On the Complexity of CSP-based Ideal Membership Problems

Andrei A. Bulatov
Simon Fraser University

Joint work with Akbar Rafiey

CiE, 2023

Overview

- Polynomials and ideals
- Polynomials in complexity and algorithms
- Constraint Satisfaction Problem
- CSPs and ideals
- Tractability
- Search and Applications

Polynomials and Ideals

Rings and Ideals

Let $\mathbb{F}$ be a field and $\mathbb{F}[x_1, \dots, x_n]$ the ring of polynomials over $\mathbb{F}$. Here $\mathbb{F} = \mathbb{R}$ or $\mathbb{C}$.

An **ideal** $\mathcal{I} \subseteq \mathbb{F}[x_1, \dots, x_n]$ is a set of polynomials such that for any $f, g \in \mathcal{I}$ and $h \in \mathbb{F}[x_1, \dots, x_n]$ we have
$f + g, h \cdot f \in \mathcal{I}$.

Ideal Membership Problem

Ideal Membership Problem (IMP).

Input: An ideal $\mathcal{I} \subseteq \mathbb{F}[x_1, \ldots, x_n]$ and a polynomial f.

Question: Does f belong to $\mathcal{I}$?

An ideal is given by its generators, $\mathcal{I} = \langle f_1, \ldots, f_m \rangle$

Hilbert's Basis Theorem:

Every ideal of $\mathbb{F}[x_1, \ldots, x_n]$ has finitely many generators.

Solving IMP

Ideal Membership Problem (IMP).

Input: Polynomials $f, f_1, \dots, f_m \in \mathbb{F}[x_1, \dots, x_n]$.

Question: Do there exist $h_1, \dots, h_m \in \mathbb{F}[x_1, \dots, x_n]$ such that $f = h_1 \cdot f_1 + \cdots + h_m \cdot f_m$?

Search: Find $h_1, \dots, h_m \in \mathbb{F}[x_1, \dots, x_n]$ such that $f = h_1 \cdot f_1 + \cdots + h_m \cdot f_m$

Polynomials $h_1, \dots, h_m$ are called a Nullstellensatz proof that $f \in \langle f_1, \dots, f_m \rangle$

Solving IMP 2

The IMP cannot be solved simply by dividing f by $f_1, \ldots, f_m$.

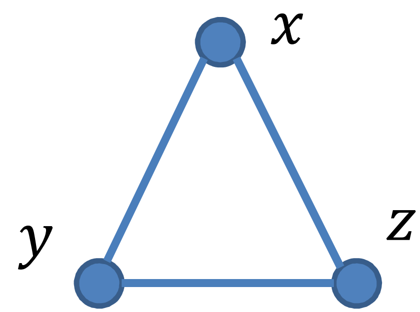
The usual way of solving the IMP is to construct a **Gröbner basis** of the ideal.
Dividing by polynomials from a Gröbner basis is much better behaved.

Polynomials in Complexity and Algorithms

IMP in Computer Science

Combinatorial problems as polynomial ideals

2-Coloring



This graph is 2-colourable iff the polynomials

$x(1-x), y(1-y), z(1-z),$ domain polynomials

$x+y-1, y+z-1, z+x-1$ instance

have a common zero

Nullstellensatz

Nullstellensatz.

Let $\mathcal{J} \subseteq \mathbb{F}[x_1, \dots, x_n]$ be a (radical) ideal and $\mathbb{V} \subseteq \mathbb{F}^n$ the set of all zeroes of polynomials from $\mathcal{J}$. Then every $f \in \mathbb{F}[x_1, \dots, x_n]$ that vanishes at every point of $\mathbb{V}$ belongs to $\mathcal{J}$.

The graph from the previous slide has no 2-coloring iff 1 belongs to the ideal generated by those polynomials:

$$1 = (-4)[x(x-1)] + (2x-1)([x+y-1] - [y+z-1] + [z+x-1])$$

IMP as a Proof System

IMP may provide a witness that an instance has no solution:

- encode your problem through polynomials $f_1, \ldots, f_m$
- check if 1 belongs to $\langle f_1, \ldots, f_m \rangle$
- or find $h_1, \ldots, h_m$ such that $1 = h_1 \cdot f_1 + \ldots + h_m \cdot f_m$

Nullstellensatz proof system

Proof complexity: What is the `size' of the smallest proof?

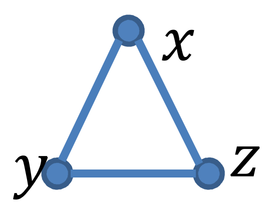
IMP and Approximation

We may want to show that a problem not only doesn't have a solution, it doesn't have anything close to a solution

Formally, construct a `loss function' that is 0 on a solution, and prove some lower bound for it

Or we may want to optimize some function on solutions

In our example



$x(1-x), y(1-y), z(1-z),$
$x+y-1, y+z-1, z+x-1$

$$f = (x+y-1)^2 + (y+z-1)^2 + (z+x-1)^2$$

To show that $f \geq 1$, represent $f-1$ as a sum of squares plus a polynomial from the ideal

IMP and SoS

Let $P = \{p_1, \ldots, p_\ell\}$ be a set of polynomials.

Polynomial f has a Sum-of-Squares (SoS) proof of nonnegativity, from P if there are polynomials $g_1, \ldots, g_k$ and $h_1, \ldots, h_\ell$ such that

$$f = \sum_{i=1}^{k} g_i^2 + \sum_{i=1}^{\ell} h_i p_i$$

Constraint Satisfaction Problem

Constraint Satisfaction Problem

Definition:

CSP(Γ)

Instance: $(V;A;\boldsymbol{C})$ where

- V is a finite set of variables
- A is a set of values
- $\boldsymbol{C}$ is a set of constraints $\{R_1(s_1), \ldots, R_q(s_q)\}$

  where each R_i belongs to Γ, a constraint language

Objective: whether there is $h: V \rightarrow A$ such that,

for any i, $R_i(h(s_i))$ is true

Examples: SAT

3-SAT = CSP(Γ_{3-SAT}):

$$(X \vee \overline{Y} \vee Z) \wedge (\overline{X} \vee \overline{U} \vee V) \wedge (U \vee T \vee Z)$$

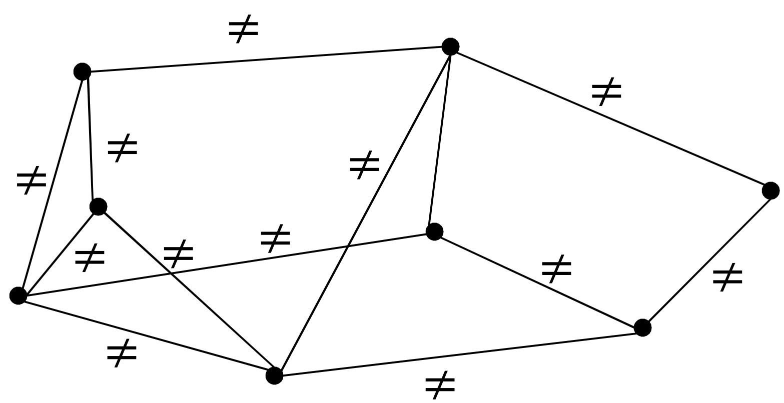
Examples: k-Coloring

k-Coloring:

Instance: A graph

CSP($\neq$)

$$G = (V, E)$$



Objective: Is it k-colorable?

H-Coloring : Edge relation of a graph H rather than $\neq$

Examples: Linear Equations

Linear Equations:

Instance: A system of linear equations

$\mathrm{CSP}(\Gamma_{\mathrm{aff}})$

$$\begin{cases} 2x_1 + x_5 + 1.5x_7 & = & 3 \\ x_2 - 2x_4 - 3x_5 & = & 0 \\ & \vdots & \\ 5x_1 - 2x_3 + 2x_7 & = & 1 \end{cases}$$

(affine relations)

Objective: Is it consistent?

Invariants and Polymorphisms

Definition Relation R is invariant w.r.t. an n-ary operation f (or f is a polymorphism of R) if, for any $\bar{a}_1, \ldots, \bar{a}_n \in R$ the tuple obtained by applying f coordinate-wise belongs to R

Pol(Γ) denotes the set of all polymorphisms of relations from Γ

Theorem (Jeavons et al., 1998**)**
If Pol(Γ) $\subseteq$ Pol(Δ), then
CSP(Δ) is polytime reducible to **CSP(Γ)**

Polymorphisms: Examples

Consider $R \in \Gamma_{aff}$, it is the set of solutions of a system

$A \cdot \vec{x} = \vec{b}$

Then operation $f(x, y, z) = x - y + z$ is a polymorphism of R

Indeed, take $\vec{x}, \vec{y}, \vec{z} \in R$, that is, $A \cdot \vec{x} = A \cdot \vec{y} = A \cdot \vec{z} = \vec{b}$

Then

$$A \cdot (\vec{x} - \vec{y} + \vec{z}) = A \cdot \vec{x} - A \cdot \vec{y} + A \cdot \vec{z} = \vec{b} - \vec{b} + \vec{b} = \vec{b}$$

Good Polymorphisms

A semilattice operation is a binary operation $\cdot$ satisfying the equations: $x \cdot x = x, \quad x \cdot y = y \cdot x, \quad x \cdot (y \cdot z) = (x \cdot y) \cdot z$

(Horn SAT)

A majority operation is a ternary operation h that satisfies the equations $g(x,x,y) = g(x,y,x) = g(y,x,x) = x$

(2-SAT)

A Maltsev operation is a ternary operation h that satisfies the equations $h(x,x,y) = h(y,x,x) = y$

(systems of linear equations)

Schaefer's Theorem

Schaefer's Dichotomy Theorem (Schaefer 1978**)**

For a Boolean constraint language Γ, $\mathrm{CSP}(\Gamma)$ is poly time iff one of the following operations is a polymorphism of Γ

- constant 0 (constant 1) operation
- disjunction $\vee$ (conjunction $\wedge$)
- majority operation $(x \wedge y) \vee (y \wedge z) \vee (z \wedge x)$
- affine (Mal'tsev) operation $x - y + z$

Otherwise it is NP-complete.

General Dichotomy Theorem

CSP Dichotomy Theorem (Bulatov, Zhuk, 2017**)**
For a constraint language Γ on a finite set, $CSP(\Gamma)$ is poly time iff a weak near-unanimity operation is a polymorphism of Γ. Otherwise it is NP-complete.

$w(x_1, \ldots, x_k)$ is WNU if

$$w(x, \ldots, x, y) = w(x, \ldots, y, x) = \cdots = w(y, \ldots, x, x)$$

IMP and CSP

IMP from CSP

Let $\mathcal{P}$ be an instance of $CSP(\Gamma)$ where Γ is a constraint language over $D = \{0, \dots, r-1\}$.

Let $\{x_1, \dots, x_n\}$ be the set of variables of $\mathcal{P}$

For every constraint $C = \langle (x_{i_1}, \dots, x_{i_k}), R \rangle$ introduce a polynomial $f_C \in \mathbb{R}[x_{i_1}, \dots, x_{i_k}]$ whose zeroes are exactly the tuples of R

$\mathcal{I}(\mathcal{P})$ is the ideal of $\mathbb{R}[x_1, \dots, x_n]$ generated by f_C, for all constraints C and domain polynomials $f_D(x_i)$, $i \leq n$.

IMP from CSP 2

$IMP(\Gamma)$:

Input: an instance $\mathcal{P}$ of $CSP(\Gamma)$ with variables $\{x_1, \dots, x_n\}$ and a polynomial $f \in \mathbb{R}[x_1, \dots, x_n]$

Question: $f \in \mathcal{I}(\mathcal{P})$?

Also, find a proof that $f \in \mathcal{I}(\mathcal{P})$

$IMP_d(\Gamma)$ is the subproblem of $IMP(\Gamma)$ in which the degree of f is bounded by d

IMP from CSP 3

$\mathcal{I}(\mathcal{P})$ is always radical, so Nullstellensatz applies

$IMP(\Gamma)$:

Input: an instance $\mathcal{P}$ of $CSP(\Gamma)$ with variables $\{x_1, \dots, x_n\}$ and a polynomial $f \in \mathbb{R}[x_1, \dots, x_n]$

Question: is every solution of $\mathcal{P}$ a zero of f?

Corollary

$IMP(\Gamma) \in coNP$

Research Questions

Question 1: For which Γ a Groebner basis of $\mathcal{I}(\mathcal{P})$ can be efficiently constructed for every $\mathcal{P}$?

Question 2: For which Γ there is a `small' Nullstellensatz proof of $f \in \mathcal{I}(\mathcal{P})$ for every $f, \mathcal{P}$?

Question 3: For which Γ the problem $IMP_d(\Gamma)$ is polynomial time?

Boolean IMP

Theorem (Mastrolilli'19, Mastrolilli,Bharati'20)
Let Γ be a constraint language over $\{0,1\}$. Then
If Γ has a majority, semilattice or affine $(x - y + z)$ polymorphism then $IMP_d(\Gamma)$ is polytime for any d

Otherwise $IMP_2(\Gamma)$ is coNP-complete

Tractable cases are through GB

Tractability

Polytime IMP

Theorem.

(1) $IMP_d(\text{semilattice})$ is polytime for every d.

(2) $IMP_d(\text{dual discriminator})$ is polytime for every d

(3) $IMP_d(\mathbb{Z}_p)$, p prime, is polytime for every d

(4) $IMP_d(\mathbb{A})$ is polytime for every d, $\mathbb{A}$ is an Abelian group

Abelian Groups Case

Consider $IMD(\mathbb{Z}_p)$

The CSP instance is a system of linear equations

$$\begin{cases} a_{11}x_1 + \cdots + a_{1n}x_n = b_1 \\ \vdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n = b_m \end{cases}$$

The polynomial encoding is exponentially long

Change the domain

Abelian Groups Case 2

Step 1. Solve the system

$$\begin{cases} x_1 = c_{1m+1}x_{m+1} + \cdots + c_{1n}x_n + b_1 \\ \vdots \\ x_m = c_{mm+1}x_{m+1} + \cdots + c_{mn}x_n + b_m \end{cases}$$

Step 2. Replace $D = \{0,1,\ldots,r-1\}$ with rth roots of unity U_r

ω is a primitive root

$x^r - 1$ domain polynomials

$x_i - \omega^{b_i} x_{m+1}^{c_{im+1}} \ldots x_n^{c_{in}}$ instance

It is a GB

Abelian Groups Case 3

Step 3. Convert the input polynomial

Let $\pi: U_r \to D$, $\pi(\omega^i) \to i$

It is represented by a polynomial

Convert $f(x_1, \ldots, x_n)$ to $f' = f(\pi(x_1), \ldots, \pi(x_n))$

Lemma.

f' belongs to the ideal generated by the polynomials from Step 2 if and only if f belongs to the ideal corresponding to the original instance.

Search and Applications

The Search Problem

The reductions shown above allow for a solution of the decision problem. However, substitutions completely mess up proofs and GB

We show a reduction of the search problem to the decision problem. It involves constructing a GB using the decision problem

Extended IMP

$\chi IMP(\Gamma)$:

Input: an instance $\mathcal{P}$ of $CSP(\Gamma)$ with variables $\{x_1, \ldots, x_n\}$ and a sequence of polynomials $f_1, \ldots, f_m \in \mathbb{R}[x_1, \ldots, x_n]$

Question: Do there exist $\alpha_1, \ldots, \alpha_m \in \mathbb{R}$ such that $\alpha_1 f_1 + \cdots + \alpha_m f_m \in \mathcal{I}(\mathcal{P})$?

Extended IMP 2

All the algebraic properties of the IMP remain true for the χIMP.

Also, all the tractable cases of the IMP remain tractable for the χIMP.

Extended IMP and the Search Problem

Theorem.
If $\chi IMP(\Gamma)$ can be solved in polynomial time then for any instance $\mathcal{P}$ of $CSP(\Gamma)$, a degree d truncated Gröbner basis can also be constructed in polynomial time.

Proof idea.

Enumerate all the monomials of degree at most d.

For each of them use the χIMP to decide if a GB should contain a polynomial with such a leading monomial and find it.

χIMP and Bit Complexity

Recall SOS proofs:

$$\underbrace{f = \sum_{i=1}^{k} g_i^2}_{} + \sum_{i=1}^{\ell} h_i p_i$$

use χIMP to decide if $f - \sum_{i=1}^{k} g_i^2$
belongs to the ideal generated by the p_i

IMP and SoS 2

- If it is known that an instance has an SoS proof of low degree, it can be found through an SDP program of polynomial size. Then the SDP program can be solved by the ellipsoid method
- Low degree SoS proofs can be found. Such proof systems are called automatizable. Used in an attempt to refute the UGC
- Accident: It turns out low degree is not enough, also need small coefficients (O'Donnell'17)
- Can almost be avoided in the majority of interesting cases, provided the IMP part is polytime (Raghavendra'17)

χIMP and Bit Complexity 2

Raghavendra and Weitz suggested 3 conditions that guarantee that an SOS proof has low bit complexity.

The approach above eliminates 2 of them for problems $CSP(\Gamma)$

Open Questions

- More polytime problems
- Connection to the standard CSP techniques (consistency?)
- Low degree restrictions. What do they correspond to in CSP?

Thank You!