Rewrite-based satisfiability procedures

Maria Paola Bonacina

Dipartimento di Informatica
Università degli Studi di Verona
Verona, Italy, EU

Talk given at Microsoft Research, Redmond, Washington, USA

21 May 2008

$\mathcal{T}$-satisfiability procedure

The inference system $\mathcal{SP}$

- Ordering
- Expansion rules
- Contraction rules

Theories: some presentations and termination results

- Records
- Integer offsets modulo
- Arrays
- Lists
- Integer offsets

$\mathcal{T}$-satisfiability procedure

$\mathcal{T}$-**satisfiability procedure**: decide satisfiability of a *conjunction of ground literals* in theory $\mathcal{T}$

S: *set of ground literals* in the signature of $\mathcal{T}$

$\mathcal{T}$: *presentation* of a theory

$Th(\mathcal{T})$: the set of theorems of $\mathcal{T}$

$\bowtie$ is either $\simeq$ or $\not\simeq$

A "good" CSO

- Simplification ordering
  - *Stable*: if $l \succ r$ then $l\sigma \succ r\sigma$ for all substitutions σ
  - *Monotonic*: if $l \succ r$ then $t[l] \succ t[r]$ for all contexts t
  - With the *subterm property*: if r is strict subterm of l ($l \rhd r$) then $l \succ r$

  These properties imply *well-founded*
- *Complete*: *total* on ground terms

"Good": $t \succ c$ for all ground compound terms t and constants c and possibly some simple additional condition for some theories

Superposition

$$\frac{C \vee l[u'] \simeq r \quad D \vee u \simeq t}{(C \vee D \vee l[t] \simeq r)\sigma}$$

σ *is mgu of* u *and* u'
u' *is not a variable*
$u\sigma \not\preceq t\sigma$
$l[u']\sigma \not\preceq r\sigma$
$\forall L \in D : (u \simeq t)\sigma \not\preceq L\sigma$
$\forall L \in C : (l[u'] \simeq r)\sigma \not\preceq L\sigma$

Paramodulation

$$\frac{C \vee l[u'] \not\simeq r \quad D \vee u \simeq t}{(C \vee D \vee l[t] \not\simeq r)\sigma}$$

$$\begin{array}{c} \sigma \text{ is mgu of } u \text{ and } u' \\ u' \text{ is not a variable} \\ u\sigma \not\preceq t\sigma \\ l[u']\sigma \not\preceq r\sigma \\ \forall L \in D : (u \simeq t)\sigma \not\preceq L\sigma \\ \forall L \in C : (l[u'] \not\simeq r)\sigma \not\preceq L\sigma \end{array}$$

Reflection

Ordered resolution with $x \simeq x$:

$$\frac{C \vee u' \not\simeq u}{C\sigma}$$

σ *is mgu of* u *and* u'
$\forall L \in C : (u' \not\simeq u)\sigma \not\prec L\sigma$

Equational Factoring

A generalization of ordered factoring:

$$\frac{C \vee u \simeq t \vee u' \simeq t'}{(C \vee t \not\simeq t' \vee u \simeq t')\sigma}$$

$$\begin{array}{c} \sigma \text{ is mgu of } u \text{ and } u' \\ u\sigma \not\preceq t\sigma \\ \forall L \in \{u' \simeq t'\} \cup C : (u \simeq t)\sigma \not\prec L\sigma \end{array}$$

Subsumption

$$\frac{C \quad D}{C} \quad D \gtrdot C$$

$D \gtrdot C$ if $D \trianglerighteq C$ and $C \not\trianglerighteq D$
$D \trianglerighteq C$ if $C\sigma \subseteq D$ (as multisets) for some substitution σ

In practice, theorem provers apply also *subsumption of variants*: if $D \trianglerighteq C$ and $C \trianglerighteq D$, the oldest clause is retained.

Simplification

$$\frac{C[u] \qquad l \simeq r}{\overline{C[r\sigma], \quad l \simeq r}}$$

$$u = l\sigma$$
$$l\sigma \succ r\sigma$$
$$C[u] \succ (l \simeq r)\sigma$$

Deletion

$$\frac{C \vee t \simeq t}{\qquad}$$

Derivation and limit

$\mathcal{SP}_{\succ}$: $\mathcal{SP}$ with CSO $\succ$

Derivation:

$$S_0 \underset{\mathcal{SP}_{\succ}}{\vdash} S_1 \underset{\mathcal{SP}_{\succ}}{\vdash} \ldots S_i \underset{\mathcal{SP}_{\succ}}{\vdash} \ldots$$

Limit: set of *persistent clauses*

$$S_\infty = \bigcup_{j \geq 0} \bigcap_{i \geq j} S_i$$

Flat terms and literals

Terms:
$depth(t) = 0$, if t is constant or variable
$depth(t) = 1 + max\{depth(t_i) : 1 \leq i \leq n\}$, if t is $f(t_1, \ldots, t_n)$
Term: *flat* if depth is 0 or 1

Literals:
$depth(l \bowtie r) = depth(l) + depth(r)$
Positive literal: *flat* if depth is 0 or 1
Negative literal: *flat* if depth is 0

Flattening

S: given set of ground literals

S': flattened version of S

$\mathcal{T} \cup S \equiv_{\mathrm{s}} \mathcal{T} \cup S'$
where $\equiv_{\mathrm{s}}$ means equisatisfiable

Records

Assume n fields denoted $1 \leq i \leq n$:

$$\begin{array}{lcl}
\forall x, v. & \mathrm{rselect}_i(\mathrm{rstore}_i(x, v)) \simeq v & 1 \leq i \leq n \\
\forall x, v. & \mathrm{rselect}_j(\mathrm{rstore}_i(x, v)) \simeq \mathrm{rselect}_j(x) & 1 \leq i \neq j \leq n \\
\forall x, y. & \bigwedge_{i=1}^{n} \mathrm{rselect}_i(x) \simeq \mathrm{rselect}_i(y) \supset x \simeq y &
\end{array}$$

First two axioms: $\mathcal{R}$
With third axiom (*extensionality*): $\mathcal{R}^e$

Reduction of $\mathcal{R}^e$ to $\mathcal{R}$

Eliminate disequalities between records by resolution with $\bigvee_{i=1}^{n} \mathrm{rselect}_i(x) \not\simeq \mathrm{rselect}_i(y) \vee x \simeq y$.

Let $S = S' \uplus S_N$, where S_N contains all the literals $l \not\simeq r$, for l and r records.

For all $L = l \not\simeq r \in S_N$ let $C_L = \bigvee_{i=1}^{n} \mathrm{rselect}_i(l) \not\simeq \mathrm{rselect}_i(r)$.

Then $\mathcal{R}^e \cup S \equiv_{\mathrm{s}} \mathcal{R} \cup S' \cup \{C_L : L \in S_N\}$.

Reduction to DNF: exponential procedure (polynomial: next time).

Rewrite-based $\mathcal{R}$-satisfiability procedure

Theorem: A fair $\mathcal{SP}_{\succ}$-strategy is guaranteed to terminate when applied to $\mathcal{R} \cup S$, where S is a set of ground flat $\mathcal{R}$-literals, and therefore it is an $\mathcal{R}$-satisfiability procedure.

Case analysis of clauses in S_∞ from $S_0 = \mathcal{R} \cup S$

(i) the empty clause

(ii) the clauses in $\mathcal{R}$:

(ii.a) $\mathrm{rselect}_i(\mathrm{rstore}_i(x, v)) \simeq v,\ 1 \leq i \leq n$
(ii.b) $\mathrm{rselect}_j(\mathrm{rstore}_i(x, v)) \simeq \mathrm{rselect}_j(x),\ 1 \leq i \neq j \leq n$

(iii) ground flat unit clauses:

(iii.a) $r \simeq r'$
(iii.b) $e \simeq e'$
(iii.c) $e \not\simeq e'$
(iii.d) $\mathrm{rstore}_i(r, e) \simeq r'$, for some i, $1 \leq i \leq n$
(iii.e) $\mathrm{rselect}_i(r) \simeq e$, for some i, $1 \leq i \leq n$

(iv) $\mathrm{rselect}_i(r) \simeq \mathrm{rselect}_i(r')$, for some i, $1 \leq i \leq n$

where: constants r's: records; constants e's: elements of appropriate sort.

Integer offsets modulo

Presentation $\mathcal{I}_k$, $k \geq 1$:

$$\begin{array}{ll} \forall x. & \mathsf{s}(\mathsf{p}(x)) \simeq x \\ \forall x. & \mathsf{p}(\mathsf{s}(x)) \simeq x \\ \forall x. & \mathsf{s}^i(x) \not\simeq x \quad \text{for } 1 \leq i \leq k-1 \\ \forall x. & \mathsf{s}^k(x) \simeq x \end{array}$$

s: successor p: predecessor

Finitely many *acyclicity axioms*

Additional (dual) axioms

Presentation $\mathcal{I}'_k$, $k \geq 1$:

$$
\begin{array}{lll}
\forall x. & \mathsf{s}(\mathsf{p}(x)) \simeq x & \\
\forall x. & \mathsf{p}(\mathsf{s}(x)) \simeq x & \\
\forall x. & \mathsf{s}^i(x) \not\simeq x & \text{for } 1 \leq i \leq k-1 \\
\forall x. & \mathsf{s}^k(x) \simeq x & \\
\forall x. & \mathsf{p}^i(x) \not\simeq x & \text{for } 1 \leq i \leq k-1 \\
\forall x. & \mathsf{p}^k(x) \simeq x &
\end{array}
$$

Rewrite-based $\mathcal{I}_k'$-satisfiability procedure

Theorem: A fair $\mathcal{SP}_{\succ}$-strategy is guaranteed to terminate when applied to $\mathcal{I}_k' \cup S$, where S is a set of ground flat $\mathcal{I}_k'$-literals, and therefore it is an $\mathcal{I}_k'$-satisfiability procedure.

Proof sketch: the only persistent clauses, that can be generated by $\mathcal{SP}_{\succ}$ from $\mathcal{I}_k' \cup S$, are unit clauses $l \bowtie r$, such that l and r are terms in the form $\mathrm{s}^j(u)$ or $\mathrm{p}^j(u)$, where $0 \leq j \leq k-1$ and u is either a constant or a variable.

Arrays

$$
\begin{array}{rc}
\forall x, z, v. & \mathrm{select}(\mathrm{store}(x, z, v), z) \simeq v \\
\forall x, z, w, v. & z \not\simeq w \supset \mathrm{select}(\mathrm{store}(x, z, v), w) \simeq \mathrm{select}(x, w) \\
\forall x, y. & \forall z.\, \mathrm{select}(x, z) \simeq \mathrm{select}(y, z) \supset x \simeq y
\end{array}
$$

First two axioms: $\mathcal{A}$
With third axiom (*extensionality*): $\mathcal{A}^e$

Reduction of $\mathcal{A}^e$ to $\mathcal{A}$

Eliminate disequalities between arrays by resolution with $\mathrm{select}(x, sk(x, y)) \not\simeq \mathrm{select}(y, sk(x, y)) \vee x \simeq y$.

Let $S = S' \uplus S_N$, where S_N contains all the literals $l \not\simeq r$, for l and r arrays.

For all $L = l \not\simeq r \in S_N$ let $L' = \mathrm{select}(l, sk(l, r)) \not\simeq \mathrm{select}(r, sk(l, r))$. It is safe to replace $sk(l, r)$ with $sk_{l,r}$.

$\mathcal{A}^e \cup S \equiv_{\mathrm{s}} \mathcal{A} \cup S' \cup \{L' :\ L \in S_N\}$.

Rewrite-based $\mathcal{A}$-satisfiability procedure

$\mathcal{A}$-good $\succ$: add
$a \succ e \succ j$ for all array constants a, element constants e and index constants j.

Theorem: A fair $\mathcal{SP}_{\succ}$-strategy is guaranteed to terminate when applied to $\mathcal{A} \cup S$, where S is a set of ground flat $\mathcal{A}$-literals, and therefore it is an $\mathcal{A}$-satisfiability procedure.

Case analysis of clauses in S_∞ from $S_0 = \mathcal{A} \cup S$

(i) the empty clause

(ii) the clauses in $\mathcal{A}$

(iii) ground flat unit clauses:

- (iii.a) $a \simeq a'$
- (iii.b) $c_1 \simeq c_2$
- (iii.c) $c_1 \not\simeq c_2$
- (iii.d) $\mathrm{store}(a, i, e) \simeq a'$
- (iii.e) $\mathrm{select}(a, i) \simeq e$ and

(iv) non-unit clauses:

- (iv.a) $\mathrm{select}(a, x) \simeq \mathrm{select}(a', x) \vee x \simeq i_1 \vee \ldots \vee x \simeq i_n \vee j_1 \bowtie j'_1 \vee \ldots \vee j_m \bowtie j'_m$
- (iv.b) $\mathrm{select}(a, i) \simeq e \vee i_1 \bowtie i'_1 \vee \ldots \vee i_n \bowtie i'_n$
- (iv.c) $e \simeq e' \vee i_1 \bowtie i'_1 \vee \ldots \vee i_n \bowtie i'_n$
- (iv.d) $e \not\simeq e' \vee i_1 \bowtie i'_1 \vee \ldots \vee i_n \bowtie i'_n$
- (iv.e) $i_1 \simeq i'_1 \vee i_2 \bowtie i'_2 \vee \ldots \vee i_n \bowtie i'_n$
- (iv.f) $i_1 \not\simeq i'_1 \vee i_2 \bowtie i'_2 \vee \ldots \vee i_n \bowtie i'_n$
- (iv.g) $t \simeq a' \vee i_1 \bowtie i'_1 \vee \ldots \vee i_n \bowtie i'_n$ where t is either a or $\mathrm{store}(a, i, e)$

where: constants a's: arrays, i's and j's: indices, e's: elements, and c's: either indices or elements.

Lists

Presentation $\mathcal{L}_{Sh}$:

$$\forall x, y.\ \mathsf{car}(\mathsf{cons}(x, y)) \simeq x$$
$$\forall x, y.\ \mathsf{cdr}(\mathsf{cons}(x, y)) \simeq y$$
$$\forall y.\ \mathsf{cons}(\mathsf{car}(y), \mathsf{cdr}(y)) \simeq y$$

Presentation $\mathcal{L}_{NO}$: replace the third axiom above by

$$\forall y.\ \neg\,\mathsf{atom}(y) \supset \mathsf{cons}(\mathsf{car}(y), \mathsf{cdr}(y)) \simeq y$$
$$\forall x, y.\ \neg\,\mathsf{atom}(\mathsf{cons}(x, y))$$

Possibly empty lists

Presentation $\mathcal{L}$:

$$\begin{aligned}
\forall x, y.\ \ \mathrm{car}(\mathrm{cons}(x, y)) &\simeq x \\
\forall x, y.\ \ \mathrm{cdr}(\mathrm{cons}(x, y)) &\simeq y \\
\forall y.\ \ y \not\simeq \mathrm{nil} \supset \mathrm{cons}(\mathrm{car}(y), \mathrm{cdr}(y)) &\simeq y \\
\forall x, y.\ \ \mathrm{cons}(x, y) &\not\simeq \mathrm{nil} \\
\mathrm{car}(\mathrm{nil}) &\simeq \mathrm{nil} \\
\mathrm{cdr}(\mathrm{nil}) &\simeq \mathrm{nil}
\end{aligned}$$

Rewrite-based $\mathcal{L}$-satisfiability procedure

$\mathcal{L}$-good $\succ$:add
$t \succ$ nil for all terms t whose root symbol is cons.

Theorem: A fair $\mathcal{SP}_{\succ}$-strategy is guaranteed to terminate when applied to $\mathcal{L} \cup S$, where S is a set of ground flat $\mathcal{L}$-literals, and therefore it is an $\mathcal{L}$-satisfiability procedure.

Case analysis of clauses in S_∞ from $S_0 = \mathcal{L} \cup S$

(i) empty clause

(ii) clauses in $\mathcal{L}$

(iii) ground flat unit clauses:

- (iii.a) $c_1 \simeq c_2$
- (iii.b) $c_1 \not\simeq c_2$
- (iii.c) $\mathrm{car}(c_1) \simeq c_2$
- (iii.d) $\mathrm{cdr}(c_1) \simeq c_2$
- (iii.e) $\mathrm{cons}(c_1, c_2) \simeq c_3$

(iv) non-unit clauses:

- (iv.a) $\mathrm{cons}(e_1, \mathrm{cdr}(e_2)) \simeq e_3 \vee \bigvee_i c_i \bowtie d_i$
- (iv.b) $\mathrm{cons}(\mathrm{car}(e_1), e_2) \simeq e_3 \vee \bigvee_i c_i \bowtie d_i$
- (iv.c) $\mathrm{cons}(\mathrm{car}(e_1), \mathrm{cdr}(e_2)) \simeq e_3 \vee \bigvee_i c_i \bowtie d_i$
- (iv.d) $\mathrm{cons}(e_1, e_2) \simeq e_3 \vee \bigvee_i c_i \bowtie d_i$
- (iv.e) $\mathrm{car}(e_1) \simeq \mathrm{car}(e_2) \vee \bigvee_i c_i \bowtie d_i$
- (iv.f) $\mathrm{cdr}(e_1) \simeq \mathrm{cdr}(e_2) \vee \bigvee_i c_i \bowtie d_i$
- (iv.g) $\mathrm{car}(e_1) \simeq e_2 \vee \bigvee_i c_i \bowtie d_i$
- (iv.h) $\mathrm{cdr}(e_1) \simeq e_2 \vee \bigvee_i c_i \bowtie d_i$
- (iv.i) $\bigvee_i c_i \bowtie d_i$

e_1, e_2, e_3, c_i, d_i, for all i, $1 \leq i \leq n$: constants (including nil).

Integer offsets

Presentation $\mathcal{I}$:

$$
\begin{array}{lll}
\forall x. & \mathsf{s}(\mathsf{p}(x)) \simeq x & \\
\forall x. & \mathsf{p}(\mathsf{s}(x)) \simeq x & \\
\forall x. & \mathsf{s}^i(x) \not\simeq x & \text{for } i > 0
\end{array}
$$

s: successor p: predecessor

Infinitely many acyclicity axioms: Problem reduction.

Some notation for integer offsets

$$A_{\mathcal{I}} = \{\mathsf{s}(\mathsf{p}(x)) \simeq x,\ \mathsf{p}(\mathsf{s}(x)) \simeq x\}$$

$$Ac(n) = \{\mathsf{s}^i(x) \not\simeq x : 0 < i \leq n\}$$

$$Ac = \bigcup_{n \geq 0} Ac(n)$$

Reduction to finitely many acyclicity axioms

Set of constants whose successor is defined by S:

$$C_S = \{c : \mathsf{s}(c) \simeq c' \in S \vee \mathsf{p}(c') \simeq c \in S\}$$

Theorem: For all n, $n \geq |C_S|$, if $A_{\mathcal{I}} \cup Ac(n) \cup S$ is satisfiable, then $A_{\mathcal{I}} \cup Ac \cup S$ is satisfiable.

Rewrite-based $\mathcal{I}$-satisfiability procedure

Theorem: A fair $\mathcal{SP}_{\succ}$-strategy is guaranteed to terminate when applied to $A_{\mathcal{I}} \cup Ac(n) \cup S$, where S is a set of ground flat $\mathcal{I}$-literals and $n = |C_S|$, and therefore it is an $\mathcal{I}$-satisfiability procedure.

Case analysis of clauses in S_∞ from $S_0 = A_\mathcal{I} \cup Ac(n) \cup S$

(i) the empty clause,

(ii) the clauses in $A_\mathcal{I}$

(iii) clauses $\mathsf{s}^i(x) \not\simeq \mathsf{p}^j(x)$, $i \geq 0$, $j \geq 0$, $1 \leq i + j \leq n$

(iv) ground unit clauses:

- (iv.a) $c \simeq c'$,
- (iv.b) $\mathsf{s}(c) \simeq c'$,
- (iv.c) $\mathsf{p}(c) \simeq c'$,

(v) clauses $\mathsf{s}^i(c) \not\simeq \mathsf{p}^j(c')$, $i \geq 0$, $j \geq 0$, $0 \leq i + j \leq n - 1$.

References

- Alessandro Armando, Maria Paola Bonacina, Silvio Ranise and Stephan Schulz. *New results on rewrite-based satisfiability procedures*. *ACM Trans. on Computational Logic*, To appear. (Presented in part at *FroCoS 2005* and *PDPAR 2005*)
- Maria Paola Bonacina and Mnacho Echenim. *On variable-inactivity and polynomial T-satisfiability procedures*. *Journal of Logic and Computation*, 18(1): 77-96, Feb. 2008. (Presented in part at *PDPAR 2006*)