22c:295 Seminar in AI — Decision Procedures

Rewriting

Cesare Tinelli

tinelli@cs.uiowa.edu

The University of Iowa

Outline

- Rewriting
- Termination
- Completion

Sources:
Harrison, John. *Introduction to Logic and Automated Theorem Proving*. Unpublished manuscript. Used by permission.

A Change in Notation

From now on, when we write

$$\Gamma \models \varphi,$$

we will assume that all the free variables of φ and of each formula in Γ are universally quantified.

This is done for convenience, but note that it does change the meaning of $\models$ for non-closed formulas.

Example
Without implicit quantifiers: $p(x) \not\models p(y)$.
With the implicit quantifiers: $p(x) \models p(y)$.

Rewriting

Consider the general problem of establishing $E \models s = t$ where E is a set of equations.

Congruence closure handles the case when all equations are ground. (How?)

There cannot be a simple procedure for the more general case because first order logic with equality is, in general, undecidable.

However, often the kind of equational reasoning needed is straightforward: equations are used in a predictable direction to *simplify* expressions.

Using equations in a directional fashion is called *rewriting*, and there are indeed cases when this technique gives us a decision procedure.

Rewriting

Suppose t is a term and $l = r$ is an equation.

We say that t' results from *rewriting* t with $l = r$ iff there is a subterm s of t and a substitution θ such that

1. $s = \theta(l)$,
2. $s' = \theta(r)$ and
3. t' is the result of replacing an occurrence of s by s' in t.

We call *rewrite rules* any (oriented) equations like $l = r$ above.

Given a set R of rewrite rules, we write $t \longrightarrow_R t'$ iff there is some rule $(l = r) \in R$ which rewrites t to t'.

Rewriting

Theorem (Soundness or Rewriting) If $t \longrightarrow_R t'$, then $R \models t = t'$.

Proof Every rewrite can be duplicated by a single instantiation followed by a chain of congruences. $\square$

What about completeness?

It depends on the rewrite rules.

When a set of (oriented) equations R is *canonical*, the question of whether $R \models s = t$ for two terms s and t can be answered by rewriting.

We will make this more precise later.

Abstract Reduction Relations

An abstract reduction relation is any binary relation on a set X.

We will denote a generic abstract reduction relation by $\longrightarrow$.

Every set R of rewrite rules induces an reduction relation on terms. We will denote that relation by $\longrightarrow_R$.

We will also denote by

- $\longleftarrow$ the inverse of $\longrightarrow$ (i.e. $x \longrightarrow y$ iff $y \longleftarrow x$).
- $\longrightarrow^+$ the transitive closure of $\longrightarrow$.
- $\longrightarrow^*$ the reflexive-transitive closure of $\longrightarrow$.
- $\longleftrightarrow^*$ the reflexive-symmetric-transitive closure of $\longrightarrow$.

Abstract Reduction Relations

Let $\longrightarrow$ be an abstract reduction relation on some set X.

An element $x \in X$ is said to be in *normal form* (NF) with respect to $\longrightarrow$ iff there is no $y \in X$ such that $x \longrightarrow y$.

The relation $\longrightarrow$ is said to be *terminating*, *strongly normalizing* (SN), or *noetherian* iff there is no infinite reduction sequence:

$$x_0 \longrightarrow \cdots \longrightarrow x_n \longrightarrow \cdots$$

Note that $\longrightarrow$ is terminating iff $\longleftarrow$ is well-founded.

Confluence

Let $\longrightarrow$ be an abstract reduction relation on some set X.

- $\longrightarrow$ has the *diamond property* iff whenever $x \longrightarrow y$ and $x \longrightarrow y'$, there is a z such that $y \longrightarrow z$ and $y' \longrightarrow z$.
- $\longrightarrow$ is *confluent* or *Church-Rosser* (CR) if $\longrightarrow^*$ has the diamond property.
- $\longrightarrow$ is *canonical* if it is confluent and terminating.
- $\longrightarrow$ is *weakly confluent* or *weakly Church-Rosser* (WCR) if whenever $x \longrightarrow y$ and $x \longrightarrow y'$, there is a z such that $y \longrightarrow^* z$ and $y' \longrightarrow^* z$.

These notions are closely related: For instance, the diamond property implies confluence which implies weak confluence.

Confluence

Weak confluence does not in general imply confluence, but adding termination changes the story.

Newman's Lemma If $\longrightarrow$ is terminating and weakly confluent, then it is confluent.

Proof It suffi ces to show that if $x \longrightarrow^* y$ and $x \longrightarrow^* y'$ with y and y' in normal form, then $y = y'$. (Why?) This can be proved by well-founded induction on $\longleftarrow$. Assume x writes to two normal forms: y and y'. The only interesting case is when x differs from both y and y'. (Why?) In that case, $x \longrightarrow w \longrightarrow^* y$ and $x \longrightarrow w' \longrightarrow^* y'$. By weak confluence, there must be a z such that $w \longrightarrow^* z$ and $w' \longrightarrow^* z$. Since w and w' are predecessors of x wrt $\longleftarrow$, by well-founded induction there must be a u such that $y \longrightarrow^* u$ and $z \longrightarrow^* u$, and a u' such that $z \longrightarrow^* u'$ and $y' \longrightarrow^* u'$. But y and y' are in normal form, so it must be that $y = u = z = u' = y'$. $\square$

Canonical Rewrite Systems

Theorem If R is a set of rewrite rules, then for all terms s and t, $s \longleftrightarrow_R^* t$ iff $R \models s = t$.

Let $s \downarrow_R t$ denote that s and t are *joinable*, i.e., there exists a z such that $s \longrightarrow_R^* u$ and $t \longrightarrow_R^* y$.

Theorem If $\longrightarrow_R$ is confluent, then for any s and t, $s \longleftrightarrow_R^* t$ iff $s \downarrow_R t$.

Corollary If $\longrightarrow_R$ is terminating and weakly confluent, then it is canonical. Therefore, $R \models s = t$ can be decided by rewriting s and t to normal forms and comparing them.

Proof By Newman's Lemma, termination and weak confluence imply confluence. Also, termination implies the existence of normal forms. Thus, by the above theorems, s and t have the same normal forms iff $s \downarrow_R t$ iff $s \longleftrightarrow_R^* t$ iff $R \models s = t$. $\square$

Reduction Orderings

A binary relation $>$ on terms is said to be a *rewrite ordering* if it is an ordering (i.e., an irreflexive and transitive relation) and is closed under instantiation and simple congruences, i.e.

- It is never the case that $t > t$.
- If $s > t$ and $t > u$, then $s > u$.
- If $s > t$, then $\theta(s) > \theta(t)$ for any substitution θ.
- If $s > t$, then $f(u_1, \ldots, u_{i-1}, s, u_{i+1}, \ldots, u_n) > f(u_1, \ldots, u_{i-1}, t, u_{i+1}, \ldots, u_n)$.

A rewrite ordering $>$ whose converse $<$ is well-founded is said to be a *reduction ordering*.

Reduction Orderings

Lemma If $>$ is a reduction ordering and $l > r$ for each equation $l = r$ in R, then the rewrite relation $\longrightarrow_R$ is terminating.

Proof It is not hard to see that if $s \longrightarrow_R t$, then $s > t$. Thus, because $<$ is well-founded, $\longrightarrow_R$ must be terminating. $\square$

By this lemma, reduction orderings are very useful for proving the termination of a rewrite system R.

Measure-based Orderings

Let us denote by $|t|$ the number of variables and function symbol occurrences in t.

We might hope to define a reduction ordering $s > t$ by $|s| > |t|$. However, this fails the instantiation property:

If $s > t$, then $\theta(s) > \theta(t)$ for any substitution θ.

Example Let $\theta = \{y \mapsto f(x, x, x)\}$.
$f(x, x, x) > g(x, y)$ but $\theta(f(x, x, x)) \not> \theta(g(x, y))$.

What can we do to fix this?

Let $|t|_x$ denote the number of occurrences of x in t.
Define $s > t$ if $|s| > |t|$ and $|s|_x > |t|_x$ for each variable x in t.

Exercise Prove that the latter $>$ is a reduction ordering.

In Search of Less Partial Reduction Orderings

The simple reduction ordering we defined earlier is not total. For instance, it does not order the following pairs of terms:

- $(x * y) * z, \;\; x * (y * z)$
- $x * (y + z), \;\; x * y + x * z$

To order such terms, we need more sophisticated orderings.

Note While it is unreasonable to expect a reduction ordering to be total on arbitrary terms, reduction orderings that order more pairs of terms are preferable.

Lexicographic Path Orderings (simplifi ed version)

A sequence $s_1, \ldots, s_m$ is *lexicographically greater than* a sequence $t_1, \ldots, t_m$ with respect to an ordering $>$ on terms if there is some $1 \leq n \leq m$ such that $s_i = t_i$ for all $i < n$ and $s_n > t_n$.

Let $\succ$ be an ordering over function symbols. The *lexicographic path ordering* $\succ_{lpo}$ on terms induced by $\succ$ is defined as follows:

- $f(s_1, \ldots, s_m) \succ_{lpo} f(t_1, \ldots, t_m)$ if $s_1, \ldots, s_m$ is lexicographically greater than $t_1, \ldots, t_m$ wrt $\succ_{lpo}$;
- $f(s_1, \ldots, s_m) \succ_{lpo} t$ if $s_i \succeq_{lpo} t$ for some $1 \leq i \leq m$;
- $f(s_1, \ldots, s_m) \succ_{lpo} g(t_1, \ldots, t_n)$ if $f \succ g$ and $f(s_1, \ldots, s_m) \succ_{lpo} t_i$ for each $1 \leq i \leq m$.

Properties of the LPO

For every ordering $\succ$ over function symbols:

- $\succ_{lpo}$ is a rewrite ordering;
- $\succ_{lpo}$ has the *subterm property*, i.e., $s \succ_{lpo} t$ for all proper subterms t of s;
- $\prec_{lpo}$ is well-founded whenever $\prec$ is (making $\succ_{lpo}$ a reduction ordering).
- if $s \succ_{lpo} t$ then $\mathit{vars}(t) \subseteq \mathit{vars}(s)$;

Any rewrite ordering with the subterm property is called a *simplification ordering*.

Checking for confluence

Once we have established that a rewrite systems R is terminating (perhaps using an appropriate reduction ordering), we only need to check for weak confluence to conclude that R is confluent and hence canonical.

Example Consider the system G consisting of the group axioms:

- $(x \cdot y) \cdot z = x \cdot (y \cdot z)$
- $1 \cdot x = x$
- $i(x) \cdot x = 1$

An LPO is enough to show that G is terminating here (**Exercise:** prove it). Is it confluent?

The term $(i(x) \cdot x) \cdot y$ can be rewritten to different terms that are not joinable. (How?) Thus, G is not confluent.

Checking for confluence

How do we check for (weak) confluence in general?

Given termination, we can decide weak confluence by discovering whether any starting term s can be rewritten to different normal forms.

Suppose $s \longrightarrow_R t_1$ and $s \longrightarrow_R t_2$.
There are three possible situations:

Critical Pairs

- The two rewrites apply to disjoint subterms. **Example:** $\underline{(1 \cdot a)} \cdot (i(b) \cdot b) \to a \cdot (i(b) \cdot b)$, with rule $1 \cdot x = x$, and $(1 \cdot a) \cdot \underline{(i(b) \cdot b)} \to (1 \cdot a) \cdot 1$, with rule $i(x) \cdot x = 1$.
- One rewrite applies to a term that is at or below position corresponding to a variable in the other rewrite. **Example:** $(b \cdot c) \cdot \underline{(1 \cdot a)} \to (b \cdot c) \cdot a$, with $1 \cdot x = x$, and $\underline{(b \cdot c) \cdot (1 \cdot a)} \to b \cdot (c \cdot (1 \cdot a))$, with $(x \cdot y) \cdot \underline{z} = x \cdot (y \cdot z)$.
- One rewrite applies to a term that is inside the term the other rewrite applies to, but is not at or below a variable position in the other rewrite rule. **Example:** $\underline{(i(a) \cdot a)} \cdot b \to 1 \cdot b$, with $i(x) \cdot x = 1$, and $\underline{(i(a) \cdot a) \cdot b} \to i(a) \cdot (a \cdot b)$ with $\underline{(x \cdot y)} \cdot z = x \cdot (y \cdot z)$.

The first two cases cannot break weak confluence. (Why?) Thus, only the third case needs to be considered.

Critical Pairs

Let $t[s]$ denote that s is a (possibly non-proper) subterm of t and let $t[s']$ denote the term obtained by replacing s with s' in t.

Consider $R_1 = \{l_1 = r_1\}$ and $R_2 = \{l_2 = r_2\}$ with $\mathit{vars}(R_1) \cap \mathit{vars}(R_2) = \emptyset$.

If $l_1[s]$ with s non-variable, and θ is a (idempotent) most general unifier of s and l_2, then

$$\theta(l_1) \longrightarrow_{R_1} \theta(r_1) \;\text{ and }\; \theta(l_1) \longrightarrow_{R_2} \theta(l_1[\theta(r_2)])$$

The pair $\langle \theta(r_1),\ \theta(l_1[\theta(r_2)]) \rangle$ is called a *critical pair*.

Theorem A term rewriting system is weakly confluent iff all its critical pairs are joinable.

Critical Pairs

Example What are the critical pairs for the group axioms?

1. $(x_1 \cdot y) \cdot z = x_1 \cdot (y \cdot z)$
2. $1 \cdot x_2 = x_2$
3. $i(x_3) \cdot x_3 = 1$

1 and 2 with $\theta = \{x_1 \mapsto 1, y \mapsto x_2\}$ gives
$\langle 1 \cdot (x_2 \cdot z),\ x_2 \cdot z \rangle$.

1 and 3 with $\theta = \{x_1 \mapsto i(x_3), y \mapsto x_3\}$ gives
$\langle i(x_3) \cdot (x_3 \cdot z),\ 1 \cdot z \rangle$.

1 and 1' with $\theta = \{x_1 \mapsto x_1' \cdot y', y \mapsto z'\}$ gives
$\langle (x_1' \cdot y') \cdot (z' \cdot z),\ (x_1' \cdot (y' \cdot z')) \cdot z \rangle$.

The first and third pairs are joinable, but the second is not. Thus this rewrite system is not weakly confluent.

Completion

It is straightforward to check whether each critical pair is joinable. However, we can be more ambitious.

Suppose $\langle s, t \rangle$ is a non-joinable critical pair, which means that normal form of s is s', the normal form of t is t', and $s' \neq t'$.

We can imagine adding $s' = t'$ or $t' = s'$ to our rewrite system to achieve confluence.

The process of repeatedly adding normalized critical pairs to the rewrite system is known as *completion*.

Two things can go wrong:

- It may not be possible to add $s' = t'$ or $t' = s'$ while respecting the term ordering.
- The completion process may run forever.

However, often completion is successful.

Interreduction

Completion often results in a large set of rewrite rules.

A natural question is whether the set can be reduced.

Theorem Let $\longrightarrow_R$ be a canonical (i.e. terminating and confluent) abstract reduction relation on a set X. Suppose another abstract reduction relation $\longrightarrow_S$ has the following two properties:

- For any $x, y \in X$, if $x \longrightarrow_S y$, then $x \longrightarrow_R^+ y$.
- For any $x, y \in X$, if $x \longrightarrow_R y$, then there is a $y' \in X$ with $x \longrightarrow_S y'$.

Then $\longrightarrow_S$ is also canonical and defines the same equivalence.

Interreduction

Corollary If R is a canonical rewrite system and $(l = r) \in R$, then if l is reducible by the other equations, the system $R - \{l = r\}$ is also canonical and defines the same equational theory.

Corollary If R is a canonical rewrite system and $(l = r) \in R$, let S be the result of replacing the equation $l = r$ in R with $l = r'$ where r' is the R-normal form of r. Then S is also canonical and defines the same equational theory.