Clones and the complexity of TermSAT

Tomasz A. Gorazd[1] Jacek Krzaczkowski[2]

[1]Algorithmics Research Group
Jagiellonian University, Kraków

[2]Institute of Computer Science
UMCS, Lublin

Algorithmic Complexity and Universal Algebra, Szeged, 2007

Definition

For an algebra $\mathbf{A}$ the term satisfiability problem $(\mathrm{TERM\text{-}SAT}(\mathbf{A}))$ is a decision problem with

Instance: A pair of terms (s, t)

Question: Does the equation

$$s^{\mathbf{A}}(\overline{x}) = t^{\mathbf{A}}(\overline{x})$$

have a solution?

Definition

For an algebra $\mathbf{A}$ the term satisfiability problem ($\mathrm{TERM\text{-}SAT}(\mathbf{A})$) is a decision problem with

Instance: A pair of terms (s, t) **with the tables of the fundamental operations of $\mathbf{A}$ corresponding to all function symbols occurring in s and t.**

Question: Does the equation

$$s^{\mathbf{A}}(\overline{x}) = t^{\mathbf{A}}(\overline{x})$$

have a solution?

Definition

For an algebra $\mathbf{A}$ the term satisfiability problem $(\mathrm{TERM\text{-}SAT}(\mathbf{A}))$ is a decision problem with

Instance: A pair of terms (s, t) **with the tables of the fundamental operations of A corresponding to all function symbols occurring in s and t.**

Question: Does the equation

$$s^{\mathbf{A}}(\overline{x}) = t^{\mathbf{A}}(\overline{x})$$

have a solution?

If (s, t) is a pair of polynomials we get the polynomial satisfiability problem $(\mathrm{POL\text{-}SAT}(\mathbf{A}))$.

Lattices (*Schwarz*)

For a lattice $\mathbf{L}$

- $\mathrm{POL\text{-}SAT}(\mathbf{L})$ in P if $\mathbf{L}$ is distributive
- $\mathrm{POL\text{-}SAT}(\mathbf{L})$ is NP-complete, else.

Lattices (*Schwarz*)

For a lattice $\mathbf{L}$

- $\mathrm{POL\text{-}SAT}(\mathbf{L})$ in P if $\mathbf{L}$ is distributive
- $\mathrm{POL\text{-}SAT}(\mathbf{L})$ is NP-complete, else.

Groups (*Goldmann, Russell*)

For a group $\mathbf{G}$

- $\mathrm{POL\text{-}SAT}(\mathbf{G})$ in P if $\mathbf{G}$ is nilpotent.
- $\mathrm{POL\text{-}SAT}(\mathbf{G})$ is NP-complete if $\mathbf{G}$ is not solvable.

Question 1

Does the computational complexity of $\mathrm{TERM\text{-}SAT}(\mathbf{A})$ depend on $Clo(\mathbf{A})$, the clone of term operations of $\mathbf{A}$?

Example

- $\mathrm{POL\text{-}SAT}(\mathrm{S}_3, \circ)$ is in P. (*G. Horváth, C.Szabó*)

Example

- $\mathrm{POL\text{-}SAT}(\mathrm{S}_3, \circ)$ is in P. (*G. Horváth, C.Szabó*)
- $\mathrm{POL\text{-}SAT}(\mathrm{S}_3, \circ, [])$ is NP-complete. (*P. Idziak*)
  $[x, y] = x^{-1} \circ y^{-1} \circ x \circ y$

Example

- $\mathrm{POL\text{-}SAT}(\mathrm{S}_3, \circ)$ is in P. (*G. Horváth, C.Szabó*)
- $\mathrm{POL\text{-}SAT}(\mathrm{S}_3, \circ, [])$ is NP-complete. (*P. Idziak*)
  $[x, y] = x^{-1} \circ y^{-1} \circ x \circ y$
- $Clo(S_3, \circ) = Clo(S_3, \circ, [])$

Theorem

For any two-element algebra $\mathbf{A}$ *the computational complexity of* $\mathrm{TERM\text{-}SAT}(\mathbf{A})$ *depends only on* $Clo(\mathbf{A})$.

Definition

We say that $\mathrm{TERM\text{-}SAT}$ for a clone C is

- **representation-independent** iff for arbitrary algebras $\mathbf{A}, \mathbf{B}$ such that $Clo(\mathbf{A}) = Clo(\mathbf{B}) = C$, $\mathrm{TERM\text{-}SAT}(\mathbf{A})$ and $\mathrm{TERM\text{-}SAT}(\mathbf{B})$ are polynomial-time equivalent.
- **representation-dependent**, else.

Definition

We say that $\mathrm{TERM\text{-}SAT}$ for a clone C is

- **representation-independent** iff for arbitrary algebras $\mathbf{A}, \mathbf{B}$ such that $Clo(\mathbf{A}) = Clo(\mathbf{B}) = C$, $\mathrm{TERM\text{-}SAT}(\mathbf{A})$ and $\mathrm{TERM\text{-}SAT}(\mathbf{B})$ are polynomial-time equivalent.
- **representation-dependent**, else.

If $\mathrm{TERM\text{-}SAT}$ is **representation-independent** for C we say

- $\mathrm{TERM\text{-}SAT}$ for C is in P.
  or
- $\mathrm{TERM\text{-}SAT}$ for C is NP-complete.
  or
- $\mathrm{TERM\text{-}SAT}$ for C is . . .

Goal

Characterize the clones where TERM-SAT is representation-independent.

Full clone

Theorem

For a primal algebra $\mathbf{A}$, $\mathrm{TERM\text{-}SAT}(\mathbf{A})$ *is NP-complete.*

Full clone

Theorem

For a primal algebra $\mathbf{A}$, $\mathrm{TERM\text{-}SAT}(\mathbf{A})$ *is NP-complete.*

Maximal clones

Theorem

For every maximal clone C *on a set* A *with* $|A| > 2$ *the* $\mathrm{TERM\text{-}SAT}$ *for* C *is* **representation-independent**.

Moreover, $\mathrm{TERM\text{-}SAT}(\mathbf{A})$, *where* $Clo(\mathbf{A}) = C$,

- *is in P, if C is affine or determined by a singleton,*
- *is NP-complete otherwise.*

Question 2

How hard is TERM-SAT for the previous clones really?

Definition

- **DQL** is the class of decision problems solvable by **deterministic** multitype Turing machine in quasilinear time i.e. $O(n(log(n)^k))$.
- **NQL** is the class of decision problems solvable by **nondeterministic** multitype Turing machine in quasilinear time.
- For **completeness in NQL** we use reductions done by deterministic multitype Turing machines in quasilinear time.

Theorem (Schnorr 1978)

- **SAT** is NQL-complete,
- $3-$**colorability** is NQL-complete,
- **Anticlique** is NQL-complete,
- **Graph isomorphism** is in NQL.

Theorem (Schnorr 1978)

- **SAT** is NQL-complete,
- $3-$**colorability** is NQL-complete,
- **Anticlique** is NQL-complete,
- **Graph isomorphism** is in NQL.

Observation

For an algebra $\mathbf{A}$ with a finite number of basic operations $\mathrm{TERM\text{-}SAT}(\mathbf{A})$ is in NQL.

Theorem

For a two element algebra $\mathbf{A} = (2, f_1, f_2, \ldots, f_r)$

- $\mathrm{TERM\text{-}SAT}(\mathbf{A})$ *is NQL-complete if* $Clo(2, d, \neg) \subseteq Clo(\mathbf{A})$
- $\mathrm{TERM\text{-}SAT}(\mathbf{A})$ *is DQL, else.*

$$d(x, y, z) = (x \wedge y) \vee (y \wedge z) \vee (z \wedge x)$$

Theorem

For a three element primal algebra $\mathbf{A} = (3, f_1, f_2, \ldots, f_r)$ $\mathrm{TERM\text{-}SAT}(\mathbf{A})$ *is NQL-complete*

Theorem

For a three element primal algebra $\mathbf{A} = (3, f_1, f_2, \ldots, f_r)$ $\mathrm{TERM\text{-}SAT}(\mathbf{A})$ *is NQL-complete*

Theorem

For a three element algebra $\mathbf{A} = (3, f_1, f_2, \ldots, f_r)$ *such that* $Clo(\mathbf{A})$ *is maximal*

- $\mathrm{TERM\text{-}SAT}(\mathbf{A})$ *is NQL-complete if* $\mathrm{TERM\text{-}SAT}(\mathbf{A})$ *is NP-complete*
- $\mathrm{TERM\text{-}SAT}(\mathbf{A})$ *is in DQL, else*

Problem

Is $\mathrm{TERM\text{-}SAT}(\mathbf{A})$ *for every primal algebra* $\mathbf{A}$ *NQL-complete?*

Problem

Is $\mathrm{TERM\text{-}SAT}(\mathbf{A})$ *for every primal algebra* $\mathbf{A}$ *NQL-complete?*

Theorem

If the answer to the previous problem is positive then for an algebra $\mathbf{A} = (A, f_1, f_2, \ldots, f_r)$ *such that* $Clo(\mathbf{A})$ *is maximal*

- $\mathrm{TERM\text{-}SAT}(\mathbf{A})$ *is NQL-complete if* $\mathrm{TERM\text{-}SAT}(\mathbf{A})$ *is NP-complete,*
- $\mathrm{TERM\text{-}SAT}(\mathbf{A})$ *is in DQL, else.*

Theorem

Let C be a maximal clone on a set A generated by an order relation. For an algebra $\mathbf{A} = (A, f_1, f_2, \ldots, f_r)$ such that $Clo(\mathbf{A}) = C$

- $\mathrm{TERM\text{-}SAT}(\mathbf{A})$ *is NQL-complete if* $A > 2$
- $\mathrm{TERM\text{-}SAT}(\mathbf{A})$ *is in DQL, else*

Thank you