On Polynomial-Time Decidability of k-Negations Fragments of FO Theories

Christoph Haase[1] Alessio Mansutti[2] Amaury Pouly[1,3]

[1] University of Oxford

[2] IMDEA Software Institute

[3] Université Paris Cité, CNRS, IRIF

advanced reasoning in arithmetic theories

The Frobenius problem

Given coins in denominations

$$m_1 < \cdots < m_k \in \mathbb{N},$$

what is the largest value c that cannot be generated? Does such a c exist?

The Frobenius problem

Given coins in denominations

$$m_1 < \cdots < m_k \in \mathbb{N},$$

what is the largest value c that cannot be generated? Does such a c exist?

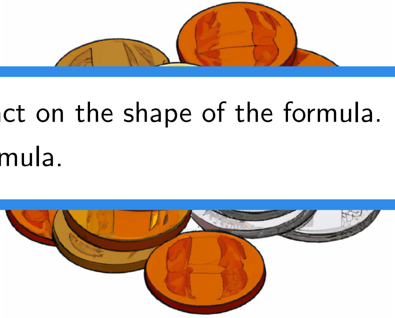
In integer linear arithmetic (a.k.a. Presburger arithmetic):

$$\exists c : \neg\mathsf{gen}(c) \land \forall d : d > c \implies \mathsf{gen}(d)$$

$$\mathsf{gen}(x) \coloneqq \exists y_1 \ldots \exists y_k : x = m_1 \cdot y_1 + \cdots + m_k \cdot y_k \land \bigwedge_{i=1}^{k} y_i \geq 0$$

The Frobenius problem

Giver



Input of the problem has little to no impact on the shape of the formula.

The problem statement influences the formula.

what

generated? Does such a c exist?

In integer linear arithmetic (a.k.a. Presburger arithmetic):

$$\exists c : \neg \mathsf{gen}(c) \land \forall d : d > c \implies \mathsf{gen}(d)$$

$$\mathsf{gen}(x) := \exists y_1 \ldots \exists y_k : x = m_1 \cdot y_1 + \cdots + m_k \cdot y_k \land \bigwedge_{i=1}^{k} y_i \geq 0$$

Short Presburger arithmetic

Presburger arithmetic (PA): first-order theory of $(\mathbb{Z}, 0, 1, +, \leq)$

Short PA: fix the number of variables and all Boolean connectives.

The input of the validity problem becomes a sequence of coefficients.

Short Presburger arithmetic

Presburger arithmetic (PA): first-order theory of $(\mathbb{Z}, 0, 1, +, \leq)$

Short PA: fix the number of variables and all Boolean connectives.
The input of the validity problem becomes a sequence of coefficients.

Theorem (Kannan; Polyhedral Combinatorics 1990)

Deciding the validity of Short PA sentences of the form $\forall^k \exists^\ell \Phi$ is in P.

(note: it implies that the Frobenius problem is in P in fixed dimension)

Short Presburger arithmetic

Presburger arithmetic (PA): first-order theory of $(\mathbb{Z}, 0, 1, +, \leq)$

Short PA: fix the number of variables and all Boolean connectives.
The input of the validity problem becomes a sequence of coefficients.

Theorem (Kannan; Polyhedral Combinatorics 1990)

Deciding the validity of Short PA sentences of the form $\forall^k \exists^\ell \Phi$ is in P.

(note: it implies that the Frobenius problem is in P in fixed dimension)

Theorem (Nguyen and Pak; SIAM J. Comput. 2022)

Deciding Short PA sentences of the form $\exists^j \forall^k \exists^\ell \Phi$ is NP-hard for some $j, k, \ell \in \mathbb{N}$.

(note: with further alternations the problem climbs the polynomial hierarchy)

What happens for Weak Presburger arithmetic?

Weak PA: first-order theory of $(\mathbb{Z}, 0, 1, +, =)$

Theorem (Chistikov, Haase, Hadizadeh, M.; MFCS 2022)

Weak PA is PA-complete (that is, 2AExp$_{pol}$-complete).

What happens for Weak Presburger arithmetic?

Weak PA: first-order theory of $(\mathbb{Z}, 0, 1, +, =)$

Theorem (Chistikov, Haase, Hadizadeh, M.; MFCS 2022)

Weak PA is PA-complete (that is, 2AExp$_{pol}$-complete).

Question: Do the results of Nguyen and Pak carry over to Weak PA?

What happens for Weak Presburger arithmetic?

Weak PA: first-order theory of $(\mathbb{Z}, 0, 1, +, =)$

Theorem (Chistikov, Haase, Hadizadeh, M.; MFCS 2022)

Weak PA is PA-complete (that is, 2AExp$_{pol}$-complete).

Question: Do the results of Nguyen and Pak carry over to Weak PA?

Answer: No! Fixing the number of negations suffices to get P.

In this paper...

We identify a set of sufficient conditions for a FO theory to admit a polynomial time validity problem when the number of negations is fixed

In this paper...

We identify a set of sufficient conditions for a FO theory to admit a polynomial time validity problem when the number of negations is fixed

$$\Phi \coloneqq \alpha \;\mid\; \Phi \land \Phi \;\mid\; \neg\Phi \;\mid\; \exists x.\Phi$$

$$\alpha \coloneqq \text{ atomic formulae}$$

Note: number of alternations and disjunctions is fixed,
but unbounded number of variables, conjunctions and atomic formulae

In this paper...

We identify a set of sufficient conditions for a FO theory to admit a polynomial time validity problem when the number of negations is fixed

$$\Phi \coloneqq \alpha \;\mid\; \Phi \wedge \Phi \;\mid\; \neg\Phi \;\mid\; \exists x.\Phi$$
$$\alpha \coloneqq \text{ atomic formulae}$$

Note: number of alternations and disjunctions is fixed,
but unbounded number of variables, conjunctions and atomic formulae

We apply the framework to linear arithmetic theories (e.g. Weak PA)

k-negations fragments

The k-negations fragment of a FO theory is the set of all formulae built from

$$\Phi := \alpha \;\mid\; \Phi \wedge \Phi \;\mid\; \neg\Phi \;\mid\; \exists x.\Phi$$

$$\alpha := \text{ atomic formulae}$$

using at most k negations.

k-negations fragments

The k-negations fragment of a FO theory is the set of all formulae built from

$$\Phi := \alpha \;\mid\; \Phi \wedge \Phi \;\mid\; \neg\Phi \;\mid\; \exists x.\Phi$$
$$\alpha := \text{ atomic formulae}$$

using at most k negations.

Let Φ and Ψ be from the j and k-negations fragments of a FO theory. Then,

- $\neg\Phi$ is from the $(j+1)$-negations fragment,
- $\Phi \implies \Psi$ is from the $(j+k+2)$-negations fragment.

k-negations fragments

The k-negations fragment of a FO theory is the set of all formulae built from

$$\Phi \coloneqq \alpha \mid \Phi \land \Phi \mid \neg\Phi \mid \exists x.\Phi$$
$$\alpha \coloneqq \text{ atomic formulae}$$

using at most k negations.

Let Φ and Ψ be from the j and k-negations fragments of a FO theory. Then,

- $\neg\Phi$ is from the $(j+1)$-negations fragment,
- $\Phi \implies \Psi$ is from the $(j+k+2)$-negations fragment.

Example: $(\exists \boldsymbol{y} : A \cdot \boldsymbol{x} + A' \cdot \boldsymbol{y} = \boldsymbol{b}) \implies (\exists \boldsymbol{z} : C \cdot \boldsymbol{y} + C' \cdot \boldsymbol{z} = \boldsymbol{d})$
is in the 2-negations fragment of Weak PA.

k-negations fragments

The k-negations fragment of a FO theory is the set of all formulae built from

$$\Phi \coloneqq \alpha \mid \Phi \land \Phi \mid \neg\Phi \mid \exists x.\Phi$$

using at mos

Let Φ and Ψ Then,

- $\neg\Phi$ is fr
- $\Phi \implies$

For Weak PA, this is essentially as good as it gets:

deciding formulae of the form (a_i, b_i in input)

$$\exists x \forall y : \bigwedge_{i=1}^{n} (a_i \cdot y = x - b_i \implies y = 3 \cdot x + 1)$$

is NP-hard.

Example: $(\exists \boldsymbol{y} : A \cdot \boldsymbol{x} + A' \cdot \boldsymbol{y} = \boldsymbol{b}) \implies (\exists \boldsymbol{z} : C \cdot \boldsymbol{y} + C' \cdot \boldsymbol{z} = \boldsymbol{d})$

is in the 2-negations fragment of Weak PA.

Question 1: normal forms?

Difference Normal form for propositional logic [Hausdorff, 1914]:

$$\Phi_1 - (\Phi_2 - \ldots (\Phi_{n-1} - \Phi_n)) \qquad (\Phi_1 - \Phi_2 := \Phi_1 \wedge \neg\Phi_2)$$

where Φ_i is a negation-free DNF formula.

Question 1: normal forms?

Difference Normal form for propositional logic [Hausdorff, 1914]:

$$\Phi_1 - (\Phi_2 - \ldots(\Phi_{n-1} - \Phi_n)) \qquad\qquad (\Phi_1 - \Phi_2 := \Phi_1 \wedge \neg\Phi_2)$$

where Φ_i is a negation-free DNF formula.

$$[\![\exists x \Phi]\!] := \{\boldsymbol{w} \in [X \to A] : \text{ there is } a \in A \text{ such that } \boldsymbol{w}[x \leftarrow a] \in [\![\Phi]\!]\}$$

$$[\![\forall x (\Psi \mid \Phi)]\!] := \{\boldsymbol{w} \in [\![\exists x \Phi]\!] : \text{for all } a \in A \text{ if } \boldsymbol{w}[x \leftarrow a] \in [\![\Phi]\!] \text{ then } \boldsymbol{w}[x \leftarrow a] \in [\![\Psi]\!]\}$$

Question 1: normal forms?

Difference Normal form for propositional logic [Hausdorff, 1914]:

$$\Phi_1 - (\Phi_2 - \dots (\Phi_{n-1} - \Phi_n)) \qquad\qquad (\Phi_1 - \Phi_2 := \Phi_1 \wedge \neg\Phi_2)$$

where Φ_i is a negation-free DNF formula.

$$[\![\exists x \Phi]\!] := \{\boldsymbol{w} \in [X \to A] : \text{ there is } a \in A \text{ such that } \boldsymbol{w}[x \leftarrow a] \in [\![\Phi]\!]\}$$

$$[\![\forall x(\Psi \mid \Phi)]\!] := \{\boldsymbol{w} \in [\![\exists x \Phi]\!] : \text{for all } a \in A \text{ if } \boldsymbol{w}[x \leftarrow a] \in [\![\Phi]\!] \text{ then } \boldsymbol{w}[x \leftarrow a] \in [\![\Psi]\!]\}$$

$$[\![\exists x(\Phi - \Psi)]\!] = [\![\exists x \Phi]\!] \setminus [\![\forall x(\Psi \mid \Phi)]\!] \qquad [\![\forall x(\Psi_1 - \Psi_2 \mid \Phi)]\!] = [\![\forall x(\Psi_1 \mid \Phi)]\!] \setminus [\![\exists x \Psi_2]\!]$$

Question 1: normal forms?

Difference Normal form for propositional logic [Hausdorff, 1914]:

$$\Phi_1 - (\Phi_2 - \ldots (\Phi_{n-1} - \Phi_n)) \qquad\qquad (\Phi_1 - \Phi_2 := \Phi_1 \wedge \neg\Phi_2)$$

where Φ_i is a negation-free DNF formula.

$$[\![\exists x \Phi]\!] := \{\boldsymbol{w} \in [X \to A] : \text{ there is } a \in A \text{ such that } \boldsymbol{w}[x \leftarrow a] \in [\![\Phi]\!]\}$$

$$[\![\forall x (\Psi \,|\, \Phi)]\!] := \{\boldsymbol{w} \in [\![\exists x \Phi]\!] : \text{for all } a \in A \text{ if } \boldsymbol{w}[x \leftarrow a] \in [\![\Phi]\!] \text{ then } \boldsymbol{w}[x \leftarrow a] \in [\![\Psi]\!]\}$$

$$[\![\exists x : \Phi_1 - (\Phi_2 - (\Phi_3 - \Phi_4))]\!] = [\![\exists x \Phi_1]\!] \setminus \Big([\![\forall x(\Phi_2 \,|\, \Phi_1)]\!] \setminus \big([\![\exists x \Phi_3]\!] \setminus [\![\forall x(\Phi_4 \,|\, \Phi_3)]\!]\big)\Big)$$

Key point: it suffices to study quantification on negation-free DNF formulae

Question 2: representation for conjunctions of atomic formulae?

mathematical level

(definable sets, $\wedge, \neg$, $(\exists, X)$, `valid?`)

(formulae, $\wedge, \neg$, $(\exists, X)$, `valid?`)

(???, $\wedge, \neg$, $(\exists, X)$, `valid?`)

algorithmic level

Question 2: representation for conjunctions of atomic formulae?

mathematical level

$$\big(\text{definable sets},\ \wedge, \neg,\ (\exists, X),\ \texttt{valid?}\big)$$

$$\big(\text{formulae},\ \wedge, \neg,\ (\exists, X),\ \texttt{valid?}\big) \qquad \big(\text{???},\ \wedge, \neg,\ (\exists, X),\ \texttt{valid?}\big)$$

algorithmic level

- Difference normal form partially fixes the representation...
- but we are free to choose the representation for conjunctions of atomic formulae

Example: for Weak PA, we will use shifted lattices $\boldsymbol{v} + \boldsymbol{p}_1 \cdot \mathbb{Z} + \dots \boldsymbol{p}_d \cdot \mathbb{Z}$

Difference normal form + representations

We consider the FO theory of a structure $\mathcal{A} = (A, \sigma, I)$ to be the structure

$$\mathsf{FO}(\mathcal{A}) \coloneqq (\llbracket \mathcal{A} \rrbracket,\ \top,\ \bot,\ \wedge,\ \vee,\ -,\ (\exists, \boldsymbol{X}),\ (\underbrace{\forall(\cdot,\cdot)}_{\text{relative universal quantifier}}, \boldsymbol{X}),\ \implies)$$

- $\llbracket \mathcal{A} \rrbracket \subseteq 2^{[X \to A]}$: set of definable sets

Difference normal form + representations

We consider the FO theory of a structure $\mathcal{A} = (A, \sigma, I)$ to be the structure

$$\mathsf{FO}(\mathcal{A}) \coloneqq ([\![\mathcal{A}]\!],\ \top,\ \bot,\ \wedge,\ \vee,\ -,\ (\exists, \boldsymbol{X}),\ (\underbrace{\forall(\cdot,\cdot)}_{\text{relative universal quantifier}}, \boldsymbol{X}),\ \implies)$$

- $[\![\mathcal{A}]\!] \subseteq 2^{[X \to A]}$: set of definable sets
- let D be a representation of (at least) all conjunctions of atomic formulae
- we represent $[\![\mathcal{A}]\!]$ as diffnf(D), where

$$\text{diffnf}(D) \coloneqq \text{syntactic chains of relative complements of elements in un}(D)$$
$$\text{un}(D) \coloneqq \text{syntactic unions of elements in } D$$

k-negations fragment in PTIME: sufficient conditions

1. provide a PTIME translation from conjunctions of atomic formulae to D

k-negations fragment in PTIME: sufficient conditions

1. provide a PTIME translation from conjunctions of atomic formulae to D

2. show that $(D, \wedge, \implies)$ has a "polynomial signature",

k-negations fragment in PTIME: sufficient conditions

1. provide a PTIME translation from conjunctions of atomic formulae to D
2. show that $(D, \wedge, \implies)$ has a "polynomial signature",
3. $(\mathrm{un}(D), \implies)$ has a UXP signature with parameter the length of the union, and

k-negations fragment in PTIME: sufficient conditions

1. provide a PTIME translation from conjunctions of atomic formulae to D
2. show that $(D, \wedge, \Longrightarrow)$ has a "polynomial signature",
3. $(\mathrm{un}(D), \Longrightarrow)$ has a UXP signature with parameter the length of the union, and
4. $(\mathrm{diffnf}(D), (\exists, \boldsymbol{X}), (\forall(\cdot,\cdot), \boldsymbol{X}))$ has a UXP signature with parameter depth, where
   - for $(\exists, \boldsymbol{X})$ it suffices to look at inputs from D
   - for $(\forall(\cdot,\cdot), \boldsymbol{X})$ it suffices to look at inputs from $\mathrm{un}(D) \times D$

k-negations fragment in PTIME: the case of Weak PA

$D \coloneqq$ set of tuples $(\boldsymbol{v}, \boldsymbol{p}_1, \dots \boldsymbol{p}_d)$ representing the shifted lattices
$\boldsymbol{v} + \boldsymbol{p}_1 \cdot \mathbb{Z} + \dots \boldsymbol{p}_d \cdot \mathbb{Z}$; numbers encoded in binary

k-negations fragment in PTIME: the case of Weak PA

$D :=$ set of tuples $(\boldsymbol{v}, \boldsymbol{p}_1, \dots \boldsymbol{p}_d)$ representing the shifted lattices $\boldsymbol{v} + \boldsymbol{p}_1 \cdot \mathbb{Z} + \dots \boldsymbol{p}_d \cdot \mathbb{Z}$; numbers encoded in binary

✓ provide a PTIME translation from $A \cdot \boldsymbol{x} = \boldsymbol{b}$ to $(\boldsymbol{v}, \boldsymbol{p}_1, \dots \boldsymbol{p}_d)$

done using a PTIME algorithm for Hermite normal form

k-negations fragment in PTIME: the case of Weak PA

$D \coloneqq$ set of tuples $(\boldsymbol{v}, \boldsymbol{p}_1, \dots \boldsymbol{p}_d)$ representing the shifted lattices $\boldsymbol{v} + \boldsymbol{p}_1 \cdot \mathbb{Z} + \dots \boldsymbol{p}_d \cdot \mathbb{Z}$; numbers encoded in binary

- ✓ provide a PTIME translation from $A \cdot \boldsymbol{x} = \boldsymbol{b}$ to $(\boldsymbol{v}, \boldsymbol{p}_1, \dots \boldsymbol{p}_d)$

  done using a PTIME algorithm for Hermite normal form

- ✓ show that $(D, \land, \implies)$ has a polynomial signature,

- ✓ $(\mathrm{un}(D), \implies)$ has a UXP signature with parameter the length of the union

k-negations fragment in PTIME: the case of Weak PA

$D \coloneqq$ set of tuples $(\boldsymbol{v}, \boldsymbol{p}_1, \dots \boldsymbol{p}_d)$ representing the shifted lattices $\boldsymbol{v} + \boldsymbol{p}_1 \cdot \mathbb{Z} + \dots \boldsymbol{p}_d \cdot \mathbb{Z}$; numbers encoded in binary

✓ provide a PTIME translation from $A \cdot \boldsymbol{x} = \boldsymbol{b}$ to $(\boldsymbol{v}, \boldsymbol{p}_1, \dots \boldsymbol{p}_d)$

done using a PTIME algorithm for Hermite normal form

✓ show that $(D, \land, \implies)$ has a polynomial signature,

✓ $(\mathrm{un}(D), \implies)$ has a UXP signature with parameter the length of the union

✓ $(\mathrm{diffnf}(D), (\exists, \boldsymbol{X}), (\forall(\cdot,\cdot), \boldsymbol{X}))$ has a UXP signature with parameter depth, where

- for $(\exists, \boldsymbol{X})$ it suffices to look at inputs from D
- for $(\forall(\cdot,\cdot), \boldsymbol{X})$ it suffices to look at inputs from $\mathrm{un}(D) \times D$

k-negations fragment in PTIME: the case of Weak PA

$D \coloneqq$ set of tuples $(\boldsymbol{v}, \boldsymbol{p}_1, \dots \boldsymbol{p}_d)$ representing the shifted lattices $\boldsymbol{v} + \boldsymbol{p}_1 \cdot \mathbb{Z} + \dots \boldsymbol{p}_d \cdot \mathbb{Z}$; numbers encoded in binary

Lemma

The relative universal quantifier $\forall \boldsymbol{x}(\bigvee_{j=1}^{L} X_j, Y)$, where $\bigvee_{j=1}^{L} X_j \in \mathrm{un}(D)$ and $Y \in D$, is equivalent to a combination of $\wedge$, $\vee$, $-$ and $\exists \boldsymbol{x}$ applied to the sets $X_1, \dots, X_L, Y$. This combination can be computed in PTIME when L is fixed.

✓ $(\mathrm{un}(D), \implies)$ has a UXP signature with parameter the length of the union

✓ $(\mathrm{diffnf}(D), (\exists, \boldsymbol{X}), (\forall(\cdot,\cdot), \boldsymbol{X}))$ has a UXP signature with parameter depth, where

- for $(\exists, \boldsymbol{X})$ it suffices to look at inputs from D
- for $(\forall(\cdot,\cdot), \boldsymbol{X})$ it suffices to look at inputs from $\mathrm{un}(D) \times D$

Conclusion

- We studied the validity problem for FO formulae with a fixed amount of negations
- Suitable normal form: difference normal form
- Identified a minimal set of computational problems that are sufficient to show that validity is in PTIME; they do not involve complementation
- Applied the framework to Weak PA
- Same technique can be applied to Weak LRA and a few abstract domains