SOLVING EQUATIONS – KITH AND KIN

Paweł M. Idziak and Jacek Krzaczkowski

Theoretical Computer Science at Jagiellonian University in Krakow

May 24, 2018

Algebras and Lattices in Hawaii
in honor of Ralph Freese, Wiliam Lampe, J.B. Nation

Solving equations

- Linear equations
- Diophantine equations – Hilbert's 10th problem
- SAT

- POLSAT – equations of polynomials over finite algebras
- SYSPOLSAT – finite systems of equations of polynomials over finite algebras

Equations satisfiability and CSP

Fact (Feder, Madelaine & Stewart 2004; Larose & Zádori 2006)

- for every finite relational structure $\mathbb{D}$ there is a finite algebra $\mathbf{A}[\mathbb{D}]$ such that the problem $\mathrm{CSP}(\mathbb{D})$ is polynomially equivalent to $\textsc{SysPolSat}(\mathbf{A}[\mathbb{D}])$,
- for every finite algebra $\mathbf{A}$ there exists a relational structure $\mathbb{D}[\mathbf{A}]$ such that the problems $\textsc{SysPolSat}(\mathbf{A})$ and $\mathrm{CSP}(\mathbb{D}[\mathbf{A}])$ are polynomially equivalent.

Fact

- for every finite relational structure $\mathbb{D}$ there is a finite algebra $\mathbf{A}[\mathbb{D}]$ such that the problem $\mathrm{CSP}(\mathbb{D})$ is polynomially equivalent to $\textsc{PolSat}(\mathbf{A}[\mathbb{D}])$.
- TBD ??

Defining equations satisfiability?

- fixed finite algebra as a template

Examples

Groups (Goldmann & Russell 1999)

Polynomial satisfiability problem ($\textsc{PolSat}$) is NP-complete for non-solvable groups and in P for nilpotent groups.

Rings (Burris & Lawrence 1993; Horváth 2011)

Let $\mathbf{A}$ be a finite ring. Then $\textsc{PolSat}(\mathbf{A})$ is in P, whenever $\mathbf{A}$ is nilpotent and NP-complete otherwise.

Lattices (Schwarz 2004)

Let $\mathbf{A}$ be a finite lattice. Then $\textsc{PolSat}(\mathbf{A}) \in \mathrm{P}$ if $\mathbf{A}$ is distributive and NP-complete otherwise.

Defining equations satisfiability?

- fixed finite algebra as a template

Defining equations satisfiability?

- fixed finite algebra as a template
- finite vs infinite language
  – operations' description on the fly

Defining equations satisfiability?

- fixed finite algebra as a template
- finite vs infinite language
  – operations' description on the fly
- syntactic trees vs circuits (with gates)

Fact (Goldmann, Russell)

PolSat is NP-complete for non-solvable groups and in P for nilpotent groups.

Fact (Goldmann, Russell)

PolSat is NP-complete for non-solvable groups and in P for nilpotent groups.

Kosicka Bela observations 2003

For (solvable but non-nilpotent) symmetric group S_3:

- PolSat$(\mathrm{S}_3; \cdot, {}^{-1})$ is in P (Horváth & Szabó)
- PolSat$(\mathrm{S}_3; \cdot, {}^{-1}, \text{a couple of additional polynomials})$ is NP-complete.

Fact (Goldmann, Russell)

PolSat is NP-complete for non-solvable groups and in P for nilpotent groups.

Kosicka Bela observations 2003

For (solvable but non-nilpotent) symmetric group S_3:

- $\textsc{PolSat}\big(\mathrm{S}_3; \cdot, {}^{-1}\big)$ is in P (Horváth & Szabó)
- $\textsc{PolSat}\big(\mathrm{S}_3; \cdot, {}^{-1}, _{\text{a couple of additional polynomials}}\big)$ is NP-complete.

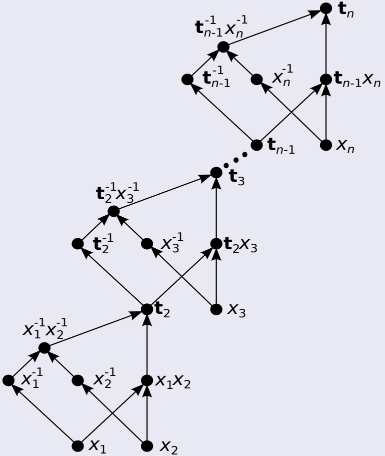
Fact (Horváth & Szabó 2012)

For (solvable but non-nilpotent) alternating group A_4:

- $\textsc{PolSat}\big(\mathrm{A}_4; \cdot, {}^{-1}\big)$ is in P,
- $\textsc{PolSat}\big(\mathrm{A}_4; \cdot, {}^{-1}, [,]\big)$, where $[x, y] = x^{-1}y^{-1}xy$, is NP-complete.

exponential syntactic tree vs polynomial size circuit

$$t_n(x_1, x_2, \ldots, x_n) = [\ldots[[x_1, x_2], x_3]\ldots x_n]$$



Definition

$\textsc{Csat}(\mathbf{A})$
given a circuit over $\mathbf{A}$ with two output gates g_1, g_2
is there a valuation of input gates $\overline{x} = (x_1, \ldots, x_n)$ that gives the same output on g_1, g_2, i.e. $g_1(\overline{x}) = g_2(\overline{x})$.

Back to groups

PolSat (Goldmann & Russell 1999)

Polynomial satisfiability problem (PolSat) is NP-complete for non-solvable groups and in P for nilpotent groups.

CSat (Horváth & Szabó 2011)

Circuit satisfiability problem (CSat) is NP-complete for non-nilpotent groups and in P for nilpotent groups.

Defining equations satisfiability?

- fixed finite algebra as a template
- finite vs infinite language
  – operations' description on the fly
- syntactic trees vs circuits (with gates)

Defining equations satisfiability?

- fixed finite algebra as a template
- finite vs infinite language
  – operations' description on the fly
- syntactic trees vs circuits (with gates)
- quotients

Quotients

Fact

There is a finite algebra $\mathbf{A}$ with a congruence α such that $\textsc{Csat}(\mathbf{A})$ is in P while $\textsc{Csat}(\mathbf{A}/\alpha)$ is NP-complete.

Fact (Klíma, Tesson & Thérien 2007)

There is a finite algebra $\mathbf{A}$ with a congruence α such that $\mathrm{S}\textsc{Csat}(\mathbf{A})$ is in P while $\mathrm{S}\textsc{Csat}(\mathbf{A}/\alpha)$ is NP-complete.

Defining equations satisfiability?

- fixed finite algebra as a template
- finite vs infinite language
  – operations' description on the fly
- syntactic trees vs circuits (with gates)
- quotients

Theorem (LICS'18)

Let $\mathbf{A}$ be a finite algebra of finite type from a congruence modular variety.

1. If $\mathbf{A}$ has no quotient $\mathbf{A}'$ with $\textsc{CSat}(\mathbf{A}')$ being NP-complete then $\mathbf{A}$ is isomorphic to a direct product $\mathbf{N} \times \mathbf{D}$, where $\mathbf{N}$ is a nilpotent algebra and $\mathbf{D}$ is a subdirect product of 2-element algebras each of which is polynomially equivalent to the 2-element lattice.
2. If $\mathbf{A}$ decomposes into a direct product $\mathbf{N} \times \mathbf{D}$, where $\mathbf{N}$ is a supernilpotent algebra and $\mathbf{D}$ is a subdirect product of 2-element algebras each of which is polynomially equivalent to the 2-element lattice, then for every quotient $\mathbf{A}'$ of $\mathbf{A}$ the problem $\textsc{CSat}(\mathbf{A}')$ is solvable in polynomial time.

easy, moderate and sometimes heavy use of TCT

Poly-time algorithms

If $\mathbf{A}$ is a supernilpotent algebra (or a distributive lattice) then there is a constant d so that for each natural number n there is $S_n \subseteq A^n$ such that

- $|S_n|$ is $O(n^d)$,
- for two n-ary polynomials s and t the equation $s(\overline{x}) = t(\overline{x})$ has a solution $\overline{x} \in A^n$ iff it has a solution in S_n.

$\sim$ & $\sim$ & Kawałek

There exist nilpotent (but not supernilpotent) algebras $\mathbf{A}$ such that:

- $\textsc{Csat}(\mathbf{A})$ is in P,
- $\textsc{Csat}(\mathbf{A})$ can not be solved in polynomial time using algorithm checking a small set of potential solutions which depends only on the number of input gates of a given circuit (unless $\mathrm{P} = \mathrm{NP}$).

$\sim$ & $\sim$ & Kawałek

There exist nilpotent (but not supernilpotent) algebras **A** such that:

- $\textsc{Csat}(\mathbf{A})$ is in P,
- $\textsc{Csat}(\mathbf{A})$ can not be solved in polynomial time using algorithm checking a small set of potential solutions which depends only on the number of input gates of a given circuit (unless P = NP).

$\mathbf{A} = (\mathbb{Z}_6; +, f)$, where $f(x) = x \mod 2$.

	tractable	open	intractable
CEQV	supernilpotent Aichinger & Mudrinski	nil but not supernil	non nilpotent
CSAT	supernil $\times$ DL-like	nil but not supernil	non (nil $\times$ DL-like)
MCSAT	affine $\times$ DL-like	—	otherwise
SCSAT	affine Gaussian elimination	—	otherwise Larose & Zádori