1 *proves that instance* Θ *has a solution only if the instance after consistency reductions* Θ_{nice} *has a solution.*

Theorem 6.

V^1 *proves that instance* Θ *has a solution only if factorized instance* Θ_L *has a solution.*

Lemma 3.

V^1 *proves that for every matrix* $[A|B]$ *there is a row-echelon matrix* $[A'|B']$ *having the same solution set.*

Theorem 7.

Consider two CSP instances, the initial instance $\Theta = (\mathcal{X}, \mathcal{A}')$ *and the factorized instance* $\Theta_L = (\mathcal{X}, \mathcal{A}'_L)$, *and suppose that the solution set to the initial instance factorized by congruences is a proper subset of the solution set to the factorized instance, i.e.* $\{\mathcal{X} \to \mathcal{A}'\}/\Sigma \subsetneq \{\mathcal{X} \to \mathcal{A}'_L\}$.

Then V^1 *proves that there exists a subsequence of instance digraphs* $\mathcal{X} = \mathcal{X}_0, ..., \mathcal{X}_t$ *(and a subsequence of target digraphs* $\mathcal{A} = \mathcal{A}_0, ..., \mathcal{A}_s$*), where* $t \leq n(n-1)$ *is the number of edges removed from* $\mathcal{X}$, $\{\mathcal{X}_t \to \mathcal{A}'_s\}/\Sigma \neq \{\mathcal{X} \to \mathcal{A}'_L\}$, *and if one removes any other edge from* $\mathcal{X}_t$, *every solution to* Θ_L *will be a solution to* $\{\mathcal{X}_{t+1} \to \mathcal{A}'_s\}/\Sigma$.

Lemma 4.

Consider two CSP instances, the initial instance $\Theta = (\mathcal{X}, \mathcal{A}')$ *and the instance* $\Theta_{t,s} = (\mathcal{X}_t, \mathcal{A}'_s)$, *where* $t \leq n(n-1)$ *is the number of edges removed from the initial digraph* $\mathcal{X}$ *and* $s \leq k^2$ *is the number of edges added to the target digraph* $\mathcal{A}$. V^1 *proves that instance* Θ *has a solution only if* $\Theta_{t,s}$ *has a solution.*

Results

Theorem 8.

Consider two CSP instances, the initial instance $\Theta = (\mathcal{X}, \mathcal{A}')$ *and the instance* $\Theta_{t,s} = (\mathcal{X}_t, \mathcal{A}'_s)$*, where* $t \leq n(n-1)$ *is the number of edges removed from the initial digraph* $\mathcal{X}$ *and* $s \leq k^2$ *is the number of edges added to the target digraph* $\mathcal{A}$*. Suppose that the solution set to the initial instance factorized by congruences is a proper subset of the intersection of the solution set to instance* $\Theta_{t,s}$ *factorized by congruences and the solution set to the factorized instance* Θ_L*, i.e.* $\{\mathcal{X} \to \mathcal{A}'\}/\Sigma \subsetneq \{\mathcal{X}_t \to \mathcal{A}'_s\}/\Sigma \cap \{\mathcal{X} \to \mathcal{A}'_L\}$*.*

Then V^1 *proves that there exists a subsequence of instance digraphs* $\mathcal{X} = \mathcal{X}_0, ..., \mathcal{X}_r$ *(and a subsequence of target digraphs* $\mathcal{A} = \mathcal{A}_0, ..., \mathcal{A}_f$*), where* $r \leq n(n-1)$ *is the number of edges removed from* $\mathcal{X}$ *such that* $\{\mathcal{X}_r \to \mathcal{A}'_f\}/\Sigma \neq \{\mathcal{X}_t \to \mathcal{A}'_s\}/\Sigma \cap \{\mathcal{X} \to \mathcal{A}'_L\}$ *and if one removes any other edge from* $\mathcal{X}_r$*, every solution to* $\{\mathcal{X}_t \to \mathcal{A}'_s\}/\Sigma \cap \{\mathcal{X} \to \mathcal{A}'_L\}$ *will be a solution to* $\{\mathcal{X}_{r+1} \to \mathcal{A}'_f\}/\Sigma$*.*

Thank you for your attention!