Quantifier Elimination Approach to Existential Linear Arithmetic with GCD

Mikhail R. Starchak

Saint-Petersburg State University

m.starchak@spbu.ru

October 25, 2021

The Diophantine Problem for Addition and Divisibility

Theorem (A.P. Bel'tyukov 1976, L. Lipshitz 1978)

The existential theory of the structure $\langle \mathbb{Z}; 1, +, -, \leq, | \rangle$ *is decidable.*

The Diophantine Problem for Addition and Divisibility

Theorem (A.P. Bel'tyukov 1976, L. Lipshitz 1978)

The existential theory of the structure $\langle \mathbb{Z}; 1, +, -, \leq, | \rangle$ *is decidable.*

Divisibility and GCD

We have $\exists\mathrm{Def}\langle \mathbb{Z}; 1, +, -, \leq, | \rangle = \exists\mathrm{Def}\langle \mathbb{Z}; 1, +, -, \leq, \mathrm{GCD} \rangle$

$$\begin{aligned} x \mid y \ &\Leftrightarrow \ \mathrm{GCD}(x, y) = x \vee \mathrm{GCD}(x, y) = -x \\ \mathrm{GCD}(x, y) = z \ &\Leftrightarrow \ 0 \leq z \wedge z \mid x \wedge z \mid y \wedge \exists u \, (x \mid u \wedge y \mid u + z) \\ \neg\mathrm{GCD}(x, y) = z \ &\Leftrightarrow \ z + 1 \leq 0 \vee \neg z \mid x \vee \neg z \mid y \vee \exists v \, (v \mid x \wedge v \mid y \wedge z + 1 \leq v) \end{aligned}$$

The Diophantine Problem for Addition and Divisibility

Theorem (A.P. Bel'tyukov 1976, L. Lipshitz 1978)

The existential theory of the structure $\langle \mathbb{Z}; 1, +, -, \leq, | \rangle$ *is decidable.*

Divisibility and GCD

We have $\exists\mathrm{Def}\langle \mathbb{Z}; 1, +, -, \leq, | \rangle = \exists\mathrm{Def}\langle \mathbb{Z}; 1, +, -, \leq, \mathrm{GCD} \rangle$

$$
\begin{aligned}
x \mid y &\Leftrightarrow \mathrm{GCD}(x, y) = x \vee \mathrm{GCD}(x, y) = -x \\
\mathrm{GCD}(x, y) = z &\Leftrightarrow 0 \leq z \wedge z \mid x \wedge z \mid y \wedge \exists u\, (x \mid u \wedge y \mid u + z) \\
\neg\mathrm{GCD}(x, y) = z &\Leftrightarrow z + 1 \leq 0 \vee \neg z \mid x \vee \neg z \mid y \vee \exists v\, (v \mid x \wedge v \mid y \wedge z + 1 \leq v)
\end{aligned}
$$

- L_σ FOL of a signature σ. $\langle M; \sigma \rangle$ structure of a signature σ and domain M.
- $\exists L_\sigma$ Existential L_σ-formulas: $\exists \boldsymbol{y} \varphi(\boldsymbol{x}, \boldsymbol{y})$ for QFL_σ-formula $\varphi(\boldsymbol{x}, \boldsymbol{y})$.

The Diophantine Problem for Addition and Divisibility

Theorem (A.P. Bel'tyukov 1976, L. Lipshitz 1978)

The existential theory of the structure $\langle \mathbb{Z}; 1, +, -, \leq, | \rangle$ *is decidable.*

Divisibility and GCD

We have $\exists\mathrm{Def}\langle \mathbb{Z}; 1, +, -, \leq, | \rangle = \exists\mathrm{Def}\langle \mathbb{Z}; 1, +, -, \leq, \mathrm{GCD} \rangle$

$$\begin{aligned} x \mid y &\Leftrightarrow \mathrm{GCD}(x,y) = x \vee \mathrm{GCD}(x,y) = -x \\ \mathrm{GCD}(x,y) = z &\Leftrightarrow 0 \leq z \wedge z \mid x \wedge z \mid y \wedge \exists u\,(x \mid u \wedge y \mid u + z) \\ \neg\mathrm{GCD}(x,y) = z &\Leftrightarrow z + 1 \leq 0 \vee \neg z \mid x \vee \neg z \mid y \vee \exists v\,(v \mid x \wedge v \mid y \wedge z + 1 \leq v) \end{aligned}$$

- L_σ FOL of a signature σ. $\langle M; \sigma \rangle$ structure of a signature σ and domain M.
- $\exists L_\sigma$ Existential L_σ-formulas: $\exists \boldsymbol{y} \varphi(\boldsymbol{x}, \boldsymbol{y})$ for QFL_σ-formula $\varphi(\boldsymbol{x}, \boldsymbol{y})$.
- $\mathrm{Def}\langle M; \sigma \rangle$ the set of all L_σ-definable in M.
- $\exists\mathrm{Def}\langle M; \sigma \rangle$ and $\mathrm{QFDef}\langle M; \sigma \rangle$ for $\exists L_\sigma$- and quantifier-free definable relations, respectively.

Positive existential definability with divisibility

- QF-formula $\varphi(\boldsymbol{x})$ is positive (PQF-formula) if it is constructed from atomic formulas with only logical connectives $\wedge$ and $\vee$.
- $\exists$-formula $\exists \boldsymbol{y} \varphi(\boldsymbol{x}, \boldsymbol{y})$ is positive if $\varphi(\boldsymbol{x}, \boldsymbol{y})$ is PQF-formula.

Positive existential definability with divisibility

- QF-formula $\varphi(\boldsymbol{x})$ is positive (PQF-formula) if it is constructed from atomic formulas with only logical connectives $\wedge$ and $\vee$.
- $\exists$-formula $\exists \boldsymbol{y} \varphi(\boldsymbol{x}, \boldsymbol{y})$ is positive if $\varphi(\boldsymbol{x}, \boldsymbol{y})$ is PQF-formula.
- P$\exists$Def$\langle M; \sigma \rangle$ the set of all P$\exists$-defibable in $\langle M; \sigma \rangle$.
- PQFDef$\langle M; \sigma \rangle$ positively QF-definable in $\langle M; \sigma \rangle$.

Positive existential definability with divisibility

- QF-formula $\varphi(\boldsymbol{x})$ is positive (PQF-formula) if it is constructed from atomic formulas with only logical connectives $\wedge$ and $\vee$.
- $\exists$-formula $\exists \boldsymbol{y} \varphi(\boldsymbol{x}, \boldsymbol{y})$ is positive if $\varphi(\boldsymbol{x}, \boldsymbol{y})$ is PQF-formula.
- P$\exists$Def$\langle M; \sigma\rangle$ the set of all P$\exists$-defibable in $\langle M; \sigma\rangle$.
- PQFDef$\langle M; \sigma\rangle$ positively QF-definable in $\langle M; \sigma\rangle$.

Example

We have $\exists\mathrm{Def}\langle \mathbb{Z}; 1, +, -, \leq, |\rangle = \mathrm{P}\exists\mathrm{Def}\langle \mathbb{Z}; 1, +, -, \leq, |\rangle$

$$x \nmid y \Leftrightarrow x = 0 \wedge (1 \leq y \vee y \leq -1) \vee \exists z \Big(1 \leq z \wedge (z \leq x - 1 \vee z \leq -x - 1) \wedge x \mid y + z\Big).$$

Positive existential definability with divisibility

- QF-formula $\varphi(\boldsymbol{x})$ is positive (PQF-formula) if it is constructed from atomic formulas with only logical connectives $\wedge$ and $\vee$.
- $\exists$-formula $\exists \boldsymbol{y} \varphi(\boldsymbol{x}, \boldsymbol{y})$ is positive if $\varphi(\boldsymbol{x}, \boldsymbol{y})$ is PQF-formula.
- $\mathrm{P}\exists\mathrm{Def}\langle M; \sigma\rangle$ the set of all P$\exists$-defibable in $\langle M; \sigma\rangle$.
- $\mathrm{PQFDef}\langle M; \sigma\rangle$ positively QF-definable in $\langle M; \sigma\rangle$.

Example

We have $\exists\mathrm{Def}\langle \mathbb{Z}; 1, +, -, \leq, | \rangle = \mathrm{P}\exists\mathrm{Def}\langle \mathbb{Z}; 1, +, -, \leq, | \rangle$

$$x \nmid y \Leftrightarrow x = 0 \wedge (1 \leq y \vee y \leq -1) \vee \exists z \Big(1 \leq z \wedge (z \leq x - 1 \vee z \leq -x - 1) \wedge x \mid y + z\Big).$$

Corollary

$\mathrm{Def}\langle \mathbb{Z}; 1, +, -, \leq, | \rangle \neq \exists\mathrm{Def}\langle \mathbb{Z}; 1, +, -, \leq, | \rangle$, *since the elementary theory is undecidable.*

Positive existential definability with divisibility

- QF-formula $\varphi(\boldsymbol{x})$ is positive (PQF-formula) if it is constructed from atomic formulas with only logical connectives $\wedge$ and $\vee$.
- $\exists$-formula $\exists \boldsymbol{y} \varphi(\boldsymbol{x}, \boldsymbol{y})$ is positive if $\varphi(\boldsymbol{x}, \boldsymbol{y})$ is PQF-formula.
- $\mathrm{P}\exists\mathrm{Def}\langle M; \sigma\rangle$ the set of all P$\exists$-defibable in $\langle M; \sigma\rangle$.
- $\mathrm{PQFDef}\langle M; \sigma\rangle$ positively QF-definable in $\langle M; \sigma\rangle$.

Example

We have $\exists\mathrm{Def}\langle \mathbb{Z}; 1, +, -, \leq, |\rangle = \mathrm{P}\exists\mathrm{Def}\langle \mathbb{Z}; 1, +, -, \leq, |\rangle$

$$x \nmid y \Leftrightarrow x = 0 \wedge (1 \leq y \vee y \leq -1) \vee \exists z \Big(1 \leq z \wedge (z \leq x - 1 \vee z \leq -x - 1) \wedge x \mid y + z\Big).$$

Corollary

$\mathrm{Def}\langle \mathbb{Z}; 1, +, -, \leq, |\rangle \neq \exists\mathrm{Def}\langle \mathbb{Z}; 1, +, -, \leq, |\rangle$, *since the elementary theory is undecidable.*

By Presburger's quantifier-elimination algorithm:
$\mathrm{P}\exists\mathrm{Def}\langle \mathbb{Z}; 1, +, -, \leq\rangle = \mathrm{PQFDef}\langle \mathbb{Z}; 1, +, -, \leq, 2\,|, 3\,|, 4\,| \ldots\rangle = \mathrm{Def}\langle \mathbb{Z}; 1, +, -, \leq\rangle$.

Positive existential definability with divisibility

- QF-formula $\varphi(\boldsymbol{x})$ is positive (PQF-formula) if it is constructed from atomic formulas with only logical connectives $\wedge$ and $\vee$.
- $\exists$-formula $\exists \boldsymbol{y} \varphi(\boldsymbol{x}, \boldsymbol{y})$ is positive if $\varphi(\boldsymbol{x}, \boldsymbol{y})$ is PQF-formula.
- P$\exists$Def$\langle M; \sigma \rangle$ the set of all P$\exists$-defibable in $\langle M; \sigma \rangle$.
- PQFDef$\langle M; \sigma \rangle$ positively QF-definable in $\langle M; \sigma \rangle$.

Example

We have $\exists\mathrm{Def}\langle \mathbb{Z}; 1, +, -, \leq, | \rangle = \mathrm{P}\exists\mathrm{Def}\langle \mathbb{Z}; 1, +, -, \leq, | \rangle$

$$x \nmid y \Leftrightarrow x = 0 \wedge (1 \leq y \vee y \leq -1) \vee \exists z \Big(1 \leq z \wedge (z \leq x - 1 \vee z \leq -x - 1) \wedge x \mid y + z \Big).$$

Corollary

$\mathrm{Def}\langle \mathbb{Z}; 1, +, -, \leq, | \rangle \neq \exists\mathrm{Def}\langle \mathbb{Z}; 1, +, -, \leq, | \rangle$, *since the elementary theory is undecidable.*

By Presburger's quantifier-elimination algorithm:
$\mathrm{P}\exists\mathrm{Def}\langle \mathbb{Z}; 1, +, -, \leq \rangle = \mathrm{PQFDef}\langle \mathbb{Z}; 1, +, -, \leq, 2 \mid, 3 \mid, 4 \mid \ldots \rangle = \mathrm{Def}\langle \mathbb{Z}; 1, +, -, \leq \rangle$.
How can we describe $\mathrm{P}\exists\mathrm{Def}\langle \mathbb{Z}; 1, +, -, \leq, | \rangle$?

Intermediate structures

- Coprimeness relation: $x \perp y \rightleftharpoons \mathrm{GCD}(x, y) = 1$.
- $\mathrm{P}\exists\mathrm{Def}\langle \mathbb{Z}; 1, +, -, \leq \rangle \subset \mathrm{P}\exists\mathrm{Def}\langle \mathbb{Z}; 1, +, -, \leq, \perp \rangle \subseteq \mathrm{P}\exists\mathrm{Def}\langle \mathbb{Z}; 1, +, -, \leq, | \rangle$.

Intermediate structures

- Coprimeness relation: $x \perp y \rightleftharpoons \mathrm{GCD}(x, y) = 1$.
- $\mathrm{P}\exists\mathrm{Def}\langle \mathbb{Z}; 1, +, -, \leq \rangle \subset \mathrm{P}\exists\mathrm{Def}\langle \mathbb{Z}; 1, +, -, \leq, \perp \rangle \subseteq \mathrm{P}\exists\mathrm{Def}\langle \mathbb{Z}; 1, +, -, \leq, | \rangle$.

Questions

- Set of non-squares is $\exists$-definable in $\langle \mathbb{Z}; 1, +, -, \leq, | \rangle$? [L. van den Dries and A. Wilkie 2003]
- Order $\leq$ is $\exists$-definable in $\langle \mathbb{Z}; 1, +, -, | \rangle$? [M. Bozga and R. Iosif 2005]

Intermediate structures

- Coprimeness relation: $x \perp y \rightleftharpoons \mathrm{GCD}(x, y) = 1$.
- $\mathrm{P}\exists\mathrm{Def}\langle\mathbb{Z}; 1, +, -, \leq\rangle \subset \mathrm{P}\exists\mathrm{Def}\langle\mathbb{Z}; 1, +, -, \leq, \perp\rangle \subseteq \mathrm{P}\exists\mathrm{Def}\langle\mathbb{Z}; 1, +, -, \leq, |\rangle$.

Questions

- Set of non-squares is $\exists$-definable in $\langle\mathbb{Z}; 1, +, -, \leq, |\rangle$? [L. van den Dries and A. Wilkie 2003]
- Order $\leq$ is $\exists$-definable in $\langle\mathbb{Z}; 1, +, -, |\rangle$? [M. Bozga and R. Iosif 2005]
- Dis-coprimeness $\not\perp$ is P$\exists$-definable in $\langle\mathbb{Z}; 1, +, -, \leq, \perp\rangle$ or in $\langle\mathbb{Z}; 1, +, -, \perp\rangle$?

Intermediate structures

- Coprimeness relation: $x \perp y \rightleftharpoons \mathrm{GCD}(x,y)=1$.
- $\mathrm{P\exists Def}\langle \mathbb{Z}; 1,+,-,\leq\rangle \subset \mathrm{P\exists Def}\langle \mathbb{Z}; 1,+,-,\leq,\perp\rangle \subseteq \mathrm{P\exists Def}\langle \mathbb{Z}; 1,+,-,\leq,|\rangle$.

Questions

- Set of non-squares is $\exists$-definable in $\langle \mathbb{Z}; 1,+,-,\leq,|\rangle$? [L. van den Dries and A. Wilkie 2003]
- Order $\leq$ is $\exists$-definable in $\langle \mathbb{Z}; 1,+,-,|\rangle$? [M. Bozga and R. Iosif 2005]
- Dis-coprimeness $\not\perp$ is P$\exists$-definable in $\langle \mathbb{Z}; 1,+,-,\leq,\perp\rangle$ or in $\langle \mathbb{Z}; 1,+,-,\perp\rangle$?

Theorem (D. Richard 1989)

The elementary theory of the structure $\langle \mathbb{Z}; 1,+,\perp\rangle$ *is undecidable.*

Intermediate structures

- Coprimeness relation: $x \perp y \rightleftharpoons \mathrm{GCD}(x, y) = 1$.
- $\mathrm{P}\exists\mathrm{Def}\langle \mathbb{Z}; 1, +, -, \leq \rangle \subset \mathrm{P}\exists\mathrm{Def}\langle \mathbb{Z}; 1, +, -, \leq, \perp \rangle \subseteq \mathrm{P}\exists\mathrm{Def}\langle \mathbb{Z}; 1, +, -, \leq, | \rangle$.

Questions

- Set of non-squares is $\exists$-definable in $\langle \mathbb{Z}; 1, +, -, \leq, | \rangle$? [L. van den Dries and A. Wilkie 2003]
- Order $\leq$ is $\exists$-definable in $\langle \mathbb{Z}; 1, +, -, | \rangle$? [M. Bozga and R. Iosif 2005]
- Dis-coprimeness $\not\perp$ is P$\exists$-definable in $\langle \mathbb{Z}; 1, +, -, \leq, \perp \rangle$ or in $\langle \mathbb{Z}; 1, +, -, \perp \rangle$?

Theorem (D. Richard 1989)

The elementary theory of the structure $\langle \mathbb{Z}; 1, +, \perp \rangle$ is undecidable.

Quantifier elimination to describe P$\exists$-definable sets in $\langle \mathbb{Z}; 1, +, \perp \rangle$:

Intermediate structures

- Coprimeness relation: $x \perp y \rightleftharpoons \mathrm{GCD}(x, y) = 1$.
- $\mathrm{P}\exists\mathrm{Def}\langle\mathbb{Z}; 1, +, -, \leq\rangle \subset \mathrm{P}\exists\mathrm{Def}\langle\mathbb{Z}; 1, +, -, \leq, \perp\rangle \subseteq \mathrm{P}\exists\mathrm{Def}\langle\mathbb{Z}; 1, +, -, \leq, |\rangle$.

Questions

- Set of non-squares is $\exists$-definable in $\langle\mathbb{Z}; 1, +, -, \leq, |\rangle$? [L. van den Dries and A. Wilkie 2003]
- Order $\leq$ is $\exists$-definable in $\langle\mathbb{Z}; 1, +, -, |\rangle$? [M. Bozga and R. Iosif 2005]
- Dis-coprimeness $\not\perp$ is P$\exists$-definable in $\langle\mathbb{Z}; 1, +, -, \leq, \perp\rangle$ or in $\langle\mathbb{Z}; 1, +, -, \perp\rangle$?

Theorem (D. Richard 1989)

The elementary theory of the structure $\langle\mathbb{Z}; 1, +, \perp\rangle$ *is undecidable.*

Quantifier elimination to describe P$\exists$-definable sets in $\langle\mathbb{Z}; 1, +, \perp\rangle$:

- Extend the signature $\langle 1, +, \perp\rangle \rightsquigarrow \sigma$ with some P$\exists$-definable predicates.

Intermediate structures

- Coprimeness relation: $x \perp y \rightleftharpoons \mathrm{GCD}(x, y) = 1$.
- $\mathrm{P}\exists\mathrm{Def}\langle \mathbb{Z}; 1, +, -, \leq \rangle \subset \mathrm{P}\exists\mathrm{Def}\langle \mathbb{Z}; 1, +, -, \leq, \perp \rangle \subseteq \mathrm{P}\exists\mathrm{Def}\langle \mathbb{Z}; 1, +, -, \leq, | \rangle$.

Questions

- Set of non-squares is $\exists$-definable in $\langle \mathbb{Z}; 1, +, -, \leq, | \rangle$? [L. van den Dries and A. Wilkie 2003]
- Order $\leq$ is $\exists$-definable in $\langle \mathbb{Z}; 1, +, -, | \rangle$? [M. Bozga and R. Iosif 2005]
- Dis-coprimeness $\not\perp$ is P$\exists$-definable in $\langle \mathbb{Z}; 1, +, -, \leq, \perp \rangle$ or in $\langle \mathbb{Z}; 1, +, -, \perp \rangle$?

Theorem (D. Richard 1989)

The elementary theory of the structure $\langle \mathbb{Z}; 1, +, \perp \rangle$ is undecidable.

Quantifier elimination to describe P$\exists$-definable sets in $\langle \mathbb{Z}; 1, +, \perp \rangle$:

- Extend the signature $\langle 1, +, \perp \rangle \rightsquigarrow \sigma$ with some P$\exists$-definable predicates.
- For every $\exists x \varphi(x, \boldsymbol{y})$, where $\underline{\varphi(x, \boldsymbol{y}) \text{ is PQF}L_\sigma\text{-formula}}$, construct an equivalent in $\mathbb{Z}$ $\underline{\text{PQF}L_\sigma\text{-formula } \psi(\boldsymbol{y})}$.

P∃-definability in $\langle \mathbb{Z}; 1, +, \perp \rangle$

Positive Existential Definitions

- $x = 0 \Leftrightarrow x + 1 \perp x + 1 \wedge 3 \perp x + 2$
- $y = -x \Leftrightarrow x + y = 0$ and $x = y \Leftrightarrow \exists t (t = -y \wedge x + t = 0)$
- $\mathrm{GCD}(x, y) = d \Leftrightarrow \exists u \exists v \, (x = du \wedge y = dv \wedge u \perp v)$

P∃-definability in $\langle \mathbb{Z}; 1, +, \perp \rangle$

Positive Existential Definitions

- $x = 0 \Leftrightarrow x + 1 \perp x + 1 \wedge 3 \perp x + 2$
- $y = -x \Leftrightarrow x + y = 0$ and $x = y \Leftrightarrow \exists t (t = -y \wedge x + t = 0)$
- $\mathrm{GCD}(x, y) = d \Leftrightarrow \exists u \exists v \, (x = du \wedge y = dv \wedge u \perp v)$
- $x \neq 0 \Leftrightarrow \exists t \, (x \perp t \wedge x \perp t + 4)$ and $x \neq y \Leftrightarrow \exists t (t = -y \wedge x + t \neq 0)$

P∃-definability in $\langle \mathbb{Z}; 1, +, \perp \rangle$

Positive Existential Definitions

- $x = 0 \Leftrightarrow x + 1 \perp x + 1 \wedge 3 \perp x + 2$
- $y = -x \Leftrightarrow x + y = 0$ and $x = y \Leftrightarrow \exists t(t = -y \wedge x + t = 0)$
- $\mathrm{GCD}(x, y) = d \Leftrightarrow \exists u \exists v\, (x = du \wedge y = dv \wedge u \perp v)$
- $x \neq 0 \Leftrightarrow \exists t\, (x \perp t \wedge x \perp t + 4)$ and $x \neq y \Leftrightarrow \exists t(t = -y \wedge x + t \neq 0)$

$$t \equiv 1 (\mathrm{mod}\ 2) \wedge t \equiv 1 (\mathrm{mod}\ 3) \wedge \bigwedge_{p \in P_x \setminus \{2,3\}} t \equiv 2 (\mathrm{mod}\ p),$$

where P_x is the set of prime divisors of x.

P∃-definability in $\langle \mathbb{Z}; 1, +, \perp \rangle$

Positive Existential Definitions

- $x = 0 \Leftrightarrow x + 1 \perp x + 1 \wedge 3 \perp x + 2$
- $y = -x \Leftrightarrow x + y = 0$ and $x = y \Leftrightarrow \exists t(t = -y \wedge x + t = 0)$
- $\mathrm{GCD}(x, y) = d \Leftrightarrow \exists u \exists v\,(x = du \wedge y = dv \wedge u \perp v)$
- $x \neq 0 \Leftrightarrow \exists t\,(x \perp t \wedge x \perp t + 4)$ and $x \neq y \Leftrightarrow \exists t(t = -y \wedge x + t \neq 0)$

$$t \equiv 1 (\mathrm{mod}\ 2) \wedge t \equiv 1 (\mathrm{mod}\ 3) \wedge \bigwedge_{p \in P_x \setminus \{2,3\}} t \equiv 2 (\mathrm{mod}\ p),$$

where P_x is the set of prime divisors of x.

- $x = y$ is PQF-definable in $\langle \mathbb{Z}; 1, +, -, \perp \rangle$ and $x \neq y$ is PQF-definable in $\langle \mathbb{Z}; 1, +, -, \neq 0, \perp \rangle$

P∃-definability in $\langle \mathbb{Z}; 1, +, \perp \rangle$

Positive Existential Definitions

- $x = 0 \Leftrightarrow x + 1 \perp x + 1 \wedge 3 \perp x + 2$
- $y = -x \Leftrightarrow x + y = 0$ and $x = y \Leftrightarrow \exists t(t = -y \wedge x + t = 0)$
- $\mathrm{GCD}(x, y) = d \Leftrightarrow \exists u \exists v\,(x = du \wedge y = dv \wedge u \perp v)$
- $x \neq 0 \Leftrightarrow \exists t\,(x \perp t \wedge x \perp t + 4)$ and $x \neq y \Leftrightarrow \exists t(t = -y \wedge x + t \neq 0)$

$$t \equiv 1 (\mathrm{mod}\ 2) \wedge t \equiv 1 (\mathrm{mod}\ 3) \wedge \bigwedge_{p \in P_x \setminus \{2,3\}} t \equiv 2 (\mathrm{mod}\ p),$$

where P_x is the set of prime divisors of x.

- $x = y$ is PQF-definable in $\langle \mathbb{Z}; 1, +, -, \perp \rangle$ and $x \neq y$ is PQF-definable in $\langle \mathbb{Z}; 1, +, -, \neq 0, \perp \rangle$

Proposition (PQF-undefinability of dis-equality)

The relation $x \neq 0$ is not PQF-definable in the structure $\langle \mathbb{Z}; 1, +, -, \perp \rangle$.

Extension of the signature. The first main result.

PQF-undefinability of dis-equality proof.

- Euclidean algorithm: $(f(\boldsymbol{y}) + ax, g(\boldsymbol{y}) + bx) \rightsquigarrow (\widetilde{f}(\boldsymbol{y}), \widetilde{g}(\boldsymbol{y}) + cx)$ such that $\mathrm{GCD}(f(\boldsymbol{y}) + ax, g(\boldsymbol{y}) + bx) = \mathrm{GCD}(\widetilde{f}(\boldsymbol{y}), \widetilde{g}(\boldsymbol{y}) + cx)$.

Extension of the signature. The first main result.

PQF-undefinability of dis-equality proof.

- Euclidean algorithm: $(f(\boldsymbol{y}) + ax, g(\boldsymbol{y}) + bx) \rightsquigarrow (\widetilde{f}(\boldsymbol{y}), \widetilde{g}(\boldsymbol{y}) + cx)$ such that $\mathrm{GCD}(f(\boldsymbol{y}) + ax, g(\boldsymbol{y}) + bx) = \mathrm{GCD}(\widetilde{f}(\boldsymbol{y}), \widetilde{g}(\boldsymbol{y}) + cx)$.
- Suppose $\varphi(x) \rightleftharpoons \bigvee_{j \in J} \left(\bigwedge_{i \in I_j} a_i \perp b_i + c_i x \right)$ defines $x \neq 0$.
- $\neg\varphi(0)$ is $\bigwedge_{j \in J} \left(\bigvee_{i \in I_j} a_i \not\perp b_i \right) \rightsquigarrow$ take such $i_j \in I_j$ that $a_{i_j} \not\perp b_{i_j}$.

Extension of the signature. The first main result.

PQF-undefinability of dis-equality proof.

- Euclidean algorithm: $(f(\boldsymbol{y}) + ax, g(\boldsymbol{y}) + bx) \rightsquigarrow (\widetilde{f}(\boldsymbol{y}), \widetilde{g}(\boldsymbol{y}) + cx)$ such that $\mathrm{GCD}(f(\boldsymbol{y}) + ax, g(\boldsymbol{y}) + bx) = \mathrm{GCD}(\widetilde{f}(\boldsymbol{y}), \widetilde{g}(\boldsymbol{y}) + cx)$.
- Suppose $\varphi(x) \rightleftharpoons \bigvee_{j \in J} \left(\bigwedge_{i \in I_j} a_i \perp b_i + c_i x \right)$ defines $x \neq 0$.
- $\neg\varphi(0)$ is $\bigwedge_{j \in J} \left(\bigvee_{i \in I_j} a_i \not\perp b_i \right) \rightsquigarrow$ take such $i_j \in I_j$ that $a_{i_j} \not\perp b_{i_j}$.
- 1. $\underline{\text{All } a_{i_j} = 0} \rightsquigarrow$ large x .

Extension of the signature. The first main result.

PQF-undefinability of dis-equality proof.

- Euclidean algorithm: $(f(\boldsymbol{y}) + ax, g(\boldsymbol{y}) + bx) \rightsquigarrow (\widetilde{f}(\boldsymbol{y}), \widetilde{g}(\boldsymbol{y}) + cx)$ such that $\mathrm{GCD}(f(\boldsymbol{y}) + ax, g(\boldsymbol{y}) + bx) = \mathrm{GCD}(\widetilde{f}(\boldsymbol{y}), \widetilde{g}(\boldsymbol{y}) + cx)$.
- Suppose $\varphi(x) \rightleftharpoons \bigvee_{j \in J} \left(\bigwedge_{i \in I_j} a_i \perp b_i + c_i x \right)$ defines $x \neq 0$.
- $\neg\varphi(0)$ is $\bigwedge_{j \in J} \left(\bigvee_{i \in I_j} a_i \not\perp b_i \right) \rightsquigarrow$ take such $i_j \in I_j$ that $a_{i_j} \not\perp b_{i_j}$.
- 1. $\underline{\text{All } a_{i_j} = 0} \rightsquigarrow$ large x . 2. Otherwise for $A = \prod_{j \in J \wedge a_{i_j} \neq 0} a_{i_j} > 0$ we have $\neg\varphi(A)$.

Extension of the signature. The first main result.

PQF-undefinability of dis-equality proof.

- Euclidean algorithm: $(f(\mathbf{y}) + ax, g(\mathbf{y}) + bx) \rightsquigarrow (\widetilde{f}(\mathbf{y}), \widetilde{g}(\mathbf{y}) + cx)$ such that $\mathrm{GCD}(f(\mathbf{y}) + ax, g(\mathbf{y}) + bx) = \mathrm{GCD}(\widetilde{f}(\mathbf{y}), \widetilde{g}(\mathbf{y}) + cx)$.
- Suppose $\varphi(x) \rightleftharpoons \bigvee_{j \in J} \left(\bigwedge_{i \in I_j} a_i \perp b_i + c_i x \right)$ defines $x \neq 0$.
- $\neg\varphi(0)$ is $\bigwedge_{j \in J} \left(\bigvee_{i \in I_j} a_i \not\perp b_i \right) \rightsquigarrow$ take such $i_j \in I_j$ that $a_{i_j} \not\perp b_{i_j}$.
- 1. $\underline{\text{All } a_{i_j} = 0} \rightsquigarrow$ large x . 2. Otherwise for $A = \prod_{j \in J \wedge a_{i_j} \neq 0} a_{i_j} > 0$ we have $\neg\varphi(A)$.

Proposition

Fix $d \geq 2$. The relation $\mathrm{GCD}(x, y) = d$ is not PQF-definable in $\langle \mathbb{Z}; 1, +, -, \neq, \perp \rangle$.

Extension of the signature. The first main result.

PQF-undefinability of dis-equality proof.

- Euclidean algorithm: $(f(\mathbf{y}) + ax, g(\mathbf{y}) + bx) \rightsquigarrow (\widetilde{f}(\mathbf{y}), \widetilde{g}(\mathbf{y}) + cx)$ such that $\mathrm{GCD}(f(\mathbf{y}) + ax, g(\mathbf{y}) + bx) = \mathrm{GCD}(\widetilde{f}(\mathbf{y}), \widetilde{g}(\mathbf{y}) + cx)$.
- Suppose $\varphi(x) \rightleftharpoons \bigvee_{j \in J} \left(\bigwedge_{i \in I_j} a_i \perp b_i + c_i x \right)$ defines $x \neq 0$.
- $\neg\varphi(0)$ is $\bigwedge_{j \in J} \left(\bigvee_{i \in I_j} a_i \not\perp b_i \right) \rightsquigarrow$ take such $i_j \in I_j$ that $a_{i_j} \not\perp b_{i_j}$.
- 1. $\underline{\text{All } a_{i_j} = 0}$ $\rightsquigarrow$ large x . 2. Otherwise for $A = \prod_{j \in J \wedge a_{i_j} \neq 0} a_{i_j} > 0$ we have $\neg\varphi(A)$.

Proposition

Fix $d \geq 2$. The relation $\mathrm{GCD}(x, y) = d$ is not PQF-definable in $\langle \mathbb{Z}; 1, +, -, \neq, \perp \rangle$.

Theorem

$\mathrm{P}\exists\mathrm{Def}\langle \mathbb{Z}; 1, +, \perp \rangle = \mathrm{PQFDef}\langle \mathbb{Z}; 1, +, -, \neq, \perp, \mathrm{GCD}_2, \mathrm{GCD}_3, \mathrm{GCD}_4, ... \rangle$.

Extension of the signature. The first main result.

PQF-undefinability of dis-equality proof.

- Euclidean algorithm: $(f(\mathbf{y}) + ax, g(\mathbf{y}) + bx) \rightsquigarrow (\widetilde{f}(\mathbf{y}), \widetilde{g}(\mathbf{y}) + cx)$ such that $\mathrm{GCD}(f(\mathbf{y}) + ax, g(\mathbf{y}) + bx) = \mathrm{GCD}(\widetilde{f}(\mathbf{y}), \widetilde{g}(\mathbf{y}) + cx)$.
- Suppose $\varphi(x) \rightleftharpoons \bigvee_{j \in J} \left(\bigwedge_{i \in I_j} a_i \perp b_i + c_i x \right)$ defines $x \neq 0$.
- $\neg\varphi(0)$ is $\bigwedge_{j \in J} \left(\bigvee_{i \in I_j} a_i \not\perp b_i \right) \rightsquigarrow$ take such $i_j \in I_j$ that $a_{i_j} \not\perp b_{i_j}$.
- 1. $\underline{\text{All } a_{i_j} = 0}$ $\rightsquigarrow$ large x . 2. $\underline{\text{Otherwise}}$ for $A = \prod_{j \in J \wedge a_{i_j} \neq 0} a_{i_j} > 0$ we have $\neg\varphi(A)$.

Proposition

Fix $d \geq 2$. The relation $\mathrm{GCD}(x, y) = d$ is not PQF-definable in $\langle \mathbb{Z}; 1, +, -, \neq, \perp \rangle$.

Theorem

$\mathrm{P}\exists\mathrm{Def}\langle \mathbb{Z}; 1, +, \perp \rangle = \mathrm{PQFDef}\langle \mathbb{Z}; 1, +, -, \neq, \perp, \mathrm{GCD}_2, \mathrm{GCD}_3, \mathrm{GCD}_4, \ldots \rangle$.

Fix the signature $\sigma = \langle 1, +, -, \neq, \perp, \mathrm{GCD}_2, \mathrm{GCD}_3, \mathrm{GCD}_4, \ldots \rangle$.

Quantifier elimination algorithm

For every $\underline{\mathrm{PQF}L_\sigma\text{-formula } \varphi(x, \mathbf{y})}$ the algorithm assigns to $\exists x \varphi(x, \mathbf{y})$ an equivalent in $\mathbb{Z}$ $\underline{\mathrm{PQF}L_\sigma\text{-formula } \psi(\mathbf{y})}$.

GCD-Lemma

$$\exists x \bigwedge_{i\in[1..m]} \mathrm{GCD}(a_i, b_i + x) = d_i. \quad (1)$$

Lemma (GCD-Lemma)

For the system (1) with $a_i, b_i, d_i \in \mathbb{Z}$, $a_i \neq 0$, $d_i > 0$ for every $i \in [1..m]$, we define for every prime p the integer $M_p = \max_{i\in[1..m]} v_p(d_i)$ and the index sets $J_p = \{i \in [1..m] : v_p(d_i) = M_p\}$ and $I_p = \{i \in J_p : v_p(a_i) > M_p\}$. Then (1) has a solution in $\mathbb{Z}$ iff the following conditions simultaneously hold:

1. $\bigwedge_{i\in[1..m]} d_i \mid a_i$
2. $\bigwedge_{i,j\in[1..m]} \mathrm{GCD}(d_i, d_j) \mid b_i - b_j$
3. $\bigwedge_{i,j\in[1..m]} \mathrm{GCD}(a_i, d_j, b_i - b_j) \mid d_i$
4. *For every prime $p \leq m$ and every $I \subseteq I_p$ such that $|I| = p$ there are such $i, j \in I$, $i \neq j$ that $v_p(b_i - b_j) > M_p$.*

GCD-Lemma

$$\exists x \bigwedge_{i\in[1..m]} \mathrm{GCD}(a_i, b_i + x) = d_i. \quad (1) \qquad \begin{cases} \mathrm{GCD}(6, x) = 2 \\ \mathrm{GCD}(6, x) = 3 \end{cases}$$

Lemma (GCD-Lemma)

For the system (1) with $a_i, b_i, d_i \in \mathbb{Z}$, $a_i \neq 0$, $d_i > 0$ for every $i \in [1..m]$, we define for every prime p the integer $M_p = \max_{i\in[1..m]} v_p(d_i)$ and the index sets $J_p = \{i \in [1..m] : v_p(d_i) = M_p\}$ and $I_p = \{i \in J_p : v_p(a_i) > M_p\}$. Then (1) has a solution in $\mathbb{Z}$ iff the following conditions simultaneously hold:

1. $\bigwedge_{i\in[1..m]} d_i \mid a_i$
2. $\bigwedge_{i,j\in[1..m]} \mathrm{GCD}(d_i, d_j) \mid b_i - b_j$
3. $\bigwedge_{i,j\in[1..m]} \mathrm{GCD}(a_i, d_j, b_i - b_j) \mid d_i$
4. *For every prime $p \leq m$ and every $I \subseteq I_p$ such that $|I| = p$ there are such $i, j \in I$, $i \neq j$ that $v_p(b_i - b_j) > M_p$.*

GCD-Lemma

$$\exists x \bigwedge_{i\in[1..m]} \mathrm{GCD}(a_i, b_i + x) = d_i. \quad (1) \qquad \begin{cases}\mathrm{GCD}(6,x)=2\\ \mathrm{GCD}(6,x)=3\end{cases} \qquad \begin{cases}\mathrm{GCD}(6,x)=1\\ \mathrm{GCD}(2,1+x)=1\end{cases}$$

Lemma (GCD-Lemma)

For the system (1) with $a_i, b_i, d_i \in \mathbb{Z}$, $a_i \neq 0$, $d_i > 0$ for every $i \in [1..m]$, we define for every prime p the integer $M_p = \max_{i\in[1..m]} v_p(d_i)$ and the index sets $J_p = \{i \in [1..m] : v_p(d_i) = M_p\}$ and $I_p = \{i \in J_p : v_p(a_i) > M_p\}$. Then (1) has a solution in $\mathbb{Z}$ iff the following conditions simultaneously hold:

1. $\bigwedge_{i\in[1..m]} d_i \mid a_i$
2. $\bigwedge_{i,j\in[1..m]} \mathrm{GCD}(d_i, d_j) \mid b_i - b_j$
3. $\bigwedge_{i,j\in[1..m]} \mathrm{GCD}(a_i, d_j, b_i - b_j) \mid d_i$
4. *For every prime $p \leq m$ and every $I \subseteq I_p$ such that $|I| = p$ there are such $i, j \in I$, $i \neq j$ that $v_p(b_i - b_j) > M_p$.*

Quantifier elimination algorithm (sketch)

$$\exists x \left(\bigwedge_{i \in [1..m]} \mathrm{GCD}(f_i(\boldsymbol{y}), g_i(\boldsymbol{y}) + c_i x) = d_i \wedge \bigwedge_{i \in [m+1..l]} f_i(\boldsymbol{y}) \neq c_i x \right)$$

Quantifier elimination algorithm (sketch)

$$\exists x \left(\bigwedge_{i \in [1..m]} \mathrm{GCD}(f_i(\boldsymbol{y}), g_i(\boldsymbol{y}) + c_i x) = d_i \wedge \bigwedge_{i \in [m+1..l]} f_i(\boldsymbol{y}) \neq c_i x \right)$$

$$C = \underset{i=1..l}{\mathrm{LCM}}(c_i) \rightsquigarrow$$

Quantifier elimination algorithm (sketch)

$$\exists x \left(\bigwedge_{i \in [1..m]} \mathrm{GCD}(f_i(\boldsymbol{y}), g_i(\boldsymbol{y}) + c_i x) = d_i \wedge \bigwedge_{i \in [m+1..l]} f_i(\boldsymbol{y}) \neq c_i x \right)$$

$C = \underset{i=1..l}{\mathrm{LCM}}(c_i) \rightsquigarrow$ multiply by $\frac{C}{c_i} \rightsquigarrow$

Quantifier elimination algorithm (sketch)

$$\exists x \left(\bigwedge_{i \in [1..m]} \mathrm{GCD}(f_i(\boldsymbol{y}), g_i(\boldsymbol{y}) + c_i x) = d_i \wedge \bigwedge_{i \in [m+1..l]} f_i(\boldsymbol{y}) \neq c_i x \right)$$

$C = \underset{i=1..l}{\mathrm{LCM}}(c_i) \rightsquigarrow$ multiply by $\frac{C}{c_i} \rightsquigarrow$ replace Cx by $\widetilde{x}$ and adjoin $\mathrm{GCD}(C, \widetilde{x}) = C$

Quantifier elimination algorithm (sketch)

$$\exists x \underbrace{\left(\bigwedge_{i\in[1..m]} \mathrm{GCD}(f_i(\boldsymbol{y}), g_i(\boldsymbol{y}) + x) = d_i \wedge \bigwedge_{i\in[m+1..l]} f_i(\boldsymbol{y}) \neq x \right)}_{\varphi(x,\boldsymbol{y})}$$

Quantifier elimination algorithm (sketch)

$$\exists x \underbrace{\left(\bigwedge_{i \in [1..m]} \mathrm{GCD}(f_i(\boldsymbol{y}), g_i(\boldsymbol{y}) + x) = d_i \wedge \bigwedge_{i \in [m+1..l]} f_i(\boldsymbol{y}) \neq x \right)}_{\varphi(x,\boldsymbol{y})}$$

Case 1. For **some** $i \in [1..m]$ we have $f_i(\boldsymbol{y}) = 0$.

Quantifier elimination algorithm (sketch)

$$\exists x \underbrace{\left(\bigwedge_{i \in [1..m]} \mathrm{GCD}(f_i(\boldsymbol{y}), g_i(\boldsymbol{y}) + x) = d_i \wedge \bigwedge_{i \in [m+1..l]} f_i(\boldsymbol{y}) \neq x \right)}_{\varphi(x,\boldsymbol{y})}$$

Case 1. For **some** $i \in [1..m]$ we have $f_i(\boldsymbol{y}) = 0$.

$$\rightsquigarrow \bigvee_{i \in [1..m]} \left(f_i(\boldsymbol{y}) = 0 \wedge \bigvee_{s \in \{-1,1\}} \varphi(s \cdot d_i - g_i(\boldsymbol{y}), \boldsymbol{y}) \right).$$

Quantifier elimination algorithm (sketch)

$$\exists x \underbrace{\left(\bigwedge_{i \in [1..m]} \mathrm{GCD}(f_i(\boldsymbol{y}), g_i(\boldsymbol{y}) + x) = d_i \wedge \bigwedge_{i \in [m+1..l]} f_i(\boldsymbol{y}) \neq x \right)}_{\varphi(x, \boldsymbol{y})}$$

Case 1. For **some** $i \in [1..m]$ we have $f_i(\boldsymbol{y}) = 0$.

$$\rightsquigarrow \bigvee_{i \in [1..m]} \left(f_i(\boldsymbol{y}) = 0 \wedge \bigvee_{s \in \{-1,1\}} \varphi(s \cdot d_i - g_i(\boldsymbol{y}), \boldsymbol{y}) \right).$$

Case 2. For **all** $i \in [1..m]$ we have $f_i(\boldsymbol{y}) \neq 0$.

Quantifier elimination algorithm (sketch)

$$\exists x \underbrace{\left(\bigwedge_{i \in [1..m]} \mathrm{GCD}(f_i(\boldsymbol{y}), g_i(\boldsymbol{y}) + x) = d_i \wedge \bigwedge_{i \in [m+1..l]} f_i(\boldsymbol{y}) \neq x \right)}_{\varphi(x, \boldsymbol{y})}$$

Case 1. For **some** $i \in [1..m]$ we have $f_i(\boldsymbol{y}) = 0$.

$$\rightsquigarrow \bigvee_{i \in [1..m]} \left(f_i(\boldsymbol{y}) = 0 \wedge \bigvee_{s \in \{-1,1\}} \varphi(s \cdot d_i - g_i(\boldsymbol{y}), \boldsymbol{y}) \right).$$

Case 2. For **all** $i \in [1..m]$ we have $f_i(\boldsymbol{y}) \neq 0$.

$\rightsquigarrow$ apply GCD-Lemma: $\bigwedge_{i \in [1..m]} f_i(\boldsymbol{y}) \neq 0 \wedge \underline{\psi_{GCD}(\boldsymbol{y})}$.

Quantifier elimination algorithm (sketch)

$$\underbrace{\exists x \left(\bigwedge_{i \in [1..m]} \mathrm{GCD}(f_i(\boldsymbol{y}), g_i(\boldsymbol{y}) + x) = d_i \wedge \bigwedge_{i \in [m+1..l]} f_i(\boldsymbol{y}) \neq x \right)}_{\varphi(x,\boldsymbol{y})}$$

Case 1. For **some** $i \in [1..m]$ we have $f_i(\boldsymbol{y}) = 0$.

$$\rightsquigarrow \bigvee_{i \in [1..m]} \left(f_i(\boldsymbol{y}) = 0 \wedge \bigvee_{s \in \{-1,1\}} \varphi(s \cdot d_i - g_i(\boldsymbol{y}), \boldsymbol{y}) \right).$$

Case 2. For **all** $i \in [1..m]$ we have $f_i(\boldsymbol{y}) \neq 0$.

$\rightsquigarrow$ apply GCD-Lemma: $\displaystyle\bigwedge_{i \in [1..m]} f_i(\boldsymbol{y}) \neq 0 \wedge \underline{\psi_{GCD}(\boldsymbol{y})}$.

Formula $\psi_{GCD}(\boldsymbol{y})$ is a conjunction of conditions 1 – 4 of GCD-Lemma.

Quantifier elimination algorithm (sketch)

$$\exists x \underbrace{\left(\bigwedge_{i \in [1..m]} \mathrm{GCD}(f_i(\boldsymbol{y}), g_i(\boldsymbol{y}) + x) = d_i \wedge \bigwedge_{i \in [m+1..l]} f_i(\boldsymbol{y}) \neq x \right)}_{\varphi(x, \boldsymbol{y})}$$

Case 1. For **some** $i \in [1..m]$ we have $f_i(\boldsymbol{y}) = 0$.

$$\rightsquigarrow \bigvee_{i \in [1..m]} \left(f_i(\boldsymbol{y}) = 0 \wedge \bigvee_{s \in \{-1,1\}} \varphi(s \cdot d_i - g_i(\boldsymbol{y}), \boldsymbol{y}) \right).$$

Case 2. For **all** $i \in [1..m]$ we have $f_i(\boldsymbol{y}) \neq 0$.

$$\rightsquigarrow \text{apply GCD-Lemma:} \quad \bigwedge_{i \in [1..m]} f_i(\boldsymbol{y}) \neq 0 \wedge \underline{\psi_{GCD}(\boldsymbol{y})}.$$

Formula $\psi_{GCD}(\boldsymbol{y})$ is a conjunction of conditions 1 – 4 of GCD-Lemma.
Consider condition 3:

For every $i, j \in [1..m]$ we have $\underline{\mathrm{GCD}\left(\mathrm{GCD}\left(f_i(\boldsymbol{y}), d_j\right), g_i(\boldsymbol{y}) - g_j(\boldsymbol{y})\right) \mid d_i}$

Quantifier elimination algorithm (sketch)

$$\exists x \underbrace{\left(\bigwedge_{i \in [1..m]} \mathrm{GCD}(f_i(\boldsymbol{y}), g_i(\boldsymbol{y}) + x) = d_i \wedge \bigwedge_{i \in [m+1..l]} f_i(\boldsymbol{y}) \neq x \right)}_{\varphi(x,\boldsymbol{y})}$$

Case 1. For **some** $i \in [1..m]$ we have $f_i(\boldsymbol{y}) = 0$.

$$\rightsquigarrow \bigvee_{i \in [1..m]} \left(f_i(\boldsymbol{y}) = 0 \wedge \bigvee_{s \in \{-1,1\}} \varphi(s \cdot d_i - g_i(\boldsymbol{y}), \boldsymbol{y}) \right).$$

Case 2. For **all** $i \in [1..m]$ we have $f_i(\boldsymbol{y}) \neq 0$.

$$\rightsquigarrow \text{apply GCD-Lemma: } \bigwedge_{i \in [1..m]} f_i(\boldsymbol{y}) \neq 0 \wedge \underline{\psi_{GCD}(\boldsymbol{y})}.$$

Formula $\psi_{GCD}(\boldsymbol{y})$ is a conjunction of conditions 1 – 4 of GCD-Lemma.
Consider condition 3:

For every $i, j \in [1..m]$ we have $\underline{\mathrm{GCD}\left(\mathrm{GCD}\left(f_i(\boldsymbol{y}), d_j\right), g_i(\boldsymbol{y}) - g_j(\boldsymbol{y})\right) \mid d_i}$

$$\rightsquigarrow \bigvee_{a \mid d_j} \Big(\mathrm{GCD}(f_i(\boldsymbol{y}), d_j) = a$$

Quantifier elimination algorithm (sketch)

$$\underbrace{\exists x \left(\bigwedge_{i \in [1..m]} \mathrm{GCD}(f_i(\boldsymbol{y}), g_i(\boldsymbol{y}) + x) = d_i \wedge \bigwedge_{i \in [m+1..l]} f_i(\boldsymbol{y}) \neq x \right)}_{\varphi(x,\boldsymbol{y})}$$

Case 1. For **some** $i \in [1..m]$ we have $f_i(\boldsymbol{y}) = 0$.

$$\rightsquigarrow \bigvee_{i \in [1..m]} \left(f_i(\boldsymbol{y}) = 0 \wedge \bigvee_{s \in \{-1,1\}} \varphi(s \cdot d_i - g_i(\boldsymbol{y}), \boldsymbol{y}) \right).$$

Case 2. For **all** $i \in [1..m]$ we have $f_i(\boldsymbol{y}) \neq 0$.

$\rightsquigarrow$ apply GCD-Lemma: $\bigwedge_{i \in [1..m]} f_i(\boldsymbol{y}) \neq 0 \wedge \underline{\psi_{GCD}(\boldsymbol{y})}$.

Formula $\psi_{GCD}(\boldsymbol{y})$ is a conjunction of conditions 1 – 4 of GCD-Lemma.
Consider condition 3:

For every $i, j \in [1..m]$ we have $\underline{\mathrm{GCD}\left(\mathrm{GCD}\left(f_i(\boldsymbol{y}), d_j\right), g_i(\boldsymbol{y}) - g_j(\boldsymbol{y})\right) \mid d_i}$

$$\rightsquigarrow \bigvee_{a \mid d_j} \left(\mathrm{GCD}(f_i(\boldsymbol{y}), d_j) = a \wedge \bigvee_{d \mid d_i} \mathrm{GCD}(a, g_i(\boldsymbol{y}) - g_j(\boldsymbol{y})) = d \right).$$

Corollaries

Theorem

$\mathrm{P}\exists\mathrm{Def}\langle \mathbb{Z}; 1, +, \perp \rangle = \mathrm{PQFDef}\langle \mathbb{Z}; 1, +, -, \neq, \perp, \mathrm{GCD}_2, \mathrm{GCD}_3, \mathrm{GCD}_4, \ldots \rangle.$

Corollaries

Theorem

$\mathrm{P}\exists\mathrm{Def}\langle \mathbb{Z}; 1, +, \perp\rangle = \mathrm{PQFDef}\langle \mathbb{Z}; 1, +, -, \neq, \perp, \mathrm{GCD}_2, \mathrm{GCD}_3, \mathrm{GCD}_4, \ldots\rangle.$

Corollary 1. Dis-coprimeness $\not\perp$ is not P∃-definable in $\langle \mathbb{Z}; 1, +, -, \perp\rangle$.

Corollaries

Theorem

$\mathrm{P}\exists\mathrm{Def}\langle\mathbb{Z}; 1, +, \perp\rangle = \mathrm{PQFDef}\langle\mathbb{Z}; 1, +, -, \neq, \perp, \mathrm{GCD}_2, \mathrm{GCD}_3, \mathrm{GCD}_4, \ldots\rangle.$

Corollary 1. Dis-coprimeness $\not\perp$ is not P$\exists$-definable in $\langle\mathbb{Z}; 1, +, -, \perp\rangle$.

Proof

- Assume $\not\perp$ is P$\exists$-definable.
- $\neg\mathrm{GCD}(x, y) = d \Leftrightarrow d \nmid x \vee d \nmid y \vee \exists u \exists v\, (x = du \wedge y = dv \wedge u \not\perp v)$.

Corollaries

Theorem

$\mathrm{P}\exists\mathrm{Def}\langle\mathbb{Z};1,+,\perp\rangle = \mathrm{PQFDef}\langle\mathbb{Z};1,+,-,\neq,\perp,\mathrm{GCD}_2,\mathrm{GCD}_3,\mathrm{GCD}_4,\ldots\rangle.$

Corollary 1. Dis-coprimeness $\not\perp$ is not P$\exists$-definable in $\langle\mathbb{Z};1,+,-,\perp\rangle$.

Proof

- Assume $\not\perp$ is P$\exists$-definable.
- $\neg\mathrm{GCD}(x,y)=d \Leftrightarrow d\nmid x \vee d\nmid y \vee \exists u\exists v\,(x=du \wedge y=dv \wedge u\not\perp v)$.
- $d\nmid x \Leftrightarrow \bigvee\limits_{k=1..d-1} d\mid x+k \rightsquigarrow$ similar to PA case, we can eliminate all the quantifiers

Corollaries

Theorem

$\mathrm{P}\exists\mathrm{Def}\langle\mathbb{Z}; 1, +, \perp\rangle = \mathrm{PQFDef}\langle\mathbb{Z}; 1, +, -, \neq, \perp, \mathrm{GCD}_2, \mathrm{GCD}_3, \mathrm{GCD}_4, \ldots\rangle.$

Corollary 1. Dis-coprimeness $\not\perp$ is not P∃-definable in $\langle\mathbb{Z}; 1, +, -, \perp\rangle$.

Proof

- Assume $\not\perp$ is P∃-definable.
- $\neg\mathrm{GCD}(x, y) = d \Leftrightarrow d \nmid x \vee d \nmid y \vee \exists u \exists v\, (x = du \wedge y = dv \wedge u \not\perp v)$.
- $d \nmid x \Leftrightarrow \bigvee\limits_{k=1..d-1} d \mid x + k \rightsquigarrow$ similar to PA case, we can eliminate all the quantifiers and $\underline{\mathrm{Th}\langle\mathbb{Z}; 1, +, \perp\rangle}$ is decidable.

Corollaries

Theorem

$\mathrm{P}\exists\mathrm{Def}\langle\mathbb{Z};1,+,\perp\rangle = \mathrm{PQFDef}\langle\mathbb{Z};1,+,-,\neq,\perp,\mathrm{GCD}_2,\mathrm{GCD}_3,\mathrm{GCD}_4,\ldots\rangle.$

Corollary 1. Dis-coprimeness $\not\perp$ is not P∃-definable in $\langle\mathbb{Z};1,+,-,\perp\rangle$.

Proof

- Assume $\not\perp$ is P∃-definable.
- $\neg\mathrm{GCD}(x,y) = d \Leftrightarrow d \nmid x \vee d \nmid y \vee \exists u \exists v\,(x = du \wedge y = dv \wedge u \not\perp v)$.
- $d \nmid x \Leftrightarrow \bigvee\limits_{k=1..d-1} d \mid x+k \rightsquigarrow$ similar to PA case, we can eliminate all the quantifiers and $\underline{\mathrm{Th}\langle\mathbb{Z};1,+,\perp\rangle}$ is decidable.

Corollary 2. The order relation $\leq$ is not P∃-definable in $\langle\mathbb{Z};1,+,-,\perp\rangle$. (consider $x \geq 0$).

Corollaries

Theorem

$\mathrm{P}\exists\mathrm{Def}\langle\mathbb{Z};1,+,\perp\rangle = \mathrm{PQFDef}\langle\mathbb{Z};1,+,-,\neq,\perp,\mathrm{GCD}_2,\mathrm{GCD}_3,\mathrm{GCD}_4,\ldots\rangle.$

Corollary 1. Dis-coprimeness $\not\perp$ is not P∃-definable in $\langle\mathbb{Z};1,+,-,\perp\rangle$.

Proof

- Assume $\not\perp$ is P∃-definable.
- $\neg\mathrm{GCD}(x,y) = d \Leftrightarrow d \nmid x \vee d \nmid y \vee \exists u \exists v\,(x = du \wedge y = dv \wedge u \not\perp v)$.
- $d \nmid x \Leftrightarrow \bigvee_{k=1..d-1} d \mid x+k \rightsquigarrow$ similar to PA case, we can eliminate all the quantifiers and $\underline{\mathrm{Th}\langle\mathbb{Z};1,+,\perp\rangle}$ is decidable.

Corollary 2. The order relation $\leq$ is not P∃-definable in $\langle\mathbb{Z};1,+,-,\perp\rangle$. (consider $x \geq 0$).

Consider $\langle\mathbb{N};S,\perp\rangle$, where S is the successor function $x \mapsto x+1$.

- $\mathrm{Th}\langle\mathbb{N};S,\perp\rangle$ is undecidable. [A.R. Woods 1981, D. Richard 1982]

Corollaries

Theorem

$\mathrm{P}\exists\mathrm{Def}\langle\mathbb{Z}; 1, +, \perp\rangle = \mathrm{PQFDef}\langle\mathbb{Z}; 1, +, -, \neq, \perp, \mathrm{GCD}_2, \mathrm{GCD}_3, \mathrm{GCD}_4, \ldots\rangle.$

Corollary 1. Dis-coprimeness $\not\perp$ is not P∃-definable in $\langle\mathbb{Z}; 1, +, -, \perp\rangle$.

Proof

- Assume $\not\perp$ is P∃-definable.
- $\neg\mathrm{GCD}(x, y) = d \Leftrightarrow d \nmid x \vee d \nmid y \vee \exists u \exists v\,(x = du \wedge y = dv \wedge u \not\perp v)$.
- $d \nmid x \Leftrightarrow \bigvee_{k=1..d-1} d \mid x + k \rightsquigarrow$ similar to PA case, we can eliminate all the quantifiers and $\underline{\mathrm{Th}\langle\mathbb{Z}; 1, +, \perp\rangle}$ is decidable.

Corollary 2. The order relation $\leq$ is not P∃-definable in $\langle\mathbb{Z}; 1, +, -, \perp\rangle$. (consider $x \geq 0$).

Consider $\langle\mathbb{N}; S, \perp\rangle$, where S is the successor function $x \mapsto x + 1$.

- $\mathrm{Th}\langle\mathbb{N}; S, \perp\rangle$ is undecidable. [A.R. Woods 1981, D. Richard 1982]
- $x \neq 0 \Leftrightarrow \exists y(x \perp SSy)$ is not P∃-definable in $\langle\mathbb{N}; S, \perp\rangle$.

Theorem

$\mathrm{P}\exists\mathrm{Def}\langle \mathbb{Z}; 1, +, \perp\rangle = \mathrm{PQFDef}\langle \mathbb{Z}; 1, +, -, \neq, \perp, \mathrm{GCD}_2, \mathrm{GCD}_3, \mathrm{GCD}_4, \ldots\rangle$.

Corollary 1. Dis-coprimeness $\not\perp$ is not P$\exists$-definable in $\langle \mathbb{Z}; 1, +, -, \perp\rangle$.

Proof

- Assume $\not\perp$ is P$\exists$-definable.
- $\neg \mathrm{GCD}(x, y) = d \Leftrightarrow d \nmid x \vee d \nmid y \vee \exists u \exists v \, (x = du \wedge y = dv \wedge u \not\perp v)$.
- $d \nmid x \Leftrightarrow \bigvee\limits_{k=1..d-1} d \mid x + k \rightsquigarrow$ similar to PA case, we can eliminate all the quantifiers and $\underline{\mathrm{Th}\langle \mathbb{Z}; 1, +, \perp\rangle}$ is decidable.

Corollary 2. The order relation $\leq$ is not P$\exists$-definable in $\langle \mathbb{Z}; 1, +, -, \perp\rangle$. (consider $x \geq 0$).

Consider $\langle \mathbb{N}; S, \perp\rangle$, where S is the successor function $x \mapsto x + 1$.

- $\mathrm{Th}\langle \mathbb{N}; S, \perp\rangle$ is undecidable. [A.R. Woods 1981, D. Richard 1982]
- $x \neq 0 \Leftrightarrow \exists y (x \perp SSy)$ is not P$\exists$-definable in $\langle \mathbb{N}; S, \perp\rangle$.

Theorem $\mathrm{P}\exists\mathrm{Def}\langle \mathbb{N}; S, \perp\rangle = \mathrm{PQFDef}\langle \mathbb{N}; S, \neq 0, \perp\rangle$.

Decidable $\forall\exists$-fragment of L_{PAD}-Theory of $\mathbb{Z}$

We know: $\forall\exists$-Theory of the structure $\langle \mathbb{Z}; 1, +, -, \leq, | \rangle$ is undecidable.

Decidable $\forall\exists$-fragment of L_{PAD}-Theory of $\mathbb{Z}$

We know: $\forall\exists$-Theory of the structure $\langle \mathbb{Z}; 1, +, -, \leq, | \rangle$ is undecidable.
(DPRM-theorem + *universal* formula:
$y = x^2 \Leftrightarrow x \mid y \wedge x + 1 \mid x + y \wedge \forall z (x \mid z \wedge x + 1 \mid x + z \Rightarrow x + y \mid x + z))$

Decidable $\forall\exists$-fragment of L_{PAD}-Theory of $\mathbb{Z}$

We know: $\forall\exists$-Theory of the structure $\langle \mathbb{Z}; 1, +, -, \leq, | \rangle$ is undecidable.
(DPRM-theorem + *universal* formula:
$y = x^2 \Leftrightarrow x \mid y \wedge x + 1 \mid x + y \wedge \forall z (x \mid z \wedge x + 1 \mid x + z \Rightarrow x + y \mid x + z))$

Decidable Fragments

Here $\underline{\varphi_i(\boldsymbol{x})}$ will be some QFL_{PAD}-formulas

Decidable $\forall\exists$-fragment of L_{PAD}-Theory of $\mathbb{Z}$

We know: $\forall\exists$-Theory of the structure $\langle \mathbb{Z}; 1, +, -, \leq, | \rangle$ is undecidable.
(DPRM-theorem + *universal* formula:
$y = x^2 \Leftrightarrow x \mid y \wedge x + 1 \mid x + y \wedge \forall z (x \mid z \wedge x + 1 \mid x + z \Rightarrow x + y \mid x + z))$

Decidable Fragments

Here $\underline{\varphi_i(\boldsymbol{x})}$ will be some QFL_{PAD}-formulas

- By G.A. Pérez and R. Raha (2020).

$$\forall \boldsymbol{x} \, \exists \boldsymbol{y} \bigvee_{i \in I} \bigwedge_{j \in J_i} \Big(f_j(\boldsymbol{x}) \mid g_j(\boldsymbol{x}, \boldsymbol{y}) \wedge f_j(\boldsymbol{x}) \geq 0) \Big) \wedge \underline{\varphi_i(\boldsymbol{x})} \wedge \boldsymbol{x} \geq 0 \wedge \boldsymbol{y} \geq 0.$$

Decidable $\forall\exists$-fragment of L_{PAD}-Theory of $\mathbb{Z}$

We know: $\forall\exists$-Theory of the structure $\langle \mathbb{Z}; 1, +, -, \leq, | \rangle$ is undecidable.
(DPRM-theorem + *universal* formula:
$y = x^2 \Leftrightarrow x \mid y \wedge x + 1 \mid x + y \wedge \forall z (x \mid z \wedge x + 1 \mid x + z \Rightarrow x + y \mid x + z))$

Decidable Fragments

Here $\underline{\varphi_i(\boldsymbol{x})}$ will be some QFL_{PAD}-formulas

- By G.A. Pérez and R. Raha (2020).

$$\forall \boldsymbol{x} \, \exists \boldsymbol{y} \bigvee_{i \in I} \bigwedge_{j \in J_i} \Big(f_j(\boldsymbol{x}) \mid g_j(\boldsymbol{x}, \boldsymbol{y}) \wedge f_j(\boldsymbol{x}) \geq 0) \Big) \wedge \underline{\varphi_i(\boldsymbol{x})} \wedge \boldsymbol{x} \geq 0 \wedge \boldsymbol{y} \geq 0.$$

- Our result.

$$\forall \boldsymbol{x} \, \exists \boldsymbol{y} \bigvee_{i \in I} \bigwedge_{j \in J_i} \Big(\mathrm{GCD}(f_j(\boldsymbol{x}, \boldsymbol{y}), g_j(\boldsymbol{x}, \boldsymbol{y})) = d_j \Big) \wedge \underline{\varphi_i(\boldsymbol{x})}.$$

Decidable $\forall\exists$-fragment of L_{PAD}-Theory of $\mathbb{Z}$

We know: $\forall\exists$-Theory of the structure $\langle \mathbb{Z}; 1, +, -, \leq, | \rangle$ is undecidable.
(DPRM-theorem + *universal* formula:
$y = x^2 \Leftrightarrow x \mid y \wedge x + 1 \mid x + y \wedge \forall z (x \mid z \wedge x + 1 \mid x + z \Rightarrow x + y \mid x + z))$

Decidable Fragments

Here $\underline{\varphi_i(\mathbf{x})}$ will be some QFL_{PAD}-formulas

- By G.A. Pérez and R. Raha (2020). Divisibility.

$$\forall \mathbf{x} \, \exists \mathbf{y} \bigvee_{i \in I} \bigwedge_{j \in J_i} \left(\underline{\mathrm{GCD}(f_j(\mathbf{x}), g_j(\mathbf{x}, \mathbf{y})) = f_j(\mathbf{x})} \wedge f_j(\mathbf{x}) \geq 0 \right) \wedge \underline{\varphi_i(\mathbf{x})} \wedge \mathbf{x} \geq 0 \wedge \mathbf{y} \geq 0.$$

- Our result. Coprimeness.

$$\forall \mathbf{x} \, \exists \mathbf{y} \bigvee_{i \in I} \bigwedge_{j \in J_i} \left(\underline{\mathrm{GCD}(f_j(\mathbf{x}, \mathbf{y}), g_j(\mathbf{x}, \mathbf{y})) = d_j} \right) \wedge \underline{\varphi_i(\mathbf{x})}.$$

Decidable $\forall\exists$-fragment of L_{PAD}-Theory of $\mathbb{Z}$

We know: $\forall\exists$-Theory of the structure $\langle \mathbb{Z}; 1, +, -, \leq, | \rangle$ is undecidable.
(DPRM-theorem + *universal* formula:
$y = x^2 \Leftrightarrow x \mid y \wedge x+1 \mid x+y \wedge \forall z(x \mid z \wedge x+1 \mid x+z \Rightarrow x+y \mid x+z))$

Decidable Fragments

Here $\underline{\varphi_i(\boldsymbol{x})}$ will be some QFL_{PAD}-formulas

- By G.A. Pérez and R. Raha (2020). Divisibility.

$$\forall \boldsymbol{x} \exists \boldsymbol{y} \bigvee_{i \in I} \bigwedge_{j \in J_i} \left(\underline{\mathrm{GCD}(f_j(\boldsymbol{x}), g_j(\boldsymbol{x}, \boldsymbol{y})) = f_j(\boldsymbol{x})} \wedge f_j(\boldsymbol{x}) \geq 0 \right) \wedge \underline{\varphi_i(\boldsymbol{x})} \wedge \boldsymbol{x} \geq 0 \wedge \boldsymbol{y} \geq 0.$$

- Our result. Coprimeness.

$$\forall \boldsymbol{x} \exists \boldsymbol{y} \bigvee_{i \in I} \bigwedge_{j \in J_i} \left(\underline{\mathrm{GCD}(f_j(\boldsymbol{x}, \boldsymbol{y}), g_j(\boldsymbol{x}, \boldsymbol{y})) = d_j} \right) \wedge \underline{\varphi_i(\boldsymbol{x})}.$$

Proof sketch: isolate $y_i \in \boldsymbol{y}$

Decidable $\forall\exists$-fragment of L_{PAD}-Theory of $\mathbb{Z}$

We know: $\forall\exists$-Theory of the structure $\langle \mathbb{Z}; 1, +, -, \leq, | \rangle$ is undecidable.
(DPRM-theorem + *universal* formula:
$y = x^2 \Leftrightarrow x \mid y \wedge x+1 \mid x+y \wedge \forall z (x \mid z \wedge x+1 \mid x+z \Rightarrow x+y \mid x+z))$

Decidable Fragments

Here $\underline{\varphi_i(\boldsymbol{x})}$ will be some QFL_{PAD}-formulas

- By G.A. Pérez and R. Raha (2020). Divisibility.

$$\forall \boldsymbol{x} \exists \boldsymbol{y} \bigvee_{i \in I} \bigwedge_{j \in J_i} \left(\underline{\mathrm{GCD}(f_j(\boldsymbol{x}), g_j(\boldsymbol{x}, \boldsymbol{y})) = f_j(\boldsymbol{x})} \wedge f_j(\boldsymbol{x}) \geq 0 \right) \wedge \underline{\varphi_i(\boldsymbol{x})} \wedge \boldsymbol{x} \geq 0 \wedge \boldsymbol{y} \geq 0.$$

- Our result. Coprimeness.

$$\forall \boldsymbol{x} \exists \boldsymbol{y} \bigvee_{i \in I} \bigwedge_{j \in J_i} \left(\underline{\mathrm{GCD}(f_j(\boldsymbol{x}, \boldsymbol{y}), g_j(\boldsymbol{x}, \boldsymbol{y})) = d_j} \right) \wedge \underline{\varphi_i(\boldsymbol{x})}.$$

Proof sketch: isolate $y_i \in \boldsymbol{y} \rightsquigarrow$ eliminate $\exists y_i$

Decidable $\forall\exists$-fragment of L_{PAD}-Theory of $\mathbb{Z}$

We know: $\forall\exists$-Theory of the structure $\langle \mathbb{Z}; 1, +, -, \leq, | \rangle$ is undecidable.
(DPRM-theorem + *universal* formula:
$y = x^2 \Leftrightarrow x \mid y \wedge x + 1 \mid x + y \wedge \forall z(x \mid z \wedge x + 1 \mid x + z \Rightarrow x + y \mid x + z))$

Decidable Fragments

Here $\underline{\varphi_i(\mathbf{x})}$ will be some QFL_{PAD}-formulas

- By G.A. Pérez and R. Raha (2020). Divisibility.

$$\forall \mathbf{x} \exists \mathbf{y} \bigvee_{i \in I} \bigwedge_{j \in J_i} \left(\underline{\mathrm{GCD}(f_j(\mathbf{x}), g_j(\mathbf{x}, \mathbf{y})) = f_j(\mathbf{x})} \wedge f_j(\mathbf{x}) \geq 0 \right) \wedge \underline{\varphi_i(\mathbf{x})} \wedge \mathbf{x} \geq 0 \wedge \mathbf{y} \geq 0.$$

- Our result. Coprimeness.

$$\forall \mathbf{x} \exists \mathbf{y} \bigvee_{i \in I} \bigwedge_{j \in J_i} \left(\underline{\mathrm{GCD}(f_j(\mathbf{x}, \mathbf{y}), g_j(\mathbf{x}, \mathbf{y})) = d_j} \right) \wedge \underline{\varphi_i(\mathbf{x})}.$$

Proof sketch: isolate $y_i \in \mathbf{y} \rightsquigarrow$ eliminate $\exists y_i \rightsquigarrow$ rewrite GCD using *universal* quantifiers

Decidable $\forall\exists$-fragment of L_{PAD}-Theory of $\mathbb{Z}$

We know: $\forall\exists$-Theory of the structure $\langle \mathbb{Z}; 1, +, -, \leq, | \rangle$ is undecidable.
(DPRM-theorem + *universal* formula:
$y = x^2 \Leftrightarrow x \mid y \wedge x+1 \mid x+y \wedge \forall z(x \mid z \wedge x+1 \mid x+z \Rightarrow x+y \mid x+z))$

Decidable Fragments

Here $\underline{\varphi_i(\boldsymbol{x})}$ will be some QFL_{PAD}-formulas

- By G.A. Pérez and R. Raha (2020). Divisibility.

$$\forall \boldsymbol{x} \exists \boldsymbol{y} \bigvee_{i \in I} \bigwedge_{j \in J_i} \left(\underline{\mathrm{GCD}(f_j(\boldsymbol{x}), g_j(\boldsymbol{x}, \boldsymbol{y})) = f_j(\boldsymbol{x})} \wedge f_j(\boldsymbol{x}) \geq 0 \right) \wedge \underline{\varphi_i(\boldsymbol{x})} \wedge \boldsymbol{x} \geq 0 \wedge \boldsymbol{y} \geq 0.$$

- Our result. Coprimeness.

$$\forall \boldsymbol{x} \exists \boldsymbol{y} \bigvee_{i \in I} \bigwedge_{j \in J_i} \left(\underline{\mathrm{GCD}(f_j(\boldsymbol{x}, \boldsymbol{y}), g_j(\boldsymbol{x}, \boldsymbol{y})) = d_j} \right) \wedge \underline{\varphi_i(\boldsymbol{x})}.$$

Proof sketch: isolate $y_i \in \boldsymbol{y} \rightsquigarrow$ eliminate $\exists y_i \rightsquigarrow$ rewrite GCD using *universal* quantifiers $\rightsquigarrow$ $\forall$-Theory of $\langle \mathbb{Z}; 1, +, -, \leq, | \rangle$ is decidable since $\exists$-Theory is decidable.

Positive existential arithmetic with addition and coprimeness

Decidability of $\mathrm{P}\exists\mathrm{Th}\langle\mathbb{Z}; 1, +, -, \leq, |\rangle$ by [Bel'tyukov 1976, Lipshitz 1978]:

$$\mathrm{PQF}L_{PAD}\text{-formula } \varphi(\boldsymbol{x})$$

Positive existential arithmetic with addition and coprimeness

Decidability of $\mathrm{P}\exists\mathrm{Th}\langle\mathbb{Z}; 1, +, -, \leq, |\rangle$ by [Bel'tyukov 1976, Lipshitz 1978]:

$$\mathrm{PQF}L_{PAD}\text{-formula } \varphi(\boldsymbol{x})$$

$\rightsquigarrow$ equi-satisfiable $\mathrm{PQF}L_{PAD}$-formula $\bigvee_{j\in J} \varphi_j(\boldsymbol{y_j}) \wedge \boldsymbol{y_j} \geq 0$ $\underline{\text{without } \leq \text{ in } \varphi_j(\boldsymbol{y_j})}$.

Positive existential arithmetic with addition and coprimeness

Decidability of $P\exists Th\langle\mathbb{Z}; 1, +, -, \leq, |\rangle$ by [Bel'tyukov 1976, Lipshitz 1978]:

$$\mathrm{PQF}L_{PAD}\text{-formula } \varphi(\boldsymbol{x})$$

$\rightsquigarrow$ equi-satisfiable $\mathrm{PQF}L_{PAD}$-formula $\bigvee_{j\in J}\varphi_j(\boldsymbol{y_j}) \wedge \boldsymbol{y_j} \geq 0$ without $\leq$ in $\varphi_j(\boldsymbol{y_j})$.

$\rightsquigarrow$ for **such** $\varphi_j(\boldsymbol{y_j})$ we can construct a constant ν_j such that $\exists\boldsymbol{y_j}\varphi_j(\boldsymbol{y_j})$ in $\mathbb{N}$ iff $\exists\boldsymbol{y_j}\varphi_j(\boldsymbol{y_j})$ in the p-adic integers for every prime $p \leq \nu_j$ [Weispfenning 1988].

Positive existential arithmetic with addition and coprimeness

Decidability of $\mathrm{P}\exists\mathrm{Th}\langle\mathbb{Z}; 1, +, -, \leq, |\rangle$ by [Bel'tyukov 1976, Lipshitz 1978]:

$$\mathrm{PQF}L_{PAD}\text{-formula } \varphi(\boldsymbol{x})$$

$$\rightsquigarrow \text{ equi-satisfiable } \mathrm{PQF}L_{PAD}\text{-formula } \bigvee_{j \in J} \varphi_j(\boldsymbol{y_j}) \wedge \boldsymbol{y_j} \geq 0 \ \underline{\text{without } \leq \text{ in } \varphi_j(\boldsymbol{y_j})}.$$

$\rightsquigarrow$ for such $\varphi_j(\boldsymbol{y_j})$ we can construct a constant ν_j such that $\underline{\exists \boldsymbol{y_j} \varphi_j(\boldsymbol{y_j}) \text{ in } \mathbb{N}}$ iff $\exists \boldsymbol{y_j} \varphi_j(\boldsymbol{y_j})$ in the p-adic integers for every prime $p \leq \nu_j$ [Weispfenning 1988].

Constructing $\varphi_j(\boldsymbol{y_j})$ is rather sophisticated

Positive existential arithmetic with addition and coprimeness

Decidability of $\mathrm{P}\exists\mathrm{Th}\langle\mathbb{Z}; 1, +, -, \leq, |\rangle$ by [Bel'tyukov 1976, Lipshitz 1978]:

$$\mathrm{PQF}L_{PAD}\text{-formula } \varphi(\boldsymbol{x})$$

$\rightsquigarrow$ equi-satisfiable PQFL_{PAD}-formula $\bigvee_{j \in J} \varphi_j(\boldsymbol{y_j}) \wedge \boldsymbol{y_j} \geq 0$ <u>without $\leq$ in $\varphi_j(\boldsymbol{y_j})$</u>.

$\rightsquigarrow$ for such $\varphi_j(\boldsymbol{y_j})$ we can construct a constant ν_j such that <u>$\exists \boldsymbol{y_j} \varphi_j(\boldsymbol{y_j})$ in $\mathbb{N}$</u> iff $\exists \boldsymbol{y_j} \varphi_j(\boldsymbol{y_j})$ in the p-adic integers for every prime $p \leq \nu_j$ [Weispfenning 1988].

Constructing $\varphi_j(\boldsymbol{y_j})$ is rather sophisticated $\rightsquigarrow$ more quantifier-elimination spirit

Positive existential arithmetic with addition and coprimeness

Decidability of $\mathrm{P}\exists\mathrm{Th}\langle\mathbb{Z}; 1, +, -, \leq, |\rangle$ by [Bel'tyukov 1976, Lipshitz 1978]:

$$\mathrm{PQF}L_{PAD}\text{-formula } \varphi(\boldsymbol{x})$$

$\rightsquigarrow$ equi-satisfiable PQFL_{PAD}-formula $\bigvee_{j \in J} \varphi_j(\boldsymbol{y_j}) \wedge \boldsymbol{y_j} \geq 0$ without $\leq$ in $\varphi_j(\boldsymbol{y_j})$.

$\rightsquigarrow$ for such $\varphi_j(\boldsymbol{y_j})$ we can construct a constant ν_j such that $\exists \boldsymbol{y_j} \varphi_j(\boldsymbol{y_j})$ in $\mathbb{N}$ iff $\exists \boldsymbol{y_j} \varphi_j(\boldsymbol{y_j})$ in the p-adic integers for every prime $p \leq \nu_j$ [Weispfenning 1988].

Constructing $\varphi_j(\boldsymbol{y_j})$ is rather sophisticated $\rightsquigarrow$ more quantifier-elimination spirit

Decidability of $\mathrm{P}\exists\mathrm{Th}\langle\mathbb{Z}; 1, +, -, \leq, \perp\rangle$.

Step 1. Variable isolation: PQFL_{PAC}-formula $\phi(\boldsymbol{x})$

Positive existential arithmetic with addition and coprimeness

Decidability of $P\exists Th\langle \mathbb{Z}; 1, +, -, \leq, | \rangle$ by [Bel'tyukov 1976, Lipshitz 1978]:

$$\text{PQF}L_{PAD}\text{-formula } \varphi(\boldsymbol{x})$$

$\rightsquigarrow$ equi-satisfiable PQFL_{PAD}-formula $\bigvee_{j \in J} \varphi_j(\boldsymbol{y_j}) \wedge \boldsymbol{y_j} \geq 0$ without $\leq$ in $\varphi_j(\boldsymbol{y_j})$.

$\rightsquigarrow$ for such $\varphi_j(\boldsymbol{y_j})$ we can construct a constant ν_j such that $\exists \boldsymbol{y_j} \varphi_j(\boldsymbol{y_j})$ in $\mathbb{N}$ iff $\exists \boldsymbol{y_j} \varphi_j(\boldsymbol{y_j})$ in the p-adic integers for every prime $p \leq \nu_j$ [Weispfenning 1988].

Constructing $\varphi_j(\boldsymbol{y_j})$ is rather sophisticated $\rightsquigarrow$ more quantifier-elimination spirit

Decidability of $P\exists Th\langle \mathbb{Z}; 1, +, -, \leq, \perp \rangle$.

Step 1. Variable isolation: PQFL_{PAC}-formula $\phi(\boldsymbol{x}) \rightsquigarrow$ equi-satisfiable $\bigvee_{j \in J} \phi_j(\boldsymbol{y_j})$, where

- Every list $\boldsymbol{y_j}$ has at most the same size as $\boldsymbol{x}$.

Positive existential arithmetic with addition and coprimeness

Decidability of $P\exists Th\langle\mathbb{Z}; 1, +, -, \leq, |\rangle$ by [Bel'tyukov 1976, Lipshitz 1978]:

$$PQFL_{PAD}\text{-formula } \varphi(\boldsymbol{x})$$

$\rightsquigarrow$ equi-satisfiable $PQFL_{PAD}$-formula $\bigvee_{j\in J} \varphi_j(\boldsymbol{y_j}) \wedge \boldsymbol{y_j} \geq 0$ without $\leq$ in $\varphi_j(\boldsymbol{y_j})$.

$\rightsquigarrow$ for such $\varphi_j(\boldsymbol{y_j})$ we can construct a constant ν_j such that $\exists \boldsymbol{y_j}\varphi_j(\boldsymbol{y_j})$ in $\mathbb{N}$ iff $\exists \boldsymbol{y_j}\varphi_j(\boldsymbol{y_j})$ in the p-adic integers for every prime $p \leq \nu_j$ [Weispfenning 1988].

Constructing $\varphi_j(\boldsymbol{y_j})$ is rather sophisticated $\rightsquigarrow$ more quantifier-elimination spirit

Decidability of $P\exists Th\langle\mathbb{Z}; 1, +, -, \leq, \perp\rangle$.

Step 1. Variable isolation: $PQFL_{PAC}$-formula $\phi(\boldsymbol{x}) \rightsquigarrow$ equi-satisfiable $\bigvee_{j\in J} \phi_j(\boldsymbol{y_j})$, where

- Every list $\boldsymbol{y_j}$ has at most the same size as $\boldsymbol{x}$.
- $\phi_j(\boldsymbol{y_j})$ has form $\boldsymbol{z_j} \geq 0 \wedge t_j \geq 0 \wedge \widetilde{\varphi}(\boldsymbol{z_j}) \wedge \bigwedge_{i\in[1..m_j]} \mathrm{GCD}(f_{i,j}(\boldsymbol{z_j}), g_{i,j}(\boldsymbol{z_j}) + c_{i,j}t_j) = d_{i,j}$, where $f_{i,j}(\boldsymbol{z_j})$ has non-negative coefficients and positive constant terms.

Positive existential arithmetic with addition and coprimeness

Decidability of $P\exists Th\langle\mathbb{Z}; 1, +, -, \leq, |\rangle$ by [Bel'tyukov 1976, Lipshitz 1978]:

$$PQFL_{PAD}\text{-formula } \varphi(\boldsymbol{x})$$

$\rightsquigarrow$ equi-satisfiable $PQFL_{PAD}$-formula $\bigvee_{j\in J} \varphi_j(\boldsymbol{y_j}) \wedge \boldsymbol{y_j} \geq 0$ without $\leq$ in $\varphi_j(\boldsymbol{y_j})$.

$\rightsquigarrow$ for such $\varphi_j(\boldsymbol{y_j})$ we can construct a constant ν_j such that $\exists \boldsymbol{y_j} \varphi_j(\boldsymbol{y_j})$ in $\mathbb{N}$ iff $\exists \boldsymbol{y_j} \varphi_j(\boldsymbol{y_j})$ in the p-adic integers for every prime $p \leq \nu_j$ [Weispfenning 1988].

Constructing $\varphi_j(\boldsymbol{y_j})$ is rather sophisticated $\rightsquigarrow$ more quantifier-elimination spirit

Decidability of $P\exists Th\langle\mathbb{Z}; 1, +, -, \leq, \perp\rangle$.

Step 1. Variable isolation: $PQFL_{PAC}$-formula $\phi(\boldsymbol{x}) \rightsquigarrow$ equi-satisfiable $\bigvee_{j\in J} \phi_j(\boldsymbol{y_j})$, where

- Every list $\boldsymbol{y_j}$ has at most the same size as $\boldsymbol{x}$.
- $\phi_j(\boldsymbol{y_j})$ has form $\boldsymbol{z_j} \geq 0 \wedge t_j \geq 0 \wedge \widetilde{\varphi}(\boldsymbol{z_j}) \wedge \bigwedge_{i\in[1..m_j]} \mathrm{GCD}(f_{i,j}(\boldsymbol{z_j}), g_{i,j}(\boldsymbol{z_j}) + c_{i,j} t_j) = d_{i,j}$,

  where $f_{i,j}(\boldsymbol{z_j})$ has non-negative coefficients and positive constant terms.

Step 2. Quantifier elimination: Apply GCD-Lemma to eliminate each t_j.

Generalize this approach to prove the BL-Theorem?

Difficulties:

- *Every variable* $t \in \boldsymbol{y}$ can appear in *right-hand side* polynomials

$$\mathrm{GCD}(f(\boldsymbol{z}), g(\boldsymbol{z}) + ct) = h(\boldsymbol{z}) + dt$$

with $c, d > 0$. $\rightsquigarrow$ Lipshitz's basic transformations (Lemma 2).

Generalize this approach to prove the BL-Theorem?

Difficulties:

- *Every variable* $t \in \boldsymbol{y}$ can appear in *right-hand side* polynomials

$$\mathrm{GCD}(f(\boldsymbol{z}), g(\boldsymbol{z}) + ct) = h(\boldsymbol{z}) + dt$$

  with $c, d > 0$. $\rightsquigarrow$ Lipshitz's basic transformations (Lemma 2).

- Application of *GCD-Lemma* to systems of the form

$$\bigwedge_{i \in [1..m]} \mathrm{GCD}(f_i(\boldsymbol{z}), g_i(\boldsymbol{z}) + t) = h_i(\boldsymbol{z})$$

  requires *introducing new variables*.

Generalize this approach to prove the BL-Theorem?

Difficulties:

- *Every variable* $t \in \boldsymbol{y}$ can appear in *right-hand side* polynomials

$$\mathrm{GCD}(f(\boldsymbol{z}), g(\boldsymbol{z}) + ct) = h(\boldsymbol{z}) + dt$$

with $c, d > 0$. $\rightsquigarrow$ Lipshitz's basic transformations (Lemma 2).

- Application of *GCD-Lemma* to systems of the form

$$\bigwedge_{i \in [1..m]} \mathrm{GCD}(f_i(\boldsymbol{z}), g_i(\boldsymbol{z}) + t) = h_i(\boldsymbol{z})$$

requires *introducing new variables*.
Consider (2): $\underline{\mathrm{GCD}(h_i(\boldsymbol{z}), h_j(\boldsymbol{z})) \mid g_i(\boldsymbol{z}) - g_j(\boldsymbol{z})}$

Generalize this approach to prove the BL-Theorem?

Difficulties:

- *Every variable* $t \in \boldsymbol{y}$ can appear in *right-hand side* polynomials

$$\mathrm{GCD}(f(\boldsymbol{z}), g(\boldsymbol{z}) + ct) = h(\boldsymbol{z}) + dt$$

  with $c, d > 0$. $\rightsquigarrow$ Lipshitz's basic transformations (Lemma 2).
- Application of *GCD-Lemma* to systems of the form

$$\bigwedge_{i \in [1..m]} \mathrm{GCD}(f_i(\boldsymbol{z}), g_i(\boldsymbol{z}) + t) = h_i(\boldsymbol{z})$$

  requires *introducing new variables*.
  Consider (2): $\underline{\mathrm{GCD}(h_i(\boldsymbol{z}), h_j(\boldsymbol{z})) \mid g_i(\boldsymbol{z}) - g_j(\boldsymbol{z})}$
  for each (i, j), $1 \leq i < j \leq m$, we introduce $\zeta_{i,j}$, such that

$$\rightsquigarrow \exists \zeta_{i,j} \left(\mathrm{GCD}(h_i(\boldsymbol{z}), h_j(\boldsymbol{z})) = \zeta_{i,j} \wedge \mathrm{GCD}(\zeta_{i,j}, g_i(\boldsymbol{z}) - g_j(\boldsymbol{z})) = \zeta_{i,j} \right).$$

Generalize this approach to prove the BL-Theorem?

Difficulties:

- *Every variable* $t \in \boldsymbol{y}$ can appear in *right-hand side* polynomials

$$\mathrm{GCD}(f(\boldsymbol{z}), g(\boldsymbol{z}) + ct) = h(\boldsymbol{z}) + dt$$

with $c, d > 0$. $\rightsquigarrow$ Lipshitz's basic transformations (Lemma 2).

- Application of *GCD-Lemma* to systems of the form

$$\bigwedge_{i \in [1..m]} \mathrm{GCD}(f_i(\boldsymbol{z}), g_i(\boldsymbol{z}) + t) = h_i(\boldsymbol{z})$$

requires *introducing new variables*.

Consider (2): $\underline{\mathrm{GCD}(h_i(\boldsymbol{z}), h_j(\boldsymbol{z})) \mid g_i(\boldsymbol{z}) - g_j(\boldsymbol{z})}$

for each (i, j), $1 \leq i < j \leq m$, we introduce $\zeta_{i,j}$, such that

$$\rightsquigarrow \exists \zeta_{i,j} \left(\mathrm{GCD}(h_i(\boldsymbol{z}), h_j(\boldsymbol{z})) = \zeta_{i,j} \wedge \mathrm{GCD}(\zeta_{i,j}, g_i(\boldsymbol{z}) - g_j(\boldsymbol{z})) = \zeta_{i,j}\right).$$

Aim: <u>eliminate all **Latin** variables</u> $\rightsquigarrow$

<u>each linear polynomial is either $a\zeta$ or a for some $a > 0$.</u>

Quasi-quantifier elimination algorithms

- Two disjoint sorts of variables: S_1 (Latin letters) and S_2 (Greek letters).

Quasi-quantifier elimination algorithms

- Two disjoint sorts of variables: S_1 (Latin letters) and S_2 (Greek letters).
- Structure $\langle M; \sigma \rangle$ and language L_σ with variables from $S_1 \cup S_2$.

Quasi-quantifier elimination algorithms

- Two disjoint sorts of variables: S_1 (Latin letters) and S_2 (Greek letters).
- Structure $\langle M; \sigma \rangle$ and language L_σ with variables from $S_1 \cup S_2$.
- Language $L_{\mathcal{A}} \subset L_\sigma$; all occurrences of <u>Latin variables are free</u> and all occurrences of <u>Greek variables are bound</u>.

- Two disjoint sorts of variables: S_1 (Latin letters) and S_2 (Greek letters).
- Structure $\langle M; \sigma \rangle$ and language L_σ with variables from $S_1 \cup S_2$.
- Language $L_{\mathcal{A}} \subset L_\sigma$; all occurrences of Latin variables are free and all occurrences of Greek variables are bound.

Quasi-QE algorithm $\mathcal{A}$ for the language $L_{\mathcal{A}}$ in the structure $\langle M; \sigma \rangle$:

Quasi-quantifier elimination algorithms

- Two disjoint sorts of variables: S_1 (Latin letters) and S_2 (Greek letters).
- Structure $\langle M; \sigma \rangle$ and language L_σ with variables from $S_1 \cup S_2$.
- Language $L_{\mathcal{A}} \subset L_\sigma$; all occurrences of Latin variables are free and all occurrences of Greek variables are bound.

Quasi-QE algorithm $\mathcal{A}$ for the language $L_{\mathcal{A}}$ in the structure $\langle M; \sigma \rangle$:
(1) $L_{\mathcal{A}}$-**formulas of elimination form:** $L_{\mathcal{A}}^{\times} \subseteq L_{\mathcal{A}}$.

Quasi-quantifier elimination algorithms

- Two disjoint sorts of variables: S_1 (Latin letters) and S_2 (Greek letters).
- Structure $\langle M; \sigma \rangle$ and language L_σ with variables from $S_1 \cup S_2$.
- Language $L_{\mathcal{A}} \subset L_\sigma$; all occurrences of Latin variables are free and all occurrences of Greek variables are bound.

Quasi-QE algorithm $\mathcal{A}$ for the language $L_{\mathcal{A}}$ in the structure $\langle M; \sigma \rangle$:
(1) $L_{\mathcal{A}}$**-formulas of elimination form:** $L^{\times}_{\mathcal{A}} \subseteq L_{\mathcal{A}}$.
(2) **Step 1:** $L_{\mathcal{A}}$-formula $\exists \boldsymbol{\alpha} \varphi(\boldsymbol{y}, \boldsymbol{\alpha}) \rightsquigarrow$ equi-satisfiable $\bigvee_{j \in J} \exists \boldsymbol{\alpha} \widetilde{\varphi}_j(\boldsymbol{y_j}, \boldsymbol{\alpha})$ and for every $j \in J$:

- Two disjoint sorts of variables: S_1 (Latin letters) and S_2 (Greek letters).
- Structure $\langle M; \sigma \rangle$ and language L_σ with variables from $S_1 \cup S_2$.
- Language $L_{\mathcal{A}} \subset L_\sigma$; all occurrences of Latin variables are free and all occurrences of Greek variables are bound.

Quasi-QE algorithm $\mathcal{A}$ for the language $L_{\mathcal{A}}$ in the structure $\langle M; \sigma \rangle$:
(1) $L_{\mathcal{A}}$**-formulas of elimination form:** $L_{\mathcal{A}}^{\times} \subseteq L_{\mathcal{A}}$.
(2) **Step 1:** $L_{\mathcal{A}}$-formula $\exists \boldsymbol{\alpha} \varphi(\boldsymbol{y}, \boldsymbol{\alpha}) \rightsquigarrow$ equi-satisfiable $\bigvee_{j \in J} \exists \boldsymbol{\alpha} \widetilde{\varphi}_j(\boldsymbol{y_j}, \boldsymbol{\alpha})$ and for every $j \in J$:

1. $\boldsymbol{y_j}$ comprises at most the same number of variables as $\boldsymbol{y}$.

Quasi-quantifier elimination algorithms

- Two disjoint sorts of variables: S_1 (Latin letters) and S_2 (Greek letters).
- Structure $\langle M;\sigma\rangle$ and language L_σ with variables from $S_1 \cup S_2$.
- Language $L_{\mathcal{A}} \subset L_\sigma$; all occurrences of Latin variables are free and all occurrences of Greek variables are bound.

Quasi-QE algorithm $\mathcal{A}$ for the language $L_{\mathcal{A}}$ in the structure $\langle M;\sigma\rangle$:
(1) $L_{\mathcal{A}}$-**formulas of elimination form:** $L_{\mathcal{A}}^{x} \subseteq L_{\mathcal{A}}$.
(2) **Step 1:** $L_{\mathcal{A}}$-formula $\exists\boldsymbol{\alpha}\varphi(\boldsymbol{y},\boldsymbol{\alpha}) \rightsquigarrow$ equi-satisfiable $\bigvee_{j\in J}\exists\boldsymbol{\alpha}\widetilde{\varphi}_j(\boldsymbol{y_j},\boldsymbol{\alpha})$ and for every $j \in J$:

1. $\boldsymbol{y_j}$ comprises at most the same number of variables as $\boldsymbol{y}$.
2. There is a variable $\widetilde{x}_j \in \boldsymbol{y_j}$ such that $[\exists\boldsymbol{\alpha}\widetilde{\varphi}_j(\boldsymbol{y_j},\boldsymbol{\alpha})]_{x}^{\widetilde{x}_j} \in L_{\mathcal{A}}^{x}$.

Quasi-quantifier elimination algorithms

- Two disjoint sorts of variables: S_1 (Latin letters) and S_2 (Greek letters).
- Structure $\langle M; \sigma \rangle$ and language L_σ with variables from $S_1 \cup S_2$.
- Language $L_{\mathcal{A}} \subset L_\sigma$; all occurrences of Latin variables are free and all occurrences of Greek variables are bound.

Quasi-QE algorithm $\mathcal{A}$ for the language $L_{\mathcal{A}}$ in the structure $\langle M; \sigma \rangle$:
(1) $L_{\mathcal{A}}$**-formulas of elimination form:** $L_{\mathcal{A}}^{x} \subseteq L_{\mathcal{A}}$.
(2) **Step 1:** $L_{\mathcal{A}}$-formula $\exists \boldsymbol{\alpha} \varphi(\boldsymbol{y}, \boldsymbol{\alpha}) \rightsquigarrow$ equi-satisfiable $\bigvee\limits_{j \in J} \exists \boldsymbol{\alpha} \widetilde{\varphi}_j(\boldsymbol{y_j}, \boldsymbol{\alpha})$ and for every $j \in J$:

1. $\boldsymbol{y_j}$ comprises at most the same number of variables as $\boldsymbol{y}$.
2. There is a variable $\widetilde{x}_j \in \boldsymbol{y_j}$ such that $[\exists \boldsymbol{\alpha} \widetilde{\varphi}_j(\boldsymbol{y_j}, \boldsymbol{\alpha})]_x^{\widetilde{x}_j} \in L_{\mathcal{A}}^{x}$.

(3) **Step 2:** $\exists x \exists \boldsymbol{\alpha} \widetilde{\varphi}(x, \boldsymbol{z}, \boldsymbol{\alpha}) \rightsquigarrow$ equivalent $L_{\mathcal{A}}$-formula $\exists \boldsymbol{\alpha} \exists \boldsymbol{\beta} \widetilde{\psi}(\boldsymbol{z}, \boldsymbol{\alpha}, \boldsymbol{\beta})$. Here $\exists \boldsymbol{\alpha} \widetilde{\varphi}(x, \boldsymbol{z}, \boldsymbol{\alpha})$ is some $L_{\mathcal{A}}^{x}$-formula.

Quasi-quantifier elimination algorithms

- Two disjoint sorts of variables: S_1 (Latin letters) and S_2 (Greek letters).
- Structure $\langle M; \sigma \rangle$ and language L_σ with variables from $S_1 \cup S_2$.
- Language $L_\mathcal{A} \subset L_\sigma$; all occurrences of <u>Latin variables are free</u> and all occurrences of <u>Greek variables are bound</u>.

Quasi-QE algorithm $\mathcal{A}$ for the language $L_\mathcal{A}$ in the structure $\langle M; \sigma \rangle$:
(1) $L_\mathcal{A}$**-formulas of elimination form:** $L_\mathcal{A}^x \subseteq L_\mathcal{A}$.
(2) **Step 1:** $L_\mathcal{A}$-formula $\exists \boldsymbol{\alpha} \varphi(\boldsymbol{y}, \boldsymbol{\alpha}) \rightsquigarrow$ <u>equi-satisfiable</u> $\bigvee_{j \in J} \exists \boldsymbol{\alpha} \widetilde{\varphi}_j(\boldsymbol{y_j}, \boldsymbol{\alpha})$ and for every $j \in J$:

1. $\boldsymbol{y_j}$ comprises at most the same number of variables as $\boldsymbol{y}$.
2. There is a variable $\widetilde{x}_j \in \boldsymbol{y_j}$ such that $[\exists \boldsymbol{\alpha} \widetilde{\varphi}_j(\boldsymbol{y_j}, \boldsymbol{\alpha})]_x^{\widetilde{x}_j} \in L_\mathcal{A}^x$.

(3) **Step 2:** $\exists x \exists \boldsymbol{\alpha} \widetilde{\varphi}(x, \boldsymbol{z}, \boldsymbol{\alpha}) \rightsquigarrow$ <u>equivalent</u> $L_\mathcal{A}$-formula $\exists \boldsymbol{\alpha} \exists \boldsymbol{\beta} \widetilde{\psi}(\boldsymbol{z}, \boldsymbol{\alpha}, \boldsymbol{\beta})$. Here $\exists \boldsymbol{\alpha} \widetilde{\varphi}(x, \boldsymbol{z}, \boldsymbol{\alpha})$ is some $L_\mathcal{A}^x$-formula.

$\mathcal{A}$ applies Step 1 and Step 2 to $L_\mathcal{A}$-formulas: $\varphi(\boldsymbol{x}) \rightsquigarrow \dots \rightsquigarrow \exists \boldsymbol{\gamma} \psi(\boldsymbol{\gamma})$ such that

$$\varphi(\boldsymbol{x}) \text{ is satisfiable in } \langle M; \sigma \rangle \text{ if and only if } \exists \boldsymbol{\gamma} \psi(\boldsymbol{\gamma}) \text{ is true in } \langle M; \sigma \rangle .$$

Quasi-quantifier elimination for addition and GCD

- $L_{\mathcal{R}}$ is the set of formulas $\exists \boldsymbol{\alpha} \bigvee_{j \in J} \varphi_j(\boldsymbol{y_j}, \boldsymbol{\alpha})$ for some finite index set J and formulas $\varphi_j(\boldsymbol{y}, \boldsymbol{\alpha})$ of the form

$$\boldsymbol{\alpha} \geq 1 \wedge \boldsymbol{y} \geq 0 \wedge \bigwedge_{i \in [1..m_j]} \mathrm{GCD}(f_{i,j}(\boldsymbol{y}, \boldsymbol{\alpha}), g_{i,j}(\boldsymbol{y}, \boldsymbol{\alpha})) = h_{i,j}(\boldsymbol{y}, \boldsymbol{\alpha}),$$

where every gcd-expression takes one of the forms:

1. $\mathrm{GCD}(f(\boldsymbol{y}), g(\boldsymbol{y})) = h(\boldsymbol{y})$

Quasi-quantifier elimination for addition and GCD

- $L_{\mathcal{R}}$ is the set of formulas $\exists \boldsymbol{\alpha} \bigvee_{j \in J} \varphi_j(\boldsymbol{y_j}, \boldsymbol{\alpha})$ for some finite index set J and formulas $\varphi_j(\boldsymbol{y}, \boldsymbol{\alpha})$ of the form

$$\boldsymbol{\alpha} \geq 1 \wedge \boldsymbol{y} \geq 0 \wedge \bigwedge_{i \in [1..m_j]} \mathrm{GCD}(f_{i,j}(\boldsymbol{y}, \boldsymbol{\alpha}), g_{i,j}(\boldsymbol{y}, \boldsymbol{\alpha})) = h_{i,j}(\boldsymbol{y}, \boldsymbol{\alpha}),$$

where every gcd-expression takes one of the forms:

1. $\mathrm{GCD}(f(\boldsymbol{y}), g(\boldsymbol{y})) = h(\boldsymbol{y})$
2. $\mathrm{GCD}(f(\boldsymbol{y}), g(\boldsymbol{y})) = a\zeta$
3. $\mathrm{GCD}(a\zeta, g(\boldsymbol{y})) = b\eta$
4. $\mathrm{GCD}(a\zeta, b\eta) = c\theta,$

Quasi-quantifier elimination for addition and GCD

- $L_{\mathcal{R}}$ is the set of formulas $\exists \boldsymbol{\alpha} \bigvee_{j \in J} \varphi_j(\boldsymbol{y_j}, \boldsymbol{\alpha})$ for some finite index set J and formulas $\varphi_j(\boldsymbol{y}, \boldsymbol{\alpha})$ of the form

$$\boldsymbol{\alpha} \geq 1 \wedge \boldsymbol{y} \geq 0 \wedge \bigwedge_{i \in [1..m_j]} \mathrm{GCD}(f_{i,j}(\boldsymbol{y}, \boldsymbol{\alpha}), g_{i,j}(\boldsymbol{y}, \boldsymbol{\alpha})) = h_{i,j}(\boldsymbol{y}, \boldsymbol{\alpha}),$$

  where every gcd-expression takes one of the forms:

  1. $\mathrm{GCD}(f(\boldsymbol{y}), g(\boldsymbol{y})) = h(\boldsymbol{y})$
  2. $\mathrm{GCD}(f(\boldsymbol{y}), g(\boldsymbol{y})) = a\zeta$
  3. $\mathrm{GCD}(a\zeta, g(\boldsymbol{y})) = b\eta$
  4. $\mathrm{GCD}(a\zeta, b\eta) = c\theta$,

- $L_{\mathcal{R}}^{x} \subseteq L_{\mathcal{R}}$ comprise formulas $\exists \boldsymbol{\alpha} \bigvee_{j \in J_2} \widetilde{\varphi}_j(x, \boldsymbol{z_j}, \boldsymbol{\alpha})$ for some finite index set J_2 and formulas $\widetilde{\varphi}_j(x, \boldsymbol{z}, \boldsymbol{\alpha})$ of the form

$$\boldsymbol{\alpha} \geq 1 \wedge \boldsymbol{z} \geq 0 \wedge x \geq 0 \wedge \widetilde{\widetilde{\varphi}}_j(\boldsymbol{z}, \boldsymbol{\alpha}) \wedge \bigwedge_{i \in [1..\widetilde{m}_j]} \mathrm{GCD}(\widetilde{f}_{i,j}(\boldsymbol{z}, \boldsymbol{\alpha}), \widetilde{g}_{i,j}(\boldsymbol{z}) + c_{i,j} x) = \widetilde{h}_{i,j}(\boldsymbol{z}, \boldsymbol{\alpha}),$$

Quasi-quantifier elimination for addition and GCD

- $L_{\mathcal{R}}$ is the set of formulas $\exists \boldsymbol{\alpha} \bigvee_{j \in J} \varphi_j(\boldsymbol{y_j}, \boldsymbol{\alpha})$ for some finite index set J and formulas $\varphi_j(\boldsymbol{y}, \boldsymbol{\alpha})$ of the form

$$\boldsymbol{\alpha} \geq 1 \wedge \boldsymbol{y} \geq 0 \wedge \bigwedge_{i \in [1..m_j]} \mathrm{GCD}(f_{i,j}(\boldsymbol{y}, \boldsymbol{\alpha}), g_{i,j}(\boldsymbol{y}, \boldsymbol{\alpha})) = h_{i,j}(\boldsymbol{y}, \boldsymbol{\alpha}),$$

  where every gcd-expression takes one of the forms:

  1. $\mathrm{GCD}(f(\boldsymbol{y}), g(\boldsymbol{y})) = h(\boldsymbol{y})$
  2. $\mathrm{GCD}(f(\boldsymbol{y}), g(\boldsymbol{y})) = a\zeta$
  3. $\mathrm{GCD}(a\zeta, g(\boldsymbol{y})) = b\eta$
  4. $\mathrm{GCD}(a\zeta, b\eta) = c\theta,$

- $L_{\mathcal{R}}^{x} \subseteq L_{\mathcal{R}}$ comprise formulas $\exists \boldsymbol{\alpha} \bigvee_{j \in J_2} \widetilde{\varphi}_j(x, \boldsymbol{z_j}, \boldsymbol{\alpha})$ for some finite index set J_2 and formulas $\widetilde{\varphi}_j(x, \boldsymbol{z}, \boldsymbol{\alpha})$ of the form

$$\boldsymbol{\alpha} \geq 1 \wedge \boldsymbol{z} \geq 0 \wedge x \geq 0 \wedge \widetilde{\widetilde{\varphi}}_j(\boldsymbol{z}, \boldsymbol{\alpha}) \wedge \bigwedge_{i \in [1..\widetilde{m}_j]} \mathrm{GCD}(\widetilde{f}_{i,j}(\boldsymbol{z}, \boldsymbol{\alpha}), \widetilde{g}_{i,j}(\boldsymbol{z}) + c_{i,j} x) = \widetilde{h}_{i,j}(\boldsymbol{z}, \boldsymbol{\alpha}),$$

- GCD-Lemma at **Step 2** of $\mathcal{R}$ to eliminate x and obtain an $L_{\mathcal{R}}$-formula.

Reduction to a fragment of Skolem Arithmetic with constants

Every $L_{\mathcal{R}}$-formula with **only Greek variables** is a P$\exists L_\sigma$-formula for $\sigma = \left\langle 1, \{a\cdot\}_{a\in\mathbb{Z}_{>0}}, \mathrm{GCD}\right\rangle$.

Reduction to a fragment of Skolem Arithmetic with constants

Every $L_{\mathcal{R}}$-formula with **only Greek variables** is a $\mathrm{P}\exists L_\sigma$-formula for $\sigma = \left\langle 1, \{a\cdot\}_{a\in\mathbb{Z}_{>0}}, \mathrm{GCD}\right\rangle$.

Theorem

The decision problem for $\exists\mathrm{Th}\langle\mathbb{Z}; 1, +, -, \leq, \mathrm{GCD}\rangle$ *is reducible to the decision problem for* $\mathrm{P}\exists\mathrm{Th}\left\langle\mathbb{Z}_{>0}; 1, \{a\cdot\}_{a\in\mathbb{Z}_{>0}}, \mathrm{GCD}\right\rangle$*, where* $a\cdot$ *is a unary functional symbol for multiplication by a positive integer* a*.*

Reduction to a fragment of Skolem Arithmetic with constants

Every $L_{\mathcal{R}}$-formula with **only Greek variables** is a $\mathrm{P}\exists L_\sigma$-formula for $\sigma = \langle 1, \{a\cdot\}_{a\in\mathbb{Z}_{>0}}, \mathrm{GCD}\rangle$.

Theorem

The decision problem for $\exists\mathrm{Th}\langle\mathbb{Z}; 1, +, -, \leq, \mathrm{GCD}\rangle$ is reducible to the decision problem for $\mathrm{P}\exists\mathrm{Th}\langle\mathbb{Z}_{>0}; 1, \{a\cdot\}_{a\in\mathbb{Z}_{>0}}, \mathrm{GCD}\rangle$, where $a\cdot$ is a unary functional symbol for multiplication by a positive integer a.

- Skolem Arithmetic with constants $\mathrm{Th}\langle\mathbb{Z}_{>0}; \{a\}_{a\in\mathbb{Z}_{>0}}, \cdot, =\rangle$ is decidable [Barth D., Beck M., Dose T., Glaßer C., Michler L., Technau M. "Emptiness Problems for Integer Circuits" 2017].

Reduction to a fragment of Skolem Arithmetic with constants

Every $L_{\mathcal{R}}$-formula with **only Greek variables** is a P$\exists L_\sigma$-formula for $\sigma = \langle 1, \{a\cdot\}_{a\in\mathbb{Z}_{>0}}, \mathrm{GCD}\rangle$.

Theorem

The decision problem for $\exists\mathrm{Th}\langle\mathbb{Z}; 1, +, -, \leq, \mathrm{GCD}\rangle$ *is reducible to the decision problem for* $\mathrm{P}\exists\mathrm{Th}\langle\mathbb{Z}_{>0}; 1, \{a\cdot\}_{a\in\mathbb{Z}_{>0}}, \mathrm{GCD}\rangle$*, where* $a\cdot$ *is a unary functional symbol for multiplication by a positive integer* a*.*

- Skolem Arithmetic with constants $\mathrm{Th}\langle\mathbb{Z}_{>0}; \{a\}_{a\in\mathbb{Z}_{>0}}, \cdot, =\rangle$ is decidable [Barth D., Beck M., Dose T., Glaßer C., Michler L., Technau M. "Emptiness Problems for Integer Circuits" 2017].
- The proof of the BL-Theorem now follows from

$$\mathrm{GCD}(x, y) = z \Leftrightarrow z \mid x \wedge z \mid y \wedge \forall t(t \mid x \wedge t \mid y \Rightarrow t \mid z),$$

where $x \mid y \rightleftharpoons \exists z(y = z \cdot x)$.

Questions

P∃-Definability in $\langle \mathbb{Z}; 1, +, \leq, \perp \rangle$

- Dis-coprimeness $\not\perp$ is P∃-definable?

Questions

P∃-Definability in $\langle \mathbb{Z}; 1, +, \leq, \perp \rangle$

- Dis-coprimeness $\not\perp$ is P∃-definable?
- More general decidable ∀∃-fragment of $\langle \mathbb{Z}; 1, +, -, \leq, | \rangle$?

Questions

P∃-Definability in $\langle \mathbb{Z}; 1, +, \leq, \perp \rangle$

- Dis-coprimeness $\not\perp$ is P∃-definable?
- More general decidable ∀∃-fragment of $\langle \mathbb{Z}; 1, +, -, \leq, | \rangle$?

Complexity of $A\boldsymbol{x} = B \wedge C\boldsymbol{x} \geq D \wedge \bigwedge_{i \in [1..m]} \mathrm{GCD}(f_i(\boldsymbol{x}), g_i(\boldsymbol{x})) = d_i$

Questions

P∃-Definability in $\langle \mathbb{Z}; 1, +, \leq, \perp \rangle$

- Dis-coprimeness $\not\perp$ is P∃-definable?
- More general decidable ∀∃-fragment of $\langle \mathbb{Z}; 1, +, -, \leq, | \rangle$?

Complexity of $A\boldsymbol{x} = B \wedge C\boldsymbol{x} \geq D \wedge \bigwedge_{i \in [1..m]} \mathrm{GCD}(f_i(\boldsymbol{x}), g_i(\boldsymbol{x})) = d_i$

- **Polynomial** upper bound on small solutions?

Questions

P∃-Definability in $\langle \mathbb{Z}; 1, +, \leq, \perp \rangle$

- Dis-coprimeness $\not\perp$ is P∃-definable?
- More general decidable ∀∃-fragment of $\langle \mathbb{Z}; 1, +, -, \leq, | \rangle$?

Complexity of $A\boldsymbol{x} = B \wedge C\boldsymbol{x} \geq D \wedge \bigwedge_{i \in [1..m]} \mathrm{GCD}(f_i(\boldsymbol{x}), g_i(\boldsymbol{x})) = d_i$

- **Polynomial** upper bound on small solutions?
- Satisfiability check in **polynomial time** when size of $\boldsymbol{x}$ is fixed?

Questions

P∃-Definability in $\langle \mathbb{Z}; 1, +, \leq, \perp \rangle$

- Dis-coprimeness $\not\perp$ is P∃-definable?
- More general decidable ∀∃-fragment of $\langle \mathbb{Z}; 1, +, -, \leq, | \rangle$?

Complexity of $A\boldsymbol{x} = B \wedge C\boldsymbol{x} \geq D \wedge \bigwedge_{i \in [1..m]} \mathrm{GCD}(f_i(\boldsymbol{x}), g_i(\boldsymbol{x})) = d_i$

- **Polynomial** upper bound on small solutions?
- Satisfiability check in **polynomial time** when size of $\boldsymbol{x}$ is fixed?
- $\underline{\exists L_{PA}\text{-formulas}}$: true and for $\underline{\exists L_{PAD}\text{-formulas}}$: false.

Questions

P∃-Definability in $\langle \mathbb{Z}; 1, +, \leq, \perp \rangle$

- Dis-coprimeness $\not\perp$ is P∃-definable?
- More general decidable ∀∃-fragment of $\langle \mathbb{Z}; 1, +, -, \leq, | \rangle$?

Complexity of $A\boldsymbol{x} = B \wedge C\boldsymbol{x} \geq D \wedge \bigwedge_{i \in [1..m]} \mathrm{GCD}(f_i(\boldsymbol{x}), g_i(\boldsymbol{x})) = d_i$

- **Polynomial** upper bound on small solutions?
- Satisfiability check in **polynomial time** when size of $\boldsymbol{x}$ is fixed?
- $\underline{\exists L_{PA}\text{-formulas}}$: true and for $\underline{\exists L_{PAD}\text{-formulas}}$: false.

Thanks for your attention !