Completeness of Inst-saturated Sets of Clauses with Equality

Alexander Maringele

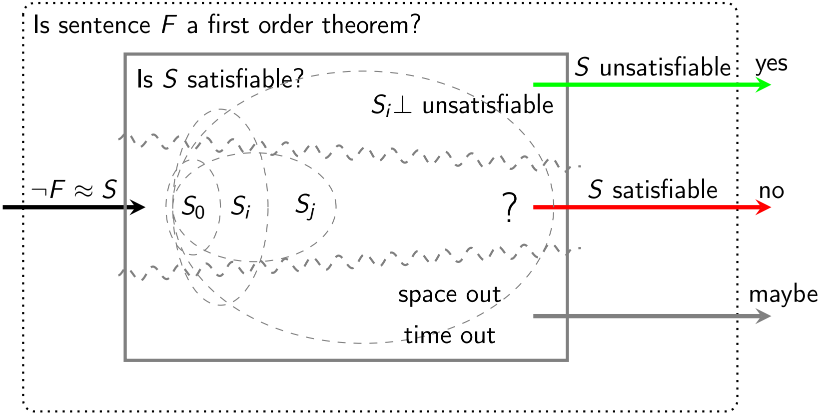
alexander.maringele@gmail.com

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

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

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

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

$\succ_{\ell}$ 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

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

where

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

Example 1

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

Lemma 2

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

- $\mathcal{L}_0 = \mathcal{L}$
- $$\mathcal{L}_{i+1} = \begin{cases} \mathcal{L}_i \setminus L \cdot \sigma & \text{if} \quad R \cup \mathsf{irred}_R(\mathcal{L}_{i, L\cdot\sigma \succ_\ell}) \models L\sigma \\ \mathcal{L}_i \cup \square & \text{if} \quad \begin{cases} (s \not\approx t) \cdot \tau \in \mathcal{L}_i \\ s\tau = t\tau,\ \mu = \mathsf{mgu}(s,t) \end{cases} \\ \mathcal{L}_i \cup L[r]\theta \cdot \rho & \text{if} \quad \begin{cases} (\ell \approx r) \cdot \sigma,\ L[\ell'] \cdot \sigma' \in \mathcal{L}_i \\ \ell\sigma \succ_{gr} r\sigma,\ \theta = \mathsf{mgu}(\ell, \ell'), \\ \ell' \notin \mathcal{V},\ \ell\sigma = \ell'\sigma' = \ell'\theta\rho, \end{cases} \\ \mathcal{L}_i & \text{otherwise} \end{cases}$$

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

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 3

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

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

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 $i \in 1 \dots k$
  - such that $C_1, \dots, C_k \models C$
- 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 4

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

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

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

- The set of S-relevant literal closures

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

- $\mathcal{L}_S^{sat}$ 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 5

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

Proof.

1. Construction of a candidate model
2. Proof that candidate is a model by contradiction

$\square$

Construction

Let S be an Inst-saturated set of clauses, i.e. $\Box \notin \mathcal{L}_S^{sat}$, SAT($S\bot$).

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

- $I_L = \{\, \epsilon_M \mid L \succ_\ell M \,\}$ I.H.: ϵ_M is defined for any $M \mid L \succ_\ell M$
- $R_L = \{s \to t \mid s \approx t \in I_L, s \succ_{gr} t\}$
- $\epsilon_L = \begin{cases} \emptyset & \text{if } L'\sigma \text{ reducible by } R_L \\ \emptyset & \text{if } I_L \models L'\sigma \text{ or } I_L \models \overline{L'}\sigma & \text{(defined)} \\ \{L'\sigma\} & \text{otherwise} & \text{(productive)} \end{cases}$
- $R_S = \bigcup_{L \in \mathcal{L}_S^{sat}} R_L$ R_S is convergent and interreduced
- $I_S = \bigcup_{L \in \mathcal{L}_S^{sat}} \epsilon_L$ I_S is consistent, $L\sigma \in I_S$ is irreducible by R_S

For the following slides let $\mathcal{L}_S, \mathcal{L}_S^{sat}, I_S, R_S$ be defined as above and let $\mathcal{I}$ be an arbitrary consistent extension of I_S.

Lemma 6

If any $L \cdot \sigma \in \mathcal{L}_S$ *exists with* $\mathcal{I} \not\models L\sigma$ *then there is a* $L' \cdot \sigma' \in \mathit{irred}_{R_S}(\mathcal{L}_S^{sat})$ *with* $\mathcal{I} \not\models L'\sigma'$.

Proof.

We have two cases

- If $L \cdot \sigma$ is not UP-redundant in $\mathcal{L}_S^{sat}$, then $L' \cdot \sigma' = L \cdot \sigma$. ✓
- If $L \cdot \sigma$ is UP-redundant in $\mathcal{L}_S^{sat}$. By construction σ is irreducible by R_S. Then we have

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

  At least one $L' \cdot \sigma' \in \mathit{irred}_{R_S}(\mathcal{L}_S^{sat})$ with $\mathcal{I} \not\models L'\sigma'$. ✓

□

Lemma 7

Whenever

$$M \cdot \tau = \min_{\succ_\ell} \{\, L' \cdot \tau' \mid L' \cdot \sigma' \in \mathit{irred}_{R_S}(\mathcal{L}_S^{sat}),\ L'\sigma' \ \mathit{false\ in}\ \mathcal{I} \,\}$$

is defined, then $M \cdot \tau$ is irreducible by R_S.

Proof

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

Now UP-inference is applicable because τ is irreducible by R_S,

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

μ is irreducible by R_S, and $M[r']\theta\mu$ is false in $\mathcal{I}$. $\lightning$

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

  Now $M \cdot \tau \succ_\ell M[r']\theta \cdot \mu \in \mathit{irred}_{R_S}(\mathcal{L}_S^{sat})$
  contradicts minimality of $M \cdot \tau$. $\lightning$

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

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

  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 $M \cdot \tau$. $\lightning$

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

Lemma 8

Let $M \cdot \tau \in \mathcal{L}_S^{sat}$*, irreducible by* R_S*, and defined (not productive). From* $\mathcal{I} \not\models M\tau$ *follows that* M *is not an equation* $(s \approx t)$*.*

Proof.

Assume $M = (s \approx t)$*. Then we have*

- $I_{M \cdot \tau} \models (s \not\approx t)\tau$
- *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 there is $(s \not\approx t)\tau \in I_{M \cdot \tau}$ *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* $(s' \not\approx t') \cdot \tau' \succ_{\ell} M \cdot \tau$ □

Lemma 9

Let $M \cdot \tau \in \mathcal{L}_S^{sat}$, irreducible by R_S, and defined (not productive). From $\mathcal{I} \not\models M\tau$ follows that M is not an inequation $(s \not\approx t)$.

Proof.

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

Lemma 10

$\mathcal{I}$ is a model for all ground instances of S

Proof.

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

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 $\mathcal{I}$

Hence the following literal closure

$$M \cdot \tau = \min_{\succ_\ell} \{ \, L' \cdot \tau' \mid L' \cdot \sigma' \in \mathit{irred}_{R_S}(\mathcal{L}_S^{sat}), \; L' \cdot \sigma' \text{ false in } \mathcal{I} \, \}$$

exists by Lemma 6, is irreducible by Lemma 7, and not productive.

- M is not an equation by lemma 8
- M is not an inequation by lemma 9

This is a contradiction.
Our assumption is false, $\mathcal{I}$ is a model for all instances of S, and S is satisfiable. $\square$