Completeness of Inst-saturated Sets of Clauses with Equality

Alexander Maringele

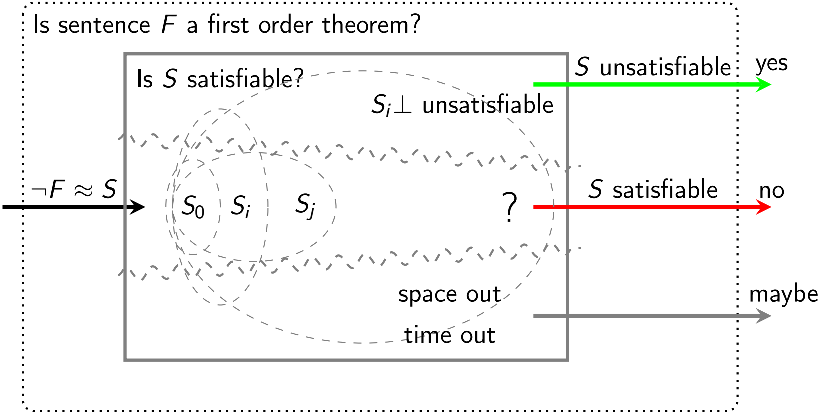
alexander.maringele@gmail.com

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

- a clause C is a multiset of literals
- literals are (in)equations of first order terms
- a closure $C \cdot \sigma$ is a pair of clause C and substitution σ

Preliminaries II

- 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

$\succ_{\ell}$ 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

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

Remark

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

We define for a set of literal closures $\mathcal{L}$
and an arbitrary ground rewrite system R

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

A literal closure $L \cdot \sigma$ is UP-redundant in $\mathcal{L}$ if for every ground rewrite system R oriented by $\succ_{gr}$ where σ is irreducible w.r.t. R

$$R \cup \mathit{irred}_R(\mathcal{L}_{L \cdot \sigma \succ_\ell}) \models L\sigma$$

with $\mathcal{L}_{L \cdot \sigma \succ_\ell} = \{\, L' \cdot \sigma' \in \mathcal{L} \mid L \cdot \sigma \succ_\ell L' \cdot \sigma' \,\}$

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

Saturation I

A UP-saturation process is
a sequence $\{\mathcal{L}_i\}_{i=0}^{\infty}$ of sets of literal closures
where $\mathcal{L}_{i+1}$ is obtained from $\mathcal{L}_i$
by adding a conclusion of an UP-inference with premises in $\mathcal{L}_i$
or by removing a UP-redundant closure w.r.t. $\mathcal{L}_i$.

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

Saturation II

Definition

Let $\mathcal{L}^\infty$ be the set of persistent closures, i.e. the lower limit of the sequence. The 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

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

Let S be a set of clauses.
A (possible non-ground) clause C is called Inst-redundant in S if each ground closure $C \cdot \sigma$ is Inst-redundant in S, i.e. there are ground closures $C_1 \cdot \sigma_1, \ldots, C_k \cdot \sigma_k$ of clauses in S such that

$$C_1 \cdot \sigma_1, \ldots, C_k \cdot \sigma_k \models C' \cdot \sigma'$$

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

Consider a set of clauses S, let $I_\bot$ be a model of $S\bot$.
A selection funciton sel maps clauses to literals such that

$$\mathrm{sel}(C) \in C$$
$$I_\bot \models \mathrm{sel}(C)\bot$$

The set of S-relevant instances of literals

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

$\mathcal{L}_S^{sat}$ 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.

Theorem

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

Proof.

1. model candidate construction
2. proof by contradiction of counterexample

$\square$

Assume $S\bot$ is satisfiable and $\Box \notin \mathcal{L}_S^{sat}$.
We define by induction on $\succ_\ell$. Assume $L = L' \cdot \sigma \in \mathcal{L}_S^{sat}$

$$I_L = \bigcup_{L \succ_\ell M} \epsilon_M \qquad \epsilon_M \text{ allready defined for all } M \text{ with } L \succ_\ell M$$

$$R_L = \{s \to t \mid s \approx t \in I_L, s \succ_{gr} t\}$$

$$\epsilon_L = \begin{cases} \emptyset & \text{if } L'\sigma \text{ reducible by } R_L \\ \emptyset & \text{if } I_L \vDash L'\sigma \text{ or } I_L \vDash \overline{L'}\sigma \text{ (i.e. } L'\sigma \text{ is defined)} \\ \{L'\sigma\} & \text{if } L'\sigma \text{ is productive (i.e. irreducible and undefined)} \end{cases}$$

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

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

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

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

$$\text{Let } D = \min_{\succ_{cl}}\{\, C' \cdot \sigma \mid C' \in S, \mathcal{I} \not\models C'\sigma \,\}$$

Then

- $D = D' \cdot \sigma$ is not Inst-redundant. Otherwise $D_1, \ldots, D_n \models D$, $D \succ_{cl} D_i$ for all i, and $\mathcal{I} \not\models D_j$ for one j 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 $y \neq x$. $\mathcal{I} \not\models D'\sigma'$ and $D \succ_{cl} D' \cdot \sigma'$ contradicts minimality.

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

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

is irreducible by R_S.

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

Assume $M \cdot \tau$ is reducible by $(\ell \to r) \in R_S$

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

τ is irreducible by R_S, hence UP-inference is applicable:

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

$$\ell'\rho = \ell''\tau = \ell''\theta\mu,\ \theta = \mathrm{mgu}(\ell', \ell''),\ \mathcal{I} \not\models M[r']\theta\mu$$

- If $M[r']\theta \cdot \mu$ is not UP-redundant in $\mathcal{L}_S^{sat}$ then $M[r']\theta \cdot \mu \in \mathcal{L}_S^{sat}$. $M[r']\theta \cdot \mu \in irred_{R_S}(\mathcal{L}_S^{sat})$ because μ is irreducible.
- If $M[r']\theta \cdot \mu$ is UP-redundant in $\mathcal{L}_S^{sat}$.
  From definiton:

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

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

Final Step I

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

We have that $M \cdot \tau$

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

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

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

Final Step II

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

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 $(s' \not\approx t') \cdot \tau'$.
   Contradicts the minimality of $M \cdot \tau$.

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

   Hence $s\tau = t\tau$ and equality resolution is applicable.
   Contradicts that the empty clause is not in $\mathcal{L}_S^{sat}$.