Decidability of Diophantine satisfiability in theories close to IOpen

Fabian Achammer   Stefan Hetzl

TU Wien

42nd Weak Arithmetic Days, Karlovassi, Greece
September 26, 2023

Diophantine satisfiability

Definition (Diophantine satisfiability decision problem)

Let $L := \{0, \mathrm{s}, +, \cdot\}$ be the base language of arithmetic and let T be a theory in a language $L' \supseteq L$. Is

$$D_T := \left\{ (t(\bar{x}), u(\bar{x})) \;\middle|\; \begin{array}{l} t(\bar{x}), u(\bar{x}) \text{ are } L\text{-terms such that} \\ T \cup \{\exists \bar{x}\, t(\bar{x}) = u(\bar{x})\} \text{ is consistent} \end{array} \right\}$$

decidable?

Diophantine satisfiability

Definition (Diophantine satisfiability decision problem)

Let $L := \{0, \mathrm{s}, +, \cdot\}$ be the base language of arithmetic and let T be a theory in a language $L' \supseteq L$. Is

$$D_T := \left\{ (t(\bar{x}), u(\bar{x})) \;\middle|\; \begin{array}{l} t(\bar{x}), u(\bar{x}) \text{ are } L\text{-terms such that} \\ T \cup \{\exists \bar{x}\, t(\bar{x}) = u(\bar{x})\} \text{ is consistent} \end{array} \right\}$$

decidable?

Observation

$D_T = \{(t, u) \mid T \vdash \forall \bar{x}\, t \neq u\}^c$. *Thus* D_T *is decidable if and only if the set of* T*-refutable Diophantine equations is decidable.*

Current results

- D_Q is decidable where Q is Robinson arithmetic[1]

[1] Jeř16.
[2] GD82.
[3] Kay93.
[4] She64.

Current results

- D_Q is decidable where Q is Robinson arithmetic[1]
- D_T is undecidable for theories T which extend $I\Delta_0 + EXP$ (consequence of the MRDP theorem)[2]

[1] Jeř16.
[2] GD82.
[3] Kay93.
[4] She64.

Current results

- D_Q is decidable where Q is Robinson arithmetic[1]
- D_T is undecidable for theories T which extend $I\Delta_0 + EXP$ (consequence of the MRDP theorem)[2]
- D_T is undecidable for theories T which extend IU_1^-[3]

[1] Jeř16.
[2] GD82.
[3] Kay93.
[4] She64.

Current results

- D_Q is decidable where Q is Robinson arithmetic[1]
- D_T is undecidable for theories T which extend $I\Delta_0 + EXP$ (consequence of the MRDP theorem)[2]
- D_T is undecidable for theories T which extend IU_1^-[3]
- Decidability of D_{IOpen} where $IOpen$ is theory of open induction over $\{0, \mathrm{s}, +, \cdot, \leq\}$ is long-standing open problem[4]

[1] Jeř16.
[2] GD82.
[3] Kay93.
[4] She64.

Current results

- D_Q is decidable where Q is Robinson arithmetic[1]
- D_T is undecidable for theories T which extend $I\Delta_0 + EXP$ (consequence of the MRDP theorem)[2]
- D_T is undecidable for theories T which extend IU_1^{-}[3]
- Decidability of D_{IOpen} where *IOpen* is theory of open induction over $\{0, \mathrm{s}, +, \cdot, \leq\}$ is long-standing open problem[4]
- We show Diophantine decidability of the theory of open induction over $\{0, \mathrm{s}, \mathrm{p}, +, \cdot\}$

[1] Jeř16.
[2] GD82.
[3] Kay93.
[4] She64.

Outline

Theories

Proof strategy

Decidability

Conclusion

IOp

- Language $L_{\mathsf{p}} := \{0, \mathsf{s}, +, \cdot, \mathsf{p}\}$

IOp

- Language $L_{\mathrm{p}} := \{0, \mathrm{s}, +, \cdot, \mathrm{p}\}$
- Base theory A: universal closures of

$$\mathrm{s}(x) \neq 0 \qquad (A_1)$$

IOp

- Language $L_{\mathrm{p}} := \{0, \mathrm{s}, +, \cdot, \mathrm{p}\}$
- Base theory A: universal closures of

$$\mathrm{s}(x) \neq 0 \qquad (A_1)$$

$$\mathrm{p}(0) = 0 \qquad (A_2)$$

$$\mathrm{p}(\mathrm{s}(x)) = x \qquad (A_3)$$

IOp

- Language $L_{\mathsf{p}} := \{0, \mathsf{s}, +, \cdot, \mathsf{p}\}$
- Base theory A: universal closures of

$$\begin{aligned} \mathsf{s}(x) &\neq 0 && (A_1)\\ \mathsf{p}(0) &= 0 && (A_2)\\ \mathsf{p}(\mathsf{s}(x)) &= x && (A_3)\\ x + 0 &= x && (A_4)\\ x + \mathsf{s}(y) &= \mathsf{s}(x + y) && (A_5) \end{aligned}$$

IOp

- Language $L_{\mathrm{p}} := \{0, \mathrm{s}, +, \cdot, \mathrm{p}\}$
- Base theory A: universal closures of

$$
\begin{aligned}
\mathrm{s}(x) &\neq 0 && (A_1)\\
\mathrm{p}(0) &= 0 && (A_2)\\
\mathrm{p}(\mathrm{s}(x)) &= x && (A_3)\\
x + 0 &= x && (A_4)\\
x + \mathrm{s}(y) &= \mathrm{s}(x + y) && (A_5)\\
x \cdot 0 &= 0 && (A_6)\\
x \cdot \mathrm{s}(y) &= x \cdot y + x && (A_7)
\end{aligned}
$$

- Induction axiom $I(\varphi(x, \bar{z}))$

$$\forall \bar{z}\ (\varphi(0, \bar{z}) \to \forall x\, (\varphi(x, \bar{z}) \to \varphi(\mathrm{s}(x), \bar{z})) \to \forall x\, \varphi(x, \bar{z}))$$

IOp

- Language $L_{\mathrm{p}} := \{0, \mathrm{s}, +, \cdot, \mathrm{p}\}$
- Base theory A: universal closures of

$$\begin{aligned}
\mathrm{s}(x) &\neq 0 && (A_1)\\
\mathrm{p}(0) &= 0 && (A_2)\\
\mathrm{p}(\mathrm{s}(x)) &= x && (A_3)\\
x + 0 &= x && (A_4)\\
x + \mathrm{s}(y) &= \mathrm{s}(x+y) && (A_5)\\
x \cdot 0 &= 0 && (A_6)\\
x \cdot \mathrm{s}(y) &= x \cdot y + x && (A_7)
\end{aligned}$$

- Induction axiom $I(\varphi(x, \bar{z}))$

$$\forall \bar{z}\ (\varphi(0, \bar{z}) \to \forall x\, (\varphi(x, \bar{z}) \to \varphi(\mathrm{s}(x), \bar{z})) \to \forall x\, \varphi(x, \bar{z}))$$

- $\mathrm{IOp} := A \cup \{I(\varphi) \mid \varphi \text{ quantifer-free } L_{\mathrm{p}}\text{-formula}\}$

IOp

Result by Shepherdson[5]

IOp is equivalent to A together with universal closures of

$$x = 0 \vee x = \mathsf{s}(\mathsf{p}(x)) \quad (B_1)$$

[5] She67.

IOp

Result by Shepherdson[5]

IOp is equivalent to A together with universal closures of

$$x = 0 \vee x = \mathsf{s}(\mathsf{p}(x)) \quad (B_1)$$

$$x + y = y + x \quad (B_2)$$

$$(x + y) + z = x + (y + z) \quad (B_3)$$

[5] She67.

IOp

Result by Shepherdson[5]

IOp is equivalent to A together with universal closures of

$$x = 0 \lor x = \mathrm{s}(\mathrm{p}(x)) \qquad (B_1)$$

$$x + y = y + x \qquad (B_2)$$

$$(x + y) + z = x + (y + z) \qquad (B_3)$$

$$x + y = x + z \to y = z \qquad (B_4)$$

[5] She67.

IOp

Result by Shepherdson[5]

IOp is equivalent to A together with universal closures of

$$x = 0 \vee x = \mathrm{s}(\mathrm{p}(x)) \qquad (B_1)$$

$$x + y = y + x \qquad (B_2)$$

$$(x + y) + z = x + (y + z) \qquad (B_3)$$

$$x + y = x + z \to y = z \qquad (B_4)$$

$$x \cdot y = y \cdot x \qquad (B_5)$$

$$x \cdot (y \cdot z) = (x \cdot y) \cdot z \qquad (B_6)$$

[5] She67.

IOp

Result by Shepherdson[5]

IOp is equivalent to A together with universal closures of

$$x = 0 \vee x = \mathrm{s}(\mathrm{p}(x)) \quad (B_1)$$
$$x + y = y + x \quad (B_2)$$
$$(x + y) + z = x + (y + z) \quad (B_3)$$
$$x + y = x + z \rightarrow y = z \quad (B_4)$$
$$x \cdot y = y \cdot x \quad (B_5)$$
$$x \cdot (y \cdot z) = (x \cdot y) \cdot z \quad (B_6)$$
$$x \cdot (y + z) = x \cdot y + x \cdot z \quad (B_7)$$

[5] She67.

IOp

Result by Shepherdson[5]

IOp is equivalent to A together with universal closures of

$$
\begin{aligned}
x = 0 \vee x = \mathsf{s}(\mathsf{p}(x)) \quad & (B_1) \\
x + y = y + x \quad & (B_2) \\
(x + y) + z = x + (y + z) \quad & (B_3) \\
x + y = x + z \rightarrow y = z \quad & (B_4) \\
x \cdot y = y \cdot x \quad & (B_5) \\
x \cdot (y \cdot z) = (x \cdot y) \cdot z \quad & (B_6) \\
x \cdot (y + z) = x \cdot y + x \cdot z \quad & (B_7)
\end{aligned}
$$

and

$$dx = dy \rightarrow \bigvee_{i=0}^{d-1} (z + i) \cdot x = (z + i) \cdot y \ (C'_d) \quad \text{for } d \geq 2.$$

[5] She67.

Related theories

- $AB := \{A_1, \ldots, A_7, B_1, \ldots, B_7\}$

[6] Sch88.

Related theories

- $AB := \{A_1, \ldots, A_7, B_1, \ldots, B_7\}$
- $AB^\exists := (AB \setminus \{A_2, A_3, B_1\}) \cup \left\{B_1^\exists\right\}$ where $B_1^\exists$ is the universal closure of

$$x = 0 \vee \exists y \, x = \mathsf{s}(y)$$

[6] Sch88.

Related theories

- $AB := \{A_1, \ldots, A_7, B_1, \ldots, B_7\}$
- $AB^{\exists} := (AB \setminus \{A_2, A_3, B_1\}) \cup \{B_1^{\exists}\}$ where $B_1^{\exists}$ is the universal closure of
$$x = 0 \vee \exists y\, x = \mathsf{s}(y)$$
- $ABC_d := AB^{\exists} \cup \{C_d \mid d \geq 2\}$ where C_d is the universal closure of
$$dx = dy \rightarrow x = y$$

[6] Sch88.

Related theories

- $AB := \{A_1, \ldots, A_7, B_1, \ldots, B_7\}$
- $AB^{\exists} := (AB \setminus \{A_2, A_3, B_1\}) \cup \{B_1^{\exists}\}$ where $B_1^{\exists}$ is the universal closure of
$$x = 0 \vee \exists y\, x = \mathsf{s}(y)$$
- $ABC_d := AB^{\exists} \cup \{C_d \mid d \geq 2\}$ where C_d is the universal closure of
$$dx = dy \to x = y$$

Theorem (Schmerl[6])

$D_{\mathsf{IOp}} = D_{AB} = D_{AB^{\exists}} = D_{ABC_d}$

[6] Sch88.

Related theories

- $AB := \{A_1, \dots, A_7, B_1, \dots, B_7\}$
- $AB^\exists := (AB \setminus \{A_2, A_3, B_1\}) \cup \{B_1^\exists\}$ where $B_1^\exists$ is the universal closure of
$$x = 0 \lor \exists y\, x = \mathrm{s}(y)$$
- $ABC_d := AB^\exists \cup \{C_d \mid d \geq 2\}$ where C_d is the universal closure of
$$dx = dy \to x = y$$

Theorem (Schmerl[6])

$D_{\mathrm{IOp}} = D_{AB} = D_{AB^\exists} = D_{ABC_d}$

Main Theorem

D_{IOp} is decidable.

---

[6] Sch88.

Outline

Theories

Proof strategy

Decidability

Conclusion

Proof strategy

- By result from Schmerl it suffices to show decidability of $D_{AB^{\exists}}$

Proof strategy

- By result from Schmerl it suffices to show decidability of $D_{AB^{\exists}}$
- Construct a specialized proof calculus $\mathcal{AB}$ operating on $\mathbb{Z}[V]$

Proof strategy

- By result from Schmerl it suffices to show decidability of $D_{AB^\exists}$
- Construct a specialized proof calculus $\mathcal{AB}$ operating on $\mathbb{Z}[V]$
- Show soundness and completeness of $\mathcal{AB}$ with respect to Diophantine satisfiability in $AB^\exists$

Proof strategy

- By result from Schmerl it suffices to show decidability of $D_{AB^{\exists}}$
- Construct a specialized proof calculus $\mathcal{AB}$ operating on $\mathbb{Z}[V]$
- Show soundness and completeness of $\mathcal{AB}$ with respect to Diophantine satisfiability in $AB^{\exists}$
- Show decidability of $\mathcal{AB}$

Terms as polynomials

- Let V be the set of variables.
- To a term t we assign the polynomial $\mathrm{poly}(t) \in \mathbb{N}[V]$ it evaluates to.
- To a $p \in \mathbb{N}[V]$ we assign a term $\underline{p}$ (by choosing a fixed ordering on V) such that

Lemma

For every term t we have $AB^{\exists} \vdash t = \underline{\mathrm{poly}(t)}$.

Equations as polynomials

- For $p \in \mathbb{Z}[V]$ and a monomial m we write $[m]p$ for the coefficient of m in p.

Equations as polynomials

- For $p \in \mathbb{Z}[V]$ and a monomial m we write $[m]p$ for the coefficient of m in p.
- We set

$$p^+ := \sum_{m:[m]p>0} ([m]p)m \qquad p^- := -\sum_{m:[m]p<0} ([m]p)m.$$

Equations as polynomials

- For $p \in \mathbb{Z}[V]$ and a monomial m we write $[m]p$ for the coefficient of m in p.
- We set

$$p^+ := \sum_{m:[m]p>0} ([m]p)m \qquad p^- := -\sum_{m:[m]p<0} ([m]p)m.$$

Consider the additive cancellation axiom

$$x + y = x + z \to y = z \quad (B_4)$$

Lemma

Let t, u be terms and set $p := \mathrm{poly}(t) - \mathrm{poly}(u)$. Then $AB^{\exists} \vdash t = u \leftrightarrow \underline{p^+} = \underline{p^-}$

Calculus $\mathcal{AB}$

signed rule

Definition (signed polynomial)

$p \in \mathbb{Z}[V]$ is *positively signed* if all coefficients of p are non-negative and the constant coefficient is positive.

Calculus $\mathcal{AB}$

signed rule

Definition (signed polynomial)

$p \in \mathbb{Z}[V]$ is *positively signed* if all coefficients of p are non-negative and the constant coefficient is positive.
p is *negatively signed* if $-p$ is positively signed.

Calculus $\mathcal{AB}$

signed rule

Definition (signed polynomial)

$p \in \mathbb{Z}[V]$ is *positively signed* if all coefficients of p are non-negative and the constant coefficient is positive.
p is *negatively signed* if $-p$ is positively signed.
p is *signed* if it is positively or negatively signed

Calculus $\mathcal{AB}$

signed rule

Definition (signed polynomial)

$p \in \mathbb{Z}[V]$ is *positively signed* if all coefficients of p are non-negative and the constant coefficient is positive.
p is *negatively signed* if $-p$ is positively signed.
p is *signed* if it is positively or negatively signed

Consider the axiom A_1

$$\mathrm{s}(x) \neq 0$$

We translate this into an initial inference rule on polynomials

$$\frac{}{p}\ \textit{signed}$$

where $p \in \mathbb{Z}[V]$ is signed

Calculus $\mathcal{AB}$

zero-or-successor rule

Consider the axiom $B_1^\exists$, the universal closure of

$$x = 0 \vee \exists y\, x = \mathrm{s}(y)$$

In $AB^\exists \setminus \{B_1^\exists\}$, instead of considering all possible instances of $B_1^\exists$ it is enough consider variable instances:

Proposition

Let t be a term and let $x_1, \ldots, x_n$ be all its free variables. Then

$$AB^\exists \setminus \left\{B_1^\exists\right\}, B_1^\exists[x_1], \ldots, B_1^\exists[x_n] \vdash B_1^\exists[t]$$

Calculus $\mathcal{AB}$

zero-or-successor rule

Let X be a set of variables. We set

$$\Theta(X) := \{\theta : X \to \mathbb{N}[V] \mid \text{ for all } x \in X : \theta(x) \in \{0, x+1\}\}$$

Calculus $\mathcal{AB}$

zero-or-successor rule

Let X be a set of variables. We set

$$\Theta(X) := \{\theta : X \to \mathbb{N}[V] \mid \text{ for all } x \in X : \theta(x) \in \{0, x+1\}\}$$

Let $\mathrm{vars}(p)$ be the set of variables that occur in $p \in \mathbb{Z}[V]$. We translate $B_1^{\exists}$ into an inference rule

$$\frac{p\theta \text{ for all } \theta \in \Theta(\mathrm{vars}(p))}{p} \; \textit{zero-or-successor}$$

where p is not signed.

Calculus $\mathcal{AB}$

Example

Let $\mathcal{AB}$ be the proof calculus operating on $\mathbb{Z}[V]$ with the inference rules *signed* and *zero-or-successor*.
We abbreviate *signed* as s and *zero-or-successor* as z:

$$\frac{}{2xy - 2x - 2y + 1}\ z$$

Calculus $\mathcal{AB}$

Example

Let $\mathcal{AB}$ be the proof calculus operating on $\mathbb{Z}[V]$ with the inference rules *signed* and *zero-or-successor*.
We abbreviate *signed* as s and *zero-or-successor* as z:

$$\dfrac{\dfrac{}{1}\,s \qquad \dfrac{}{-2y-1}\,s \qquad \dfrac{}{-2x-1}\,s \qquad \dfrac{}{2xy-1}\,z}{2xy-2x-2y+1}\,z$$

Calculus $\mathcal{AB}$

Example

Let $\mathcal{AB}$ be the proof calculus operating on $\mathbb{Z}[V]$ with the inference rules *signed* and *zero-or-successor*.
We abbreviate *signed* as s and *zero-or-successor* as z:

$$\dfrac{\dfrac{}{1}\,s \quad \dfrac{}{-2y-1}\,s \quad \dfrac{}{-2x-1}\,s \quad \dfrac{\dfrac{}{-1}\,s \quad \dfrac{}{-1}\,s \quad \dfrac{}{-1}\,s \quad \dfrac{}{2xy+2x+2y+1}\,s}{2xy-1}\,z}{2xy-2x-2y+1}\,z$$

Theorem (Soundness and Completeness of $\mathcal{AB}$)

$AB \vdash \forall \bar{x}\, t \neq u$ *if and only if* $\mathcal{AB} \vdash \mathrm{poly}(t) - \mathrm{poly}(u)$

Proof sketch.

Do proof translations in both directions. $\square$

Outline

Theories

Proof strategy

Decidability

Conclusion

Tilted polynomials

Definition (tilted polynomial)

We say $p \in \mathbb{Z}[V]$ is *positively tilted* if for all monomials m^- with $[m^-]p^- \neq 0$ there exists a monomial m^+ with $[m^+]p^+ \neq 0$ such that m^- strictly divides m^+.

Tilted polynomials

Definition (tilted polynomial)

We say $p \in \mathbb{Z}[V]$ is *positively tilted* if for all monomials m^- with $[m^-]p^- \neq 0$ there exists a monomial m^+ with $[m^+]p^+ \neq 0$ such that m^- strictly divides m^+.

We say p is *negatively tilted*, if $-p$ is positively tilted.

Tilted polynomials

Definition (tilted polynomial)

We say $p \in \mathbb{Z}[V]$ is *positively tilted* if for all monomials m^- with $[m^-]p^- \neq 0$ there exists a monomial m^+ with $[m^+]p^+ \neq 0$ such that m^- strictly divides m^+.

We say p is *negatively tilted*, if $-p$ is positively tilted.

If p is positively or negatively tilted, we say p is *tilted*.

Example

$$\left.\begin{array}{r} x^2 - x + 1 \\ xy - 2x - 2y \end{array}\right\} \text{tilted}$$

Tilted polynomials

Definition (tilted polynomial)

We say $p \in \mathbb{Z}[V]$ is *positively tilted* if for all monomials m^- with $[m^-]p^- \neq 0$ there exists a monomial m^+ with $[m^+]p^+ \neq 0$ such that m^- strictly divides m^+.

We say p is *negatively tilted*, if $-p$ is positively tilted.

If p is positively or negatively tilted, we say p is *tilted*.

Example

$$\left.\begin{array}{r} x^2 - x + 1 \\ xy - 2x - 2y \end{array}\right\} \text{tilted}$$

$$\left.\begin{array}{r} 0 \\ x - y \\ xy - x^2 - y^2 \end{array}\right\} \text{not tilted}$$

Closure property in $\mathcal{AB}$

Lemma
If $p \in \mathbb{Z}[V]$ is positively (negatively) signed, then p is positively (negatively) tilted.

Lemma
Let $p \in \mathbb{Z}[V]$ and $\theta(x) := x + 1$. Then p is positively (negatively) tilted if and only if $p\theta$ is positively (negatively) tilted.

Corollary
If $\mathcal{AB} \vdash p$, then p is tilted.

An order on $\mathbb{N}[V]$

- For $p \in \mathbb{N}[V]$ we write $\mathrm{mons}(p)$ for the multiset of monomials where each monomial m occurs $[m]p$ many times.

An order on $\mathbb{N}[V]$

- For $p \in \mathbb{N}[V]$ we write $\mathrm{mons}(p)$ for the multiset of monomials where each monomial m occurs $[m]p$ many times.
- For $p, q \in \mathbb{N}[V]$ we write $p <_{mon} q$ if for all $m \in \mathrm{mons}(p) - \mathrm{mons}(q)$ there exists an $m' \in \mathrm{mons}(q) - \mathrm{mons}(p)$ such that m strictly divides m'.

An order on $\mathbb{N}[V]$

- For $p \in \mathbb{N}[V]$ we write $\mathrm{mons}(p)$ for the multiset of monomials where each monomial m occurs $[m]p$ many times.
- For $p, q \in \mathbb{N}[V]$ we write $p <_{mon} q$ if for all $m \in \mathrm{mons}(p) - \mathrm{mons}(q)$ there exists an $m' \in \mathrm{mons}(q) - \mathrm{mons}(p)$ such that m strictly divides m'.
- Note: $p \in \mathbb{Z}[V]$ is positively (negatively) tilted if and only if $p^+ >_{mon} p^-$ ($p^- >_{mon} p^+$).

An order on $\mathbb{N}[V]$

- For $p \in \mathbb{N}[V]$ we write $\text{mons}(p)$ for the multiset of monomials where each monomial m occurs $[m]p$ many times.
- For $p, q \in \mathbb{N}[V]$ we write $p <_{mon} q$ if for all $m \in \text{mons}(p) - \text{mons}(q)$ there exists an $m' \in \text{mons}(q) - \text{mons}(p)$ such that m strictly divides m'.
- Note: $p \in \mathbb{Z}[V]$ is positively (negatively) tilted if and only if $p^+ >_{mon} p^-$ $(p^- >_{mon} p^+)$.
- $<_{mon}$ is the multiset extension of strict divisibility of monomials.

An order on $\mathbb{N}[V]$

- For $p \in \mathbb{N}[V]$ we write $\text{mons}(p)$ for the multiset of monomials where each monomial m occurs $[m]p$ many times.
- For $p, q \in \mathbb{N}[V]$ we write $p <_{mon} q$ if for all $m \in \text{mons}(p) - \text{mons}(q)$ there exists an $m' \in \text{mons}(q) - \text{mons}(p)$ such that m strictly divides m'.
- Note: $p \in \mathbb{Z}[V]$ is positively (negatively) tilted if and only if $p^+ >_{mon} p^-$ ($p^- >_{mon} p^+$).
- $<_{mon}$ is the multiset extension of strict divisibility of monomials.

Lemma

$<_{mon}$ is a well-founded partial order on $\mathbb{N}[V]$.

An order on tilted polynomials

- For $p, q \in \mathbb{Z}[V]$ we write $p \prec_{vars} q$ if $|\mathrm{vars}(p)| < |\mathrm{vars}(q)|$.

An order on tilted polynomials

- For $p, q \in \mathbb{Z}[V]$ we write $p \prec_{vars} q$ if $|\mathrm{vars}(p)| < |\mathrm{vars}(q)|$.
- For tilted p we set $\min(p) := \min_{<_{mon}}(p^+, p^-)$.

An order on tilted polynomials

- For $p, q \in \mathbb{Z}[V]$ we write $p \prec_{vars} q$ if $|\text{vars}(p)| < |\text{vars}(q)|$.
- For tilted p we set $\min(p) := \min_{<_{mon}}(p^+, p^-)$.
- For tilted p, q we write $p \prec_{mon} q$ if $\min(p) <_{mon} \min(q)$.

An order on tilted polynomials

- For $p, q \in \mathbb{Z}[V]$ we write $p \prec_{vars} q$ if $|\mathrm{vars}(p)| < |\mathrm{vars}(q)|$.
- For tilted p we set $\min(p) := \min_{<_{mon}}(p^+, p^-)$.
- For tilted p, q we write $p \prec_{mon} q$ if $\min(p) <_{mon} \min(q)$.
- Let $\prec_t$ to be the lexicographic product $\prec_{vars} \times \prec_{mon}$.

An order on tilted polynomials

- For $p, q \in \mathbb{Z}[V]$ we write $p \prec_{vars} q$ if $|\text{vars}(p)| < |\text{vars}(q)|$.
- For tilted p we set $\min(p) := \min_{<_{mon}}(p^+, p^-)$.
- For tilted p, q we write $p \prec_{mon} q$ if $\min(p) <_{mon} \min(q)$.
- Let $\prec_t$ to be the lexicographic product $\prec_{vars} \times \prec_{mon}$.

Lemma

$\prec_{vars}$, $\prec_{mon}$ and $\prec_t$ are well-founded partial orders on tilted polynomials.

Proof candidate trees

Definition

For $p \in \mathbb{Z}[V]$ we recursively define the *proof candidate tree of p* as the smallest tree $T(p)$ such that

Proof candidate trees

Definition

For $p \in \mathbb{Z}[V]$ we recursively define the *proof candidate tree of p* as the smallest tree $T(p)$ such that

- p is a node of $T(p)$

Proof candidate trees

Definition

For $p \in \mathbb{Z}[V]$ we recursively define the *proof candidate tree of* p as the smallest tree $T(p)$ such that

- p is a node of $T(p)$ and
- if q is a node of $T(p)$, q is tilted and not signed, then $T(p)$ contains all nodes $q\theta$ for $\theta \in \Theta(\mathsf{vars}(q))$.

Proof candidate trees

Definition

For $p \in \mathbb{Z}[V]$ we recursively define the *proof candidate tree of* p as the smallest tree $T(p)$ such that

- p is a node of $T(p)$ and
- if q is a node of $T(p)$, q is tilted and not signed, then $T(p)$ contains all nodes $q\theta$ for $\theta \in \Theta(\text{vars}(q))$. In that case $(q, q\theta)$ is an edge of $T(p)$.

Proof candidate trees

Finiteness of $T(p)$

Lemma

$T(p)$ is finitely branching.

Proof candidate trees

Finiteness of $T(p)$

Lemma

$T(p)$ is finitely branching.

Lemma

Let $p \in \mathbb{Z}[V]$ be tilted and let $\theta \in \Theta(\mathrm{vars}(p))$. Then $p \succ_t p\theta$.

Proof candidate trees

Finiteness of $T(p)$

Lemma

$T(p)$ is finitely branching.

Lemma

Let $p \in \mathbb{Z}[V]$ be tilted and let $\theta \in \Theta(\mathrm{vars}(p))$. Then $p \succ_t p\theta$.

Proposition

$T(p)$ is finite.

Proof.

We use Kőnig's lemma:

Proof candidate trees

Finiteness of $T(p)$

Lemma

$T(p)$ is finitely branching.

Lemma

Let $p \in \mathbb{Z}[V]$ be tilted and let $\theta \in \Theta(\mathrm{vars}(p))$. Then $p \succ_t p\theta$.

Proposition

$T(p)$ is finite.

Proof.

We use Kőnig's lemma:

- $T(p)$ is finitely branching.

Proof candidate trees

Finiteness of $T(p)$

Lemma

$T(p)$ is finitely branching.

Lemma

Let $p \in \mathbb{Z}[V]$ be tilted and let $\theta \in \Theta(\mathrm{vars}(p))$. Then $p \succ_t p\theta$.

Proposition

$T(p)$ is finite.

Proof.

We use Kőnig's lemma:

- $T(p)$ is finitely branching.
- If a branch in $T(p)$ only contains tilted polynomials, then it is well-ordered by $\prec_t$ which means it is finite.

Proof candidate trees

Finiteness of $T(p)$

Lemma

$T(p)$ is finitely branching.

Lemma

Let $p \in \mathbb{Z}[V]$ be tilted and let $\theta \in \Theta(\mathrm{vars}(p))$. Then $p \succ_t p\theta$.

Proposition

$T(p)$ is finite.

Proof.

We use Kőnig's lemma:

- $T(p)$ is finitely branching.
- If a branch in $T(p)$ only contains tilted polynomials, then it is well-ordered by $\prec_t$ which means it is finite.
- If a branch in $T(p)$ contains a non-tilted polynomial, the branch must be finite since no edges originate from non-tilted polynomials.

Decision procedure

Lemma

$\mathcal{AB} \vdash p$ if and only if all leaves of $T(p)$ are signed polynomials.

Decision procedure

Lemma

$\mathcal{AB} \vdash p$ if and only if all leaves of $T(p)$ are signed polynomials.

Corollary

$\mathcal{AB}$ is decidable.

Decision procedure.

Construct $T(p)$ and check if all leaves are signed polynomials. $\square$

Calculus $\mathcal{ABC}$

Consider the additional axiom C, the universal closure of

$$x \neq 0 \to (x \cdot y = x \cdot z \to y = z)$$

Calculus $\mathcal{ABC}$

Consider the additional axiom C, the universal closure of

$$x \neq 0 \to (x \cdot y = x \cdot z \to y = z)$$

Over AB, it is equivalent to the universal closure of

$$y \neq z \to \mathsf{s}(x) \cdot y \neq \mathsf{s}(x) \cdot z.$$

Calculus $\mathcal{ABC}$

Consider the additional axiom C, the universal closure of

$$x \neq 0 \to (x \cdot y = x \cdot z \to y = z)$$

Over AB, it is equivalent to the universal closure of

$$y \neq z \to \mathsf{s}(x) \cdot y \neq \mathsf{s}(x) \cdot z.$$

This translates into the inference rule

$$\frac{q}{pq} \; \textit{factor}$$

where p is signed.

Calculus $\mathcal{ABC}$

Consider the additional axiom C, the universal closure of

$$x \neq 0 \to (x \cdot y = x \cdot z \to y = z)$$

Over AB, it is equivalent to the universal closure of

$$y \neq z \to \mathsf{s}(x) \cdot y \neq \mathsf{s}(x) \cdot z.$$

This translates into the inference rule

$$\frac{q}{pq}\ \mathit{factor}$$

where p is signed.

Let $\mathcal{ABC}$ be the proof calculus consisting of the rules from $\mathcal{AB}$ and the additional rule *factor*.

Theorem (Soundness and Completeness of $\mathcal{ABC}$)

$\mathcal{ABC} \vdash \mathrm{poly}(t) - \mathrm{poly}(u)$ *if and only if* $ABC \vdash \forall \bar{x}\, t \neq u$

Equivalence of $\mathcal{AB}$ and $\mathcal{ABC}$

Lemma

If p is signed and θ is a substitution, then $p\theta$ is signed.

Lemma

If p and q are signed, then pq is signed.

Equivalence of $\mathcal{AB}$ and $\mathcal{ABC}$

Lemma

If p is signed and θ is a substitution, then $p\theta$ is signed.

Lemma

If p and q are signed, then pq is signed.

Proposition

$\mathcal{ABC} \vdash p$ *if and only if* $\mathcal{AB} \vdash p$.

Proof sketch for $\Rightarrow$.

Equivalence of $\mathcal{AB}$ and $\mathcal{ABC}$

Lemma

If p is signed and θ is a substitution, then $p\theta$ is signed.

Lemma

If p and q are signed, then pq is signed.

Proposition

$\mathcal{ABC} \vdash p$ *if and only if* $\mathcal{AB} \vdash p$.

Proof sketch for $\Rightarrow$.

- Move instances of *factor* above instances of *zero-or-successor* (uses that signed polynomials are closed under substitution).

Equivalence of $\mathcal{AB}$ and $\mathcal{ABC}$

Lemma

If p is signed and θ is a substitution, then $p\theta$ is signed.

Lemma

If p and q are signed, then pq is signed.

Proposition

$\mathcal{ABC} \vdash p$ if and only if $\mathcal{AB} \vdash p$.

Proof sketch for $\Rightarrow$.

- Move instances of *factor* above instances of *zero-or-successor* (uses that signed polynomials are closed under substitution).
- Top-most chains of *factor* inferences can be replaced by a single *signed* using previous lemma.

$\square$

Equivalence of $\mathcal{AB}$ and $\mathcal{ABC}$

Lemma

If p is signed and θ is a substitution, then $p\theta$ is signed.

Lemma

If p and q are signed, then pq is signed.

Proposition

$\mathcal{ABC} \vdash p$ *if and only if* $\mathcal{AB} \vdash p$.

Proof sketch for $\Rightarrow$.

- Move instances of *factor* above instances of *zero-or-successor* (uses that signed polynomials are closed under substitution).
- Top-most chains of *factor* inferences can be replaced by a single *signed* using previous lemma.

$\square$

Corollary

$D_{AB} = D_{ABC}$

Outline

Theories

Proof strategy

Decidability

Conclusion

Summary

Main Theorem

D_{IOp} is decidable.

Proof sketch.

- By result from Schmerl it suffices to prove decidability of D_{AB}
- Construct a specialized proof calculus $\mathcal{AB}$ operating on $\mathbb{Z}[V]$.
- Show soundness and completeness with respect to disequalities using proof-theoretic methods.
- Show that $\mathcal{AB}$ is decidable with closure properties and an appropriate well-order.

$\square$

Outlook

Theory T	D_T decidable?
Q	yes[7]
IOp, AB, ABC_d, ABC	yes
PA^-	unknown
IOpen	unknown
extensions of IU_1^-	no[8]
extensions of $I\Delta_0 + EXP$	no[9]

[7] Jeř16.
[8] Kay93.
[9] GD82.

References I

[GD82] Haim Gaifman and C. Dimitracopoulos. „Fragments of Peano's Arithmetic and the MRDP theorem". In: *Monographie de L'Enseignement Mathematique* 30 (Jan. 1982), pp. 187–206.

[Jeř16] Emil Jeřábek. „Division by zero". In: *Archive for Mathematical Logic* 55.7-8 (2016), pp. 997–1013. DOI: 10.1007/s00153-016-0508-5. URL: https://doi.org/10.1007%2Fs00153-016-0508-5.

[Kay93] Richard Kaye. „Hilbert's tenth problem for weak theories of arithmetic". In: *Annals of Pure and Applied Logic* 61.1 (1993), pp. 63–73. ISSN: 0168-0072. DOI: https://doi.org/10.1016/0168-0072(93)90198-M. URL: https://www.sciencedirect.com/science/article/pii/016800729390198M.

References II

[Sch88] Ulf R. Schmerl. „Diophantine equations in fragments of arithmetic“. In: *Annals of Pure and Applied Logic* 38.2 (1988), pp. 135–170. ISSN: 0168-0072. DOI: https://doi.org/10.1016/0168-0072(88)90051-6. URL: https://www.sciencedirect.com/science/article/pii/0168007288900516.

[She64] J. Shepherdson. „A Non-Standard Model for a Free Variable Fragment of Number Theory“. In: *Bulletin de l'Académie Polonaise des Sciences, Série des Sciences Mathématiques, Astronomiques et Physiques* 12 (1964).

[She67] J. Shepherdson. „The rule of induction in the three variable arithmetic based on $+$ and $-$“. en. In: *Annales scientifiques de l'Université de Clermont. Mathématiques* 35.4 (1967), pp. 25–31.