Completeness of Inst-saturated Sets of Clauses with Equality

Alexander Maringele

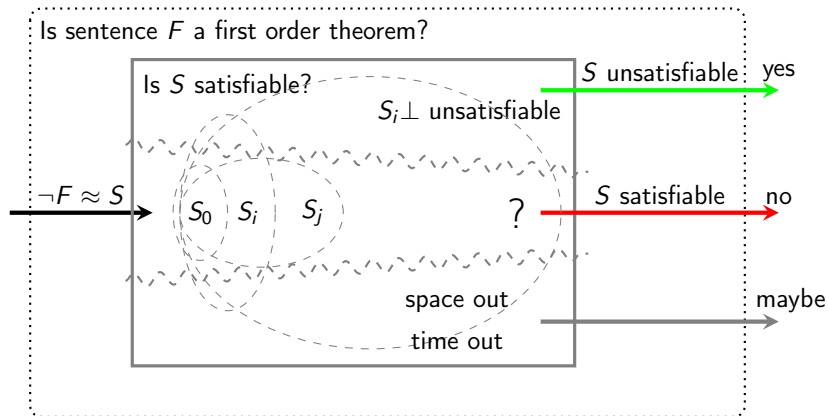alexander.maringele@gmail.com

December 6th, 2017

📄 Harald Ganzinger and Konstantin Korovin.
Integrating Equational Reasoning into Instantiation-Based
Theorem Proving.
In *18th CSL 2004. Proceedings*, volume 3210 of *LNCS*, pages
71–84, 2004.

Instantiation-based first order theorem proving
The big picture

$S_0 = S$, S_{i+1} is inferred from S_i by a sound calculus.

Preliminaries I
Equational First Order Logic

- first order signature with function (and predicate) symbols
- terms s, t, ℓ, r (and predicates $P, Q, \bullet$)
- atoms are equations of terms $s \approx t$ (or predicates $P \approx \bullet$)
- literals are atoms or negated atoms
- clauses are a multisets of literals
- closures are pairs of clauses and ground substitutions

$$(\, f(x) \approx b \vee x \not\approx a \,) \cdot \{ \, x \mapsto f(a) \, \}$$

Preliminaries II
Equational First Order Logic

- orderings

$\succ_{gr}$ order on ground terms, literals, and clauses defined by
a total, well-founded, and monotone extension of
a total simplification ordering $\succ'_{gr}$ on ground terms

$$s \not\approx t \succ_{gr} s \approx t, \ L \vee L \succ_{gr} L \qquad\qquad (P \succ_{gr} \bullet)$$

$\succ_\ell$ an arbitrary total well-founded extension of $\succ_{gr}$ such that

$$L\sigma \succ_{gr} L'\sigma' \Rightarrow L \cdot \sigma \succ_\ell L' \cdot \sigma'$$

$\succ_{cl}$ an arbitrary total well-founded extension of $\succ_{gr}$ such that

$$C\tau \succ_{gr} D\rho \Rightarrow C \cdot \tau \succ_{cl} D \cdot \rho$$
$$(C\tau = D\rho \text{ and } C\theta = D) \Rightarrow C \cdot \tau \succ_{cl} D \cdot \rho$$

Unit Paramodulation

$$\frac{(\ell \approx r) \cdot \sigma \quad L[\ell'] \cdot \sigma'}{L[r]\theta \cdot \rho} \; \theta \qquad\qquad \frac{(s \not\approx t) \cdot \tau}{\Box} \; \mu$$

where

- $\ell\sigma \succ_{gr} r\sigma$, $\theta = \mathsf{mgu}(\ell, \ell')$, $\ell\sigma = \ell'\sigma' = \ell'\theta\rho$, $\ell' \notin \mathcal{V}$
- $s\tau = t\tau$, $\mu = \mathsf{mgu}(s, t)$

Example

The set of literal closures $\{ (f(x) \approx b) \cdot \{x \mapsto a\},\ a \approx b,\ f(b) \not\approx b \}$
is inconsistent, but the empty clause is not derivable if $a \succ_{gr} b$.

Lemma
*If σ, σ' are irreducible by a ground rewrite system R
then ρ is irreducible by R.*

UP-Redundancy

- ▶ We define the set

$$irred_R(\mathcal{L}) = \{\, L \cdot \sigma \in \mathcal{L} \mid \sigma \text{ is irreducible w.r.t. } R \,\}$$

  for a set of literal closures $\mathcal{L}$ and a ground rewrite system R.

- ▶ Let $\mathcal{L}_{L \cdot \sigma \succ_\ell} = \{\, L' \cdot \sigma' \in \mathcal{L} \mid L \cdot \sigma \succ_\ell L' \cdot \sigma' \,\}$.

- ▶ A literal closure $L \cdot \sigma$ is UP-redundant in $\mathcal{L}$ if

$$R \cup irred_R(\mathcal{L}_{L \cdot \sigma \succ_\ell}) \vDash L\sigma$$

  for every ground rewrite system R
  oriented by $\succ_{gr}$ where σ is irreducible w.r.t. R.

- ▶ $\mathcal{R}_{UP}(\mathcal{L})$ denotes the set of all UP-redundant closures in $\mathcal{L}$.

UP-Saturation

The UP-saturation process for $\mathcal{L}$ is a sequence $\{\mathcal{L}_i\}_{i=0}^{\infty}$ where

- $\mathcal{L}_0 = \mathcal{L}$

- $\mathcal{L}_{i+1} = \begin{cases} \mathcal{L}_i \backslash L \cdot \sigma & \text{if} \quad R \cup \mathrm{irred}_R(\mathcal{L}_{i,L \cdot \sigma \succ_\ell}) \vDash L\sigma \\[2ex] \mathcal{L}_i \cup \square & \text{if} \quad \begin{cases} (s \not\approx t) \cdot \tau \in \mathcal{L}_i \\ s\tau = t\tau, \ \mu = \mathrm{mgu}(s,t) \end{cases} \\[3ex] \mathcal{L}_i \cup L[r]\theta \cdot \rho & \text{if} \quad \begin{cases} (\ell \approx r) \cdot \sigma, \ L[\ell'] \cdot \sigma' \in \mathcal{L}_i \\ \ell\sigma \succ_{gr} r\sigma, \ \theta = \mathrm{mgu}(\ell, \ell'), \\ \ell' \notin \mathcal{V}, \ \ell\sigma = \ell'\sigma' = \ell'\theta\rho, \end{cases} \\[3ex] \mathcal{L}_i & \text{otherwise} \end{cases}$

Let $\mathcal{L}^{\infty}$ be the set of persistent closures.

UP-Fairness

The UP-saturation process is UP-fair if for every UP-inference with premises in $\mathcal{L}^\infty$ the conclusion is UP-redundant w.r.t. $\mathcal{L}_j$ for some j. For a set of literals $\mathcal{L}$ we define the saturated set of literal closures $\mathcal{L}^{sat} = \mathcal{L}^\infty \backslash \mathcal{R}_{UP}(\mathcal{L}^\infty)$ for some UP-saturation process $\{\mathcal{L}_i\}_{i=0}^{\infty}$ with $\mathcal{L}_0 = \mathcal{L}$.

Lemma
The set $\mathcal{L}^{sat}$ is unique because for any two UP-fair saturation processes $\{\mathcal{L}_i\}_{i=0}^{\infty}$ and $\{\mathcal{L}_i'\}_{i=0}^{\infty}$ with $\mathcal{L}_0 = \mathcal{L}_0'$ we have

$$\mathcal{L}^\infty \backslash \mathcal{R}_{UP}(\mathcal{L}^\infty) = \mathcal{L}'^\infty \backslash \mathcal{R}_{UP}(\mathcal{L}'^\infty)$$

Lemma (Irreducibility of minimal false literal closure)

If

- $\mathcal{L}$ *is a set of literal closures.* $\square \notin \mathcal{L}^{sat}$
- R *is a (convergent and interreduced)*
  ground rewrite system oriented by $\succ_{gr}$
- $\ell \to r \in R \Rightarrow (\ell' \approx r') \cdot \rho \in \mathcal{L}^{sat}$ *with* $\ell \to r = (\ell' \approx r')\rho$
- I *is an interpretation and every* $L\sigma \in I$ *is irreducible by* R, *and*
- $M \cdot \tau = \min_{\succ_\ell} \{\, L \cdot \sigma \mid L \cdot \sigma \in irred_R(\mathcal{L}^{sat}),\ L\sigma$ *is false in* $I \,\}$

Then $M \cdot \tau$ *is irreducible by* R.

(By definition only τ *is irreducible by* R)

Proof.

1. Assume $M \cdot \tau$ is reducible by $\ell \to r \in R$ and
   $(\ell' \to r') \cdot \rho \in \mathcal{L}^{sat}$. Since τ is irreducible by R:

$$\frac{(\ell' \to r') \cdot \rho \quad M[\ell''] \cdot \tau}{M[r']\theta \cdot \mu} \quad \begin{array}{l} \theta = \mathrm{mgu}(\ell', \ell'') \\ \ell'\rho = \ell''\tau = \ell''\theta\mu \end{array}$$

   and $M \cdot \tau \succ_\ell M[r']\theta \cdot \mu$, μ is irreducible by R

2. 2.1 Assume $M[r']\theta \cdot \mu$ is UP-redundant.

$$R \cup irred_R(M' \cdot \tau' \mid) \models M[r']\theta\mu$$

□

Inst-Redundancy

Let S be a set of clauses.

- A ground closure C is Inst-redundant in S if for some k
  - $C_i' \in S$, $C_i = C_i' \cdot \sigma_i'$, $C \succ_{cl} C_i$ for $i \in 1 \ldots k$
  - such that $C_1, \ldots, C_k \models C$

- A (possible non-ground) clause C is called Inst-redundant in S if each ground closure $C \cdot \sigma$ is Inst-redundant in S.

- $R_{Inst}(S)$ denotes the set of all Inst-redundant clauses in S.

Example
$S = \{\, f(x) \approx x,\ f(a) \approx a,\ f(f(x)) \approx f(x) \,\}$
$R_{Inst}(S) = \{\, f(f(x)) \approx f(x) \,\}$

Selection

Let S be a set of clauses S, let $I_\perp$ be a model of $S\perp$.

▶ A selection function sel maps clauses to literals such that

$$\text{sel}(C) \in C \qquad\qquad I_\perp \models \text{sel}(C)\perp$$

▶ The set of S-relevant literal closures

$$\mathcal{L}_S = \left\{ L \cdot \sigma \mid \begin{array}{l} L \vee C \in S,\, L = \text{sel}(L \vee C) \\ (L \vee C) \cdot \sigma \text{ is not Inst-redundant in S,} \end{array} \right\}$$

▶ $\mathcal{L}_S^{sat}$ denotes the satuarion process of $\mathcal{L}_S$.

▶ A set of clauses S is Inst-saturated w.r.t. a selection function, if $\mathcal{L}_S^{sat}$ does not contain the empty clause.

Completeness

Theorem
If a set of clauses S is Inst-saturated, and $S\perp$ is satisfiable, then S is also satisfiable.

Proof.

1. Construct candidate model
2. Assumed counterexample fails

Conclude candidate is model   □

Model Construction I

Let S be an Inst-saturated set of clauses.

- $S\perp$ is satisfiable
- $\square \notin \mathcal{L}_S^{sat}$

Let $L = L' \cdot \sigma \in \mathcal{L}_S^{sat}$. We define by induction on $\succ_\ell$

- $I_L = \bigcup_{L \succ_\ell M} \epsilon_M$ ϵ_M allready defined for all M with $L \succ_\ell M$
- $R_L = \{s \to t \mid s \approx t \in I_L, s \succ_{gr} t\}$
- $\epsilon_L = \begin{cases} \quad \emptyset & \text{if } L'\sigma \text{ reducible by } R_L \\ \quad \emptyset & \text{if } I_L \vDash L'\sigma \text{ or } I_L \vDash \overline{L'}\sigma \text{ (defined)} \\ \{L'\sigma\} & \text{if } L'\sigma \text{ is productive (irreducible, undefined)} \end{cases}$

Model Construction II

- $R_S = \bigcup_{L \in \mathcal{L}_S^{\text{sat}}} R_L$ $\qquad$ R_S is convergent and interreduced

- $I_S = \bigcup_{L \in \mathcal{L}_S^{\text{sat}}} \epsilon_L$ $\qquad\qquad\qquad$ I_S is consistent,
$\qquad\qquad\qquad\qquad\qquad\qquad$ $L\sigma \in L_S$ is irreducible by R_S

- Let $\mathcal{I}$ be an arbitrary total consistent extension of I_S.

Lemma
$\mathcal{I}$ is a model for all ground instances of clauses in S.

Counterexample I

Assume $\mathcal{I}$ is not a model of S.

$$\text{Let } D = \min_{\succ_{cl}} \{ \, C' \cdot \sigma \mid C' \in S, \ C'\sigma \text{ false in } \mathcal{I} \, \}$$

Then

▶ $D = D' \cdot \sigma$ is not Inst-redundant.

Otherwise there are $D_1, \ldots, D_n \models D$, $D \succ_{cl} D_i$ for all i, and D_j false in $\mathcal{I}$ for one j, which contradicts minimality.

▶ $x\sigma$ irreducible by R_S for every variable x in D'.

Otherwise let $(\ell \to r)\tau \in R_L$ and $x\sigma = x\sigma[l\tau]_p$ for some variable x in D'. We define substitution σ' with $x\sigma' = x\sigma[r\tau]_p$ and $y\sigma' = y\sigma$ for $y \neq x$. $D'\sigma'$ is false in $\mathcal{I}$ and $D \succ_{cl} D' \cdot \sigma'$, which contradicts minimality.

Counterexample II

Since D is not Inst-redundant in S, we have for some literal L, that $D' = L \vee D''$, $\text{sel}(D') = L$, $L \cdot \sigma \in \mathcal{L}_S$, $L\sigma$ is false in $\mathcal{I}$

Assume $L \cdot \sigma$ is UP-redundant in $\mathcal{L}_S^{sat}$.

By construction σ is irreducible by R_S. Then we have

$$R_S \cup irred_{R_S}(\{L' \cdot \sigma' \in \mathcal{L}_S^{sat} \mid L \cdot \sigma \succ_\ell L' \cdot \sigma'\}) \models L\sigma$$

Therefore there is $L' \cdot \sigma' \in irred_{R_S}(\mathcal{L}_S^{sat})$ that is false in $\mathcal{I}$.

We choose the minimal of those.

Counterexample III

We define

$$M \cdot \tau = \min_{\succ_\ell} \big\{ \, L' \cdot \tau' \mid L' \cdot \sigma' \in irred_{R_S}(\mathcal{L}_S^{sat}), \, \mathcal{I} \not\models M'\tau' \, \big\}$$

Assume $M \cdot \tau$ is reducible by $(\ell \to r) \in R_S$
and $(\ell \to r)$ is produced by $(\ell' \approx r') \cdot \rho \in \mathcal{L}_S^{sat}$

UP-inference is applicable because τ is irreducible by R_S

$$\frac{(\ell' \approx r') \cdot \rho \quad M[\ell''] \cdot \tau}{M[r']\theta \cdot \mu} \; UP$$

$M[r']\theta\mu$ is false in $\mathcal{I}$.

Counterexample IV

- If $M[r']\theta \cdot \mu$ is not UP-redundant in $\mathcal{L}_S^{sat}$ then $M[r']\theta \cdot \mu \in \mathcal{L}_S^{sat}$.

  $M \cdot \tau \succ_\ell M[r']\theta \cdot \mu \in irred_{R_S}(\mathcal{L}_S^{sat})$ (μ is irreducible by R_S)
  contradicts minimality of $M \cdot \tau$.

- If $M[r']\theta \cdot \mu$ is UP-redundant in $\mathcal{L}_S^{sat}$ then

  $$R_S \cup irred_{R_S}(\{M' \cdot \tau' \in \mathcal{L}_S^{sat} \mid M[r']\theta \cdot \mu \succ_\ell M'\tau'\}) \models M[r']\theta\mu$$

  Hence there is $M' \cdot \tau' \in \mathcal{L}_S^{sat}$ false in $\mathcal{I}$ such that
  $M \cdot \tau \succ_\ell M[r']\theta \cdot \mu \succ_\ell M' \cdot \tau'$,
  $M' \cdot \tau'$ contradicts minimality of $M \cdot \tau$.

Hence $M \cdot \tau$ is irreducible by R_S.

Counterexample V

Under the assumption that $\mathcal{I}$ is not a model
a minimal ground literal $M \cdot \tau$ exists that is

- false in $\mathcal{I}$
- in $\mathcal{L}_S^{sat}$
- irreducible by R_S
- not productive.

Hence $I_{M \cdot \tau} \models \overline{M} \tau$ with two possible cases:

1. $M \cdot \tau$ is equation $(s \approx t) \cdot \tau$ $\qquad\qquad$ $I_{M \cdot \tau} \models (s \not\approx t)\tau$
2. $M \cdot \tau$ is inequation $(s \not\approx t) \cdot \tau$ $\qquad\qquad$ $I_{M \cdot \tau} \models (s \approx t)\tau$

Both cases lead to a contradiction (next slide).
We reject the assumption and conclude
that $\mathcal{I}$ is a model for all ground instances of S.

Counterexample VI

1. Assume $M \cdot \tau$ is equation $(s \approx t) \cdot \tau$:
   - $I_{M \cdot \tau} \models (s \not\approx t)\tau$
   - All literals in $I_{M \cdot \tau}$ are irreducible by $R_{M \cdot \tau}$
   - $s\tau$ and $t\tau$ are irreducible by $R_{M \cdot \tau}$
   - $R_{M \cdot \tau}$ is a convergent term rewrite system

   Hence $(s \not\approx t)\tau \in I_{M \cdot \tau}$ and produced to $I_{M \cdot \tau}$ by a $(s' \not\approx t') \cdot \tau'$.
   Then $(s' \not\approx t')\tau' \succ_{gr} (s \approx t)\tau$ and $(s' \not\approx t') \cdot \tau' \succ_{\ell} M \cdot \tau$
   Contradiction to minimality of $M \cdot \tau$ w.r.t. $\succ_{\ell}$.

2. Assume $M \cdot \tau$ is inequation $(s \not\approx t) \cdot \tau$. We have
   - $I_{M \cdot \tau} \models (s \approx t)\tau$
   - $s\tau$ and $t\tau$ are irreducible by $R_{M \cdot \tau}$

   Hence $s\tau = t\tau$ and equality resolution is applicable.
   Contradiction to $\square \notin \mathcal{L}_S^{sat}$.

- UP for literal closures

$$\frac{(\ell \approx r) \cdot \sigma \quad L[\ell'] \cdot \sigma'}{L[r]\theta \cdot \rho} \; \theta \qquad\qquad \frac{(s \not\approx t) \cdot \tau}{\Box} \; \mu$$

  - $\ell\sigma \succ_{gr} r\sigma$, $\theta = \mathrm{mgu}(\ell, \ell')$, $\ell\sigma = \ell'\sigma' = \ell'\theta\rho$, $\ell' \notin \mathcal{V}$
  - $s\tau = t\tau$, $\mu = \mathrm{mgu}(s, t)$

- UPL for literals (clauses)

$$\frac{\ell \approx r \quad L[\ell']}{L[r]\theta} \; \theta \qquad\qquad \frac{s \not\approx t}{\Box} \; \mu$$

  - $\ell\sigma \succ_{gr} r\sigma$ for some grounding substitution σ,
    $\theta = \mathrm{mgu}(\ell, \ell')$, $\ell' \notin \mathcal{V}$
  - $\mu = \mathrm{mgu}(s, t)$

Summary