A fixed-point theorem for Horn formula equations

Stefan Hetzl
(joint work with Johannes Kloibhofer)

Institute of Discrete Mathematics and Geometry
TU Wien, Vienna, Austria

8th Workshop on Horn Clauses for Verification and Synthesis

March 28, 2021

Introduction

Motivation:

- Integrate constrained Horn clause solving in broader logical context
- Connect to formula equations, 2nd order quantifier elimination (Schröder 1890, Ackermann 1935, Behmann 1950, Boolean Unification 1980ies, 1990ies, ...)

Contribution:

- Solving constrained Horn clause set is special case of solving formula equation
- Formulate fixed-point iteration *in the logic*
- Prove fixed-point theorem for Horn formula equations
- Several applications and corollaries

Formula Equations

- **Definition.** A *formula equation* is a sentence of the form $\exists \overline{X}\, \varphi$ where $\overline{X}$ are predicate variables and φ is first-order.
- **Definition** A formula equation $\exists \overline{X}\, \varphi$ is
  - *solvable* if there is $[\overline{X} \backslash \overline{\psi}]$ s.t. $\models \varphi[\overline{X} \backslash \overline{\psi}]$
    "syntactically solvable" in [Rümmer, Hojjat, Kuncak '13]
  - *valid* if $\exists \overline{X}\, \varphi$ is valid
    "semantically solvable" in [Rümmer, Hojjat, Kuncak '13]
  - *satisfiable* if $\exists \overline{X}\, \varphi$ is satisfiable
    "satisfiable" in [Gurfinkel, Bjørner '19]
- Equivalent to the form $\exists \overline{X}\, (\varphi_1 \leftrightarrow \varphi_2)$, hence "equation".

Constrained Horn Clauses and Formula Equations

- A constrained clause is a formula C of the form

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

  where X_i, Y_j are predicate variables and φ is a formula without predicate variables. C is called
  - *Horn* if $k \leq 1$
  - *dual Horn* if $n \leq 1$
  - *linear* if $k, n \leq 1$
- **Definition.** If S is a set of constrained Horn clauses, then

$$\exists \overline{X} \, \forall^* \bigwedge_{C \in S} C$$

  is called *Horn formula equation*.

Example

- Let

$$A_1 \equiv \forall u\, s(u) \neq 0 \qquad A_2 \equiv \forall u \forall v\, (s(u) = s(v) \rightarrow u = v)$$

and $A \equiv A_1 \wedge A_2$, then

$$A \rightarrow \exists X \exists Y \forall u \Big(X(0) \wedge (X(u) \rightarrow Y(s(u))) \wedge (Y(u) \rightarrow X(s(u))) \wedge \neg(Y(u) \wedge X(u)) \Big)$$

is logically equivalent to a Horn formula equation E.

- **Proposition.** E is valid but not (FOL-)solvable.
- Fixed-point semantics of logic program (iterate T_P operator)
$X(0)$, $Y(s(0))$, $X(s^2(0))$, $Y(s^3(0))$, $X(s^4(0))$, ...
least fixed point of T_P is minimal model:
$\{X(s^n(0)) \mid n \in \mathbb{N} \text{ even}\} \cup \{Y(s^n(0)) \mid n \in \mathbb{N} \text{ odd}\}$.

First-order logic with least fixed-point operator

- FO[LFP] central in finite model theory / descriptive complexity (Immerman-Vardi theorem '82)
- An occurrence of X in φ is *positive* if it occurs under an even number of negations
- If X occurs only positively in $\varphi(X, \overline{u})$, then

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

  is a monotone operator.
- Knaster-Tarski theorem $\Rightarrow F_\varphi$ has a least fixed-point
- Introduce syntax for new predicate symbols $[\mathrm{lfp}_X \varphi(X, \overline{u})]$ where

$$M \models [\mathrm{lfp}_X \varphi(X, \overline{u})](\overline{t}) \quad \text{iff} \quad \overline{t}^M \in \mathrm{lfp}(F_\varphi)$$

- Extension to simultaneous least fixed-points

The fixed-point theorem

- **Definition.** A Horn formula equation $\exists \overline{X}\, \psi$ induces a tuple of formulas Φ_ψ (essentially first-order definition of T_P-operator).
- **Theorem.** Let $\exists X_1 \cdots \exists X_n\, \psi$ 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 $M \models \psi[\overline{X} \backslash \overline{R}]$ for a structure M and relations $R_1, \ldots, R_n$ in M, then $M \models \bigwedge_{j=1}^{n} (\mu_j \to R_j)$.
- **Corollary.** Dual version for dual Horn formula equations.
- **Corollary.** Linear version from combining Horn and dual Horn.
- **Corollary.** Horn / dual Horn / linear Horn formula equation is valid iff it is FO[LFP]-solvable.

Example

- Let

$$A_1 \equiv \forall u\, s(u) \neq 0 \qquad A_2 \equiv \forall u \forall v\, (s(u) = s(v) \to u = v)$$

and $A \equiv A_1 \wedge A_2$, then

$$A \to \exists X \exists Y \forall u \Big(X(0) \wedge (X(u) \to Y(s(u))) \wedge (Y(u) \to X(s(u))) \wedge \neg(Y(u) \wedge X(u)) \Big)$$

is logically equivalent to a Horn formula equation E.

- **Corollary.** E has a solution in FO[LFP].
- $\Phi_E = (\varphi_X, \varphi_Y)$ where

$$\begin{aligned} \varphi_X(X, Y, u) &\equiv A \wedge (u = 0 \vee \exists v\, (Y(v) \wedge u = s(v))) \\ \varphi_Y(X, Y, u) &\equiv A \wedge \exists v\, (X(v) \wedge u = s(v)) \end{aligned}$$

- The solution of E is $\overline{\mu} = ([\mathrm{lfp}_X \Phi_\psi], [\mathrm{lfp}_Y \Phi_\psi])$

Applications to program verification

- Hoare triples $\{\varphi\}p\{\psi\}$ for imperative programming language
- Verification conditions written as

$$\mathsf{vc}(\{\varphi\}p\{\psi\}) \;\equiv\; \exists \bar{I} \forall^* \, \tilde{\mathsf{vc}}\{\varphi\}p\{\psi\}$$

  are a linear Horn formula equation.

- **Corollary.** Partial correctness is expressible as FO[LFP]-formula.
- **Corollary.** wp and sp expressible as FO[LFP]-formulas.
  [Blass, Gurevich '87]

Further Applications

- Linear Horn formula equations and interpolation
- Generalisation of result of [Ackermann '35] on SOQE
- Algorithmic step in approach to inductive theorem proving by tree grammars [Eberhard, H '15]
- Future work: Decidability of affine solution problem [H, Zivota '20] (needs abstract fixed-point theorem)

Conclusion

- Construction of least fixed point *in the logic*
  $\Longrightarrow$ Fixed-point theorem for Horn formula equation
- Validity = FO[LFP]-solvability of Horn formula equations
- Expressibility of partial correctness, wp, and sp in FO[LFP]
- Efficacy of interpolation (linear Horn, loop invariant generation)
- Further corollaries in various topics in computational logic

Future Work

- Base fixed-point theorem on abstract interpretation
- More detailed results on relationship to interpolation
- Decidability of classes of (Horn) formula equations
- Relate algorithms for SOQE and Horn clause solving