Rewrite Closure for Ground and Cancellative AC-Theories

Ashish Tiwari

Tiwari@csl.sri.com

Computer Science Laboratory
SRI International
Menlo Park CA 94025

In the beginning...

- Deductive systems – inference rules
- Special relational symbol, equality – Unrestricted paramodulation

$$\frac{s \approx t, C[u] \approx v}{C[t]\sigma \approx v\sigma}$$

if $\sigma = mgu(s, u)$.

Deductive system "understands" logical symbols and equality.

Term Rewriting

Superposition: a restricted paramodulation step.

$$\frac{s \approx t, C[u] \approx v}{C[t]\sigma \approx v\sigma}$$

if $\sigma = mgu(s, u)$, $s \succ t$, and $C[u] \succ v$.

Attractive: Ordering $\succ$ on terms can be used to get a proof-ordering and a notion of redundancy and simplification.

Rewrite based theorem proving: various restrictions, mostly ordering based, imposed on clausal inference rules.

Decision Procedures

Effective deduction systems need powerful decision procedures tightly integrated into them.

- Presburger arithmetic interpreted over naturals, integers, or rationals
- Ground theory of equality
- Others

More specialized relational symbols, $>$, $<$, etc: transitive and restricted monotonicity.

Rewrite Techniques for Transitive Relations

- Chaining: Computing transitive closure

$$\frac{s > t, u > v}{s\sigma > v\sigma}$$

  if σ is the mgu of t and u.

- Ordered Chaining: Restrict the above inference rule

  $s\sigma \not\preceq t\sigma$ and $u\sigma \not\preceq v\sigma$.

- Extend to clausal theorem proving

Partial equivalence relations?

Partial Equivalence Relations

Transitive, non-symmetric, and monotone relation: $\gg$

Assume no variables.

- Partial Paramodulation:

$$\frac{s \gg t, C[t] \gg v}{C[s] \gg v}$$

- Ordered Partial Paramodulation:

$$\frac{s \gg t, C[t] \gg v}{C[s] \gg v}$$

  if $t \succ s$ and $C[t] \succ v$.

But: Even in the ground case, this may not terminate.

Non-termination Example

Consider $\{a \gg b,\ fb \gg b\}$ and $\succ$ is the rpo over $b \succ f \succ a$.

$$
\begin{array}{lr}
\{a \gg b\} & \{fb \gg b\} \\
\hline
\{a \gg b,\ fa \gg b\} & \{fb \gg b\} \\
\hline
\{a \gg b,\ fa \gg b,\ ffa \gg b\} & \{fb \gg b\} \\
\hline
\vdots &
\end{array}
$$

Using ordered partial paramodulation we can infer $f^n a \gg b$ and no simplifications/deletions are possible.

Recap...

Reln	Simple Inference	Ordered Inference	Ground Case?	Use
$\approx$	paramodulation	superposition	EXP time	CC
$>$	chaining	Ordered chaining	transitive closure	Graph
$\gg$	Partial paramodulation	Ordered partial paramodulation	non-terminating!	GTT

Questions

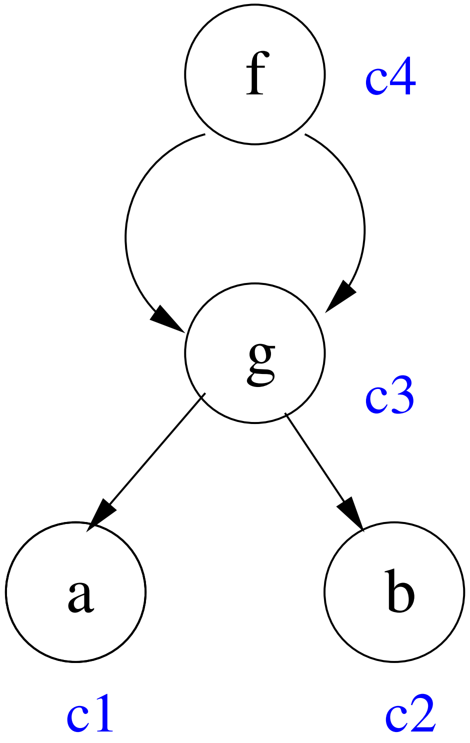
How to go from:

- superposition calculi for ground theories to congruence closure?
- partial ordered paramodulation for ground theories to tree automata algorithms?
- individual algorithms for equality and partial congruence relations to a combination of both?

Use new names for subterms.

Extended Signature

Consider the input set $I\!I_0 = \{fgabgab \approx a, a \to b\}$.



D-rules, D_0, represent term structure:

$$\begin{array}{rclrcl} a & \to & c_1 & b & \to & c_2 \\ gc_1c_2 & \to & c_3 & fc_3c_3 & \to & c_4 \end{array}$$

C-rules

represent a binary relation on vertices:

$$c_1 \quad \to \quad c_2$$

C-equations represent

an equivalence relation on vertices:

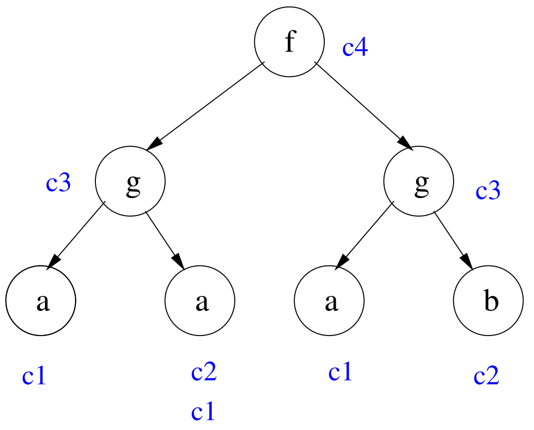
$$c_4 \quad \approx \quad c_1$$

Bottom-up Tree Automata

New Constants	States of the automaton
D-rules	Regular transitions
C-rules	ϵ-transition
Rewrite Sequence	Run

Thus, corresponding to the transitions

$\{a \to c_1, b \to c_2, gc_1c_2 \to c_3, fc_3c_3 \to c_4, c_1 \to c_2\}$, we have a run:



Putting it all together

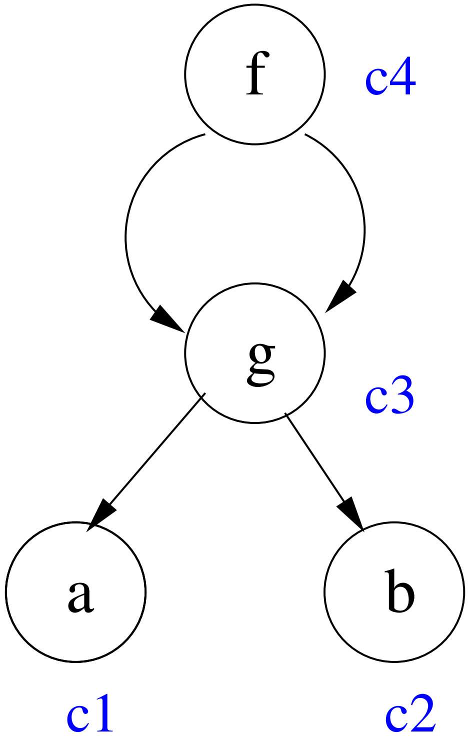
1. Extended signature
2. Superposition to handle equality
3. Ordered partial paramodulation to handle transitive and monotone relations

In [BT:CADE00], we showed that (1) and (2) can be combined to give abstract congruence closure.

Here, we show that (1), (2), and (3) together give a set of logical inference rules to construct a "rewrite closure"—completion for a set of ground equations ($\approx$) and inequations ($\gg$).

Extended Signature

Consider the input set $I\!I_0 = \{fgabgab \approx a, a \gg b\}$.



D-rules, D_0, represent term structure:

$$\begin{array}{rclrcl} a & \to & c_1 & b & \to & c_2 \\ gc_1c_2 & \to & c_3 & fc_3c_3 & \to & c_4 \end{array}$$

C-rules

represent a binary relation on vertices:

$$c_1 \to c_2$$

C-equations represent

an equivalence relation on vertices:

$$c_4 \approx c_1$$

Constructing Rewrite Closures

$\mathbb{I} = \mathbb{E} \cup \mathbb{R}$: The input set of equations and inequations.

E : Directed rules (to handle equations and term representation).

$R = F \cup B$: Directed rules partitioned into *forward* and *backward* rules (to handle the inequations).

i	$\mathbb{I}_i$	E_i	B_i	F_i	Rules
0	$\mathbb{I}_0$	$\emptyset$	$\emptyset$	$\emptyset$	
1	$\{c_4 \approx c_1, c_1 \gg c_2\}$	D_0			$Ext^* \cup Sim^*$
2	$\{c_1 \gg c_2\}$	$\cup\{c_1 \to c_4\}$			Ori
3	$\emptyset$			$\{c_1 \to c_2\}$	Ori

Example: Contd

i	Π_i	E_i	B_i	F_i	Rules
3	$\emptyset$	$\{a \to c_1, gc_1c_2 \to c_3, b \to c_2, fc_3c_3 \to c_4, c_1 \to c_4\}$	$\emptyset$	$\{c_1 \to c_2\}$	
4	$\emptyset$		$\{c_4 \to c_2\}$		Par, Ori
5	$\emptyset$	$\cup\{gc_4c_2 \to c_3\}$			Sup, Ori
6	$\emptyset$		$\cup\{c_3 \to gc_2c_2\}$		Par, Ori

Inference Rules

Extension: $$\frac{(\mathit{\Pi}[s], E, R)}{(\mathit{\Pi}[c], E \cup \{s \to c\}, R)}$$

Simplification1: $$\frac{(\mathit{\Pi}[s], E \cup \{s \to c\}, R)}{(\mathit{\Pi}[c], E \cup \{s \to c\}, R)}$$

Orientation Rules

Orientation1: $$\frac{(\mathbb{I} \cup \{s \approx c\}, E, R)}{(\mathbb{I}, E \cup \{s \to c\}, R)}$$

Orientation2: $$\frac{(\mathbb{I} \cup \{s \to c\}, E, R)}{(\mathbb{I}, E, R \cup \{s \to c\})}$$

Deduction Rules

Superposition:
$$\frac{(\mathit{I\!I}, E \cup \{t \to c, s[t] \to d\}, R)}{(\mathit{I\!I}, E \cup \{t \to c, s[c] \to d\}, R)}$$

Chaining:
$$\frac{(\mathit{I\!I}, E, R \cup \{d \to_B s, t[s] \to_F c\})}{(\mathit{I\!I}, E, R \cup \{\cdots, t[d] \to c\})}$$

Deduction Rules

Paramodulation:

$$\frac{(\mathit{II}, E \cup \{f(\ldots, d', \ldots) \rightarrow c\}, R \cup \{d \rightarrow_B d'\})}{(\mathit{II}, E \cup \{\cdots\}, R \cup \{\cdots, f(\ldots, d, \ldots) \rightarrow c\})}$$

Simplification Rules

Simplification2:
$$\frac{(I\!I, E \cup \{s \to c\}, R[s])}{(I\!I, E \cup \{\cdots\}, R[c])}$$

Composition:
$$\frac{(I\!I, E \cup \{c \to d, s \to c\}, R)}{(I\!I, E \cup \{c \to d, s \to d\}, R)}$$

Results

1. Termination: If $\mathbb{I}$ is finite, then any derivation using the inference rules and starting from $(\mathbb{I}, \emptyset, \emptyset, \emptyset)$ is finite.

2. Correctness: Let

   $$(\mathbb{I} = \mathbb{E} \cup \mathbb{R}, \emptyset, \emptyset, \emptyset) \ \vdash^! \ (\emptyset, E, B, F)$$

   be a maximal derivation. Then, for all terms s and t in $\mathcal{T}(\Sigma)$,

   $$s \rightarrow^*_{\mathbb{E}^{\pm} \cup \mathbb{R}} t$$

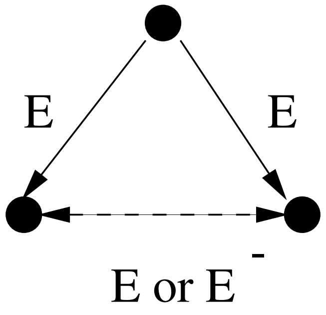
   if and only if

   $$s \rightarrow^*_{E \cup F} \circ \leftarrow^*_{E \cup B^-} t$$

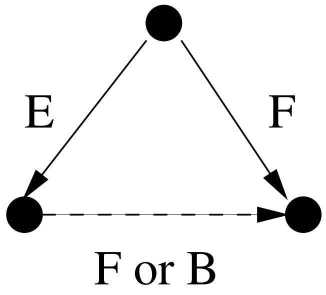
Proof is based on proof orderings and proof simplification arguments.

Proof Transformations

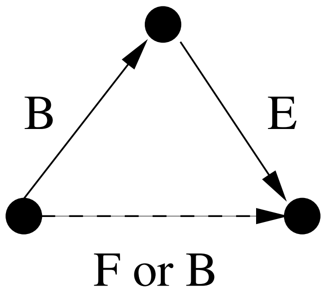
Deduction Steps



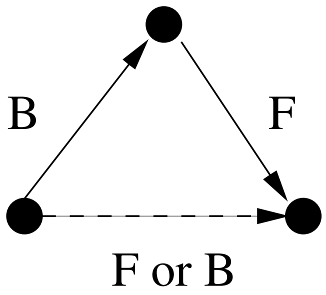
Superposition



Paramodulation1

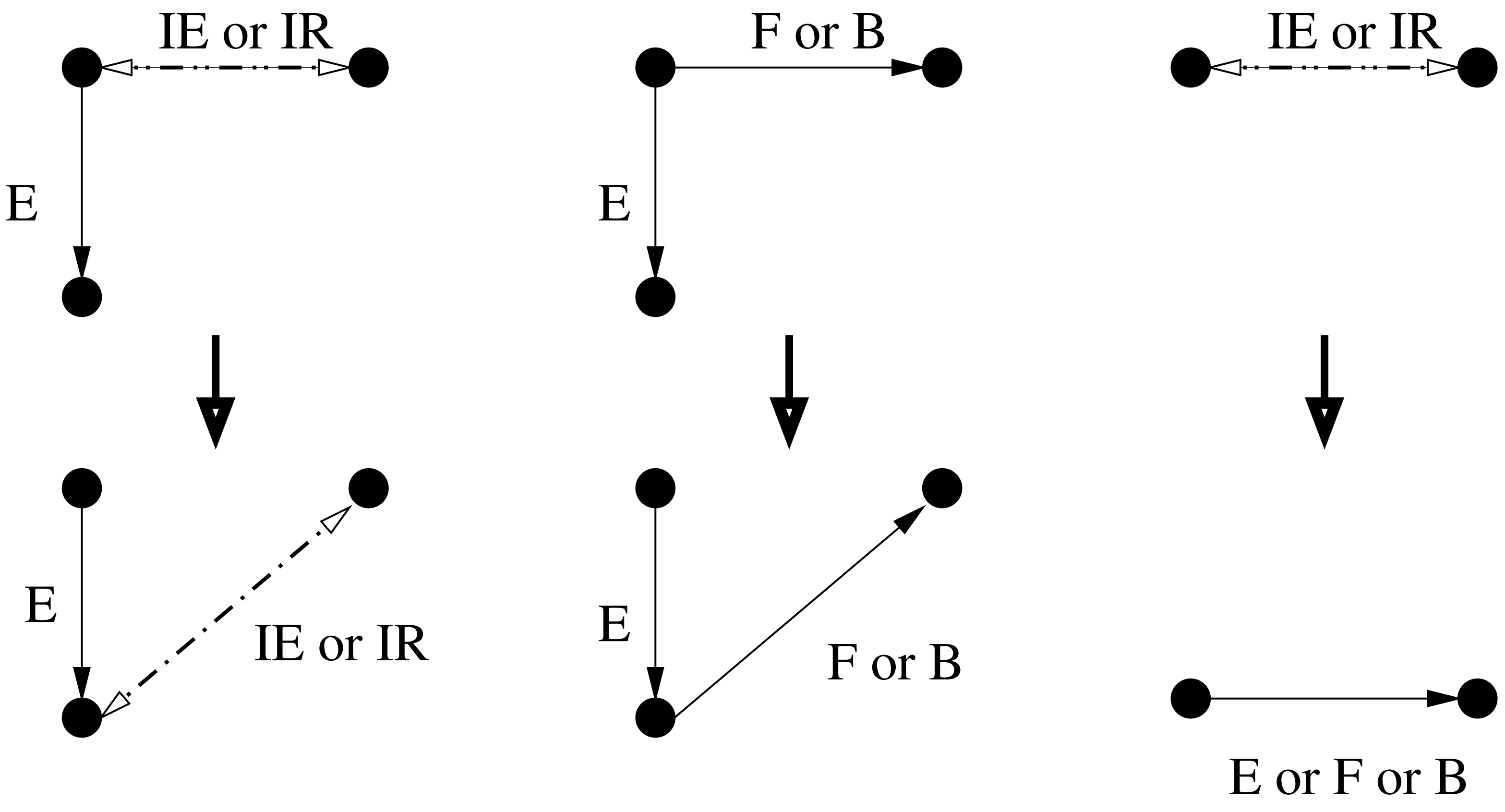


Paramodulation2



Chaining

Simplification Steps



Simplification1 Simplification2 Orientation

Features

- Termination: We get a set of decision procedures.
- Extended signature: We use simplified term representation and require much simpler orderings, $\succ$, on terms.
- Efficiency: The derivation length is bounded by a polynomial.
- Combination: The efficiency of congruence closure is combined with tree automata techniques for reachability.
- Extension: The inference rules can be generalized to handle cancellative AC-symbols.

Ground Cancellative AC Theories

Let f be a AC symbol which also satisfies:

$$\begin{array}{ccc} f(x_1, x_2, \ldots, x_m) & op & f(x_1, y_2, \ldots, y_m) \\ & \mathit{iff} & \\ f(x_2, \ldots, x_m) & op & f(y_2, \ldots, y_m), \end{array}$$

where $op \in \{\approx, \gg\}$.

Examples: addition and multiplication over $\mathbb{R}^+$, with $\approx$ and $\rightarrow$ interpreted as equality and greater-than relation:

$$x + y > x + z \quad \mathit{iff} \quad y > z \quad x + y = x + z \quad \mathit{iff} \quad y = z$$

and if $x > 0$, then

$$xy > xz \quad \mathit{iff} \quad y > z \quad xy = xz \quad \mathit{iff} \quad y = z$$

Extending the Rewrite Closure

Apart from D-rules, reverse D-rules, and C-rule, we also need rules of the form:

$$f(c_1, c_2, \ldots, c_m) \rightarrow f(d_1, d_2, \ldots, d_n)$$

- The ordered chaining, paramodulation, and superposition inferences can be extended to the AC case appropriately.
- The new set of inference rules are terminating (Dickson's lemma).
- Correctness of the new set of rules is shown using proof orderings.

Remarks

- If we remove the cancellative axiom:
  - equational theory is still decidable.
  - rewrite relation – Petri net reachability for special signature.
- Reachability in cancellative monoid is the dual of solving a system of linear diophantine equations.

  The system

  $$\begin{array}{rcrcrcl}\{4x_1 & - & x_2 & - & 2x_3 & = & 0, \\ 3x_1 & - & 4x_2 & + & 5x_3 & = & 0\}\end{array}$$

  has a non-trivial solution iff $e \to^+ e$ in the rewrite system

  $$\{c_1^4 c_2^3 \to e, e \to c_1 c_2^4, c_2^5 \to c_1^2\}$$

Summary

- Presented a set of efficient decision procedures for deciding the rewrite relation induced by a set of ground equations and inequations
- Inference rules are derived from standard and non-symmetric completion, done over extended signature
- The inference rules can be extended to include cancellative AC symbols

Future Work

- Extend to the theory of reals and other such theories
- Deciding properties of TRSs, e.g. confluence