iProver-Eq: An Instantiation-based Theorem Prover with Equality

Konstantin Korovin and *Christoph Sticksel*
(joint work with Renate Schmidt)

The University of Manchester

17th July 2010

Instantiation-based Methods and Equality

- Instantiation-based methods
  - Decision procedure for Bernays-Schönfinkel fragment (verification, planning/scheduling, knowledge representation)
  - Performs well in plain first-order logic
  - Complementary to “traditional” first-order calculi

- Equational reasoning
  - Essential part in theory reasoning
  - Natural concept in many applications
  - Not well explored in instantiation-based setting

- Here: Instantiation-based calculus Inst-Gen-Eq
  - Ganzinger and Korovin [2004]
  - Complete for first-order clause logic modulo equality

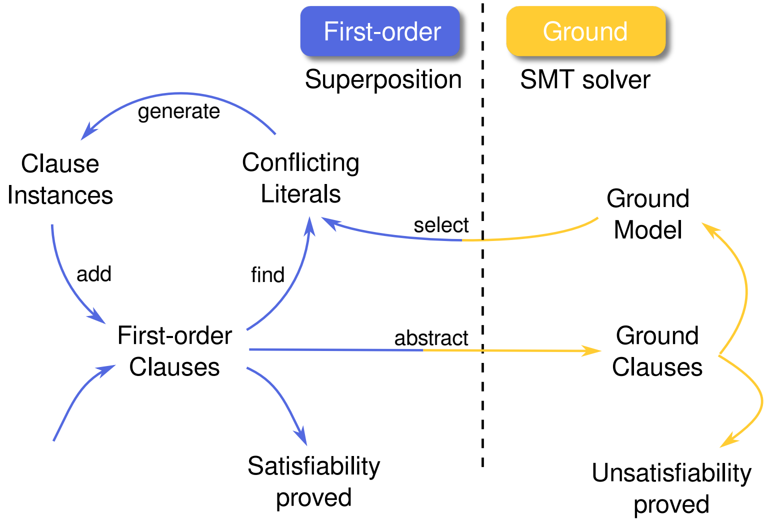
What is iProver-Eq?

- *iProver* is the implementation of the Inst-Gen calculus where equality is handled only axiomatically
- *iProver-Eq* is the extension of *iProver* with superposition-based equational reasoning

- Distinctive feature: modular combination of first-order reasoning and ground satisfiability checking

- Proof procedure consists of
  - Ground reasoning on the abstraction of the clause set by an SMT solver
  - Equational reasoning on first-order literals in a candidate model
  - Instantiation of clauses with substitutions from superposition proofs

iProver-Eq System Overview



Inst-Gen-Eq by Example: Finding inconsistencies

First-order clauses

$$f(x, y) \simeq f(y, x)$$

$$f(u, v) \not\simeq g(z) \ \vee \ u \simeq z$$

$$f(a, b) \simeq g(c)$$

$$a \not\simeq b$$

Ground abstraction

$$f(\bot, \bot) \simeq f(\bot, \bot)$$

$$f(\bot, \bot) \not\simeq g(\bot) \ \vee \ \bot \simeq \bot$$

$$f(a, b) \simeq g(c)$$

$$a \not\simeq b$$

Unit superposition proof: Selected literals inconsistent

$$\cfrac{\cfrac{f(a,b) \simeq g(c) \qquad \cfrac{f(x,y) \simeq f(y,x) \qquad f(u,v) \not\simeq g(z)}{f(v,u) \not\simeq g(z)}\,[u/x, v/y]}{g(c) \not\simeq g(z)}\,[a/v, b/u]}{\square}\,[c/z]$$

Inst-Gen-Eq by Example: Finding inconsistencies

First-order clauses

$$f(x,y) \simeq f(y,x)$$

$$f(u,v) \not\simeq g(z) \ \vee \ u \simeq z$$

$$f(a,b) \simeq g(c)$$

$$a \not\simeq b$$

Ground abstraction

$$f(\bot,\bot) \simeq f(\bot,\bot)$$

$$f(\bot,\bot) \not\simeq g(\bot) \ \vee \ \bot \simeq \bot$$

$$f(a,b) \simeq g(c)$$

$$a \not\simeq b$$

Unit superposition proof: Selected literals inconsistent

$$\cfrac{\cfrac{f(a,b) \simeq g(c) \qquad \cfrac{f(x,y) \simeq f(y,x) \qquad f(u,v) \not\simeq g(z)}{f(v,u) \not\simeq g(z)}\,[u/x, v/y]}{g(c) \not\simeq g(z)}\,[a/v, b/u]}{\square}\,[c/z]$$

Inst-Gen-Eq by Example: Finding inconsistencies

First-order clauses

$$\underline{f(x,y) \simeq f(y,x)}$$

$$\underline{f(u,v) \not\simeq g(z)} \lor u \simeq z$$

$$\underline{f(a,b) \simeq g(c)}$$

$$\underline{a \not\simeq b}$$

Ground abstraction

$$f(\bot,\bot) \simeq f(\bot,\bot)$$

$$f(\bot,\bot) \not\simeq g(\bot) \lor \bot \simeq \bot$$

$$f(a,b) \simeq g(c)$$

$$a \not\simeq b$$

Unit superposition proof: Selected literals inconsistent

$$\cfrac{f(a,b) \simeq g(c) \qquad \cfrac{f(x,y) \simeq f(y,x) \qquad f(u,v) \not\simeq g(z)}{f(v,u) \not\simeq g(z)}\,[u/x, v/y]}{\cfrac{g(c) \not\simeq g(z)}{\square}\,[c/z]}\,[a/v, b/u]$$

Inst-Gen-Eq by Example: Finding inconsistencies

First-order clauses

$$\underline{f(x,y) \simeq f(y,x)}$$

$$\underline{f(u,v) \not\simeq g(z)} \quad \vee \quad u \simeq z$$

$$\underline{f(a,b) \simeq g(c)}$$

$$\underline{a \not\simeq b}$$

Ground abstraction

$$f(\bot,\bot) \simeq f(\bot,\bot)$$

$$f(\bot,\bot) \not\simeq g(\bot) \quad \vee \quad \bot \simeq \bot$$

$$f(a,b) \simeq g(c)$$

$$a \not\simeq b$$

Unit superposition proof: Selected literals inconsistent

$$\cfrac{\cfrac{f(a,b) \simeq g(c) \qquad \cfrac{f(x,y) \simeq f(y,x) \qquad f(u,v) \not\simeq g(z)}{f(v,u) \not\simeq g(z)}\,[u/x, v/y]}{g(c) \not\simeq g(z)}\,[a/v, b/u]}{\square}\,[c/z]$$

Inst-Gen-Eq by Example: Generating instances

Unit superposition proof: Substitution extraction

$$\cfrac{\cfrac{f(a,b) \simeq g(c) \qquad \cfrac{f(x,y) \simeq f(y,x) \quad f(u,v) \not\simeq g(z)}{f(v,u) \not\simeq g(z)}\;[u/x, v/y]}{g(c) \not\simeq g(z)}\;[a/v, b/u]}{\square}\;[c/z]$$

First-order clauses

$$\underline{f(x,y) \simeq f(y,x)}$$

$$\underline{f(u,v) \not\simeq g(z)} \;\vee\; u \simeq z$$

$$\underline{f(a,b) \simeq g(c)}$$

$$\underline{a \not\simeq b}$$

First-order instances

$$f(b,a) \simeq f(a,b)$$

$$f(b,a) \not\simeq g(c) \;\vee\; b \simeq c$$

Inst-Gen-Eq by Example: Generating instances

Unit superposition proof: Substitution extraction

$$\dfrac{f(a,b) \simeq g(c) \qquad \dfrac{f(x,y) \simeq f(y,x) \quad f(u,v) \not\simeq g(z)}{f(v,u) \not\simeq g(z)}\,[u/x, v/y]}{\dfrac{g(c) \not\simeq g(z)}{\square}\,[c/z]}\,[a/v, b/u]$$

First-order clauses

$$\underline{f(x,y) \simeq f(y,x)}$$

$$\underline{f(u,v) \not\simeq g(z)} \;\vee\; u \simeq z$$

$$\underline{f(a,b) \simeq g(c)}$$

$$\underline{a \not\simeq b}$$

First-order instances

$$f(b,a) \simeq f(a,b)$$

$$f(b,a) \not\simeq g(c) \;\vee\; b \simeq c$$

Inst-Gen-Eq by Example: Generating instances

Unit superposition proof: Substitution extraction

$$\dfrac{f(a,b)\simeq g(c) \qquad \dfrac{f(x,y)\simeq f(y,x) \qquad f(u,v)\not\simeq g(z)}{f(v,u)\not\simeq g(z)}\;[u/x,v/y]}{\dfrac{g(c)\not\simeq g(z)}{\square}\;[c/z]}\;[a/v,b/u]$$

First-order clauses

$$\underline{f(x,y)\simeq f(y,x)}$$

$$\underline{f(u,v)\not\simeq g(z)} \;\vee\; u\simeq z$$

$$\underline{f(a,b)\simeq g(c)}$$

$$\underline{a\not\simeq b}$$

First-order instances

$$f(b,a)\simeq f(a,b)$$

$$f(b,a)\not\simeq g(c) \;\vee\; b\simeq c$$

Inst-Gen-Eq by Example: Generating instances

Unit superposition proof: Substitution extraction

$$\dfrac{f(a,b) \simeq g(c) \qquad \dfrac{f(x,y) \simeq f(y,x) \qquad f(u,v) \not\simeq g(z)}{f(v,u) \not\simeq g(z)}\;[u/x, v/y]}{\dfrac{g(c) \not\simeq g(z)}{\square}\;[c/z]}\;[a/v, b/u]$$

First-order clauses

$$\underline{f(x,y) \simeq f(y,x)}$$

$$\underline{f(u,v) \not\simeq g(z)} \;\vee\; u \simeq z$$

$$\underline{f(a,b) \simeq g(c)}$$

$$\underline{a \not\simeq b}$$

First-order instances

$$f(b,a) \simeq f(a,b)$$

$$f(b,a) \not\simeq g(c) \;\vee\; b \simeq c$$

Inst-Gen-Eq by Example: Generating instances

Unit superposition proof: Substitution extraction

$$\dfrac{f(a,b) \simeq g(c) \qquad \dfrac{f(x,y) \simeq f(y,x) \qquad f(u,v) \not\simeq g(z)}{f(v,u) \not\simeq g(z)}\,[u/x, v/y]}{\dfrac{g(c) \not\simeq g(z)}{\square}\,[c/z]}\,[a/v, b/u]$$

First-order clauses

$\underline{f(x,y) \simeq f(y,x)}$

$\underline{f(u,v) \not\simeq g(z)} \ \vee \ u \simeq z$

$\underline{f(a,b) \simeq g(c)}$

$\underline{a \not\simeq b}$

First-order instances

$f(b,a) \simeq f(a,b)$

$f(b,a) \not\simeq g(c) \ \vee \ b \simeq c$

Answer computation and completeness

Unit superposition proof

$$
\dfrac{f(a,b) \simeq g(c) \qquad \dfrac{f(x,y) \simeq f(y,x) \qquad f(u,v) \not\simeq g(z)}{f(v,u) \not\simeq g(z)}\,[u/x, v/y]}{\dfrac{g(c) \not\simeq g(z)}{\square}\,[c/z]}\,[a/v, b/u]
$$

- Instances from all proofs from selected literals required
- Shorter proofs do not subsume longer proofs
- Literal variants may occur in the same proof

Answer computation and completeness

Unit superposition proof

$$\dfrac{\dfrac{f(a,b)\simeq g(c) \qquad \dfrac{f(x,y)\simeq f(y,x) \qquad f(u,v)\not\simeq g(z)}{f(v,u)\not\simeq g(z)}\;[u/x,v/y]}{g(c)\not\simeq g(z)}\;[a/v,b/u]}{\square}\;[c/z]$$

- Instances from all proofs from selected literals required
- Shorter proofs do not subsume longer proofs
- Literal variants may occur in the same proof

Answer computation and completeness

Unit superposition proof

$$
\dfrac{\dfrac{f(a,b) \simeq g(c) \qquad \dfrac{f(x,y) \simeq f(y,x) \qquad f(u,v) \not\simeq g(z)}{f(v,u) \not\simeq g(z)}\;[u/x, v/y]}{g(c) \not\simeq g(z)}\;[a/v, b/u]}{\square}\;[c/z]
$$

- Instances from all proofs from selected literals required
- Shorter proofs do not subsume longer proofs
- Literal variants may occur in the same proof

Labelled Unit Superposition

- Find inconsistent first-order literals
- Compute instantiating substitutions in labels

Superposition

$$\frac{\mathcal{T} : l \simeq r \quad \mathcal{T}' : L[l']}{(\mathcal{T} \sqcap \mathcal{T}')\sigma : L[r]\sigma} \ (\sigma)$$

σ is mgu of l and l'

Variant merging

$$\frac{\mathcal{T} : L \quad \mathcal{T}' : L'}{\mathcal{T} \sqcup \mathcal{T}'\theta : L} \ (\theta)$$

$L = L'\theta$

Equality resolution

$$\frac{\mathcal{T} : (l \not\simeq r)}{\mathcal{T}\sigma : \square} \ (\sigma)$$

σ is mgu of l and r

- Uniform treatment of literal variants
- Preserve proof structure for redundancy elimination

Summary

- iProver-Eq is an instantiation-based automated theorem prover for first-order clause logic

- Labelled unit superposition calculus generates instances

- Modularly integrates any SMT solver as ground solver
- Currently CVC3, any other can be used, Z3 or Yices, e.g.

- Written in OCaml, using C/C++ interface of SMT solvers

- Currently running in this year's CASC