Amplification of algorithmic problems: decidable problems

Alexander Rybalov

Sobolev Institute of Mathematics, Omsk

September, 2016

Presburger Arithmetic (PA)

Definition

Presburger Arithmetic is the first-order theory of the structure $< \mathbb{N}, + >$.

Theorem (Presburger, 1929)

Presburger Arithmetic is decidable.

Theorem (Fischer, Rabin, 1974)

There is no algorithm for deciding of Presburger Arithmetic with worst-case complexity less than $2^{2^{cn}}$ with some universal constant $c > 0$.

Decidability Problem of PA

- INPUT: a first-order closed formula Φ of the signature $\{+\}$
- OUTPUT: YES, if Φ holds in $< \mathbb{N}, + >$;
  NO, otherwise

$\forall x \exists y (x = y + y)$ does not hold in $< \mathbb{N}, + >$
$\exists x \exists y (x = y + y)$ holds in $< \mathbb{N}, + >$

- INPUT: a first-order closed formula Φ of the signature $\{+\}$
- OUTPUT: YES, if Φ holds in $< \mathbb{N}, + >$;
  NO, otherwise
  I DON'T KNOW, sometimes
  (very rarely)

Asymptotic density

Definition

Let I be all inputs, I_n – all inputs of size n. **Asymptotic density** of set $S \subseteq I$

$$\mu(S) = \lim_{n \to \infty} \frac{|S \cap I_n|}{|I_n|}.$$

Asymptotic density

Definition

Let I be all inputs, I_n – all inputs of size n. **Asymptotic density** of set $S \subseteq I$

$$\mu(S) = \lim_{n \to \infty} \frac{|S \cap I_n|}{|I_n|}.$$

Remark

$\frac{|S \cap I_n|}{|I_n|}$ is the probability to get an input from S during random and uniform generation of inputs of size n.

Generic sets

Definition

A set $S \subseteq I$ is called

- generic if $\mu(S) = 1$
- negligible if $\mu(S) = 0$
- strongly negligible if there are constants $0 < \sigma < 1$ and $C > 0$ such that for every n

$$\frac{|S \cap I_n|}{|I_n|} < C\sigma^n,$$

- strongly generic if $S \setminus I$ is strongly negligible

Generic decidability

Definition

$S \subseteq I$ is (strongly) generically decidable (within polynomial time, exponential time, etc.) if there is a set G such that:

1. G is (strongly) generic
2. G is decidable (within polynomial, exponential time, etc.)
3. $S \cap G$ is decidable (within polynomial, exponential time, etc.)

Generic decidability

Definition

$S \subseteq I$ is (strongly) generically decidable (within polynomial time, exponential time, etc.) if there is a set G such that:

1. G is (strongly) generic
2. G is decidable (within polynomial, exponential time, etc.)
3. $S \cap G$ is decidable (within polynomial, exponential time, etc.)

Definition

A generic algorithm deciding S works on input a in the following way:
1. decides $a \in G$?
2. if $a \notin G$ then outputs "I DON'T KNOW"
3. if $a \in G$ then decides $a \in S \cap G$?

Generic decidability is not enough!

1. Problem Π feasible (polynomial) on G
2. G – generic and
$$\frac{|G \cap I_n|}{|I_n|} = \frac{n-1}{n}$$

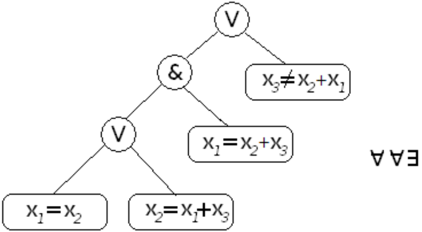
Polynomial algorithm for generation of **bad inputs** of Π:
Step 1. Generate random input x of size n.
Step 2. If $x \in G$ goto step 1, end otherwise.
Probability to get inputs only from G within n^2 rounds:

$$\left(\frac{n-1}{n}\right)^{n^2} = \left(\left(1 - \frac{1}{n}\right)^n\right)^n \to e^{-n}$$

Theorem

There is no strongly generic set of formulas on which Presburger Arithmetic is decidable in exponential time.

Arithmetical formulas are coded by binary trees (size is the number of vertices):



$$\forall x_1 \forall x_2 \exists x_3 (((x_1 = x_2) \vee (x_2 = x_1 + x_3))\&(x_1 = x_2 + x_3)) \vee (x_3 \neq x_2 + x_1)$$

Suppose we can check truthfulness of formulas from some strongly generic set G.
How to check a formula $\Phi \notin G$?
We can generate formulas from

$$AND(\Phi) = \{\Phi \wedge \Psi,\ \Psi - \text{arbitrary formula}\}$$

and

$$OR(\Phi) = \{\Phi \vee \Psi,\ \Psi - \text{arbitrary formula}\}$$

until gets a formula Δ from G.
If $\Delta = \Phi \wedge \Psi$ and Δ is true, then Φ is true!
If $\Delta = \Phi \vee \Psi$ and Δ is false, then Φ is false!
Otherwise continue to generate formulas from $AND(\Phi)$ and $OR(\Phi)$.

$$AND(\Phi)^+ = \{\Phi \wedge \Psi,\ \Psi - \text{arbitrary true formula}\},$$

$$OR(\Phi)^- = \{\Phi \vee \Psi,\ \Psi - \text{arbitrary false formula}\}.$$

Lemma

For any Φ sets $AND(\Phi)^+$ and $OR(\Phi)^-$ are not strongly negligible. Moreover, there is a constant $C > 0$ such that

$$\frac{|AND(\Phi)^+ \cap \mathcal{F}_n|}{|\mathcal{F}_n|} > \frac{C}{(16n)^{3k}}$$

for any $n > k$, where k is the size of Φ. The same bound is true for the set $OR(\Phi)^-$.

$\Rightarrow G \cap AND(\Phi)^+$ and $G \cap OR(\Phi)^-$ are not empty

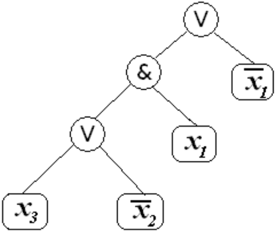
- INPUT: boolean formula $\Phi(x_1, \ldots, x_n)$
- OUTPUT:

  YES, if there exists $\bar{a} \in \{0, 1\}^n$ such that $\Phi(\bar{a}) = 1$,
  NO, otherwise.

Theorem (Cook, 1971)

SAT is NP-complete.

Representation of formulas



$$((x_3 \vee \bar{x}_2)\& x_1) \vee \bar{x}_1$$

Generic amplification of SAT

Theorem

If $P \neq NP$ and $BPP = P$ then there is no polynomial strongly generic set of formulas on which SAT is decidable in polynomial time.

Definition

Problem $S \in BPP$ if S solvable by an NP-machine such that

- If the answer is 'yes' then at least 2/3 of the computation paths accept.
- If the answer is 'no' then at most 1/3 of the computation paths accept.

Conjecture No. 2 in Computer Science

BPP=P

Generic amplification of SAT

1. We can check **satisfiability** of formulas from strongly generic set G.
2. How to check formula Φ not from G?
3. Generate random Ψ of appropriate size and check:

$$\Phi \wedge \Psi \in G \text{ and } \Phi \wedge \Psi \text{ satisfiable } \Rightarrow \Phi \text{ satisfiable}$$

$$\Phi \wedge \neg\Psi \in G \text{ and } \Phi \wedge \neg\Psi \text{ satisfiable } \Rightarrow \Phi \text{ satisfiable}$$

4. If Φ was decided END, else GOTO step 3.