Diophantine formulas

Emil Jeřábek

jerabek@math.cas.cz

http://math.cas.cz/~jerabek/

Institute of Mathematics of the Czech Academy of Sciences, Prague

Journées sur les Arithmétiques Faibles 35, June 2016, Lisbon

Undecidability theorems

The first incompleteness theorem
(Gödel–Rosser–Church–Kleene–Tarski–Mostowski–Robinson)

Theorem

Robinson's arithmetic Q is essentially undecidable

That is, any consistent extension of Q is undecidable

Undecidability for Σ_1-sentences

More specifically:

Theorem

If $T \supseteq Q$ is consistent, the sets of T-provable and T-refutable Σ_1 sentences are recursively inseparable

Corollary

If $T \supseteq Q$ is consistent,

- the set of Σ_1 sentences provable in T, and
- the set of Σ_1 sentences consistent with T

are undecidable

Diophantine formulas

Here: Σ_1 sentences = proxy for recursively enumerable sets

A much smaller class of sentences might do:

Theorem (Matiyasevich–Robinson–Davis–Putnam)

All recursively enumerable sets are Diophantine

Definition

A Diophantine formula $\varphi(\vec{x})$ is

$$\exists \vec{y}\, t(\vec{x}, \vec{y}) = s(\vec{x}, \vec{y})$$

where t and s are terms in the language $0, S, +, \cdot$

Diophantine undecidability

Formalized MRDP theorem:

Theorem [GD'82]

$I\Delta_0 + EXP$ proves that every Σ_1 formula is equivalent to a Diophantine formula

Corollary

If $T \supseteq I\Delta_0 + EXP$ is consistent,

- the set of T-provable Diophantine sentences, and
- the set of T-consistent Diophantine sentences

are undecidable

Without exponentiation?

Provable Diophantine sentences: boring answer

Theorem

If $T \supseteq Q$ is $\exists_1$-sound, the set of T-provable Diophantine sentences is undecidable

(Fails for unsound theories . . . but nevermind.)

Consistent Diophantine sentences: more interesting

Definition

$\mathrm{D}_T = \{\varphi$ Dioph. sent. : $T + \varphi$ consistent$\}$

IOW, Diophantine equations solvable in a model of T

Diophantine satisfiability

Decidability of D_T (T consistent):

- $T \supseteq I\Delta_0 + EXP$: undecidable [GD'82]
- $T \supseteq IU_1^-$: still undecidable! [Kaye'90,'93]
- Kaye's argument also works for $T \supseteq PV_1$
- $T = IOpen$: problem raised by [Shep'64]
  - wide open till this day; some partial results:
  - [Wilk'77]: characterization based on $\forall_1$-conservativity of $IOpen$ over DOR + $\exists$ homomorphism to $\hat{\mathbb{Z}}$
  - [vdD'81]: bivariate equations decidable
  - [Ote'90]: $IOpen + Lagrange$ $\forall_1$-conservative over $IOpen$
- $T = PA^-$ (discretely ordered rings): much like $IOpen$

Even weaker theories?

Main result of this talk:

Theorem

D_Q is decidable

Robinson's arithmetic

Q

(Q1) $Sx \neq 0$

(Q2) $Sx = Sy \rightarrow x = y$

(Q3) $x = 0 \vee \exists y\, Sy = x$

(Q4) $x + 0 = x$

(Q5) $x + Sy = S(x + y)$

(Q6) $x \cdot 0 = 0$

(Q7) $x \cdot Sy = x \cdot y + x$

Overview

The proof of decidability of D_Q involves several separate steps, some of them of independent interest

- black-hole models
- term splitting
- term normalization and term models
- universal fragment of Q

Black-hole model of Q

Model $\mathbb{N}^\infty \vDash Q$

- domain $\mathbb{N} \cup \{\infty\}$
- $S(\infty) = \infty + x = x + \infty = \infty \cdot x = x \cdot \infty = \infty$
  except for $\infty \cdot 0 = 0$

Terms evaluate to ∞ at $\vec{\infty}$ unless prevented by axioms!

$$\mathbb{N}^\infty \vDash t(\infty, \dots, \infty) = n \neq \infty \implies Q \vdash t(x_1, \dots, x_k) = \underline{n}$$

Lemma

D_Q reduces to Q-satisfiability of equations of the form

$$t(\vec{x}) = \underline{n}$$

Term splitting

Idea

Simplify the LHS in $t(\vec{x}) = \underline{n}$ down to variables:

- $t + s = \underline{n} \iff t = \underline{k}$ & $s = \underline{m}$ for some $k + m = n$
- $t \cdot s = \underline{0} \iff t = \underline{0}$ or $s = \underline{0}$
- for $n \neq 0$:
  $t \cdot s = \underline{n} \iff t = \underline{k}$ & $s = \underline{m}$ for some $km = n$

nondeterministic reduction
of satisfiability of $t(\vec{x}) = \underline{n}$
to satisfiability of a system of equations $x_i = \underline{n_i}$
$\implies$ easy to check

Term splitting (cont'd)

Problem

This reduction not sound in Q!

$$Q \nvdash t = 0 \to t \cdot s = 0$$

Proposition

D_T is decidable for $T = Q + \forall x\,(0 \cdot x = 0)$

Lemma

D_Q reduces to Q-satisfiability of systems of equations

$$0 \cdot t_i(\vec{x}) = \underline{n_i}$$

Simultaneous division by zero

The problem is subtle

Example

The system

$$\begin{aligned} 0 \cdot (x + \underline{2}) &= \underline{5} \\ 0 \cdot (y + 0 \cdot x) &= \underline{7} \\ 0 \cdot Sy &= \underline{4} \end{aligned}$$

is Q-unsatisfiable, but each pair of equations is satisfiable

Witnessing satisfiability

We need a convenient supply of models of Q

Let E be a set of equations we want to satisfy

Obvious idea

Build a "free" term model of E

- elements = (equivalence classes of) terms
- identify terms only when forced so by $Q + E$
- might collapse or otherwise misbehave ...

Let's find out when it works

Term normalization

Lemma

The term rewriting system R_Q given by

$$\begin{aligned} t + 0 &\longrightarrow t \\ t + Ss &\longrightarrow S(t + s) \\ t \cdot 0 &\longrightarrow 0 \\ t \cdot Ss &\longrightarrow t \cdot s + t \end{aligned}$$

is strongly normalizing and confluent

R_Q-normal terms are of the form $S^n t$,
where t is 0 or "irreducible"

Normalization with zero multiples

Definition

Assume

- $\{t_i : i < k\}$ are irreducible terms s.t. $0 \cdot t_i \not\trianglelefteq t_j$
- $\{n_i : i < k\} \subseteq \mathbb{N}$

$R_{\vec{t},\vec{n}} = R_Q +$

$$0 \cdot t_i \longrightarrow S^{n_i}0 \qquad \text{for } i < k$$

Lemma

$R_{\vec{t},\vec{n}}$ is still strongly normalizing and confluent

Models with zero multiples

Lemma

Assume

- $\{t_i : i < k\}$ are irreducible terms s.t. $0 \cdot t_i \not\subseteq t_j$
- $\{n_i : i < k\} \subseteq \mathbb{N}$

Then $\{0 \cdot t_i = \underline{n_i} : i < k\}$ is satisfiable in a model of Q

Idea: model consisting of $R_{\vec{t},\vec{n}}$-normal terms

Problem

Predecessors!

$\Longrightarrow$ need to find out what models embed in models of Q

Universal fragment of Q

All but one axiom of Q are universal:

(Q1) $Sx \neq 0$

(Q2) $Sx = Sy \to x = y$

(Q3) $x = 0 \vee \exists y\, Sy = x$

(Q4) $x + 0 = x$

(Q5) $x + Sy = S(x + y)$

(Q6) $x \cdot 0 = 0$

(Q7) $x \cdot Sy = x \cdot y + x$

But there's more to it:

Universal fragment of Q

Lemma

$\forall_1$ consequences of Q are axiomatized by Q124–7 and

$$x + y = \underline{n} \to \bigvee_{m \le n} y = \underline{m}$$

$$x \cdot y = \underline{n} \to x = 0 \vee \bigvee_{m \le n} y = \underline{m}$$

for $n \in \mathbb{N}$

Our term models satisfy these axioms $\implies$ all is well

Putting it all together

Lemma

An equation $t(\vec{x}) = \underline{n}$ is Q-solvable iff it has a witness:

- partial labelling of subterms of t by numbers $m \le n$
- t is labelled n
- suitable consistency conditions

Theorem

D_Q is decidable

Complexity: upper bound

Follow-up question

What is the computational complexity of D_Q?

Upper bound:

- witnesses for solvability: involve term normalization
- naively exponential: constant terms $\to$ unary numerals
- using compact representation: polynomial time

Theorem

D_Q is in NP

Complexity: lower bound

Theorem [MA'78]

The following problem is NP-complete:

Given $a, b \in \mathbb{N}$ in binary, are there $x, y \in \mathbb{N}$ s.t.

$$x^2 + ay = b\ ?$$

Corollary

If $T \supseteq Q$ is consistent, D_T is NP-hard

Theorem

D_Q is NP-complete

Problems

Question

Are D_{PA^-} or D_{IOpen} decidable?

Question

Is Q-satisfiability of existential sentences decidable?

Thank you for attention!

References

- L. van den Dries: Which curves over **Z** have points with coordinates in a discrete ordered ring?, Trans. AMS 264 (1981), 181–189
- H. Gaifman, C. Dimitracopoulos: Fragments of Peano's arithmetic and the MRDP theorem, in: Logic and algorithmic, Univ. Genève, 1982, 187–206
- E. Jeřábek: Division by zero, arXiv:1604.07309 [math.LO]
- R. Kaye: Diophantine induction, APAL 46 (1990), 1–40
- R. Kaye: Hilbert's tenth problem for weak theories of arithmetic, APAL 61 (1993), 63–73

References (cont'd)

- K. L. Manders, L. M. Adleman: *NP*-complete decision problems for binary quadratics, J. Comp. Sys. Sci. 16 (1978), 168–184
- M. Otero: On Diophantine equations solvable in models of open induction, JSL 55 (1990), 779–786
- rainmaker: Decidability of diophantine equation in a theory, MathOverflow, 2014, `http://mathoverflow.net/q/194491`
- J. C. Shepherdson: A nonstandard model for a free variable fragment of number theory, Bul. Acad. Pol. Sci., Sér. Math. Astron. Phys. 12 (1964), 79–86
- A. J. Wilkie: Some results and problems on weak systems of arithmetic, in: Logic Colloquium '77, North-Holland, 1978, 285–296