Higher-Order Quantified Boolean Satisfiability

Dmitry Chistikov[1], Christoph Haase[2], Zahra Hadizadeh[3] and **Alessio Mansutti**[2]

[1]University of Warwick, UK

[2]University of Oxford, UK

[3]Sharif University of Technology, Iran

advanced reasoning in arithmetic theories

In this paper...

- We introduce an **higher-order Boolean satisfiability problem** (HOSAT) that
  - is a natural extension of the quantified Boolean formula problem (QBF)
  - characterises complexity classes in the weak $k\textsc{Exp}$ hierarchy, for all $k \geq 1$.

- We use HOSAT to settle the complexity of **weak Presburger arithmetic**, i.e. the first-order theory of the structure $\langle \mathbb{Z}, 0, 1, +, = \rangle$.

HOSAT: Motivation

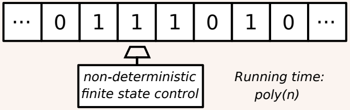
Is the Boolean satisfiability problem "simple to use" for lower bounds?

HOSAT: Motivation

Is the Boolean satisfiability problem "simple to use" for lower bounds?

It is a very natural problem w.r.t. NP :

Turing machines:



Does the TM accepts the input **w**?

SAT:

$$\exists a \exists b \exists c \exists d : (a \vee \neg b \vee c) \wedge (\neg a \vee d \vee b) \wedge (a \vee d) \wedge (\neg b \vee \neg d \vee \neg c) \wedge (c \vee b) \wedge (c \vee \neg a)$$

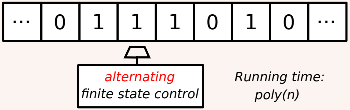
Is the sentence true?

HOSAT: Motivation

Is the Boolean satisfiability problem "simple to use" for lower bounds?

It is a very natural problem w.r.t. PH and $\mathrm{PS}\textsc{pace}$:

Turing machines:



Does the TM accepts the input **w**?

QBF:

$$\exists a \forall b \forall c \exists d : (a \vee \neg b \vee c) \wedge (\neg a \vee d \vee b) \wedge (a \vee d) \wedge (\neg b \vee \neg d \vee \neg c) \wedge (c \vee b) \wedge (c \vee \neg a)$$

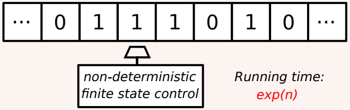
Is the sentence true?

HOSAT: Motivation

Is the Boolean satisfiability problem "simple to use" for lower bounds?

Well-understood problem w.r.t. $\textsc{NExp}$:

Turing machines:



Does the TM accepts the input **w**?

Succinct SAT:

$f : [1, n] \to \{\wedge, \vee, \neg\} \times [1, n] \times [1, n]$

$n \in \mathbb{N}$ in binary.

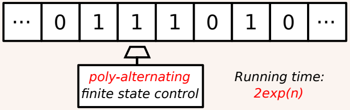
$\exists \mathbf{x} \bigwedge_{i \in [1,n], f(i) = (\mathit{op}, j, k)} x_i \Leftrightarrow x_j \; \mathit{op} \; x_k$?

HOSAT: Motivation

Is the Boolean satisfiability problem "simple to use" for lower bounds?

Unnatural for classes above $\textsc{NExp}$!

Turing machines:



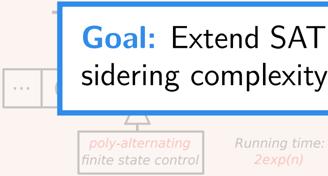
Does the TM accepts the input **w**?

How does Succinct succinct QBF even looks like?

HOSAT: Motivation

Is the Boolean satisfiability problem "simple to use" for lower bounds?

Unnatural for classes above $\mathrm{NE{\small XP}}$!



Goal: Extend SAT so that it "scales well" when considering complexity classes above $\mathrm{NE{\small XP}}$.

inct QBF
even looks like?

Does the TM accepts the input **w**?

HOSAT: Definition

- **Higher-order Boolean functions:** $\mathbb{B}_{0,n} := \mathbb{B} := \{0,1\}; \quad k,n \in \mathbb{N}$

  $\mathbb{B}_{k+1,n} := [(\mathbb{B}_{k,n})^n \to \mathbb{B}].$

  E.g. given $g_1, \dots, g_n \in \mathbb{B}_{1,n} := [\mathbb{B}^n \to \mathbb{B}]$ and $f \in \mathbb{B}_{2,n}$, we have $f(g_1, \dots, g_n) \in \mathbb{B}$.

- **Quantifier-free generalised Boolean formulas:**

  $$\Phi := \top \mid f(g_1, \dots, g_n) \mid \neg\Phi \mid \Phi \wedge \Phi \qquad \text{(function applications are well-typed)}$$

- **Generalised Boolean formulas of order** 0**:**

  $$\exists \mathbf{f}_1 : \mathbb{B}\, \forall \mathbf{f}_2 : \mathbb{B} \dots \exists \mathbf{f}_d : \mathbb{B}\ \Phi \qquad (\Phi \text{ quantifier-free})$$

- **Generalised Boolean formulas of order** $k \geq 1$**:**

  $$\exists \mathbf{f}_1 : \mathbb{B}_{k,n} \forall \mathbf{f}_2 : \mathbb{B}_{k,n} \dots \exists \mathbf{f}_d : \mathbb{B}_{k,n}\ \Phi \qquad (\Phi \text{ of order } k-1)$$

HOSAT: Definition

- **Higher-order Boolean functions:**

$$\mathbb{B}_{0,n} := \mathbb{B} := \{0,1\}; \qquad k,n \in \mathbb{N}$$

$$\mathbb{B}_{k+1,n} := [(\mathbb{B}_{k,n})^n \to \mathbb{B}].$$

E.g. given $g_1, \ldots, g_n \in \mathbb{B}_{1,n} := [\mathbb{B}^n \to \mathbb{B}]$ and $f \in \mathbb{B}_{2,n}$, we have $f(g_1, \ldots, g_n) \in \mathbb{B}$.

- **Quantifier-free generalised Boolean formulas:**

$$\Phi := \top \mid f(g_1, \ldots, g_n) \mid \neg\Phi \mid \Phi \wedge \Phi \qquad \text{(function applications are well-typed)}$$

- **Generalised Boolean formulas of order 0:**

$$\exists \mathbf{f}_1 : \mathbb{B}\, \forall \mathbf{f}_2 : \mathbb{B} \ldots \exists \mathbf{f}_d : \mathbb{B}\ \Phi \qquad (\Phi \text{ quantifier-free})$$

- **Generalised Boolean formulas of order $k \geq 1$:**

$$\exists \mathbf{f}_1 : \mathbb{B}_{k,n} \forall \mathbf{f}_2 : \mathbb{B}_{k,n} \ldots \exists \mathbf{f}_d : \mathbb{B}_{k,n}\ \Phi \qquad (\Phi \text{ of order } k-1)$$

HOSAT: Definition

- **Higher-order Boolean functions:** $\mathbb{B}_{0,n} := \mathbb{B} := \{0,1\}; \qquad k,n \in \mathbb{N}$

  $\mathbb{B}_{k+1,n} := [(\mathbb{B}_{k,n})^n \to \mathbb{B}]$.

  E.g. given $g_1, \dots, g_n \in \mathbb{B}_{1,n} := [\mathbb{B}^n \to \mathbb{B}]$ and $f \in \mathbb{B}_{2,n}$, we have $f(g_1, \dots, g_n) \in \mathbb{B}$.

- **Quantifier-free generalised Boolean formulas:**

  $$\Phi := \top \mid f(g_1, \dots, g_n) \mid \neg\Phi \mid \Phi \wedge \Phi \qquad \text{(function applications are well-typed)}$$

- **Generalised Boolean formulas of order 0:**

  $$\exists \mathbf{f}_1 : \mathbb{B}\, \forall \mathbf{f}_2 : \mathbb{B} \dots \exists \mathbf{f}_d : \mathbb{B}\ \Phi \qquad (\Phi \text{ quantifier-free})$$

- **Generalised Boolean formulas of order $k \geq 1$:**

  $$\exists \mathbf{f}_1 : \mathbb{B}_{k,n} \forall \mathbf{f}_2 : \mathbb{B}_{k,n} \dots \exists \mathbf{f}_d : \mathbb{B}_{k,n}\ \Phi \qquad (\Phi \text{ of order } k-1)$$

HOSAT: Definition

HOSAT(k,d) : d-alternating satisfiability problem of order k

Input: A sentence Φ of order k and alternation depth d for functions in $\mathbb{B}_{k,n}$.
Output: Is Φ valid?

$$\mathsf{HOSAT}(k,*) := \bigcup_{d\in\mathbb{N}_+} \mathsf{HOSAT}(k,d) \qquad \mathsf{HOSAT} := \bigcup_{k\in\mathbb{N}_+} \mathsf{HOSAT}(k,*)$$

HOSAT: Definition

HOSAT(k,d) : d-alternating satisfiability problem of order k

Input: A sentence Φ of order k and alternation depth d for functions in $\mathbb{B}_{k,n}$.
Output: Is Φ valid?

$$\text{HOSAT}(k,\ *) := \bigcup_{d\in\mathbb{N}_+} \text{HOSAT}(k,\ d) \qquad \text{HOSAT} := \bigcup_{k\in\mathbb{N}_+} \text{HOSAT}(k,\ *)$$

Theorem 1

1. *HOSAT(k,d) is complete for* $\Sigma_d^{k\text{EXP}}$
2. *HOSAT(k,$*$) is complete for STA*$(*,\mathit{exp}_2^k(n^{O(1)}),O(n))$
3. *HOSAT is* TOWER*-complete.*

HOSAT: Related work

Instances of HOSAT were already considered by several authors in the past.

- HOSAT$(1,1)$:
  - was used by Babai et al. (1991) to show the left to right inclusion of $\mathrm{NE{\scriptstyle XP}} = \mathrm{MIP}$
  - is related to Dependency QBF: $\forall \mathbf{y} \exists x_1(Y_1) \dots \exists x_m(Y_m)\ \Phi$ is equivalent to

$$\exists f_1 : [\mathbb{B}^{|Y_1|} \to \mathbb{B}] \dots \exists f_m : [\mathbb{B}^{|Y_m|} \to \mathbb{B}]\ \forall \mathbf{y}\ \Phi[f_i(Y_i)/x_i]$$

- HOSAT$(1,d)$ was used by Lohrey (2012) to show $\Sigma_d^{\mathrm{E{\scriptstyle XP}}}$-hardness of model checking Σ_d-MSO sentences over hierarchical graph unfoldings

- HOSAT is similar to the "Boolean set theory" used by Statman (1979) to show that the *normalisation* problem for simply typed λ-terms is $\mathrm{T{\scriptstyle OWER}}$-hard.

HOSAT: Related work

Instances of HOSAT were already considered by several authors in the past.

- HOSAT$(1,1)$:
  - was used by Babai et al. (1991) to show the left to right inclusion of $\mathrm{NE{\small XP}} =$ MIP
  - is related to Dependency QBF: $\forall \mathbf{y} \exists x_1(Y_1) \dots \exists x_m(Y_m)\ \Phi$ is equivalent to

$$\exists f_1 : [\mathbb{B}^{|Y_1|} \to \mathbb{B}] \dots \exists f_m : [\mathbb{B}^{|Y_m|} \to \mathbb{B}]\ \forall \mathbf{y}\ \Phi[f_i(Y_i)/x_i]$$

- HOSAT$(1,d)$ was used by Lohrey (2012) to show $\Sigma_d^{\mathrm{E{\small XP}}}$-hardness of model checking Σ_d-MSO sentences over hierarchical graph unfoldings

- HOSAT is similar to the "Boolean set theory" used by Statman (1979) to show that the *normalisation* problem for simply typed λ-terms is $\mathrm{T{\small OWER}}$-hard.

HOSAT: Related work

Instances of HOSAT were already considered by several authors in the past.

- HOSAT$(1,1)$:
  - was used by Babai et al. (1991) to show the left to right inclusion of $\mathrm{NE{\scriptsize XP}} =$ MIP
  - is related to Dependency QBF: $\forall \mathbf{y} \exists x_1(Y_1) \dots \exists x_m(Y_m)\ \Phi$ is equivalent to

$$\exists f_1 : [\mathbb{B}^{|Y_1|} \to \mathbb{B}] \dots \exists f_m : [\mathbb{B}^{|Y_m|} \to \mathbb{B}]\ \forall \mathbf{y}\ \Phi[f_i(Y_i)/x_i]$$

- HOSAT$(1,d)$ was used by Lohrey (2012) to show $\Sigma_d^{\mathrm{E{\scriptsize XP}}}$-hardness of model checking Σ_d-MSO sentences over hierarchical graph unfoldings

- HOSAT is similar to the "Boolean set theory" used by Statman (1979) to show that the *normalisation* problem for simply typed λ-terms is $\mathrm{T{\scriptsize OWER}}$-hard.

(Weak) Presburger arithmetic

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

"There is no maximum integer" $\forall \mathrm{x}\, \exists \mathrm{y} : \mathrm{x} + 1 \leq \mathrm{y}$

Theorem (Fischer & Rabin, '74; Berman '80)

Presburger arithmetic is complete for STA($*$,exp$_2^2(n^{O(1)})$,$O(n)$) (= HOSAT(2,$*$)).

(Weak) Presburger arithmetic

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

"There is no maximum integer" $\forall \mathrm{x}\, \exists \mathrm{y} : \mathrm{x} + 1 \leq \mathrm{y}$

Theorem (Fischer & Rabin, '74; Berman '80)

Presburger arithmetic is complete for STA($*$,exp$_2^2(n^{O(1)})$,$O(n)$) (= HOSAT(2,$*$)).

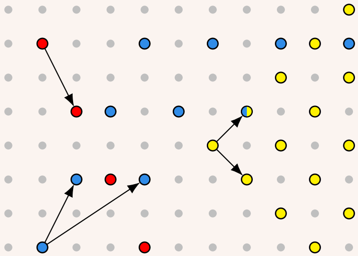
Weak Presburger arithmetic: first-order theory of $\langle \mathbb{Z}, 0, 1, +, = \rangle$

- the theory originally considered by Presburger
- well-understood expressivity-wise [Chistikov & Haase, ICALP'2020]
- has not been studied complexity-wise.

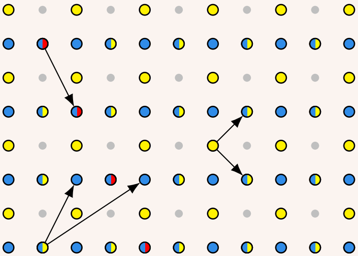
Weak PA: can it be easier than PA?

Quite different theories, geometric-wise:

PA



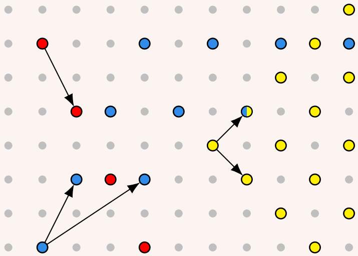
Weak PA



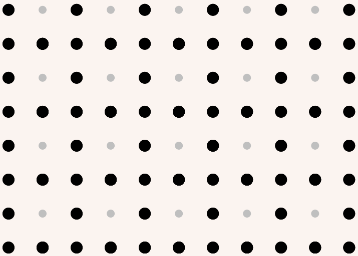
Weak PA: can it be easier than PA?

Quite different theories, geometric-wise:

PA



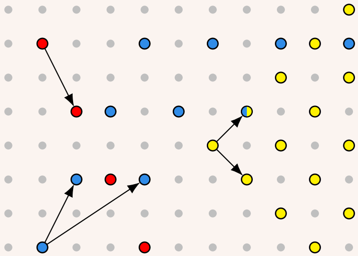
Weak PA



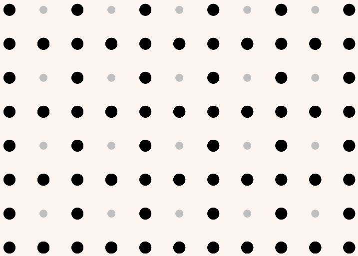
Weak PA: can it be easier than PA?

Quite different theories, geometric-wise:

PA



Weak PA



For some fragments, taking $=$ instead of $\leq$ matters:

- $\exists \mathbf{x} \in \mathbb{Z}^d \; A \cdot \mathbf{x} \leq \mathbf{b}$ is NP-complete; $\exists \mathbf{x} \in \mathbb{Z}^d \; A \cdot \mathbf{x} = \mathbf{b}$ is $\mathrm{P}\textsc{Time}$-complete
- $\exists x_1 \forall x_2 \dots \exists x_d \; A \cdot \mathbf{x} \leq \mathbf{b}$ is $\mathrm{PS}\textsc{pace}$-hard; $\exists x_1 \forall x_2 \dots \exists x_d \; A \cdot \mathbf{x} = \mathbf{b}$ is still $\mathrm{P}\textsc{Time}$

Answer: No.

Theorem 2

The following fragments of Weak PA are already as hard as PA:

- ***positive fragment:*** $\Phi := a_1 x_1 + \cdots + a_d x_d = c \mid \Phi \wedge \Phi \mid \Phi \vee \Phi \mid \exists x.\Phi \mid \forall x.\Phi$
- ***quantified Horn fragment:*** $\exists x_1 \forall x_2 \ldots \exists x_d . \bigwedge_{i \in I} A_i \cdot \mathbf{x} = \mathbf{c}_i \Rightarrow B_i \cdot \mathbf{x} = \mathbf{d}_i$

Proofs by reductions from HOSAT$(2,*)$.

Answer: No.

Theorem 2

The following fragments of Weak PA are already as hard as PA:

- ***positive fragment:*** $\Phi := a_1 x_1 + \cdots + a_d x_d = c \mid \Phi \wedge \Phi \mid \Phi \vee \Phi \mid \exists x.\Phi \mid \forall x.\Phi$
- ***quantified Horn fragment:*** $\exists x_1 \forall x_2 \ldots \exists x_d. \bigwedge_{i \in I} A_i \cdot \mathbf{x} = \mathbf{c}_i \Rightarrow B_i \cdot \mathbf{x} = \mathbf{d}_i$

Proofs by reductions from HOSAT$(2,*)$.

For the reduction it suffices to show how to:

- encode the functions from $\mathbb{B}_{1,n}$ and $\mathbb{B}_{2,n}$
- encode function application.

Encoding functions in Weak PA

- **Functions in $\mathbb{B}_{1,n} = [\mathbb{B}^n \to \mathbb{B}]$:** f encoded as $\hat{f} \in [2^{2^n}] := [0, 2^{2^n} - 1]$ s.t.

$$f(b_1, \ldots, b_n) = b \quad \text{if and only if} \quad \begin{array}{l} \text{the } j\text{-th bit of } \hat{f} \text{ is set to } b, \\ \text{where } j := \sum_{i=1}^{n} b_i \cdot 2^{i-1}. \end{array}$$

Encoding functions in Weak PA

- **Functions in** $\mathbb{B}_{1,n} = [\mathbb{B}^n \to \mathbb{B}]$ **:** f encoded as $\widehat{f} \in [2^{2^n}] := [0, 2^{2^n} - 1]$ s.t.

$$f(b_1, \dots, b_n) = b \quad \text{if and only if} \quad \text{the } j\text{-th bit of } \widehat{f} \text{ is set to } b,$$
$$\text{where } j := \textstyle\sum_{i=1}^{n} b_i \cdot 2^{i-1}.$$

- **Functions in** $\mathbb{B}_{2,n}$ **:** $\widehat{f} \in \mathbb{Z}$ encodes f iff for all $b \in \mathbb{B}$, $g_1, \dots, g_n \in \mathbb{B}_{1,n}$

$$f(g_1, \dots, g_n) = b \quad \text{iff} \quad \widehat{f} \equiv_q b \text{ for all primes } q \in [k^3, (k+1)^3),$$
$$\text{where } k := \textstyle\sum_{i=1}^{n} \widehat{g}_i \cdot 2^{2^n (i-1)} + \textit{offset}.$$

Encoding functions in Weak PA

- **Functions in $\mathbb{B}_{1,n} = [\mathbb{B}^n \to \mathbb{B}]$:** f encoded as $\hat{f} \in [2^{2^n}] := [0, 2^{2^n} - 1]$ s.t.

$$f(b_1, \dots, b_n) = b \quad \text{if and only if} \quad \text{the } j\text{-th bit of } \hat{f} \text{ is set to } b, \text{ where } j := \sum_{i=1}^{n} b_i \cdot 2^{i-1}.$$

- **Functions in $\mathbb{B}_{2,n}$:** $\hat{f} \in \mathbb{Z}$ encodes f iff for all $b \in \mathbb{B}$, $g_1, \dots, g_n \in \mathbb{B}_{1,n}$

$$f(g_1, \dots, g_n) = b \quad \text{iff} \quad \hat{f} \equiv_q b \text{ for all primes } q \in [k^3, (k+1)^3), \text{ where } k := \sum_{i=1}^{n} \hat{g}_i \cdot 2^{2^n(i-1)} + \textit{offset}.$$

All functions in $\mathbb{B}_{2,k}$ admit such an encoding, thanks to Ingham's theorem and the Chinese remainder theorem.

Conclusion

- The **Higher-order Boolean satisfiability problem** is a natural extension of QBF that allows to capture all complexity classes in the weak $k\textsc{Exp}$ hierarchy ($k \geq 1$).

- **Weak Presburger arithmetic** is as hard as (standard) Presburger arithmetic, even for its **positive** and **quantified Horn** fragments.