A fixed-point theorem for Horn formula equations

Johannes Kloibhofer
(joint work with Stefan Hetzl)

Institute for Logic, Language and Computation
University of Amsterdam, Netherlands

December 15, 2021

Introduction

- Consider Horn formula equations, i.e. special existential second-order formulas
- Interested in first-order solutions
- Horn formula equations appear in various areas:
  - Second-order quantifier elimination
  - Program verification
  - Proof theory
- We prove general results and use them in manifold applications

Formula equations

Definition

A *formula equation* has the form $\exists\overline{X}\psi$, where $\overline{X}$ is a tuple of predicate variables and ψ is a first-order formula.

- Equivalent to $\exists\overline{X}(\varphi_1 \leftrightarrow \varphi_2)$, hence "equation"
- A formula equation is
  - valid: $\models \exists\overline{X}\psi$
  - solvable: There exist formulas $\overline{\chi}$ s.t. $\models \psi[\overline{X}\backslash\overline{\chi}]$
- There are valid formula equations which are not first-order solvable
- Finding $\overline{\chi}$ s.t. $\models \psi[\overline{X}\backslash\overline{\chi}]$ is also known as Boolean solution problem

Horn formula equations

Definition

A *constrained clause* is a formula C of the form

$$\gamma \vee \bigvee_{i=1}^{m} \neg X_i(\overline{t_i}) \vee \bigvee_{j=1}^{n} Y_j(\overline{s_j}),$$

where X_i, Y_j are predicate variables and γ is a first-order formula without predicate variables. C is called

1. *Horn*, if $n \leq 1$,
2. *dual-Horn*, if $m \leq 1$ and
3. *linear-Horn*, if $m, n \leq 1$.

Definition

A *Horn formula equation* $\exists \overline{X} \psi$ is a formula equation of the form $\exists \overline{X} \forall^* \bigwedge_{i=1}^{n} H_i$, where H_i is a constrained Horn clause for $i \in \{1, ..., n\}$.

Least fixed-point logic (LFP)

- Extension of first-order logic
- LFP central in finite model theory / descriptive complexity (cf. Immerman-Vardi theorem '82)
- Define function F_φ on M^k by

$$F_\varphi : \quad R \mapsto \{\overline{x} \in M^k \mid \mathcal{M} \models \varphi(R, \overline{x})\}$$

- If R occurs only positively in φ, then F_φ is monotonous
  $\Rightarrow$ Least fixed point exists due to Knaster-Tarski theorem
- Introduce LFP atomic formulas $[\mathrm{lfp}_R\ \varphi(R, \overline{x})]$, where

$$\mathcal{M} \models [\mathrm{lfp}_R\ \varphi(R, \overline{x})](\overline{a}) :\Leftrightarrow\ \overline{a} \in \mathrm{lfp}(F_\varphi)$$

- Can be extended to simultaneous fixed points

- Fixed point can be approximated by relations

$$S^0 = \varnothing, \quad S^{\alpha+1} = F_\varphi(S^\alpha), \quad S^\alpha = \bigcup_{\beta<\alpha} S^\beta$$

- LFP formula $[\mathrm{lfp}_R\ \varphi(R, \overline{x})]$ can be approximated by FO formulas

$$\varphi^0(\overline{x}) \equiv \bot, \quad \varphi^{k+1}(\overline{x}) \equiv \varphi(\varphi^k, \overline{x})$$

Example

Let $\mathcal{L} = \{E\}$ be the language of graphs. Define

$$\varphi(R, u, v) \equiv E(u, v) \vee \exists w(R(u, w) \wedge E(w, v))$$

As R occurs only positively in φ we can define $[\mathrm{lfp}_R\ \varphi(R, u, v)](x, y)$.

LFP-formula is approximated by first-order formulas

$$\begin{aligned} \varphi^0(x, y) &\equiv \bot \\ \varphi^{k+1}(x, y) &\equiv E(x, y) \vee \exists w(\varphi^k(x, w) \wedge E(w, y)) \end{aligned}$$

Proof Idea

Three different types of clauses in a Horn formula equation $\exists \overline{X} \psi$:

$$\begin{array}{lrl} (B) & \gamma & \rightarrow X_0(\overline{s}), \\ (I) & \gamma \wedge X_1(\overline{t_1}) \wedge \cdots \wedge X_m(\overline{t_m}) & \rightarrow X_0(\overline{s}), \\ (E) & \gamma \wedge X_1(\overline{t_1}) \wedge \cdots \wedge X_m(\overline{t_m}) & \rightarrow \bot, \end{array}$$

- Define a tuple Φ_ψ of first-order formulas from clauses of the form (B) and (I)
- This tuple defines LFP-formulas

Horn fixed-point theorem

Horn fixed-point theorem

Let $\exists \overline{X} \psi$ be a Horn formula equation and $\mu_j := [\mathrm{lfp}_{X_j}\ \Phi_\psi]$ for $j \in \{1, \ldots, n\}$, then

1. $\models \exists \overline{X}\, \psi \leftrightarrow \psi[\overline{X} \backslash \overline{\mu}]$ and
2. if $\mathcal{M} \models \psi[\overline{X} \backslash \overline{R}]$ for some structure $\mathcal{M}$ and relations $R_1, \ldots, R_n$ in $\mathcal{M}$, then $\mathcal{M} \models \bigwedge_{j=1}^{n} (\mu_j \to R_j)$.

- Horn formula equation valid iff it is LFP-solvable
- Analogous theorems for dual-Horn and linear-Horn formula equations
- Generalised for abstract semantics

Example

Let $\mathcal{L} = \{E, s, t\}$. Consider the Horn formula equation $\exists X \psi$, with

$$\psi \equiv \forall u, v \bigwedge \begin{cases} X(s) \\ X(u) \wedge E(u,v) \rightarrow X(v) \\ \neg X(t) \end{cases}$$

- $\Phi_\psi(R, x) \equiv x = s \vee \exists u(E(u,x) \wedge R(u))$.
- Define $\mu = [\mathrm{lfp}_X\ \Phi_\psi]$, then $\models \exists X \psi \leftrightarrow \psi[X \backslash \mu]$
- Equivalently $\models \exists X \psi \leftrightarrow \neg \mu(t)$
- Connectivity is not expressible in FO
  $\Rightarrow \exists X \psi$ not solvable in FO!

Fixed-point approximation

- Problem: Finding first-order formulas, which approximate existential second-order formulas
- First investigated by [Ackermann '35] for relational language and one unary predicate variable
- Used a method similar to modern resolution
- Extended for arbitrary predicate variables in [Wernhard '17]
- Our Idea: Express LFP-formula as an infinite disjunction of first-order formulas

Theorem

Let $\exists \overline{X} \psi$ be a Horn formula equation. Then there exists a countable set of first-order formulas Ψ s.t.

$$\exists \overline{X} \psi \equiv \bigwedge_{\varphi \in \Psi} \varphi.$$

Example

Consider the Horn formula equation $\exists X \psi$, with

$$\psi \equiv \forall u, v \bigwedge \begin{cases} X(s) \\ X(u) \wedge E(u,v) \rightarrow X(v) \\ \neg X(t) \end{cases}$$

- Define formulas

$$\varphi^0(x) \equiv x = s$$
$$\varphi^{k+1}(x) \equiv x = s \vee \exists u (E(u,x) \wedge \varphi^k(u))$$

- Then $\varphi^\omega \equiv \bigvee_{k \in \omega} \varphi^k$ is equivalent to $[\mathrm{lfp}_X \ \Phi_\psi]$.
- Thus $\exists X \psi \equiv \bigwedge_{k \in \omega} \neg \varphi^k(t)$.

Partial Correctness of while-programs

- A Hoare triple $\{\varphi\}p\{\psi\}$ consists of a program p and two first-order formulas φ and ψ.
- The verification condition $\mathrm{vc}(\{\varphi\}p\{\psi\})$ can be written as a linear-Horn formula equation s.t.

$$\models \{\varphi\}p\{\psi\} \quad \Leftrightarrow \quad \mathbb{Z} \models \mathrm{vc}(\{\varphi\}p\{\psi\})$$

- The predicate variables correspond to the loop invariants
- Fixed-point theorem: For every solution $\overline{\chi}$ of $\mathbb{Z} \models \mathrm{vc}(\{\varphi\}p\{\psi\})$ it holds

$$\mathbb{Z} \models \bigwedge_{i=1}^{n} \mu_i \rightarrow \chi_i \wedge \chi_i \rightarrow \nu_i$$

- As corollaries: The canonical solutions of our fixed-point theorem express the weakest precondition and strongest postcondition.

Affine solution problem

- Problem: Finding *affine subspaces* of $\mathbb{Q}^n$ which solve a formula equation without first-order quantifiers in the language $\mathcal{L}_{\text{aff}} = \{0, 1, +, \{c \mid c \in \mathbb{Q}\}\}$
- Decidability shown by [Hetzl, Zivota '19]
- Computed a fixed point in lattice of affine subspaces of $\mathbb{Q}^n$
- Horn fixed-point theorem not applicable
- Need generalisation!

Abstract semantics

Abstract semantics:

- First-order formulas interpreted as usual
- Second-order predicates and LFP-atoms not interpreted in $(M^k, \subseteq)$, but in different lattice $(V_k, \sqsubseteq)$ s.t.

$$(M^k, \subseteq) \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} (V_k, \sqsubseteq)$$

  forms a Galois connection for every $k \in \mathbb{N}$
- We call $(\mathcal{M}, G)$, where $G = (V_k, \alpha_k, \gamma_k)_{k \in \mathbb{N}}$, a *model abstraction*

Abstract semantics

Abstract semantics:

- First-order formulas interpreted as usual
- Second-order predicates and LFP-atoms not interpreted in $(M^k, \subseteq)$, but in different lattice $(V_k, \sqsubseteq)$ s.t.

$$(M^k, \subseteq) \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} (V_k, \sqsubseteq)$$

  forms a Galois connection for every $k \in \mathbb{N}$
- We call $(\mathcal{M}, G)$, where $G = (V_k, \alpha_k, \gamma_k)_{k \in \mathbb{N}}$, a *model abstraction*

Example:

- $(\mathbb{Q}, G_{\mathrm{aff}})$ is a model abstraction, where $G_{\mathrm{aff}} = ((\mathrm{Aff}\ \mathbb{Q}^k, \subseteq), \mathrm{aff}_k, \mathrm{id}_k)_{k \in \mathbb{N}}$ with
  - $\mathrm{Aff}\ \mathbb{Q}^k$ is the set of affine subsets of $\mathbb{Q}^k$
  - aff_k is the affine hull
  - id_k is embedding of $\mathrm{Aff}\ \mathbb{Q}^k$ in $\mathbb{Q}^k$

Abstract fixed-point theorem

Theorem (Abstract Horn fixed-point theorem)

Let $\exists \overline{X} \psi$ *be a Horn formula equation and* $\mu_j := [\mathrm{lfp}_{X_j}\ \Phi_\psi]$ *for* $j \in \{1, ..., n\}$*, then:*

1. $\models_{\mathrm{a}} \exists \overline{X}\ \psi \leftrightarrow \psi[\overline{X} \backslash \overline{\mu}]$ *and*
2. *if* $(\mathcal{M}, G) \models_{\mathrm{a}} \psi[\overline{X} \backslash \overline{R}]$ *for some model abstraction* $(\mathcal{M}, G)$ *and abstract relations* $R_1, ..., R_n$*, then* $(\mathcal{M}, G) \models_{\mathrm{a}} \bigwedge_{j=1}^{n} (\mu_j \to R_j)$*.*

- Analogous theorems for dual-Horn and linear-Horn formula equations
- Decidability of affine solution problem follows as direct corollary

Inductive theorem proving

- Consider approach to inductive theorem proving based on tree grammars by [Eberhard, Hetzl '15]
- Generate proof of universal statement:
    - First proofs of small instances are computed
    - Then second-order unification problem is deduced:
        1. $\Gamma_0(\alpha, \beta) \Rightarrow X(\alpha, 0, \beta)$
        2. $\Gamma_1(\alpha, \nu, \gamma), \bigwedge_{1 \leq i \leq n} X(\alpha, n, t_i(\alpha, \nu, \gamma)) \Rightarrow X(\alpha, s(n), \gamma)$
        3. $\Gamma_2(\alpha), \bigwedge_{1 \leq j \leq m} X(\alpha, \alpha, u_j(\alpha)) \Rightarrow B(\alpha)$
    - Every solution is an inductive invariant
- Equivalent to a Horn formula equation
- Using fixed-point theorem we get LFP-formula which implies every solution
- By fixed-point approximation get first-order formulas

Conclusion

- Horn formula equation satisfiable iff LFP-solvable
- Canonical solutions in LFP
- Applications:
  - Second-order quantifier elimination
  - Decidability of affine solution problem
  - In program verification we can define an equivalent condition to the semantics of Hoare triples
    - Canonical solutions correspond to weakest precondition and strongest postcondition
  - Algorithmic step in approach to inductive theorem proving

References I

[1] Wilhelm Ackermann. “Untersuchungen über das Eliminationsproblem der mathematischen Logik”. In: *Mathematische Annalen* 110.1 (1935), pp. 390–413. DOI: 10.1007/BF01448035.

[2] Sebastian Eberhard and Stefan Hetzl. “Inductive theorem proving based on tree grammars”. In: *Annals of Pure and Applied Logic* 166.6 (2015), pp. 665–700. DOI: 10.1016/j.apal.2015.01.002.

[3] Stefan Hetzl and Johannes Kloibhofer. “A fixed point theorem for Horn formula equations”. In: *Proceedings of the 8th Workshop on Horn Clauses for Verification and Synthesis (HCVS)* (2021). DOI: 10.4204/EPTCS.344.5.

[4] Stefan Hetzl and Sebastian Zivota. “Decidability of affine solution problems”. In: *Journal of Logic and Computation* 30.3 (2020), pp. 697–714. DOI: 10.1093/logcom/exz033.

References II

[5] Johannes Kloibhofer. “A fixed-point theorem for Horn formula equations”. MA thesis. Austria: TU Wien, 2020.

[6] Andreas Nonnengart and Andrzej Szałas. “A Fixpoint Approach to Second-Order Quantifier Elimination with Applications to Correspondence Theory”. In: *Logic at Work: Essays Dedicated to the Memory of Helena Rasiowa*. Ed. by Ewa Orłowska. Vol. 24. Studies in Fuzziness and Soft Computing. Springer, 1998, pp. 307–328.

[7] Christoph Wernhard. “The Boolean Solution Problem from the Perspective of Predicate Logic”. In: *11th International Symposium on Frontiers of Combining Systems (FroCoS)*. Vol. 10483. Lecture Notes in Computer Science. Springer, 2017, pp. 333–350. DOI: 10.1007/978-3-319-66167-4_19.