On Deciding Linear Arithmetic Constraints Over p-adic Integers for All Primes

Christoph Haase and **Alessio Mansutti**

University of Oxford

Groupement de recherche IM Informatique Mathématique

advanced reasoning in arithmetic theories

Diophantine systems and arithmetic theories

- Presburger arithmetic: first-order theory of $\langle \mathbb{Z}, 0, 1, <, + \rangle$
  Decidable (Presburger,'29) *in* 2EXPSPACE (Reddy & Loveland,'78)

- Büchi arithmetic: first-order theory of $\langle \mathbb{Z}, 0, 1, <, +, V_p \rangle$
  Decidable in non-elementary time (Bruyère, '85)

- existential theory of $\langle \mathbb{Z}, 0, 1, =, +, \cdot \rangle$
  Undecidable (Matiyasevich, Robinson, Davis & Putnam,'70)

- existential theory of $\langle \mathbb{Z}, 0, 1, <, +, | \rangle$
  Decidable (Lipshitz, '78) *in* NEXPTIME (Lechner et al., '15)

Lipshitz (1978): local-to-global principle for $\langle \mathbb{Z}, 0, 1, <, +, | \rangle$

Consider a formula $\Phi \stackrel{\text{def}}{=} \bigwedge_{i \in I} f_i(\mathbf{x}) \mid g_i(\mathbf{x})$ from $\langle \mathbb{Z}, 0, 1, <, +, | \rangle$.

If Φ is in *increasing normal form (INF)*, then

Φ has a solution over $\mathbb{Z}$ if and only if

$\bigwedge_{i \in I} v_p(f_i(\mathbf{x})) \leq v_p(g_i(\mathbf{x}))$ has a solution over $\mathbb{Z}_p$, for every prime p.

Lipshitz (1978): local-to-global principle for $\langle \mathbb{Z}, 0, 1, <, +, | \rangle$

Consider a formula $\Phi \stackrel{\text{def}}{=} \bigwedge_{i \in I} f_i(\mathbf{x}) \mid g_i(\mathbf{x})$ from $\langle \mathbb{Z}, 0, 1, <, +, | \rangle$.

If Φ is in *increasing normal form (INF)*, then

Φ has a solution over $\mathbb{Z}$ if and only if

$\bigwedge_{i \in I} v_p(f_i(\mathbf{x})) \leq v_p(g_i(\mathbf{x}))$ has a solution over $\mathbb{Z}_p$, for every prime p.

p-adic integers

Lipshitz (1978): local-to-global principle for $\langle \mathbb{Z}, 0, 1, <, +, | \rangle$

Consider a formula $\Phi \stackrel{\text{def}}{=} \bigwedge_{i \in I} f_i(\mathbf{x}) \mid g_i(\mathbf{x})$ from $\langle \mathbb{Z}, 0, 1, <, +, | \rangle$.

If Φ is in *increasing normal form (INF)*, then

Φ has a solution over $\mathbb{Z}$ if and only if

$\bigwedge_{i \in I} v_p(f_i(\mathbf{x})) \leq v_p(g_i(\mathbf{x}))$ has a solution over $\mathbb{Z}_p$, for every prime p.

$v_p(n) = \max\{k : p^k \mid n\}$

Lipshitz (1978): local-to-global principle for $\langle \mathbb{Z}, 0, 1, <, +, | \rangle$

Consider a formula $\Phi \stackrel{\text{def}}{=} \bigwedge_{i \in I} f_i(\mathbf{x}) \mid g_i(\mathbf{x})$ from $\langle \mathbb{Z}, 0, 1, <, +, | \rangle$.

If Φ is in *increasing normal form (INF)*, then

Φ has a solution over $\mathbb{Z}$ if and only if

$\bigwedge_{i \in I} v_p(f_i(\mathbf{x})) \leq v_p(g_i(\mathbf{x}))$ has a solution over $\mathbb{Z}_p$, for every prime p.

Question: Can we decide these *universality* questions in general?

In this talk...

...we consider formulae Φ from

- linear arithmetic over p-adic integers; or
- existential Büchi arithmetic,

and study the following decision problems:

p-UNIVERSALITY: Is Φ satisfiable for all bases $p \geq 2$ / p prime?

p-EXISTENCE: Is Φ satisfiable for some base $p \geq 2$ / p prime?

In this talk...

...we consider formulae Φ from

- linear arithmetic over p-adic integers; or
- existential Büchi arithmetic,

and study the following decision problems:

p-UNIVERSALITY: Is Φ satisfiable for all bases $p \geq 2$ / p prime?

p-EXISTENCE: Is Φ satisfiable for some base $p \geq 2$ / p prime?

Theorem 1

For both theories, p-UNIVERSALITY *is in* coNEXP *and* p-EXISTENCE *is in* NEXP.

Theorem 2

For Büchi arithmetic, p-UNIVERSALITY *is* coNEXP*-hard.*

p-adic numbers

Fix a prime number p.

p-adic valuation $v_p(.) \colon \mathbb{Q} \to \overline{\mathbb{Z}}$, with $\overline{\mathbb{Z}} \stackrel{\text{def}}{=} \mathbb{Z} \cup \{\infty\}$:

$$v_p(0) \stackrel{\text{def}}{=} \infty$$

$$v_p(q) = k \text{ iff } q = p^k \cdot \frac{a}{b} \text{ for some } a, b \in \mathbb{Z} \text{ coprime with } p.$$

p-adic numbers

Fix a prime number p.

p-adic valuation $v_p(.) \colon \mathbb{Q} \to \overline{\mathbb{Z}}$, with $\overline{\mathbb{Z}} \stackrel{\text{def}}{=} \mathbb{Z} \cup \{\infty\}$:

$$v_p(0) \stackrel{\text{def}}{=} \infty$$

$$v_p(q) = k \text{ iff } q = p^k \cdot \frac{a}{b} \text{ for some } a, b \in \mathbb{Z} \text{ coprime with } p.$$

p-adic numbers $\mathbb{Q}_p$:

Cauchy completion of $\mathbb{Q}$ under the p-adic norm $|q|_p \stackrel{\text{def}}{=} p^{-v_p(q)}$.

p-adic numbers : representations

p-adic expansion of $r \in \mathbb{Q}_p \setminus \{0\}$:

$$r = \sum_{i=k}^{\infty} a_i \cdot p^i \qquad \text{where } k \in \mathbb{Z},\ a_k \neq 0 \text{ and } a_i \in [0, p-1], \text{ for all } i.$$

p-adic numbers : representations

p-adic expansion of $r \in \mathbb{Q}_p \setminus \{0\}$:

$$r = \sum_{i=k}^{\infty} a_i \cdot p^i \qquad \text{where } k \in \mathbb{Z},\ a_k \neq 0 \text{ and } a_i \in [0, p-1], \text{ for all } i.$$

- $v_p(r) = k$,
- p-adic integers $\mathbb{Z}_p$: $r \in \mathbb{Q}_p$ s.t. $v_p(r) \geq 0$.

p-adic numbers : representations

p-adic expansion of $r \in \mathbb{Q}_p \setminus \{0\}$:

$$r = \sum_{i=k}^{\infty} a_i \cdot p^i \qquad \text{where } k \in \mathbb{Z},\ a_k \neq 0 \text{ and } a_i \in [0, p-1], \text{ for all } i.$$

- $v_p(r) = k$,
- p-adic integers $\mathbb{Z}_p$: $r \in \mathbb{Q}_p$ s.t. $v_p(r) \geq 0$.

lsd-first encoding for $\mathbb{Z}_p$:

- The ω-word $w = u_0 u_1 \cdots \in [0, p-1]^\omega$ encodes

$$[\![w]\!]_p = \sum_{i=0}^{\infty} u_i \cdot p^i.$$

- $v_p([\![w]\!]_p) = k$ if and only if $w \in \{0\}^{k-1}[1, p-1][0, p-1]^\omega$.

Linear arithmetic over p-adic integers

Existential theory of the structure $(\{\mathbb{Z}_p, \overline{\mathbb{Z}}\}, 0, 1, +, =, <, v_p)$.

- 0, 1, $+$ and $=$, defined for both sorts.
- $<$: *less-than* relation on $\overline{\mathbb{Z}}$.
- v_p : p-*adic valuation* ($\mathbb{Z}_p \to \overline{\mathbb{Z}}$).

Linear arithmetic over p-adic integers

Existential theory of the structure $(\{\mathbb{Z}_p, \overline{\mathbb{Z}}\}, 0, 1, +, =, <, v_p)$.

- 0, 1, $+$ and $=$, defined for both sorts.
- $<$: *less-than* relation on $\overline{\mathbb{Z}}$.
- v_p: p*-adic valuation* ($\mathbb{Z}_p \to \overline{\mathbb{Z}}$).

E.g.,

- $u = 2 \land v_p(u) = 0,$ $\qquad$ p-existential, not p-universal.

Linear arithmetic over p-adic integers

Existential theory of the structure $(\{\mathbb{Z}_p, \overline{\mathbb{Z}}\}, 0, 1, +, =, <, v_p)$.

- 0, 1, $+$ and $=$, defined for both sorts.
- $<$: *less-than* relation on $\overline{\mathbb{Z}}$.
- v_p: p-*adic valuation* ($\mathbb{Z}_p \to \overline{\mathbb{Z}}$).

E.g.,

- $u = 2 \wedge v_p(u) = 0$, p-existential, not p-universal.
- $u \neq 2 \vee v_p(u) \neq 0$, p-existential, p-universal.

Linear arithmetic over p-adic integers

Existential theory of the structure $(\{\mathbb{Z}_p, \overline{\mathbb{Z}}\}, 0, 1, +, =, <, v_p)$.

- 0, 1, $+$ and $=$, defined for both sorts.
- $<$: *less-than* relation on $\overline{\mathbb{Z}}$.
- v_p: p-*adic valuation* ($\mathbb{Z}_p \to \overline{\mathbb{Z}}$).

E.g.,

- $u = 2 \wedge v_p(u) = 0$, p-existential, not p-universal.
- $u \neq 2 \vee v_p(u) \neq 0$, p-existential, p-universal.
- $A \cdot \mathbf{u} = \mathbf{c} \wedge B \cdot \mathbf{x} \geq \mathbf{d} \wedge \bigwedge_{(i,j)\in J} v_p(u_i) = x_j$.

p-automata for linear systems (Wolper & Boigelot, '00)

(msd-first) p-automaton $\langle \Sigma_p, Q, \delta_p, \mathbf{q}_0, F \rangle$ for the system $A \cdot \mathbf{x} = \mathbf{c}$ with $A \in \mathbb{Z}^{n \times d}$ and $\mathbf{c} \in \mathbb{Z}^n$:

- alphabet: $\Sigma_p = [0, p-1]^d$,
- states: $Q = \mathbb{Z}^n$, initial state: $\mathbf{q}_0 = \mathbf{0}$, final states: $F = \{\mathbf{c}\}$,
- transition function: $\delta_p(\mathbf{q}, \mathbf{u}) = p \cdot \mathbf{q} + A \cdot \mathbf{u}$.

p-automata for linear systems (Wolper & Boigelot, '00)

(msd-first) p-automaton $\langle \Sigma_p, Q, \delta_p, \mathbf{q}_0, F \rangle$ for the system $A \cdot \mathbf{x} = \mathbf{c}$

with $A \in \mathbb{Z}^{n \times d}$ and $\mathbf{c} \in \mathbb{Z}^n$:

- alphabet: $\Sigma_p = [0, p-1]^d$,
- states: $Q = \mathbb{Z}^n$, initial state: $\mathbf{q}_0 = \mathbf{0}$, final states: $F = \{\mathbf{c}\}$,
- transition function: $\delta_p(\mathbf{q}, \mathbf{u}) = p \cdot \mathbf{q} + A \cdot \mathbf{u}$.

$$\mathbf{x} = \mathbf{u}_0 \cdot p^\ell + \mathbf{u}_1 \cdot p^{\ell-1} + \mathbf{u}_2 \cdot p^{\ell-2} + \cdots + \mathbf{u}_\ell \quad \in \ \mathbb{N}^d$$

$$A \cdot \mathbf{x} = \mathbf{c} \text{ if and only if } \mathbf{0} \xrightarrow{\mathbf{u}_0 \mathbf{u}_1 \dots \mathbf{u}_\ell} \mathbf{c}$$

$\mathbf{s} \xrightarrow{\mathbf{u}} \mathbf{t}$ iff $\delta(\mathbf{s}, \mathbf{u}) = \mathbf{t}$,

$\mathbf{s} \xrightarrow{w\,\mathbf{u}} \mathbf{t}$ iff there is $\mathbf{r} \in \mathbb{Z}^n$ such that $\mathbf{s} \xrightarrow{w} \mathbf{r}$ and $\mathbf{r} \xrightarrow{\mathbf{u}} \mathbf{t}$. $\quad \mathbf{u} \in \Sigma, w \in \Sigma^*$

p-automata for linear systems (Wolper & Boigelot, '00)

(msd-first) p-automaton $\langle \Sigma_p, Q, \delta_p, \mathbf{q}_0, F \rangle$ for the system $A \cdot \mathbf{x} = \mathbf{c}$ with $A \in \mathbb{Z}^{n \times d}$ and $\mathbf{c} \in \mathbb{Z}^n$:

- alphabet: $\Sigma_p = [0, p-1]^d$,
- states: $Q = \mathbb{Z}^n$, initial state: $\mathbf{q}_0 = \mathbf{0}$, final states: $F = \{\mathbf{c}\}$,
- transition function: $\delta_p(\mathbf{q}, \mathbf{u}) = p \cdot \mathbf{q} + A \cdot \mathbf{u}$.

$w = \mathbf{u}_0 \mathbf{u}_1 \cdots \in \Sigma_p^\omega$ is the lsd-first encoding of $[\![w]\!]_p = \sum_{i=0}^{\infty} p^i \cdot \mathbf{u}_i$.

Proposition (acceptance)

$A \cdot [\![w]\!]_p = \mathbf{c}$ if and only if in the p-automaton for $A \cdot \mathbf{x} = \mathbf{c}$, there is $\mathbf{r} \in Q$ and a strictly ascending sequence $(\lambda_i)_{i \in \mathbb{N}}$ such that

$$\mathbf{r} \xrightarrow{\mathbf{u}_{\lambda_0 - 1} \cdots \mathbf{u}_0} \mathbf{c} \quad \textit{and} \quad \mathbf{r} \xrightarrow{\mathbf{u}_{\lambda_{j+1} - 1} \cdots \mathbf{u}_j} \mathbf{r}, \textit{ for all } j \in \mathbb{N}.$$

Towards p-universality I: live states

Question: How does the set of live states looks for different p?

- Live states $\mathcal{L}$: states that reach an accepting state.

Proposition (finiteness, Wolper & Boigelot, '00)

Every live state $\mathbf{q} \in \mathcal{L}$ of the p-automaton for $A \cdot \mathbf{x} = \mathbf{c}$ is s.t.

$$\|\mathbf{q}\|_\infty \leq \max(d \cdot \|A\|_\infty, \|\mathbf{c}\|_\infty).$$

Key properties: we can restrict the set of states Q to a finite set that does not depend on the base p.

Towards p-universality II: bases for a single transition

Consider $\mathfrak{S}\colon A \cdot \mathbf{x} = \mathbf{c}$ with $A \in \mathbb{Z}^{n \times d}$, and two vectors $\mathbf{s}, \mathbf{t} \in \mathbb{Z}^n$.

Question: For which bases $p \geq 2$ does the p-automaton for $\mathfrak{S}$ have a transition $\mathbf{s} \xrightarrow{\mathbf{u}} \mathbf{t}$ for some $\mathbf{u} \in \Sigma_p$?

Towards p-universality II: bases for a single transition

Consider $\mathfrak{S}\colon A \cdot \mathbf{x} = \mathbf{c}$ with $A \in \mathbb{Z}^{n \times d}$, and two vectors $\mathbf{s}, \mathbf{t} \in \mathbb{Z}^n$.

Question: For which bases $p \geq 2$ does the p-automaton for $\mathfrak{S}$ have a transition $\mathbf{s} \xrightarrow{\mathbf{u}} \mathbf{t}$ for some $\mathbf{u} \in \Sigma_p$?

We characterise the set B of such bases:

$$
\begin{aligned}
B &= \{p \geq 2 : \exists \mathbf{u} \in \Sigma_p, \delta_p(\mathbf{s}, \mathbf{u}) = \mathbf{t}\} \\
&= \{p \in \mathbb{N} : p \geq 2 \land \exists \mathbf{u} \, (\max \mathbf{u} < p \land p \cdot \mathbf{s} + A \cdot \mathbf{u} = \mathbf{t})\}
\end{aligned}
$$

Towards p-universality II: bases for a single transition

Consider $\mathfrak{S}\colon A \cdot \mathbf{x} = \mathbf{c}$ with $A \in \mathbb{Z}^{n \times d}$, and two vectors $\mathbf{s}, \mathbf{t} \in \mathbb{Z}^n$.

Question: For which bases $p \geq 2$ does the p-automaton for $\mathfrak{S}$ have a transition $\mathbf{s} \xrightarrow{\mathbf{u}} \mathbf{t}$ for some $\mathbf{u} \in \Sigma_p$?

We characterise the set B of such bases:

$$\begin{aligned} B &= \{p \geq 2 : \exists \mathbf{u} \in \Sigma_p, \delta_p(\mathbf{s}, \mathbf{u}) = \mathbf{t}\} \\ &= \{p \in \mathbb{N} : \underbrace{p \geq 2 \wedge \exists \mathbf{u}\, (\max \mathbf{u} < p \wedge p \cdot \mathbf{s} + A \cdot \mathbf{u} = \mathbf{t})}_{\text{existential Presburger formula with free variable } p}\} \end{aligned}$$

Towards p-universality II: bases for a single transition

Consider $\mathfrak{S}\colon A \cdot \mathbf{x} = \mathbf{c}$ with $A \in \mathbb{Z}^{n \times d}$, and two vectors $\mathbf{s}, \mathbf{t} \in \mathbb{Z}^n$.

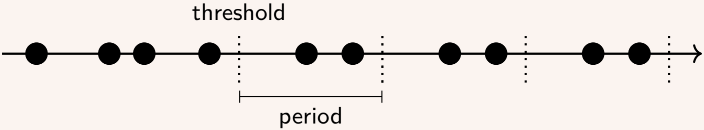
Question: For which bases $p \geq 2$ does the p-automaton for $\mathfrak{S}$ have a transition $\mathbf{s} \xrightarrow{\mathbf{u}} \mathbf{t}$ for some $\mathbf{u} \in \Sigma_p$?

We characterise the set B of such bases:

Proposition (bases characterisation)

The set B is an ultimately periodic set with period and threshold bounded by $||A \mid \mathbf{s} \mid \mathbf{t}||_\infty^{O((n+d)log(n+d))}$.

Ultimately periodic set:



Key structural result

Consider Φ from linear arithmetic over p-adic integers.

Proposition

The set B of bases $p \geq 2$ for which Φ is satisfiable is an ultimately periodic set with period and threshold bounded by $2^{2^{\mathcal{O}(|\Phi|^2)}}$.

Key structural result

Consider Φ from linear arithmetic over p-adic integers.

Proposition

The set B of bases $p \geq 2$ for which Φ is satisfiable is an ultimately periodic set with period and threshold bounded by $2^{2^{\mathcal{O}(|\Phi|^2)}}$.

- By Linnik's theorem, if B (equiv., $\mathbb{N} \setminus B$) contains a prime, then it has one bonded by $2^{2^{\mathcal{O}(|\Phi|^2)}}$

$\Rightarrow$ p-UNIVERSALITY is in coNEXP, and
p-EXISTENCE is in NEXP.

The same result is established for existential Büchi arithmetic.

Existential Büchi arithmetic

Existential theory of the structure $\langle \mathbb{N}, 0, 1, +, =, V_p \rangle$

- $V_p(0) = 1$
- if $n \geq 1$, $V_p(n) = p^{v_p(n)}$ (i.e. largest power of p that divides n)
- Note: p is not necessarily a prime number.

Existential Büchi arithmetic

Existential theory of the structure $\langle \mathbb{N}, 0, 1, +, =, V_p \rangle$

- $V_p(0) = 1$
- if $n \geq 1$, $V_p(n) = p^{v_p(n)}$ (i.e. largest power of p that divides n)
- Note: p is not necessarily a prime number.

Theorem 2

The p-UNIVERSALITY problem for existential Büchi arithmetic is hard for coNEXP.

- Proof by reduction from the coNEXP-complete problem $\mathrm{QO\Pi_1}$-SAT [L. Babai et al., CC'91].

$\mathrm{QO\Pi_1\text{-}SAT}$ to p-UNIVERSALITY

$\mathrm{QO\Pi_1\text{-}SAT}$:

Input: (Ψ, m, n) with $m \leq n$ encoded in unary and Ψ Boolean combination of $x_1, \dots, x_n, f(x_1, \dots, x_m)$.

Question: Is $\forall f \in [\{0,1\}^m \to \{0,1\}]\, \exists x_1, \dots, x_n \in \{0,1\} \Psi$ true?

Main difficulty: encode the function f using the base p.

$\mathrm{QO}\Pi_1$-SAT to p-UNIVERSALITY

$\mathrm{QO}\Pi_1$-SAT :

Input: (Ψ, m, n) with $m \leq n$ encoded in unary and Ψ Boolean combination of $x_1, \ldots, x_n, f(x_1, \ldots, x_m)$.

Question: Is $\forall f \in [\{0,1\}^m \to \{0,1\}]\, \exists x_1, \ldots, x_n \in \{0,1\} \Psi$ true?

Main difficulty: encode the function f using the base p.

$\mathrm{QO\Pi_1}$-SAT to p-UNIVERSALITY

$\mathrm{QO\Pi_1}$-SAT :

Input: (Ψ, m, n) with $m \leq n$ encoded in unary and Ψ Boolean combination of $x_1, \dots, x_n, f(x_1, \dots, x_m)$.

Question: Is $\forall f \in [\{0,1\}^m \to \{0,1\}]\, \exists x_1, \dots, x_n \in \{0,1\} \Psi$ true?

Main difficulty: encode the function f using the base p.

We say that $z \in \mathbb{N}$ encodes f iff for all $b, b_0, \dots, b_{m-1} \in [0,1]$,

$$f(b_0, \dots, b_{m-1}) = b \;\Leftrightarrow z \equiv b \bmod q, \text{for all primes } q \in [k^3, (k+1)^3),$$

$$\text{where } k = \textstyle\sum_{i=0}^{m-1} 2^i \cdot b_i.$$

$\mathrm{QO\Pi_1}$-SAT to p-UNIVERSALITY

$\mathrm{QO\Pi_1}$-SAT :

Input: (Ψ, m, n) with $m \leq n$ encoded in unary and Ψ Boolean combination of $x_1, \ldots, x_n, f(x_1, \ldots, x_m)$.

Question: Is $\forall f \in [\{0,1\}^m \to \{0,1\}]\, \exists x_1, \ldots, x_n \in \{0,1\} \Psi$ true?

Main difficulty: encode the function f using the base p.

We say that $z \in \mathbb{N}$ encodes f iff for all $b, b_0, \ldots, b_{m-1} \in [0,1]$,

Ingham's theorem

$$f(b_0, \ldots, b_{m-1}) = b \iff z \equiv b \bmod q, \text{for all primes } q \in [k^3, (k+1)^3),$$

where $k = \sum_{i=0}^{m-1} 2^i \cdot b_i$.

$\mathrm{QO\Pi_1}$-SAT to p-UNIVERSALITY

$\mathrm{QO\Pi_1}$-SAT :

Input: (Ψ, m, n) with $m \leq n$ encoded in unary and Ψ Boolean combination of $x_1, \dots, x_n, f(x_1, \dots, x_m)$.

Question: Is $\forall f \in [\{0,1\}^m \to \{0,1\}]\, \exists x_1, \dots, x_n \in \{0,1\} \Psi$ true?

Main difficulty: encode the function f using the base p.

We say that $z \in \mathbb{N}$ encodes f iff for all $b, b_0, \dots, b_{m-1} \in [0,1]$,

Chinese remainder theorem

$f(b_0, \dots, b_{m-1}) = b \iff z \equiv b \bmod q$, for all primes $q \in [k^3, (k+1)^3)$,

where $k = \sum_{i=0}^{m-1} 2^i \cdot b_i$.

$\mathrm{QO\Pi_1\text{-}SAT}$ to p-UNIVERSALITY

$\mathrm{QO\Pi_1\text{-}SAT}$:

Input: (Ψ, m, n) with $m \leq n$ encoded in unary and Ψ Boolean combination of $x_1, \dots, x_n, f(x_1, \dots, x_m)$.

Question: Is $\forall f \in [\{0,1\}^m \to \{0,1\}]\, \exists x_1, \dots, x_n \in \{0,1\} \Psi$ true?

- every f is encoded by some $z \geq 2$,
- for all $i \geq 1$, z encodes f if and only if z^i encodes f,
- q.f. formula $\phi_{\mathsf{invalid}}(z)$, true iff z does not encode some f.

(Ψ, m, n) is a yes instance of $\mathrm{QO\Pi_1\text{-}SAT}$ if and only if

$$V_p(z) = z \wedge z \geq 2 \wedge (\phi_{\mathsf{invalid}}(z) \vee \Psi^T) \text{ is } p\text{-universal.}$$

Conclusion

We studied the p-UNIVERSALITY and p-EXISTENCE problems for linear arithmetic over $\mathbb{Z}_p$ and existential Büchi arithmetic.

Theorem 1

For both theories, p-UNIVERSALITY *is in* coNEXP *and*
p-EXISTENCE *is in* NEXP.

Theorem 2

For Büchi arithmetic, p-UNIVERSALITY *is* coNEXP*-hard.*

Conclusion

We studied the p-UNIVERSALITY and p-EXISTENCE problems for linear arithmetic over $\mathbb{Z}_p$ and existential Büchi arithmetic.

Theorem 1

For both theories, p-UNIVERSALITY *is in* coNEXP *and* p-EXISTENCE *is in* NEXP.

Theorem 2

For Büchi arithmetic, p-UNIVERSALITY *is* coNEXP*-hard.*

Open problems:

- tight bound for the p-UNIVERSALITY problem of linear arithmetic over p-adic integers.
- improved upper bound on p-EXISTENCE.
- p-UNIVERSALITY for full Büchi arithmetic.