Polynomial-time Tractable Problems over the p-adic Numbers

Manuel Bodirsky

Institut für Algebra, TU Dresden

Joint work with Arno Fehm

Warsaw, 26.8.2025

ERC Synergy Grant POCOCOP (GA 101071674).

Outline

1. Computational Problems over Rings
2. Problems about $\mathbb{Q}_p$ left open by Guépin, Haase, and Worrel
3. Two polynomial-time algorithms
4. Consequences for satisfiability problems over $\mathbb{Q}$.

Satisfiability problems over rings

Fixed: Ring R.
Input: Given a system Σ of polynomial equations with integer coefficients.
Question: Is there a solution to Σ over R?

Satisfiability problems over rings

Fixed: Ring R.
Input: Given a system Σ of polynomial equations with integer coefficients.
Question: Is there a solution to Σ over R?

Computational Complexity:

Satisfiability problems over rings

Fixed: Ring R.
Input: Given a system Σ of polynomial equations with integer coefficients.
Question: Is there a solution to Σ over R?

Computational Complexity:

Ring	Linear equations	Linear inequalities	Polynomial equations
$\mathbb{R}$	in P (Gauss)	in P (Ellipsoid)	in PSPACE, NP-hard

Satisfiability problems over rings

Fixed: Ring R.
Input: Given a system Σ of polynomial equations with integer coefficients.
Question: Is there a solution to Σ over R?

Computational Complexity:

Ring	Linear equations	Linear inequalities	Polynomial equations
$\mathbb{R}$	in P (Gauss)	in P (Ellipsoid)	in PSPACE, NP-hard
$\mathbb{Q}$	in P	in P	Decidability open

Satisfiability problems over rings

Fixed: Ring R.
Input: Given a system Σ of polynomial equations with integer coefficients.
Question: Is there a solution to Σ over R?

Computational Complexity:

Ring	Linear equations	Linear inequalities	Polynomial equations
$\mathbb{R}$	in P (Gauss)	in P (Ellipsoid)	in PSPACE, NP-hard
$\mathbb{Q}$	in P	in P	Decidability open
$\mathbb{Z}$	NP-complete	in P (Hermit NF)	Undecidable

Satisfiability problems over rings

Fixed: Ring R.
Input: Given a system Σ of polynomial equations with integer coefficients.
Question: Is there a solution to Σ over R?

Computational Complexity:

Ring	Linear equations	Linear inequalities	Polynomial equations
$\mathbb{R}$	in P (Gauss)	in P (Ellipsoid)	in PSPACE, NP-hard
$\mathbb{Q}$	in P	in P	Decidability open
$\mathbb{Z}$	NP-complete	in P (Hermit NF)	Undecidable

Research directions:

Satisfiability problems over rings

Fixed: Ring R.
Input: Given a system Σ of polynomial equations with integer coefficients.
Question: Is there a solution to Σ over R?

Computational Complexity:

Ring	Linear equations	Linear inequalities	Polynomial equations
$\mathbb{R}$	in P (Gauss)	in P (Ellipsoid)	in PSPACE, NP-hard
$\mathbb{Q}$	in P	in P	Decidability open
$\mathbb{Z}$	NP-complete	in P (Hermit NF)	Undecidable

Research directions:

- different rings?

Satisfiability problems over rings

Fixed: Ring R.
Input: Given a system Σ of polynomial equations with integer coefficients.
Question: Is there a solution to Σ over R?

Computational Complexity:

Ring	Linear equations	Linear inequalities	Polynomial equations
$\mathbb{R}$	in P (Gauss)	in P (Ellipsoid)	in PSPACE, NP-hard
$\mathbb{Q}$	in P	in P	Decidability open
$\mathbb{Z}$	NP-complete	in P (Hermit NF)	Undecidable

Research directions:

- different rings?
- different constraint languages?

The p-adic Numbers

The p-adic Numbers

p: prime number.

The *p*-adic Numbers

p: prime number.
Field of *p*-adic numbers (Kummer, Hensel, . . .):

The p-adic Numbers

p: prime number.

Field of p-adic numbers (Kummer, Hensel, ...):

- Roughly: allows for *'taking modulo p^e for all e at once'*.

The p-adic Numbers

p: prime number.

Field of p-adic numbers (Kummer, Hensel, . . .):

- Roughly: allows for *'taking modulo p^e for all e at once'*.
- Many applications in number theory

The p-adic Numbers

p: prime number.

Field of p-adic numbers (Kummer, Hensel, ...):

- Roughly: allows for *'taking modulo p^e for all e at once'*.
- Many applications in number theory
- See survey on applications by Rozikov (2013)

The p-adic Numbers

p: prime number.

Field of p-adic numbers (Kummer, Hensel, ...):

- Roughly: allows for *'taking modulo p^e for all e at once'*.
- Many applications in number theory
- See survey on applications by Rozikov (2013)

p-adic valution: For $x \in \mathbb{Z}$ define $v_p(x) := \sup\{j : p^j | x\} \in \mathbb{N} \cup \{\infty\}$.

The p-adic Numbers

p: prime number.

Field of p-adic numbers (Kummer, Hensel, ...):

- Roughly: allows for *'taking modulo p^e for all e at once'*.
- Many applications in number theory
- See survey on applications by Rozikov (2013)

p-adic valution: For $x \in \mathbb{Z}$ define $v_p(x) := \sup\{j : p^j | x\} \in \mathbb{N} \cup \{\infty\}$.

Extend to $\mathbb{Q}$:

$$v_p\left(\frac{a}{b}\right) := v_p(a) - v_p(b).$$

The p-adic Numbers

p: prime number.
Field of p-adic numbers (Kummer, Hensel, ...):

- Roughly: allows for *'taking modulo p^e for all e at once'*.
- Many applications in number theory
- See survey on applications by Rozikov (2013)

p-adic valution: For $x \in \mathbb{Z}$ define $v_p(x) := \sup\{j : p^j | x\} \in \mathbb{N} \cup \{\infty\}$.
Extend to $\mathbb{Q}$:

$$v_p\left(\frac{a}{b}\right) := v_p(a) - v_p(b).$$

p-adic absolute value:

$$|x|_p := p^{-v_p(x)}$$

The p-adic Numbers

p: prime number.
Field of p-adic numbers (Kummer, Hensel, ...):

- Roughly: allows for *'taking modulo p^e for all e at once'*.
- Many applications in number theory
- See survey on applications by Rozikov (2013)

p-adic valution: For $x \in \mathbb{Z}$ define $v_p(x) := \sup\{j : p^j | x\} \in \mathbb{N} \cup \{\infty\}$.
Extend to $\mathbb{Q}$:

$$v_p\left(\frac{a}{b}\right) := v_p(a) - v_p(b).$$

p-adic absolute value:

$$|x|_p := p^{-v_p(x)}$$

$\mathbb{Q}_p$: completion of $\mathbb{Q}$ with respect to $|.|_p$
(similarly to $\mathbb{R}$ being the completion of $\mathbb{Q}$ with respect to $|.|$).

Satisfiability Problems over $\mathbb{Q}_p$

Guépin, Haase, and Worrel (LICS 2019):

Satisfiability Problems over $\mathbb{Q}_p$

Guépin, Haase, and Worrel (LICS 2019): Satisfiability of systems of linear equations with valuation constraints of the form $v_p(x) = c$

Satisfiability Problems over $\mathbb{Q}_p$

Guépin, Haase, and Worrel (LICS 2019): Satisfiability of systems of linear equations with valuation constraints of the form $v_p(x) = c$

- in NP

Satisfiability Problems over $\mathbb{Q}_p$

Guépin, Haase, and Worrel (LICS 2019): Satisfiability of systems of linear equations with valuation constraints of the form $v_p(x) = c$

- in NP
- NP-hard for $p \geq 5$

Satisfiability Problems over $\mathbb{Q}_p$

Guépin, Haase, and Worrel (LICS 2019): Satisfiability of systems of linear equations with valuation constraints of the form $v_p(x) = c$

- in NP
- NP-hard for $p \geq 5$
- "While we believe it to be the case, it remains an open problem whether an NP lower bound can be established for the cases $p = 2, 3$"

Satisfiability Problems over $\mathbb{Q}_p$

Guépin, Haase, and Worrel (LICS 2019): Satisfiability of systems of linear equations with valuation constraints of the form $v_p(x) = c$

- in NP
- NP-hard for $p \geq 5$
- "While we believe it to be the case, it remains an open problem whether an NP lower bound can be established for the cases $p = 2, 3$"

Our results answer this.

Satisfiability Problems over $\mathbb{Q}_p$

Guépin, Haase, and Worrel (LICS 2019): Satisfiability of systems of linear equations with valuation constraints of the form $v_p(x) = c$

- in NP
- NP-hard for $p \geq 5$
- "While we believe it to be the case, it remains an open problem whether an NP lower bound can be established for the cases $p = 2, 3$"

Our results answer this.

Let $\mathfrak{Q}_p := (\mathbb{Q}_p; +, 1, (\leq^p_c)_{c\in\mathbb{Z}}, (\geq^p_c)_{c\in\mathbb{Z}}, (=^p_c)_{c\in\mathbb{Z}}, (\neq^p_c)_{c\in\mathbb{Z}})$

Satisfiability Problems over $\mathbb{Q}_p$

Guépin, Haase, and Worrel (LICS 2019): Satisfiability of systems of linear equations with valuation constraints of the form $v_p(x) = c$

- in NP
- NP-hard for $p \geq 5$
- "While we believe it to be the case, it remains an open problem whether an NP lower bound can be established for the cases $p = 2, 3$"

Our results answer this.

Let $\mathfrak{Q}_p := (\mathbb{Q}_p; +, 1, (\leq^p_c)_{c \in \mathbb{Z}}, (\geq^p_c)_{c \in \mathbb{Z}}, (=^p_c)_{c \in \mathbb{Z}}, (\neq^p_c)_{c \in \mathbb{Z}})$ where

- $\leq^p_c$ is unary relation symbol for $\{x \in \mathbb{Q}_p \mid v_p(x) \leq c\}$,

Satisfiability Problems over $\mathbb{Q}_p$

Guépin, Haase, and Worrel (LICS 2019): Satisfiability of systems of linear equations with valuation constraints of the form $v_p(x) = c$

- in NP
- NP-hard for $p \geq 5$
- "While we believe it to be the case, it remains an open problem whether an NP lower bound can be established for the cases $p = 2, 3$"

Our results answer this.

Let $\mathfrak{Q}_p := (\mathbb{Q}_p; +, 1, (\leq^p_c)_{c \in \mathbb{Z}}, (\geq^p_c)_{c \in \mathbb{Z}}, (=^p_c)_{c \in \mathbb{Z}}, (\neq^p_c)_{c \in \mathbb{Z}})$ where

- $\leq^p_c$ is unary relation symbol for $\{x \in \mathbb{Q}_p \mid v_p(x) \leq c\}$,
- $\geq^p_c$, $=^p_c$, and $\neq^p_c$: defined analogously.

Satisfiability Problems over $\mathbb{Q}_p$

Guépin, Haase, and Worrel (LICS 2019): Satisfiability of systems of linear equations with valuation constraints of the form $v_p(x) = c$

- in NP
- NP-hard for $p \geq 5$
- "While we believe it to be the case, it remains an open problem whether an NP lower bound can be established for the cases $p = 2, 3$"

Our results answer this.

Let $\mathfrak{Q}_p := (\mathbb{Q}_p; +, 1, (\leq^p_c)_{c\in\mathbb{Z}}, (\geq^p_c)_{c\in\mathbb{Z}}, (=^p_c)_{c\in\mathbb{Z}}, (\neq^p_c)_{c\in\mathbb{Z}})$ where

- $\leq^p_c$ is unary relation symbol for $\{x \in \mathbb{Q}_p \mid v_p(x) \leq c\}$,
- $\geq^p_c$, $=^p_c$, and $\neq^p_c$: defined analogously.

For a structure $\mathfrak{S}$, define CSP($\mathfrak{S}$) to be the problem of deciding whether a set of atomic formulas is satisfiable over $\mathfrak{S}$.

Satisfiability Problems over $\mathbb{Q}_p$

Guépin, Haase, and Worrel (LICS 2019): Satisfiability of systems of linear equations with valuation constraints of the form $v_p(x) = c$

- in NP
- NP-hard for $p \geq 5$
- "While we believe it to be the case, it remains an open problem whether an NP lower bound can be established for the cases $p = 2, 3$"

Our results answer this.

Let $\mathfrak{Q}_p := (\mathbb{Q}_p; +, 1, (\leq^p_c)_{c \in \mathbb{Z}}, (\geq^p_c)_{c \in \mathbb{Z}}, (=^p_c)_{c \in \mathbb{Z}}, (\neq^p_c)_{c \in \mathbb{Z}})$ where

- $\leq^p_c$ is unary relation symbol for $\{x \in \mathbb{Q}_p \mid v_p(x) \leq c\}$,
- $\geq^p_c$, $=^p_c$, and $\neq^p_c$: defined analogously.

For a structure $\mathfrak{S}$, define CSP($\mathfrak{S}$) to be the problem of deciding whether a set of atomic formulas is satisfiable over $\mathfrak{S}$.

Proposition: The structure $\mathfrak{Q}_p$ and its substructure with domain $\mathbb{Q}$ have the same first-order theory,

Satisfiability Problems over $\mathbb{Q}_p$

Guépin, Haase, and Worrel (LICS 2019): Satisfiability of systems of linear equations with valuation constraints of the form $v_p(x) = c$

- in NP
- NP-hard for $p \geq 5$
- "While we believe it to be the case, it remains an open problem whether an NP lower bound can be established for the cases $p = 2, 3$"

Our results answer this.

Let $\mathfrak{Q}_p := (\mathbb{Q}_p; +, 1, (\leq^p_c)_{c \in \mathbb{Z}}, (\geq^p_c)_{c \in \mathbb{Z}}, (=^p_c)_{c \in \mathbb{Z}}, (\neq^p_c)_{c \in \mathbb{Z}})$ where

- $\leq^p_c$ is unary relation symbol for $\{x \in \mathbb{Q}_p \mid v_p(x) \leq c\}$,
- $\geq^p_c$, $=^p_c$, and $\neq^p_c$: defined analogously.

For a structure $\mathfrak{S}$, define CSP($\mathfrak{S}$) to be the problem of deciding whether a set of atomic formulas is satisfiable over $\mathfrak{S}$.

Proposition: The structure $\mathfrak{Q}_p$ and its substructure with domain $\mathbb{Q}$ have the same first-order theory, and hence the same CSP.

Satisfiability Problems over $\mathbb{Q}_p$

Guépin, Haase, and Worrel (LICS 2019): Satisfiability of systems of linear equations with valuation constraints of the form $v_p(x) = c$

- in NP
- NP-hard for $p \geq 5$
- "While we believe it to be the case, it remains an open problem whether an NP lower bound can be established for the cases $p = 2, 3$"

Our results answer this.

Let $\mathfrak{Q}_p := (\mathbb{Q}_p; +, 1, (\leq^p_c)_{c\in\mathbb{Z}}, (\geq^p_c)_{c\in\mathbb{Z}}, (=^p_c)_{c\in\mathbb{Z}}, (\neq^p_c)_{c\in\mathbb{Z}})$ where

- $\leq^p_c$ is unary relation symbol for $\{x \in \mathbb{Q}_p \mid v_p(x) \leq c\}$,
- $\geq^p_c$, $=^p_c$, and $\neq^p_c$: defined analogously.

For a structure $\mathfrak{S}$, define $\mathrm{CSP}(\mathfrak{S})$ to be the problem of deciding whether a set of atomic formulas is satisfiable over $\mathfrak{S}$.

Proposition: The structure $\mathfrak{Q}_p$ and its substructure with domain $\mathbb{Q}$ have the same first-order theory, and hence the same CSP.
(we use a quantifier-elimination result of Weispfenning'1988)

Complexity Classification: $p \geq 3$

Complexity Classification: $p \geq 3$

Theorem. Let $\mathfrak{R}$ be a reduct of $\mathfrak{Q}_p$ whose signature contains $\{+, 1\}$.

Complexity Classification: $p \geq 3$

Theorem. Let $\mathfrak{R}$ be a reduct of $\mathfrak{Q}_p$ whose signature contains $\{+, 1\}$. Then CSP$(\mathfrak{R})$ is in P if $\mathfrak{R}$ is a reduct of one of

$$(\mathbb{Q}_p; +, 1, (\leq_c^p)_{c \in \mathbb{Z}}, (\neq_c^p)_{c \in \mathbb{Z}}) \tag{1}$$

$$(\mathbb{Q}_p; +, 1, (\geq_c^p)_{c \in \mathbb{Z}}), \tag{2}$$

and is NP-complete otherwise.

Complexity Classification: $p \geq 3$

Theorem. Let $\mathfrak{R}$ be a reduct of $\mathfrak{Q}_p$ whose signature contains $\{+, 1\}$. Then CSP($\mathfrak{R}$) is in P if $\mathfrak{R}$ is a reduct of one of

$$(\mathbb{Q}_p; +, 1, (\leq^p_c)_{c \in \mathbb{Z}}, (\neq^p_c)_{c \in \mathbb{Z}}) \tag{1}$$
$$(\mathbb{Q}_p; +, 1, (\geq^p_c)_{c \in \mathbb{Z}}), \tag{2}$$

and is NP-complete otherwise.

Answers the question of Guépin, Haase, and Worrel for $p = 3$:

Complexity Classification: $p \geq 3$

Theorem. Let $\mathfrak{R}$ be a reduct of $\mathfrak{Q}_p$ whose signature contains $\{+, 1\}$. Then CSP$(\mathfrak{R})$ is in P if $\mathfrak{R}$ is a reduct of one of

$$(\mathbb{Q}_p; +, 1, (\leq^p_c)_{c\in\mathbb{Z}}, (\neq^p_c)_{c\in\mathbb{Z}}) \tag{1}$$
$$(\mathbb{Q}_p; +, 1, (\geq^p_c)_{c\in\mathbb{Z}}), \tag{2}$$

and is NP-complete otherwise.

Answers the question of Guépin, Haase, and Worrel for $p = 3$: their problem has $=^c_p$, so is NP-hard.

Complexity Classification: $p \geq 3$

Theorem. Let $\mathfrak{R}$ be a reduct of $\mathfrak{Q}_p$ whose signature contains $\{+, 1\}$. Then CSP$(\mathfrak{R})$ is in P if $\mathfrak{R}$ is a reduct of one of

$$(\mathbb{Q}_p; +, 1, (\leq_c^p)_{c \in \mathbb{Z}}, (\neq_c^p)_{c \in \mathbb{Z}}) \tag{1}$$

$$(\mathbb{Q}_p; +, 1, (\geq_c^p)_{c \in \mathbb{Z}}), \tag{2}$$

and is NP-complete otherwise.

Answers the question of Guépin, Haase, and Worrel for $p = 3$: their problem has $=_p^c$, so is NP-hard.

Comments.

- Need two polynomial-time algorithms!

Complexity Classification: $p \geq 3$

Theorem. Let $\mathfrak{R}$ be a reduct of $\mathfrak{Q}_p$ whose signature contains $\{+, 1\}$.
Then CSP$(\mathfrak{R})$ is in P if $\mathfrak{R}$ is a reduct of one of

$$(\mathbb{Q}_p; +, 1, (\leq_c^p)_{c \in \mathbb{Z}}, (\neq_c^p)_{c \in \mathbb{Z}}) \quad (1)$$

$$(\mathbb{Q}_p; +, 1, (\geq_c^p)_{c \in \mathbb{Z}}), \quad (2)$$

and is NP-complete otherwise.

Answers the question of Guépin, Haase, and Worrel for $p = 3$:
their problem has $=_p^c$, so is NP-hard.

Comments.

- Need two polynomial-time algorithms!
- Both can deal with coefficients p, c given in binary.

Complexity Classification: $p \geq 3$

Theorem. Let $\mathfrak{R}$ be a reduct of $\mathfrak{Q}_p$ whose signature contains $\{+, 1\}$. Then CSP$(\mathfrak{R})$ is in P if $\mathfrak{R}$ is a reduct of one of

$$(\mathbb{Q}_p; +, 1, (\leq^p_c)_{c \in \mathbb{Z}}, (\neq^p_c)_{c \in \mathbb{Z}}) \tag{1}$$
$$(\mathbb{Q}_p; +, 1, (\geq^p_c)_{c \in \mathbb{Z}}), \tag{2}$$

and is NP-complete otherwise.

Answers the question of Guépin, Haase, and Worrel for $p = 3$: their problem has $=^c_p$, so is NP-hard.

Comments.

- Need two polynomial-time algorithms!
- Both can deal with coefficients p, c given in binary.
- Hardness proofs: 'gadget reductions' from p-colorability, which is NP-hard for $p \geq 3$.

Complexity Classification: $p = 2$

Complexity Classification: $p = 2$

Theorem. Let $\mathfrak{R}$ be a reduct of $\mathfrak{Q}_2$ whose signature contains $\{+, 1\}$.

Complexity Classification: $p = 2$

Theorem. Let $\mathfrak{R}$ be a reduct of $\mathfrak{Q}_2$ whose signature contains $\{+, 1\}$.
Then CSP$(\mathfrak{R})$ is in *P* if

Complexity Classification: $p = 2$

Theorem. Let $\mathfrak{R}$ be a reduct of $\mathfrak{Q}_2$ whose signature contains $\{+, 1\}$. Then CSP$(\mathfrak{R})$ is in *P* if $\mathfrak{R}$ is a reduct of one of

$$(\mathbb{Q}_2; +, 1, (\leq_c^2)_{c \in \mathbb{Z}}, (\neq_c^2)_{c \in \mathbb{Z}}) \tag{3}$$

$$(\mathbb{Q}_2; +, 1, (=_c^2)_{c \in \mathbb{Z}}, (\geq_c^2)_{c \in \mathbb{Z}}), \tag{4}$$

and is NP-complete otherwise.

Complexity Classification: $p = 2$

Theorem. Let $\mathfrak{R}$ be a reduct of $\mathfrak{Q}_2$ whose signature contains $\{+, 1\}$. Then CSP$(\mathfrak{R})$ is in *P* if $\mathfrak{R}$ is a reduct of one of

$$(\mathbb{Q}_2; +, 1, (\leq^2_c)_{c\in\mathbb{Z}}, (\neq^2_c)_{c\in\mathbb{Z}}) \tag{3}$$
$$(\mathbb{Q}_2; +, 1, (=^2_c)_{c\in\mathbb{Z}}, (\geq^2_c)_{c\in\mathbb{Z}}), \tag{4}$$

and is NP-complete otherwise.

Answers the question of Guépin, Haase, and Worrel for $p = 2$:

Complexity Classification: $p = 2$

Theorem. Let $\mathfrak{R}$ be a reduct of $\mathfrak{Q}_2$ whose signature contains $\{+, 1\}$. Then CSP$(\mathfrak{R})$ is in *P* if $\mathfrak{R}$ is a reduct of one of

$$(\mathbb{Q}_2; +, 1, (\leq^2_c)_{c \in \mathbb{Z}}, (\neq^2_c)_{c \in \mathbb{Z}}) \quad (3)$$

$$(\mathbb{Q}_2; +, 1, (=^2_c)_{c \in \mathbb{Z}}, (\geq^2_c)_{c \in \mathbb{Z}}), \quad (4)$$

and is NP-complete otherwise.

Answers the question of Guépin, Haase, and Worrel for $p = 2$: their problem is captured by (4), so in P!

Algorithm 1

Proposition. There is a polynomial time algorithm that decides, given

- $m, n \in \mathbb{N}$, $p \in \mathbb{P}$,
- $c \in (\mathbb{Z} \cup \{\infty\})^n$,
- $A \in \mathbb{Q}^{m \times n}$,
- $b \in \mathbb{Q}^m$, and
- finite sets $D_1, \dots, D_n \subseteq \mathbb{Z}$,

whether there exists $x \in \mathbb{Q}^n$ with $Ax = b$ such that

- $v_p(x_j) \leq c_j$, and
- $v_p(x_j) \notin D_j$ for $j = 1, \dots, n$.

Algorithm 1

Proposition. There is a polynomial time algorithm that decides, given

- $m, n \in \mathbb{N}$, $p \in \mathbb{P}$,
- $c \in (\mathbb{Z} \cup \{\infty\})^n$,
- $A \in \mathbb{Q}^{m \times n}$,
- $b \in \mathbb{Q}^m$, and
- finite sets $D_1, \dots, D_n \subseteq \mathbb{Z}$,

whether there exists $x \in \mathbb{Q}^n$ with $Ax = b$ such that

- $v_p(x_j) \leq c_j$, and
- $v_p(x_j) \notin D_j$ for $j = 1, \dots, n$.

Remark: Cannot compute a solution in binary representation in P:

Algorithm 1

Proposition. There is a polynomial time algorithm that decides, given

- $m, n \in \mathbb{N}$, $p \in \mathbb{P}$,
- $c \in (\mathbb{Z} \cup \{\infty\})^n$,
- $A \in \mathbb{Q}^{m \times n}$,
- $b \in \mathbb{Q}^m$, and
- finite sets $D_1, \dots, D_n \subseteq \mathbb{Z}$,

whether there exists $x \in \mathbb{Q}^n$ with $Ax = b$ such that

- $v_p(x_j) \leq c_j$, and
- $v_p(x_j) \notin D_j$ for $j = 1, \dots, n$.

Remark: Cannot compute a solution in binary representation in P: all solutions of '$v_p(x) \leq c$' have doubly exponential representation size.

Algorithm 1

Proposition. There is a polynomial time algorithm that decides, given

- $m, n \in \mathbb{N}$, $p \in \mathbb{P}$,
- $c \in (\mathbb{Z} \cup \{\infty\})^n$,
- $A \in \mathbb{Q}^{m \times n}$,
- $b \in \mathbb{Q}^m$, and
- finite sets $D_1, \dots, D_n \subseteq \mathbb{Z}$,

whether there exists $x \in \mathbb{Q}^n$ with $Ax = b$ such that

- $v_p(x_j) \leq c_j$, and
- $v_p(x_j) \notin D_j$ for $j = 1, \dots, n$.

Remark: Cannot compute a solution in binary representation in P: all solutions of '$v_p(x) \leq c$' have doubly exponential representation size.

Idea: Compute linear expression E for solution space of $Ax = b$.

Algorithm 1

Proposition. There is a polynomial time algorithm that decides, given

- $m, n \in \mathbb{N}$, $p \in \mathbb{P}$,
- $c \in (\mathbb{Z} \cup \{\infty\})^n$,
- $A \in \mathbb{Q}^{m \times n}$,
- $b \in \mathbb{Q}^m$, and
- finite sets $D_1, \dots, D_n \subseteq \mathbb{Z}$,

whether there exists $x \in \mathbb{Q}^n$ with $Ax = b$ such that

- $v_p(x_j) \leq c_j$, and
- $v_p(x_j) \notin D_j$ for $j = 1, \dots, n$.

Remark: Cannot compute a solution in binary representation in P:
all solutions of '$v_p(x) \leq c$' have doubly exponential representation size.

Idea: Compute linear expression E for solution space of $Ax = b$.
Using E, test whether single constraints of the form $v_p(x) \leq c$ are unsat.

Algorithm 1

Proposition. There is a polynomial time algorithm that decides, given

- $m, n \in \mathbb{N}$, $p \in \mathbb{P}$,
- $c \in (\mathbb{Z} \cup \{\infty\})^n$,
- $A \in \mathbb{Q}^{m \times n}$,
- $b \in \mathbb{Q}^m$, and
- finite sets $D_1, \ldots, D_n \subseteq \mathbb{Z}$,

whether there exists $x \in \mathbb{Q}^n$ with $Ax = b$ such that

- $v_p(x_j) \leq c_j$, and
- $v_p(x_j) \notin D_j$ for $j = 1, \ldots, n$.

Remark: Cannot compute a solution in binary representation in P: all solutions of '$v_p(x) \leq c$' have doubly exponential representation size.

Idea: Compute linear expression E for solution space of $Ax = b$. Using E, test whether single constraints of the form $v_p(x) \leq c$ are unsat. If not, then there exists a solution to all constraints.

Algorithm 2

Theorem. There is a polynomial-time algorithm that decides, given

- $m, n \in \mathbb{N}$, $p \in \mathbb{P}$,
- $c \in (\mathbb{Z} \cup \{-\infty\})^n$,
- $A \in \mathbb{Q}^{m \times n}$, and
- $b \in \mathbb{Q}^m$,

whether there exists $x \in \mathbb{Q}^n$ with $Ax = b$ such that $v_p(x) \geq c$.

Algorithm 2

Theorem. There is a polynomial-time algorithm that decides, given

- $m, n \in \mathbb{N}$, $p \in \mathbb{P}$,
- $c \in (\mathbb{Z} \cup \{-\infty\})^n$,
- $A \in \mathbb{Q}^{m \times n}$, and
- $b \in \mathbb{Q}^m$,

whether there exists $x \in \mathbb{Q}^n$ with $Ax = b$ such that $v_p(x) \geq c$.

Algorithm 2

Theorem. There is a polynomial-time algorithm that decides, given

- $m, n \in \mathbb{N}$, $p \in \mathbb{P}$,
- $c \in (\mathbb{Z} \cup \{-\infty\})^n$,
- $A \in \mathbb{Q}^{m \times n}$, and
- $b \in \mathbb{Q}^m$,

whether there exists $x \in \mathbb{Q}^n$ with $Ax = b$ such that $v_p(x) \geq c$.

In the case $p = 2$, we can additionally treat constraints of the form $v_2(x) = c$.

Algorithm 2

Theorem. There is a polynomial-time algorithm that decides, given

- $m, n \in \mathbb{N}$, $p \in \mathbb{P}$,
- $c \in (\mathbb{Z} \cup \{-\infty\})^n$,
- $A \in \mathbb{Q}^{m \times n}$, and
- $b \in \mathbb{Q}^m$,

whether there exists $x \in \mathbb{Q}^n$ with $Ax = b$ such that $v_p(x) \geq c$.

In the case $p = 2$, we can additionally treat constraints of the form $v_2(x) = c$.

Proof ideas:

Algorithm 2

Theorem. There is a polynomial-time algorithm that decides, given

- $m, n \in \mathbb{N}$, $p \in \mathbb{P}$,
- $c \in (\mathbb{Z} \cup \{-\infty\})^n$,
- $A \in \mathbb{Q}^{m \times n}$, and
- $b \in \mathbb{Q}^m$,

whether there exists $x \in \mathbb{Q}^n$ with $Ax = b$ such that $v_p(x) \geq c$.

In the case $p = 2$, we can additionally treat constraints of the form $v_2(x) = c$.

Proof ideas:

- Substantially more involved.

Algorithm 2

Theorem. There is a polynomial-time algorithm that decides, given

- $m, n \in \mathbb{N}$, $p \in \mathbb{P}$,
- $c \in (\mathbb{Z} \cup \{-\infty\})^n$,
- $A \in \mathbb{Q}^{m \times n}$, and
- $b \in \mathbb{Q}^m$,

whether there exists $x \in \mathbb{Q}^n$ with $Ax = b$ such that $v_p(x) \geq c$.

In the case $p = 2$, we can additionally treat constraints of the form $v_2(x) = c$.

Proof ideas:

- Substantially more involved.
- Develop an appropriate row echelon form.

Algorithm 2

Theorem. There is a polynomial-time algorithm that decides, given

- $m, n \in \mathbb{N}$, $p \in \mathbb{P}$,
- $c \in (\mathbb{Z} \cup \{-\infty\})^n$,
- $A \in \mathbb{Q}^{m \times n}$, and
- $b \in \mathbb{Q}^m$,

whether there exists $x \in \mathbb{Q}^n$ with $Ax = b$ such that $v_p(x) \geq c$.

In the case $p = 2$, we can additionally treat constraints of the form $v_2(x) = c$.

Proof ideas:

- Substantially more involved.
- Develop an appropriate row echelon form.
- Example: Consider $a_1 x_1 + \cdots + a_n x_n = b$, for $a_1, \ldots, a_n, b \in \mathbb{Q}$.

Algorithm 2

Theorem. There is a polynomial-time algorithm that decides, given

- $m, n \in \mathbb{N}$, $p \in \mathbb{P}$,
- $c \in (\mathbb{Z} \cup \{-\infty\})^n$,
- $A \in \mathbb{Q}^{m \times n}$, and
- $b \in \mathbb{Q}^m$,

whether there exists $x \in \mathbb{Q}^n$ with $Ax = b$ such that $v_p(x) \geq c$.

In the case $p = 2$, we can additionally treat constraints of the form $v_2(x) = c$.

Proof ideas:

- Substantially more involved.
- Develop an appropriate row echelon form.
- Example: Consider $a_1 x_1 + \cdots + a_n x_n = b$, for $a_1, \ldots, a_n, b \in \mathbb{Q}$.
  Has a solution $x \in \mathbb{Q}^n$ with $v_p(x_j) \geq 0$ for every $j \in \{1, \ldots, n\}$
  if and only if

Algorithm 2

Theorem. There is a polynomial-time algorithm that decides, given

- $m, n \in \mathbb{N}$, $p \in \mathbb{P}$,
- $c \in (\mathbb{Z} \cup \{-\infty\})^n$,
- $A \in \mathbb{Q}^{m \times n}$, and
- $b \in \mathbb{Q}^m$,

whether there exists $x \in \mathbb{Q}^n$ with $Ax = b$ such that $v_p(x) \geq c$.

In the case $p = 2$, we can additionally treat constraints of the form $v_2(x) = c$.

Proof ideas:

- Substantially more involved.
- Develop an appropriate row echelon form.
- Example: Consider $a_1 x_1 + \cdots + a_n x_n = b$, for $a_1, \ldots, a_n, b \in \mathbb{Q}$.
  Has a solution $x \in \mathbb{Q}^n$ with $v_p(x_j) \geq 0$ for every $j \in \{1, \ldots, n\}$
  if and only if $v_p(b) \geq \min_j v_p(a_j)$.

Combining several primes, and the ordering!

Combining several primes, and the ordering!

$\mathfrak{Q}$: expansion of $(\mathbb{Q};+,1)$ with all the relations

$$\{\leq_c^p, \geq_c^p, =_c^p, \neq_c^p \mid c \in \mathbb{Z}, p \text{ prime}\}.$$

Combining several primes, and the ordering!

$\mathfrak{Q}$: expansion of $(\mathbb{Q}; +, 1)$ with all the relations

$$\{\leq_c^p, \geq_c^p, =_c^p, \neq_c^p \mid c \in \mathbb{Z}, p \text{ prime}\}.$$

Theorem. Let $\mathfrak{R}$ be a reduct of $(\mathfrak{Q}, \leq)$ that contains $\{1, +\}$.

Combining several primes, and the ordering!

$\mathfrak{Q}$: expansion of $(\mathbb{Q}; +, 1)$ with all the relations

$$\{\leq_c^p, \geq_c^p, =_c^p, \neq_c^p \mid c \in \mathbb{Z}, p \text{ prime}\}.$$

Theorem. Let $\mathfrak{R}$ be a reduct of $(\mathfrak{Q}, \leq)$ that contains $\{1, +\}$.
If $\mathfrak{R}$ contains

- $=_c^p$ for some $c \in \mathbb{Z}$ and prime $p \geq 3$,

Combining several primes, and the ordering!

$\mathfrak{Q}$: expansion of $(\mathbb{Q}; +, 1)$ with all the relations

$$\{\leq_c^p, \geq_c^p, =_c^p, \neq_c^p \mid c \in \mathbb{Z}, p \text{ prime}\}.$$

Theorem. Let $\mathfrak{R}$ be a reduct of $(\mathfrak{Q}, \leq)$ that contains $\{1, +\}$.
If $\mathfrak{R}$ contains

- $=_c^p$ for some $c \in \mathbb{Z}$ and prime $p \geq 3$,
- $\geq_{c_1}^p$ and a relation from $\{\leq_{c_2}^p, \neq_{c_2}^p\}$ for some $c_1, c_2 \in \mathbb{Z}$ and prime $p \geq 3$, or

Combining several primes, and the ordering!

$\mathfrak{Q}$: expansion of $(\mathbb{Q}; +, 1)$ with all the relations

$$\{\leq^p_c, \geq^p_c, =^p_c, \neq^p_c \mid c \in \mathbb{Z}, p \text{ prime}\}.$$

Theorem. Let $\mathfrak{R}$ be a reduct of $(\mathfrak{Q}, \leq)$ that contains $\{1, +\}$.
If $\mathfrak{R}$ contains

- $=^p_c$ for some $c \in \mathbb{Z}$ and prime $p \geq 3$,
- $\geq^p_{c_1}$ and a relation from $\{\leq^p_{c_2}, \neq^p_{c_2}\}$ for some $c_1, c_2 \in \mathbb{Z}$ and prime $p \geq 3$, or
- a relation from $\{\geq^2_{c_1}, =^2_{c_1}\}$ and a relation from $\{\leq^2_{c_2}, \neq^p_{c_2}\}$ for some $c_1, c_2 \in \mathbb{Z}$,

then CSP$(\mathfrak{R})$ is NP-complete;

Combining several primes, and the ordering!

$\mathfrak{Q}$: expansion of $(\mathbb{Q}; +, 1)$ with all the relations

$$\{\leq^p_c, \geq^p_c, =^p_c, \neq^p_c \mid c \in \mathbb{Z}, p \text{ prime}\}.$$

Theorem. Let $\mathfrak{R}$ be a reduct of $(\mathfrak{Q}, \leq)$ that contains $\{1, +\}$.
If $\mathfrak{R}$ contains

- $=^p_c$ for some $c \in \mathbb{Z}$ and prime $p \geq 3$,
- $\geq^p_{c_1}$ and a relation from $\{\leq^p_{c_2}, \neq^p_{c_2}\}$ for some $c_1, c_2 \in \mathbb{Z}$ and prime $p \geq 3$, or
- a relation from $\{\geq^2_{c_1}, =^2_{c_1}\}$ and a relation from $\{\leq^2_{c_2}, \neq^p_{c_2}\}$ for some $c_1, c_2 \in \mathbb{Z}$,

then CSP$(\mathfrak{R})$ is NP-complete; otherwise, CSP$(\mathfrak{R})$ is in P.

Combining several primes, and the ordering!

$\mathfrak{Q}$: expansion of $(\mathbb{Q}; +, 1)$ with all the relations

$$\{\leq^p_c, \geq^p_c, =^p_c, \neq^p_c \mid c \in \mathbb{Z}, p \text{ prime}\}.$$

Theorem. Let $\mathfrak{R}$ be a reduct of $(\mathfrak{Q}, \leq)$ that contains $\{1, +\}$.
If $\mathfrak{R}$ contains

- $=^p_c$ for some $c \in \mathbb{Z}$ and prime $p \geq 3$,
- $\geq^p_{c_1}$ and a relation from $\{\leq^p_{c_2}, \neq^p_{c_2}\}$ for some $c_1, c_2 \in \mathbb{Z}$ and prime $p \geq 3$, or
- a relation from $\{\geq^2_{c_1}, =^2_{c_1}\}$ and a relation from $\{\leq^2_{c_2}, \neq^p_{c_2}\}$ for some $c_1, c_2 \in \mathbb{Z}$,

then CSP$(\mathfrak{R})$ is NP-complete; otherwise, CSP$(\mathfrak{R})$ is in P.

Proof ingredient: the approximation theorem for finitely many inequivalent absolute values (see, e.g., Lang's *Algebra*).

Conclusion

- Two polynomial-time tractability results for linear systems over $\mathbb{Q}_p$.

Conclusion

- Two polynomial-time tractability results for linear systems over $\mathbb{Q}_p$.
- Have matching hardness results.

Conclusion

- Two polynomial-time tractability results for linear systems over $\mathbb{Q}_p$.
- Have matching hardness results.
- Algorithms for various primes p can be combined over $\mathbb{Q}$, and with $<$.

Conclusion

- Two polynomial-time tractability results for linear systems over $\mathbb{Q}_p$.
- Have matching hardness results.
- Algorithms for various primes p can be combined over $\mathbb{Q}$, and with $<$.

Open question: is there a polynomial-time algorithm for systems of linear (in-)equalities with coefficients of the form 2^c, for c given in binary?

Conclusion

- Two polynomial-time tractability results for linear systems over $\mathbb{Q}_p$.
- Have matching hardness results.
- Algorithms for various primes p can be combined over $\mathbb{Q}$, and with $<$.

Open question: is there a polynomial-time algorithm for systems of linear (in-)equalities with coefficients of the form 2^c, for c given in binary?

- would imply our tractability result for linear systems with valuation constraints of the form $v_2(x) = c$.

Conclusion

- Two polynomial-time tractability results for linear systems over $\mathbb{Q}_p$.
- Have matching hardness results.
- Algorithms for various primes p can be combined over $\mathbb{Q}$, and with $<$.

Open question: is there a polynomial-time algorithm for systems of linear (in-)equalities with coefficients of the form 2^c, for c given in binary?

- would imply our tractability result for linear systems with valuation constraints of the form $v_2(x) = c$.
- would imply a polynomial-time algorithm for mean-payoff-games (currently not known to be in P).

Conclusion

- Two polynomial-time tractability results for linear systems over $\mathbb{Q}_p$.
- Have matching hardness results.
- Algorithms for various primes p can be combined over $\mathbb{Q}$, and with $<$.

Open question: is there a polynomial-time algorithm for systems of linear (in-)equalities with coefficients of the form 2^c, for c given in binary?

- would imply our tractability result for linear systems with valuation constraints of the form $v_2(x) = c$.
- would imply a polynomial-time algorithm for mean-payoff-games (currently not known to be in P).
  See Bodirsky, Loho, Skomra ICALP'2025 for more on this connection.