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 13, 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

$$S_0 = \varnothing, \quad S_{\alpha+1} = F_\varphi(S_\alpha), \quad S_\alpha = \bigcup_{\beta<\alpha} S_\beta$$

- Fixed point can be approximated by relations

$$S_0 = \varnothing, \quad S_{\alpha+1} = F_\varphi(S_\alpha), \quad S_\alpha = \bigcup_{\beta<\alpha} S_\beta$$

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

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

Proof Idea

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

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

- 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 $\mathcal{M} \models \bigwedge_{j=1}^{n} (\mu_j \rightarrow R_j)$.

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

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

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

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

- Then $\Phi_\psi(R, x) \equiv x = s \vee \exists u(E(u,x) \wedge R(u))$.
- 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 $\exists X \psi \equiv \bigwedge_{k\in\omega} \neg\varphi^k(t)$.

Affine solution problem

- Problem: Finding *affine subspaces* which solve a quantifier-free formula equation in the language $\mathcal{L}_{\mathrm{aff}} = \{0, 1, +, \{c \mid c \in \mathbb{Q}\}\}$
- Decidability shown by [Hetzl, Zivota '19]
- Computed a fixed point in lattice of affine subspaces of $\mathbb{Q}^n$
- Direct corollary of abstract fixed-point theorem!

Conclusion

- Horn formula equation satisfiable iff LFP-solvable
- Canonical solutions in LFP
- Applications:
  - Second-order quantifier elimination
  - Decidability of affine solution problem [Hetzl, Zivota '20]
  - 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 by tree grammars [Eberhard, Hetzl '15]