Automated Reasoning

Rewriting-Based Deduction

Temur Kutsia

RISC, Johannes Kepler University, Linz, Austria
`kutsia@risc.jku.at`

The Equality Relation

Equality $\doteq$: A very important relation

- Reflexive
- Symmetric
- Transitive
- Substitute equals by equals
- When equality is used in a theorem, we need extra axioms which describe the properties of equality

The Equality Relation: Example

Theorem: Let G be a group with the binary operation $\cdot$, the inverse $^{-1}$, and the identity e. If $x \cdot x = e$ for all $x \in G$, then G is commutative.

Axioms:

1. For all $x, y \in G$, $x \cdot y \in G$.
2. For all $x, y, z \in G$, $(x \cdot y) \cdot z \doteq x \cdot (y \cdot z)$.
3. For all $x \in G$, $x \cdot e \doteq x$.
4. For all $x \in G$, $x \cdot x^{-1} \doteq e$.

The Equality Relation: Example (Cont.)

Express the axioms and the theorem in first-order logic with equality:

(A1) $\forall x, y.\ \exists z.\ x \cdot y \doteq z$.

(A2) $\forall x, y, z.\ (x \cdot y) \cdot z \doteq x \cdot (y \cdot z)$.

(A3) $\forall x.\ x \cdot e \doteq x$.

(A4) $\forall x.\ x \cdot i(x) \doteq e$.

(T) $\forall x.\ x \cdot x \doteq e \Rightarrow \forall u, v.\ u \cdot v \doteq v \cdot u$.

The Equality Relation: Example (Cont.)

Take the conjunction of axioms and the negation of the theorem and bring it to the Skolem normal form. We obtain the set consisting of the clauses:

1. $x \cdot y \doteq f(x, y)$.
2. $(x \cdot y) \cdot z \doteq x \cdot (y \cdot z)$.
3. $x \cdot e \doteq x$.
4. $x \cdot i(x) \doteq e$.
5. $x \cdot x \doteq e$
6. $\neg(a \cdot b \doteq b \cdot a)$.

The Equality Relation: Example (Cont.)

Take the conjunction of axioms and the negation of the theorem and bring it to the Skolem normal form. We obtain the set consisting of the clauses:

1. $x \cdot y \doteq f(x, y)$.
2. $(x \cdot y) \cdot z \doteq x \cdot (y \cdot z)$.
3. $x \cdot e \doteq x$.
4. $x \cdot i(x) \doteq e$.
5. $x \cdot x \doteq e$
6. $a \cdot b \not\doteq b \cdot a$.

The Equality Relation: Example (Cont.)

Take the conjunction of axioms and the negation of the theorem and bring it to the Skolem normal form. We obtain the set consisting of the clauses:

1. $x \cdot y \doteq f(x, y)$.
2. $(x \cdot y) \cdot z \doteq x \cdot (y \cdot z)$.
3. $x \cdot e \doteq x$.
4. $x \cdot i(x) \doteq e$.
5. $x \cdot x \doteq e$
6. $a \cdot b \not\doteq b \cdot a$.

By resolution alone, we can not derive the contradiction here.

The Equality Relation: Example (Cont.)

We need extra axioms to describe the properties of equality.

Let S be a set of clauses. The set of the equality axioms for S is the set consisting of the following clauses:

1. $x \doteq x$.
2. $x \not\doteq y \vee y \doteq x$.
3. $x \not\doteq y \vee y \not\doteq z \vee x \doteq z$.
4. $x \not\doteq y \vee \neg p(x_1, \ldots, x, \ldots, x_n) \vee p(x_1, \ldots, y, \ldots, x_n)$, where x and y appear in the same position i, for all $1 \leqslant i \leqslant n$, for every n-ary predicate symbol p appearing in S.
5. $x \not\doteq y \vee f(x_1, \ldots, x, \ldots, x_n) \doteq f(x_1, \ldots, y, \ldots, x_n)$, where x and y appear in the same position i, for all $1 \leqslant i \leqslant n$, for every n-ary function symbol f appearing in S.

The Equality Relation: Example (Cont.)

We add extra axioms:

$S:$	$x \cdot y \doteq f(x, y).$	$x \not\doteq y \vee y \not\doteq z \vee x \doteq z.$
	$(x \cdot y) \cdot z \doteq x \cdot (y \cdot z).$	$x \not\doteq y \vee x \not\doteq u \vee y \doteq u.$
	$x \cdot e \doteq x.$	$y \not\doteq x \vee u \not\doteq x \vee y \doteq u.$
	$x \cdot i(x) \doteq e.$	$x \not\doteq y \vee f(z, x) \doteq f(z, y).$
	$x \cdot x \doteq e.$	$x \not\doteq y \vee f(x, z) \doteq f(y, z).$
	$a \cdot b \not\doteq b \cdot a.$	$x \not\doteq y \vee x \cdot z \doteq y \cdot z.$
$K:$	$x \doteq x.$	$x \not\doteq y \vee z \cdot x \doteq z \cdot y.$
	$x \not\doteq y \vee y \doteq x.$	$x \not\doteq y \vee i(x) \doteq i(y).$

The Equality Relation: Example (Cont.)

We add extra axioms:

$$
\begin{array}{lll}
S: & x \cdot y \doteq f(x, y). & x \not\doteq y \vee y \not\doteq z \vee x \doteq z. \\
 & (x \cdot y) \cdot z \doteq x \cdot (y \cdot z). & x \not\doteq y \vee x \not\doteq u \vee y \doteq u. \\
 & x \cdot e \doteq x. & y \not\doteq x \vee u \not\doteq x \vee y \doteq u. \\
 & x \cdot i(x) \doteq e. & x \not\doteq y \vee f(z, x) \doteq f(z, y). \\
 & x \cdot x \doteq e. & x \not\doteq y \vee f(x, z) \doteq f(y, z). \\
 & a \cdot b \not\doteq b \cdot a. & x \not\doteq y \vee x \cdot z \doteq y \cdot z. \\
K: & x \doteq x. & x \not\doteq y \vee z \cdot x \doteq z \cdot y. \\
 & x \not\doteq y \vee y \doteq x. & x \not\doteq y \vee i(x) \doteq i(y).
\end{array}
$$

Unsatisfiability of this set can be proved by resolution.

The Equality Relation

The described approach has several drawbacks:

- Every time equality is used, one has to provide axioms that specify reflexive, symmetric, transitive, substitutive properties of equality.
- Clumsy approach.
- Generates large search space.
- Hopelessly inefficient.

The Equality Relation

The described approach has several drawbacks:

- Every time equality is used, one has to provide axioms that specify reflexive, symmetric, transitive, substitutive properties of equality.
- Clumsy approach.
- Generates large search space.
- Hopelessly inefficient.

Requires a special approach.

Rewriting-Based Deduction for Unit Equalities

We assume that the given set of clauses consists of unit equalities and one ground inequality.

Goal: Design a calculus which works on such sets, is more efficient than the described approach, and is complete.

Later this calculus can be extended to general clauses.

Equational Theory

- E: A set of equations.
- Ax: The set of equality axioms for E.
- $E \models s \doteq t$ iff $S \models s \doteq t$ for all structures S which is a model of $E \cup Ax$.
- Equational theory of E:

$$\doteq_E := \{(s, t) \mid E \models s \doteq t\}$$

- Notation: $s \doteq_E t$ iff $(s, t) \in \; \doteq_E$.

Basic Concepts in Term Rewriting

- A rewrite rule is an ordered pair of terms, written $l \to r$.
- Term rewriting system (TRS): a set of rewrite rules.

Problem

Given: A set of equations $\mathtt{E}$ and two terms s and $\mathtt{t}$.

Decide: $s \doteq_{\mathtt{E}} \mathtt{t}$ holds or not.

Problem

Given: A set of equations $\mathtt{E}$ and two terms s and $\mathtt{t}$.

Decide: $s \doteq_{\mathtt{E}} \mathtt{t}$ holds or not.

The problem is undecidable for an arbitrary $\mathtt{E}$.

Problem

Given: A set of equations E and two terms s and t.

Decide: $s \doteq_E t$ holds or not.

The problem is undecidable for an arbitrary E.

When E is finite and induces a (ground) convergent TRS, the problem is decidable.

Problem

Given: A set of equations E and two terms s and t.

Decide: $s \doteq_E t$ holds or not.

The problem is undecidable for an arbitrary E.

When E is finite and induces a (ground) convergent TRS, the problem is decidable.

What's this?

Problem

Given: A set of equations E and two terms s and t.

Decide: $s \doteq_E t$ holds or not.

Solving Idea

Refute and skolemize the goal, obtaining the ground disequation $s' \not\doteq_{E} t'$.

Solving Idea

Refute and skolemize the goal, obtaining the ground disequation $s' \dot{\neq}_E t'$.

Try to construct from E a ground convergent set of equations and rewrite rules, with the procedure called completion.

Solving Idea

Refute and skolemize the goal, obtaining the ground disequation $s' \not\doteq_{E} t'$.

Try to construct from E a ground convergent set of equations and rewrite rules, with the procedure called completion.

In the course of completion, from time to time check whether s' and t' can be rewritten to the same term with the equations and rules constructed so far.

Solving Idea

Refute and skolemize the goal, obtaining the ground disequation $s' \not\doteq_E t'$.

Try to construct from E a ground convergent set of equations and rewrite rules, with the procedure called completion.

In the course of completion, from time to time check whether s' and t' can be rewritten to the same term with the equations and rules constructed so far.

If yes, stop. You obtained a contradiction, which proves $s \doteq_E t$.

Solving Idea

Refute and skolemize the goal, obtaining the ground disequation $s' \not\doteq_E t'$.

Try to construct from E a ground convergent set of equations and rewrite rules, with the procedure called completion.

In the course of completion, from time to time check whether s' and t' can be rewritten to the same term with the equations and rules constructed so far.

If yes, stop. You obtained a contradiction, which proves $s \doteq_E t$.

If not, continue with completion. If this is not possible, then report: $s \doteq_E t$ does not hold.

What We Need To Know

- What is rewriting?
- What is a ground convergent set of equations and rewrite rules?
- What is completion?

Positions

The set of positions of a term t, $\mathrm{Pos}(t)$, is a set of strings of positive integers:

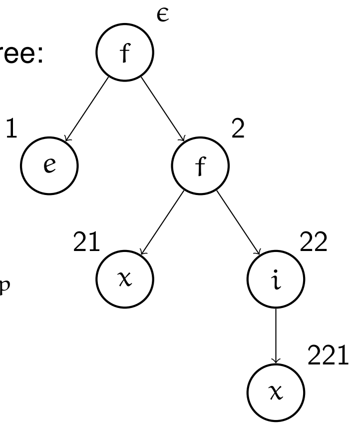
- If $t = x$, then $\mathrm{Pos}(t) := \{\epsilon\}$,
- If $t = f(t_1, \ldots, t_n)$, then

$$\mathrm{Pos}(t) := \{\epsilon\} \cup \{ip \mid 1 \leqslant i \leqslant n,\ p \in \mathrm{Pos}(t_i)\}.$$

More Notions about Terms

Term: $t = f(e, f(x, i(x)))$

Tree:



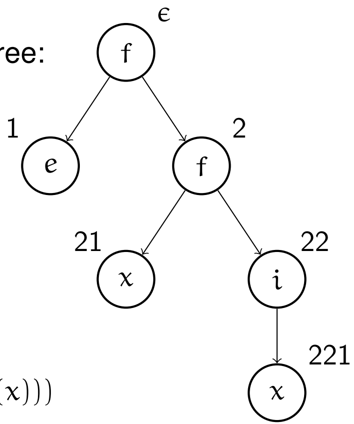
Subterm of t at position p: $t|_p$

$$\begin{aligned} t|_2 &= f(x, i(x)) \\ t|_{21} &= x \\ t|_{22} &= i(x) \end{aligned}$$

More Notions about Terms

Term: $t = f(e, f(x, i(x)))$

Tree:



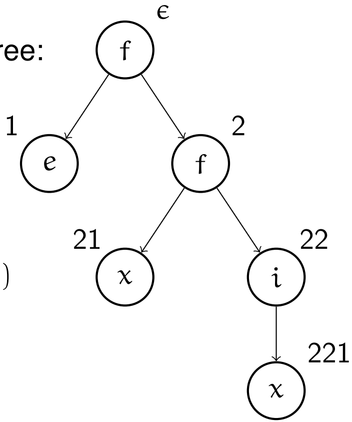
Replacing a subterm
at position p by s: $t[s]_p$

$$\begin{aligned} t[a]_\epsilon &= a \\ t[g(a,a)]_{21} &= f(e, f(g(a,a), i(x))) \\ t[i(y)]_{22} &= f(e, f(x, i(y))) \end{aligned}$$

More Notions about Terms

Term: $t = f(e, f(x, i(x)))$

Tree:



A size of t: $|t| = card(Pos(t))$

$$
\begin{aligned}
|t| &= 6 \\
|t[a]_2| &= 3 \\
|t|_{22}| &= 2
\end{aligned}
$$

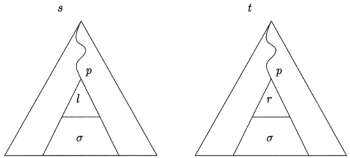
Basic Concepts in Term Rewriting

R: a term rewriting system.

- The rewrite relation induced by R, denoted $\to_R$, is a binary relation on terms defined as:

  $s \to_R t$ iff

  there exist $l \to r \in R$, a position p in s, a substitution σ such that $s|_p = \sigma(l)$ and $t = s[\sigma(r)]_p$.



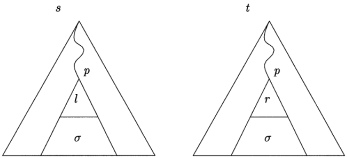
Basic Concepts in Term Rewriting

R: a term rewriting system.

- The rewrite relation induced by R, denoted $\to_R$, is a binary relation on terms defined as:

  $s \to_R t$ iff

  there exist $l \to r \in R$, a position p in s, a substitution σ such that $s|_p = \sigma(l)$ and $t = s[\sigma(r)]_p$.



- $R \subseteq \to_R$. We may omit R when it is obvious.

Basic Concepts in Term Rewriting

- s reduces to t by R iff $s \to_R t$.
- s is reducible by R iff there is a t such that $s \to_R t$.
- s is irreducible (is in normal form) by R iff s is not reducible.
- $\leftarrow_R$ stands for the inverse and $\to_R^*$ for reflexive-transitive closure of $\to_R$.
- t is a normal form of s by R iff $s \to_R^* t$ and t is irreducible by R.
- R is terminating iff $\to_R$ is well-founded, i.e., there is no infinite sequence of rewrite steps $s_1 \to_R s_2 \to_R s_3 \to_R \cdots$.

Basic Concepts in Term Rewriting

R is confluent iff for all terms s, t_1, t_2, if

$$s \to_R^* t_1 \text{ and } s \to_R^* t_2,$$

then there exists a term r such that

$$t_1 \to_R^* r \text{ and } t_2 \to_R^* r.$$

Basic Concepts in Term Rewriting

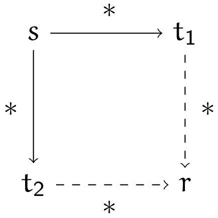
R is confluent iff for all terms s, t_1, t_2, if

$$s \to_R^* t_1 \quad \text{and} \quad s \to_R^* t_2,$$

then there exists a term r such that

$$t_1 \to_R^* r \quad \text{and} \quad t_2 \to_R^* r.$$

Graphically:



Basic Concepts in Term Rewriting

t_1 and t_2 are joinable by R if there exists a term r such that

$$t_1 \to_R^* r \text{ and } t_2 \to_R^* r.$$

Notation: $t_1 \downarrow_R t_2$.

Basic Concepts in Term Rewriting

Example

Let $+$ be a binary (infix) function symbol, s a unary function symbol, 0 a constant.

$$R := \{0 + x \to x, \quad s(x) + y \to s(x + y)\}.$$

Then:

- $s(0) + s(s(0)) \to_R s(0 + s(s(0))) \to_R s(s(s(0)))$.
- $s(0) + s(s(0)) \to_R^* s(s(s(0)))$.
- $s(s(s(0)))$ is irreducible by R and, hence, is a normal form of $s(0) + s(s(0))$, of $s(0 + s(s(0)))$, and of $s(s(s(0)))$.

Basic Concepts in Term Rewriting

A TRS $\mathcal{R}$ is convergent iff it is confluent and terminating.

A convergent TRS provides a decision procedure for the underlying equational theory: Two terms are equivalent iff they reduce to the same normal form.

Computation of normal forms by repeated reduction is a don't care non-deterministic process for convergent TRSs.

Basic Concepts in Term Rewriting

A strict order $>$ on terms is called a reduction order iff it is

1. monotonic: If $s > t$, then $r[s] > r[t]$ for all terms s, t, r;
2. stable: If $s > t$, then $\sigma(s) > \sigma(t)$ for all terms s, t and a substitution σ;
3. well-founded.

Basic Concepts in Term Rewriting

A strict order $>$ on terms is called a reduction order iff it is

1. monotonic: If $s > t$, then $r[s] > r[t]$ for all terms s, t, r;
2. stable: If $s > t$, then $\sigma(s) > \sigma(t)$ for all terms s, t and a substitution σ;
3. well-founded.

Why are reduction orders interesting?

Basic Concepts in Term Rewriting

A strict order $>$ on terms is called a reduction order iff it is

1. monotonic: If $s > t$, then $r[s] > r[t]$ for all terms s, t, r;
2. stable: If $s > t$, then $\sigma(s) > \sigma(t)$ for all terms s, t and a substitution σ;
3. well-founded.

Why are reduction orders interesting?

Theorem

A TRS R terminates iff there exists a reduction order $>$ that satisfies $l > r$ for all $l \to r \in R$.

Reduction Orders

- $|t|$: The size of the term t.
- The order $>_1$: $s >_1 t$ iff $|s| > |t|$.

Reduction Orders

- $|t|$: The size of the term t.
- The order $>_1$: $s >_1 t$ iff $|s| > |t|$.
- $>_1$ is monotonic and well-founded.

Reduction Orders

- $|t|$: The size of the term t.
- The order $>_1$: $s >_1 t$ iff $|s| > |t|$.
- $>_1$ is monotonic and well-founded.
- However, $>_1$ is not a reduction order because it is not stable:

$$|f(f(x,x),y)| = 5 > 3 = |f(y,y)|$$

For $\sigma = \{y \mapsto f(x,x)\}$:

$$|\sigma(f(f(x,x),y))| = |f(f(x,x),f(x,x))| = 7,$$
$$|\sigma(f(y,y)| = |f(f(x,x),f(x,x))| = 7.$$

Reduction Orders

- $|t|_x$: The number of occurrences of x in t.
- The order $>_2$: $s >_2 t$ iff $|s| > |t|$ and $|s|_x \geqslant |t|_x$ for all x.

Reduction Orders

- $|t|_x$: The number of occurrences of x in t.
- The order $>_2$: $s >_2 t$ iff $|s| > |t|$ and $|s|_x \geqslant |t|_x$ for all x.
- $>_2$ is a reduction order.

Methods for Construction Reduction Orders

- Polynomial orders
- Simplification orders:
  - Recursive path orders
  - Knuth-Bendix orders

Methods for Construction Reduction Orders

- Polynomial orders
- Simplification orders:
  - Recursive path orders
  - Knuth-Bendix orders

Goal: Provide a variety of different reduction orders that can be used to show termination; not only by hand, but also automatically.

Lexicographic Path Order

Main idea behind recursive path orders:

- Two terms are compared by first comparing their root symbols.
- Then recursively comparing the collections of their immediate subterms.

Lexicographic Path Order

Main idea behind recursive path orders:

- Two terms are compared by first comparing their root symbols.
- Then recursively comparing the collections of their immediate subterms.
- Collections seen as multisets yields the multiset path order. (Not considered in this course.)

Lexicographic Path Order

Main idea behind recursive path orders:

- Two terms are compared by first comparing their root symbols.
- Then recursively comparing the collections of their immediate subterms.
- Collections seen as multisets yields the multiset path order. (Not considered in this course.)
- Collections seen as tuples yields the lexicographic path order.

Lexicographic Path Order

Main idea behind recursive path orders:

- Two terms are compared by first comparing their root symbols.
- Then recursively comparing the collections of their immediate subterms.
- Collections seen as multisets yields the multiset path order. (Not considered in this course.)
- Collections seen as tuples yields the lexicographic path order.
- Combination of multisets and tuples yields the recursive path order with status. (Not considered in this course.)

Lexicographic Path Order

Let $\mathcal{F}$ be a finite signature and $>$ be a strict order on $\mathcal{F}$ (called the precedence). The lexicographic path order $>_{lpo}$ on $\mathsf{T}(\mathcal{F}, \mathcal{V})$ induced by $>$ is defined as follows:

$s >_{lpo} t$ iff

(1) $t \in Var(s)$ and $t \neq s$, or

(2) $s = f(s_1, \ldots, s_m)$, $t = g(t_1, \ldots, t_n)$, and

- (2a) $s_i \geqslant_{lpo} t$ for some i, $1 \leqslant i \leqslant m$, or
- (2b) $f > g$ and $s >_{lpo} t_j$ for all j, $1 \leqslant j \leqslant n$, or
- (2c) $f = g$, $s >_{lpo} t_j$ for all j, $1 \leqslant j \leqslant n$, and there exists i, $1 \leqslant i \leqslant m$ such that $s_1 = t_1, \ldots s_{i-1} = t_{i-1}$ and $s_i >_{lpo} t_i$.

$\geqslant_{lpo}$ stands for the reflexive closure of $>_{lpo}$.

Lexicographic Path Order

$s >_{lpo} t$ iff

(1) $t \in Var(s)$ and $t \neq s$, or

(2) $s = f(s_1, \ldots, s_m)$, $t = g(t_1, \ldots, t_n)$, and

(2a) $s_i \geqslant_{lpo} t$ for some i, $1 \leqslant i \leqslant m$, or

(2b) $f > g$ and $s >_{lpo} t_j$ for all j, $1 \leqslant j \leqslant n$, or

(2c) $f = g$, $s >_{lpo} t_j$ for all j, $1 \leqslant j \leqslant n$, and there exists i, $1 \leqslant i \leqslant m$ such that $s_1 = t_1, \ldots s_{i-1} = t_{i-1}$ and $s_i >_{lpo} t_i$.

Example

$\mathcal{F} = \{f, i, e\}$, f is binary, i is unary, e is constant, with $i > f > e$.

Lexicographic Path Order

$s >_{lpo} t$ iff

(1) $t \in Var(s)$ and $t \neq s$, or

(2) $s = f(s_1, \ldots, s_m)$, $t = g(t_1, \ldots, t_n)$, and

(2a) $s_i \geqslant_{lpo} t$ for some i, $1 \leqslant i \leqslant m$, or

(2b) $f > g$ and $s >_{lpo} t_j$ for all j, $1 \leqslant j \leqslant n$, or

(2c) $f = g$, $s >_{lpo} t_j$ for all j, $1 \leqslant j \leqslant n$, and there exists i, $1 \leqslant i \leqslant m$ such that $s_1 = t_1, \ldots s_{i-1} = t_{i-1}$ and $s_i >_{lpo} t_i$.

Example

$\mathcal{F} = \{f, i, e\}$, f is binary, i is unary, e is constant, with $i > f > e$.

- $f(x, e) >_{lpo} x$ by (1)

Lexicographic Path Order

$s >_{lpo} t$ iff

(1) $t \in Var(s)$ and $t \neq s$, or

(2) $s = f(s_1, \ldots, s_m)$, $t = g(t_1, \ldots, t_n)$, and

(2a) $s_i \geqslant_{lpo} t$ for some i, $1 \leqslant i \leqslant m$, or

(2b) $f > g$ and $s >_{lpo} t_j$ for all j, $1 \leqslant j \leqslant n$, or

(2c) $f = g$, $s >_{lpo} t_j$ for all j, $1 \leqslant j \leqslant n$, and there exists i, $1 \leqslant i \leqslant m$ such that $s_1 = t_1, \ldots s_{i-1} = t_{i-1}$ and $s_i >_{lpo} t_i$.

Example

$\mathcal{F} = \{f, i, e\}$, f is binary, i is unary, e is constant, with $i > f > e$.

- $f(x, e) >_{lpo} x$ by (1)
- $i(e) >_{lpo} e$ by (2a), because $e \geqslant_{lpo} e$.

Lexicographic Path Order

$s >_{lpo} t$ iff

(1) $t \in Var(s)$ and $t \neq s$, or

(2) $s = f(s_1, \ldots, s_m)$, $t = g(t_1, \ldots, t_n)$, and

(2a) $s_i \geqslant_{lpo} t$ for some i, $1 \leqslant i \leqslant m$, or

(2b) $f > g$ and $s >_{lpo} t_j$ for all j, $1 \leqslant j \leqslant n$, or

(2c) $f = g$, $s >_{lpo} t_j$ for all j, $1 \leqslant j \leqslant n$, and there exists i, $1 \leqslant i \leqslant m$ such that $s_1 = t_1, \ldots s_{i-1} = t_{i-1}$ and $s_i >_{lpo} t_i$.

Example (Cont.)

$\mathcal{F} = \{f, i, e\}$, f is binary, i is unary, e is constant, with $i > f > e$.

Lexicographic Path Order

$s >_{lpo} t$ iff

(1) $t \in Var(s)$ and $t \neq s$, or

(2) $s = f(s_1, \ldots, s_m)$, $t = g(t_1, \ldots, t_n)$, and

(2a) $s_i \geqslant_{lpo} t$ for some i, $1 \leqslant i \leqslant m$, or

(2b) $f > g$ and $s >_{lpo} t_j$ for all j, $1 \leqslant j \leqslant n$, or

(2c) $f = g$, $s >_{lpo} t_j$ for all j, $1 \leqslant j \leqslant n$, and there exists i, $1 \leqslant i \leqslant m$ such that $s_1 = t_1, \ldots s_{i-1} = t_{i-1}$ and $s_i >_{lpo} t_i$.

Example (Cont.)

$\mathcal{F} = \{f, i, e\}$, f is binary, i is unary, e is constant, with $i > f > e$.

- $i(f(x, y)) >^{?}_{lpo} f(i(x), i(y))$:

Lexicographic Path Order

$s >_{lpo} t$ iff

(1) $t \in Var(s)$ and $t \neq s$, or

(2) $s = f(s_1, \ldots, s_m)$, $t = g(t_1, \ldots, t_n)$, and

(2a) $s_i \geqslant_{lpo} t$ for some i, $1 \leqslant i \leqslant m$, or

(2b) $f > g$ and $s >_{lpo} t_j$ for all j, $1 \leqslant j \leqslant n$, or

(2c) $f = g$, $s >_{lpo} t_j$ for all j, $1 \leqslant j \leqslant n$, and there exists i, $1 \leqslant i \leqslant m$ such that $s_1 = t_1, \ldots s_{i-1} = t_{i-1}$ and $s_i >_{lpo} t_i$.

Example (Cont.)

$\mathcal{F} = \{f, i, e\}$, f is binary, i is unary, e is constant, with $i > f > e$.

- $i(f(x,y)) >^?_{lpo} f(i(x), i(y))$:
  - Since $i > f$, (2b) reduces it to the problems: $i(f(x,y)) >^?_{lpo} i(x)$ and $i(f(x,y)) >^?_{lpo} i(y)$.

Lexicographic Path Order

$s >_{lpo} t$ iff

(1) $t \in Var(s)$ and $t \neq s$, or

(2) $s = f(s_1, \dots, s_m)$, $t = g(t_1, \dots, t_n)$, and

(2a) $s_i \geqslant_{lpo} t$ for some i, $1 \leqslant i \leqslant m$, or

(2b) $f > g$ and $s >_{lpo} t_j$ for all j, $1 \leqslant j \leqslant n$, or

(2c) $f = g$, $s >_{lpo} t_j$ for all j, $1 \leqslant j \leqslant n$, and there exists i, $1 \leqslant i \leqslant m$ such that $s_1 = t_1, \dots s_{i-1} = t_{i-1}$ and $s_i >_{lpo} t_i$.

Example (Cont.)

$\mathcal{F} = \{f, i, e\}$, f is binary, i is unary, e is constant, with $i > f > e$.

- $i(f(x, y)) >^?_{lpo} i(x)$ is reduced by (2c) to $i(f(x, y)) >^?_{lpo} x$ and $f(x, y) >^?_{lpo} x$, which hold by (1).

Lexicographic Path Order

$s >_{lpo} t$ iff

(1) $t \in Var(s)$ and $t \neq s$, or

(2) $s = f(s_1, \ldots, s_m)$, $t = g(t_1, \ldots, t_n)$, and

(2a) $s_i \geqslant_{lpo} t$ for some i, $1 \leqslant i \leqslant m$, or

(2b) $f > g$ and $s >_{lpo} t_j$ for all j, $1 \leqslant j \leqslant n$, or

(2c) $f = g$, $s >_{lpo} t_j$ for all j, $1 \leqslant j \leqslant n$, and there exists i, $1 \leqslant i \leqslant m$ such that $s_1 = t_1, \ldots s_{i-1} = t_{i-1}$ and $s_i >_{lpo} t_i$.

Example (Cont.)

$\mathcal{F} = \{f, i, e\}$, f is binary, i is unary, e is constant, with $i > f > e$.

- $i(f(x, y)) >^{?}_{lpo} i(x)$ is reduced by (2c) to $i(f(x, y)) >^{?}_{lpo} x$ and $f(x, y) >^{?}_{lpo} x$, which hold by (1).
- $i(f(x, y)) >_{lpo} i(y)$ is shown similarly.

Lexicographic Path Order

$s >_{lpo} \mathrm{t}$ iff

(1) $\mathrm{t} \in Var(s)$ and $\mathrm{t} \neq s$, or

(2) $s = \mathrm{f}(s_1, \ldots, s_m)$, $\mathrm{t} = \mathrm{g}(\mathrm{t}_1, \ldots, \mathrm{t}_n)$, and

(2a) $s_i \geqslant_{lpo} \mathrm{t}$ for some i, $1 \leqslant i \leqslant m$, or

(2b) $\mathrm{f} > \mathrm{g}$ and $s >_{lpo} \mathrm{t}_j$ for all j, $1 \leqslant j \leqslant n$, or

(2c) $\mathrm{f} = \mathrm{g}$, $s >_{lpo} \mathrm{t}_j$ for all j, $1 \leqslant j \leqslant n$, and there exists i,
$1 \leqslant i \leqslant m$ such that $s_1 = \mathrm{t}_1, \ldots s_{i-1} = \mathrm{t}_{i-1}$ and $s_i >_{lpo} \mathrm{t}_i$.

Example (Cont.)

$\mathcal{F} = \{\mathrm{f}, \mathrm{i}, e\}$, f is binary, i is unary, e is constant, with $\mathrm{i} > \mathrm{f} > e$.

Lexicographic Path Order

$s >_{lpo} t$ iff

(1) $t \in Var(s)$ and $t \neq s$, or

(2) $s = f(s_1, \ldots, s_m)$, $t = g(t_1, \ldots, t_n)$, and

(2a) $s_i \geqslant_{lpo} t$ for some i, $1 \leqslant i \leqslant m$, or

(2b) $f > g$ and $s >_{lpo} t_j$ for all j, $1 \leqslant j \leqslant n$, or

(2c) $f = g$, $s >_{lpo} t_j$ for all j, $1 \leqslant j \leqslant n$, and there exists i, $1 \leqslant i \leqslant m$ such that $s_1 = t_1, \ldots s_{i-1} = t_{i-1}$ and $s_i >_{lpo} t_i$.

Example (Cont.)

$\mathcal{F} = \{f, i, e\}$, f is binary, i is unary, e is constant, with $i > f > e$.

- $f(f(x, y), z) >^?_{lpo} f(x, f(y, z)))$. By (2c) with $i = 1$:

Lexicographic Path Order

$s >_{lpo} t$ iff

(1) $t \in Var(s)$ and $t \neq s$, or

(2) $s = f(s_1, \ldots, s_m)$, $t = g(t_1, \ldots, t_n)$, and

(2a) $s_i \geqslant_{lpo} t$ for some i, $1 \leqslant i \leqslant m$, or

(2b) $f > g$ and $s >_{lpo} t_j$ for all j, $1 \leqslant j \leqslant n$, or

(2c) $f = g$, $s >_{lpo} t_j$ for all j, $1 \leqslant j \leqslant n$, and there exists i, $1 \leqslant i \leqslant m$ such that $s_1 = t_1, \ldots s_{i-1} = t_{i-1}$ and $s_i >_{lpo} t_i$.

Example (Cont.)

$\mathcal{F} = \{f, i, e\}$, f is binary, i is unary, e is constant, with $i > f > e$.

- $f(f(x, y), z) >_{lpo} x$ because of (1).

Lexicographic Path Order

$s >_{lpo} t$ iff

(1) $t \in Var(s)$ and $t \neq s$, or

(2) $s = f(s_1, \ldots, s_m)$, $t = g(t_1, \ldots, t_n)$, and

(2a) $s_i \geqslant_{lpo} t$ for some i, $1 \leqslant i \leqslant m$, or

(2b) $f > g$ and $s >_{lpo} t_j$ for all j, $1 \leqslant j \leqslant n$, or

(2c) $f = g$, $s >_{lpo} t_j$ for all j, $1 \leqslant j \leqslant n$, and there exists i, $1 \leqslant i \leqslant m$ such that $s_1 = t_1, \ldots s_{i-1} = t_{i-1}$ and $s_i >_{lpo} t_i$.

Example (Cont.)

$\mathcal{F} = \{f, i, e\}$, f is binary, i is unary, e is constant, with $i > f > e$.

- $f(f(x,y),z) >^?_{lpo} f(y,z)$: By (2c) with $i = 1$:
  - $f(f(x,y),z) >_{lpo} y$ and $f(f(x,y),z) >_{lpo} z$ by (1).
  - $f(x,y) >_{lpo} y$ by (1).

Lexicographic Path Order

$s >_{lpo} t$ iff

(1) $t \in Var(s)$ and $t \neq s$, or

(2) $s = f(s_1, \ldots, s_m)$, $t = g(t_1, \ldots, t_n)$, and

(2a) $s_i \geqslant_{lpo} t$ for some i, $1 \leqslant i \leqslant m$, or

(2b) $f > g$ and $s >_{lpo} t_j$ for all j, $1 \leqslant j \leqslant n$, or

(2c) $f = g$, $s >_{lpo} t_j$ for all j, $1 \leqslant j \leqslant n$, and there exists i, $1 \leqslant i \leqslant m$ such that $s_1 = t_1, \ldots s_{i-1} = t_{i-1}$ and $s_i >_{lpo} t_i$.

Example (Cont.)

$\mathcal{F} = \{f, i, e\}$, f is binary, i is unary, e is constant, with $i > f > e$.

- $f(x, y) >_{lpo} x$ by (1).

Reduction Orders

Reduction orders are not total for terms with variables.

For instance, $f(x)$ and $f(y)$ can not be ordered.

$f(x, y)$ and $f(y, x)$ can not be ordered either.

However, many reduction orders are total on ground terms.

Fortunately, in theorem proving applications one can often reason about non-ground formulas by considering the corresponding ground instances.

In such situations, ordered rewriting techniques can be applied.

Ordered Rewriting

Given: A reduction order $>$ and a set of equations E.

The rewrite system $E^>$ is defined as

$$E^> := \{\sigma(s) \to \sigma(r) \mid (s \doteq t \in E \text{ or } t \doteq s \in E) \text{ and } \sigma(s) > \sigma(t)\}$$

The rewrite relation $\to_{E^>}$ induced by $E^>$ represents ordered rewriting with respect to E and $>$.

Ordered Rewriting

Example

- If $>$ is a lexicographic path ordering with precedence $+ > a > b > c$, then $b + c > c + b > c$.
- Let $E := \{x + y \doteq y + x\}$.
- We may use the commutativity equation for ordered rewriting.
- $(b + c) + c \rightarrow_{E^>} (c + b) + c \rightarrow_{E^>} c + (c + b)$.

Ordered Rewriting

If $>$ is a reduction ordering total on ground terms, then $E^>$ contains all (non-trivial) ground instances of an equation $s \doteq t \in E$, either as a rule $\sigma(s) \to \sigma(t)$ or a rule $\sigma(t) \to \sigma(s)$.

A rewrite system R is called ground convergent if the induced ground rewrite relation (that is, the rewrite relation $\to_R$ restricted to pairs of ground terms) is terminating and confluent.

A set of equations E is called ground convergent with respect to $>$ if $E^>$ is ground convergent.

Critical Pairs

Ordered rewriting leads to the inference rule, called superposition:

$$\frac{s \doteq t \qquad r[u] \doteq v}{\sigma(r[t] \doteq v)},$$

where $\sigma = mgu(s, u)$, $\sigma(t) \not\succcurlyeq \sigma(s)$, $\sigma(v) \not\succcurlyeq \sigma(r)$, and u is not a variable.

The equation $\sigma(r[t] \doteq v)$ is called an ordered critical pair (with overlapped term $\sigma(r[u])$) between $s \doteq t$ and $r[u] \doteq v$.

Critical Pairs

Lemma

Let $>$ be a ground total reduction ordering.

A set E of equations is ground convergent with respect to $>$

iff

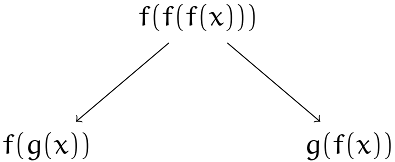
for all ordered critical pairs $\sigma(r[t] \doteq v)$ (with overlapped term $\sigma(r[u])$) between equations in E and for all ground substitutions φ,

if $\varphi(\sigma(r[u])) > \varphi(\sigma(r[t]))$ and $\varphi(\sigma(r[u])) > \varphi(\sigma(v))$, then $\varphi(\sigma(r[t])) \downarrow_{E^>} \varphi(\sigma(v))$.

Critical Pairs

Example

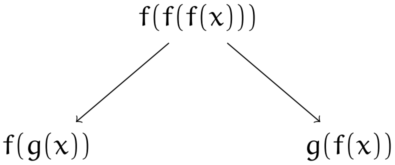
- Let $E := \{f(f(x)) \doteq g(x)\}$ and $>$ be the LPO with $f > g$.
- Take a critical pair between the equation and its renamed copy, $f(f(x)) \doteq g(x)$ and $f(f(y)) \doteq g(y)$.



Critical Pairs

Example

- Let $E := \{f(f(x)) \doteq g(x)\}$ and $>$ be the LPO with $f > g$.
- Take a critical pair between the equation and its renamed copy, $f(f(x)) \doteq g(x)$ and $f(f(y)) \doteq g(y)$.

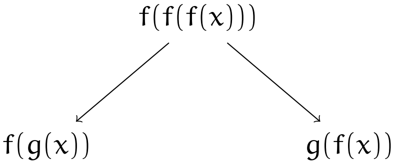


- $f(f(f(x))) > f(g(x))$ and $f(f(f(x))) > g(f(x))$, but $f(g(x)) \not\downarrow_{E_>} g(f(x))$.

Critical Pairs

Example

- Let $E := \{f(f(x)) \doteq g(x)\}$ and $>$ be the LPO with $f > g$.
- Take a critical pair between the equation and its renamed copy, $f(f(x)) \doteq g(x)$ and $f(f(y)) \doteq g(y)$.



- $f(f(f(x))) > f(g(x))$ and $f(f(f(x))) > g(f(x))$, but $f(g(x)) \not\downarrow_{E_>} g(f(x))$.
- E is not ground convergent with respect to $>$.

Adding Critical Pairs to Equations

Since critical pairs are equational consequences, adding a critical pair to the set of equations does not change the induced equational theory.

If $\mathtt{E}'$ is obtained from $\mathtt{E}$ by adding a critical pair, then $\doteq_{\mathtt{E}} = \doteq_{\mathtt{E}'}$.

The idea of adding a critical pair as a new equation is called “completion”.

Convergence

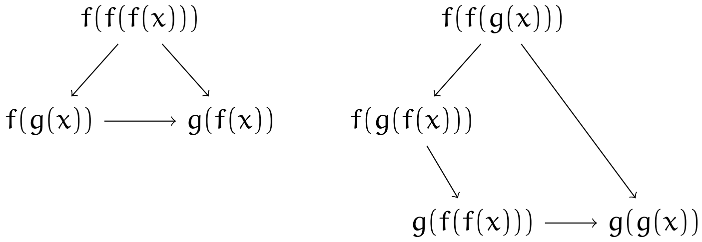
Example

- Let $E' := \{f(f(x)) \doteq g(x), f(g(x)) \doteq g(f(x))\}$
- Let $>$ be the LPO with $f > g$.

Convergence

Example

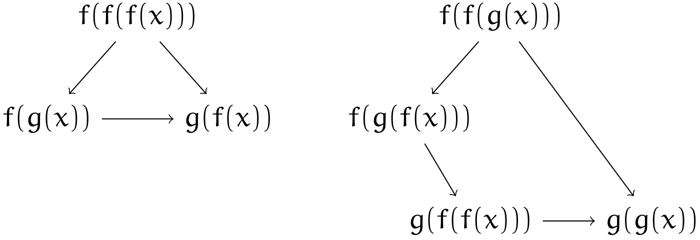
- Let $E' := \{f(f(x)) \doteq g(x), f(g(x)) \doteq g(f(x))\}$
- Let $>$ be the LPO with $f > g$.
- E' has two critical pairs. Both are joinable:



Convergence

Example

- Let $E' := \{f(f(x)) \doteq g(x), f(g(x)) \doteq g(f(x))\}$
- Let $>$ be the LPO with $f > g$.
- E' has two critical pairs. Both are joinable:



- E' is (ground) convergent.

Ordered Completion

Described as a set of inference rules.

Parametrized by a reduction ordering $>$.

Works on pairs (E, R), where E is a set of equations and R is a set of rewrite rules.

$E; R \vdash E'; R'$ means that $E'; R'$ can be obtained from $E; R$ by applying a completion inference.

Ordered Completion: Notions

Derivation: A (finite or countably infinite) sequence $(E_0; R_0) \vdash (E_1; R_1) \cdots$.

Usually, E_0 is the set of initial equations and $R_0 = \emptyset$.

The limit of a derivation: the pair $E_\omega; R_\omega$, where

$$E_\omega := \bigcup_{i \geqslant 0} \bigcap_{j \geqslant i} E_j \text{ and } R_\omega := \bigcup_{i \geqslant 0} \bigcap_{j \geqslant i} R_j.$$

Goal: to obtain a limit system that is ground convergent.

Ordered Completion: Notation

$\uplus$: Disjoint union

$s \rhd \mathtt{t}$: Strict encompassment relation. An instance of $\mathtt{t}$ is a subterm of s, but not vice versa.

$s \approxeq \mathtt{t}$ stands for $s \doteq \mathtt{t}$ or $\mathtt{t} \doteq s$.

$CP_{>}(\mathtt{E} \cup \mathtt{R})$: The set of all ordered critical pairs, with the ordering $>$, generated by equations in $\mathtt{E}$ and rewrite rules in $\mathtt{R}$ treated as equations.

Ordered Completion: Rules

DEDUCTION: $E; R \vdash E \cup \{s \doteq t\}; R$
if $s \doteq t \in CP_{>}(E \cup R)$.

ORIENTATION: $E \uplus \{s \approx t\}; R \vdash E; R \cup \{s \rightarrow t\}$, if $s > t$.

DELETION: $E \uplus \{s \doteq s\}; R \vdash E; R$.

Ordered Completion: Rules

COMPOSITION: $E; R \uplus \{s \to t\} \vdash E; R \cup \{s \to r\}$,

if $t \to_{R \cup E^{>}} r$.

SIMPLIFICATION: $E \cup \{s \approx t\}; R \vdash E \cup \{u \doteq t\}; R$,

if $s \to_R u$ or $s \to_{E^{>}} u$ with $\sigma(l) \to \sigma(r)$ for $l \approx r \in E$, $s \rhd l$.

COLLAPSE: $E; R \uplus \{s \to t\} \vdash E \cup \{u \doteq t\}; R$,

if $s \to_R u$ or $s \to_{E^{>}} u$ with $\sigma(l) \to \sigma(r)$ for $l \approx r \in E$, $s \rhd l$.

Ordered Completion: Properties

Theorem

Let $(E_0; R_0), (E_1; R_1), \ldots$ be an ordered completion derivation where all critical pairs are eventually generated (a fair derivation). Then these three properties are equivalent for all ground terms s and t:

(1) $E_0 \models s \doteq t$.

(2) $s \downarrow_{E_\omega^{>} \cup R_\omega} t$.

(3) $s \downarrow_{E_i^{>} \cup R_i} t$ for some $i \geqslant 0$.

This theorem, in particular, asserts the refutational completeness of ordered completion.

Proving by Ordered Completion: Example

Given:

1. $(x \cdot y) \cdot z \doteq x \cdot (y \cdot z)$.
2. $x \cdot e \doteq x$.
3. $x \cdot i(x) \doteq e$.
4. $x \cdot x \doteq e$.

Prove

Goal: $x \cdot y \doteq y \cdot x$.

Proving by Ordered Completion: Example

Proof by ordered completion:

- Skolemize the goal: $a \cdot b \doteq b \cdot a$.
- Take LPO as the reduction ordering with the precedence $i > f > e > a > b$
- $E_0 := \{(x \cdot y) \cdot z \doteq x \cdot (y \cdot z),\ x \cdot e \doteq x,\ x \cdot i(x) \doteq e,\ x \cdot x \doteq e\}$
- $R_0 := \emptyset$
- Start applying the rules.

Proving by Ordered Completion: Example

$$E_0 = \{(x \cdot y) \cdot z \doteq x \cdot (y \cdot z),\ x \cdot e \doteq x,\ x \cdot i(x) \doteq e,\ x \cdot x \doteq e\}$$

$$R_0 = \emptyset$$

Apply ORIENT 4 times:

$$E_4 = \emptyset$$

$$R_4 = \{(x \cdot y) \cdot z \to x \cdot (y \cdot z),\ x \cdot e \to x,\ x \cdot i(x) \to e,\ x \cdot x \to e\}$$

Proving by Ordered Completion: Example

$$E_0 = \{(x \cdot y) \cdot z \doteq x \cdot (y \cdot z),\ x \cdot e \doteq x,\ x \cdot i(x) \doteq e,\ x \cdot x \doteq e\}$$
$$R_0 = \emptyset$$

Apply ORIENT 4 times:

$$E_4 = \emptyset$$
$$R_4 = \{(x \cdot y) \cdot z \to x \cdot (y \cdot z),\ x \cdot e \to x,\ x \cdot i(x) \to e,\ x \cdot x \to e\}$$

Apply DEDUCE with the rules $(x \cdot y) \cdot z \to x \cdot (y \cdot z)$ and $x \cdot e \to x$ to the overlapping term $(x \cdot e) \cdot z$, and then ORIENT:

$$E_6 = \emptyset$$
$$R_6 = \{(x \cdot y) \cdot z \to x \cdot (y \cdot z),\ x \cdot e \to x,\ x \cdot i(x) \to e,\ x \cdot x \to e,$$
$$x_1 \cdot (e \cdot x_2) \to x_1 \cdot x_2\}$$

Proving by Ordered Completion: Example

$$E_6 = \emptyset$$
$$R_6 = \{(x \cdot y) \cdot z \rightarrow x \cdot (y \cdot z),\ x \cdot e \rightarrow x,\ x \cdot i(x) \rightarrow e,\ x \cdot x \rightarrow e,$$
$$x_1 \cdot (e \cdot x_2) \rightarrow x_1 \cdot x_2\}$$

Apply DEDUCE with the rules $x_1 \cdot (e \cdot x_2) \rightarrow x_1 \cdot x_2$ and $x \cdot i(x) \rightarrow e$ to the overlapping term $x_1 \cdot (e \cdot i(e))$:

$$E_7 = \{x_1 \cdot i(e) \doteq x_1 \cdot e\}$$
$$R_7 = \{(x \cdot y) \cdot z \rightarrow x \cdot (y \cdot z),\ x \cdot e \rightarrow x,\ x \cdot i(x) \rightarrow e,\ x \cdot x \rightarrow e,$$
$$x_1 \cdot (e \cdot x_2) \rightarrow x_1 \cdot x_2\}$$

Proving by Ordered Completion: Example

$$E_7 = \{x_1 \cdot i(e) \doteq x_1 \cdot e\}$$

$$R_7 = \{(x \cdot y) \cdot z \to x \cdot (y \cdot z),\ x \cdot e \to x,\ x \cdot i(x) \to e,\ x \cdot x \to e,$$
$$x_1 \cdot (e \cdot x_2) \to x_1 \cdot x_2\}$$

Apply ORIENT to $x_1 \cdot i(e) \doteq x_1 \cdot e$ and then COMPOSITION with the rule $x \cdot e \to x$:

$$E_9 = \emptyset$$

$$R_9 = \{(x \cdot y) \cdot z \to x \cdot (y \cdot z),\ x \cdot e \to x,\ x \cdot i(x) \to e,\ x \cdot x \to e,$$
$$x_1 \cdot (e \cdot x_2) \to x_1 \cdot x_2,\ x \cdot i(e) \to x\}$$

Proving by Ordered Completion: Example

$$E_9 = \emptyset$$

$$R_9 = \{(x \cdot y) \cdot z \to x \cdot (y \cdot z),\ x \cdot e \to x,\ x \cdot i(x) \to e,\ x \cdot x \to e,$$
$$x_1 \cdot (e \cdot x_2) \to x_1 \cdot x_2,\ x \cdot i(e) \to x\}$$

Apply DEDUCE with the rules $x \cdot x \to e$ and $x \cdot i(e) \to x$ to the overlapping term $i(e) \cdot i(e)$, and then ORIENT:

$$E_{11} = \emptyset$$

$$R_{11} = \{(x \cdot y) \cdot z \to x \cdot (y \cdot z),\ x \cdot e \to x,\ x \cdot i(x) \to e,\ x \cdot x \to e,$$
$$x_1 \cdot (e \cdot x_2) \to x_1 \cdot x_2,\ x \cdot i(e) \to x,\ i(e) \to e\}$$

Proving by Ordered Completion: Example

$$E_{11} = \emptyset$$

$$R_{11} = \{(x \cdot y) \cdot z \to x \cdot (y \cdot z),\ x \cdot e \to x,\ x \cdot i(x) \to e,\ x \cdot x \to e,\ x_1 \cdot (e \cdot x_2) \to x_1 \cdot x_2,\ x \cdot i(e) \to x,\ i(e) \to e\}$$

Apply Collapse to $x \cdot i(e) \to x$ with $i(e) \to e$:

$$E_{12} = \{x \cdot e \doteq x\}$$

$$R_{12} = \{(x \cdot y) \cdot z \to x \cdot (y \cdot z),\ x \cdot e \to x,\ x \cdot i(x) \to e,\ x \cdot x \to e,\ x_1 \cdot (e \cdot x_2) \to x_1 \cdot x_2,\ i(e) \to e\}$$

Proving by Ordered Completion: Example

$$E_{12} = \{x \cdot e \doteq x\}$$

$$R_{12} = \{(x \cdot y) \cdot z \to x \cdot (y \cdot z),\ x \cdot e \to x,\ x \cdot i(x) \to e,\ x \cdot x \to e,$$
$$x_1 \cdot (e \cdot x_2) \to x_1 \cdot x_2,\ i(e) \to e\}$$

Apply SIMPLIFICATION to $x \cdot e \doteq x$ with $x \cdot e \to x$ and then DELETE to the obtained $x \doteq x$:

$$E_{14} = \emptyset$$

$$R_{14} = \{(x \cdot y) \cdot z \to x \cdot (y \cdot z),\ x \cdot e \to x,\ x \cdot i(x) \to e,\ x \cdot x \to e,$$
$$x_1 \cdot (e \cdot x_2) \to x_1 \cdot x_2,\ i(e) \to e\}$$

Proving by Ordered Completion: Example

$$E_{14} = \emptyset$$

$$R_{14} = \{(x \cdot y) \cdot z \to x \cdot (y \cdot z),\ x \cdot e \to x,\ x \cdot i(x) \to e,\ x \cdot x \to e,$$
$$x_1 \cdot (e \cdot x_2) \to x_1 \cdot x_2,\ i(e) \to e\}$$

Apply DEDUCE to $(x \cdot y) \cdot z \to x \cdot (y \cdot z)$ and $x \cdot i(x) \to e$ with the overlapping term $(x \cdot i(x)) \cdot z$ and then ORIENT:

$$E_{16} = \emptyset$$

$$R_{16} = \{(x \cdot y) \cdot z \to x \cdot (y \cdot z),\ x \cdot e \to x,\ x \cdot i(x) \to e,\ x \cdot x \to e,$$
$$x_1 \cdot (e \cdot x_2) \to x_1 \cdot x_2,\ i(e) \to e,\ x_1 \cdot (i(x_1) \cdot x_2) \to e \cdot x_2\}$$

Proving by Ordered Completion: Example

$$E_{16} = \emptyset$$

$$R_{16} = \{(x \cdot y) \cdot z \to x \cdot (y \cdot z),\ x \cdot e \to x,\ x \cdot i(x) \to e,\ x \cdot x \to e,\ x_1 \cdot (e \cdot x_2) \to x_1 \cdot x_2,\ i(e) \to e,\ x_1 \cdot (i(x_1) \cdot x_2) \to e \cdot x_2\}$$

Apply DEDUCE to $x_1 \cdot (i(x_1) \cdot x_2) \to e \cdot x_2$ and $x \cdot x \to e$ with the overlapping term $x_1 \cdot (i(x_1) \cdot i(x_1))$:

$$E_{17} = \{e \cdot i(x) \doteq x \cdot e\}$$

$$R_{17} = \{(x \cdot y) \cdot z \to x \cdot (y \cdot z),\ x \cdot e \to x,\ x \cdot i(x) \to e,\ x \cdot x \to e,\ x_1 \cdot (e \cdot x_2) \to x_1 \cdot x_2,\ i(e) \to e,\ x_1 \cdot (i(x_1) \cdot x_2) \to e \cdot x_2\}$$

Proving by Ordered Completion: Example

$$E_{17} = \{e \cdot i(x) \doteq x \cdot e\}$$

$$R_{17} = \{(x \cdot y) \cdot z \to x \cdot (y \cdot z),\ x \cdot e \to x,\ x \cdot i(x) \to e,\ x \cdot x \to e,\ x_1 \cdot (e \cdot x_2) \to x_1 \cdot x_2,\ i(e) \to e,\ x_1 \cdot (i(x_1) \cdot x_2) \to e \cdot x_2\}$$

Apply SIMPLIFICATION to $e \cdot i(x) \doteq x \cdot e$ with $x \cdot e \to x$ and then ORIENT:

$$E_{19} = \emptyset$$

$$R_{19} = \{(x \cdot y) \cdot z \to x \cdot (y \cdot z),\ x \cdot e \to x,\ x \cdot i(x) \to e,\ x \cdot x \to e,\ x_1 \cdot (e \cdot x_2) \to x_1 \cdot x_2,\ i(e) \to e,\ x_1 \cdot (i(x_1) \cdot x_2) \to e \cdot x_2,\ e \cdot i(x) \to x\}$$

Proving by Ordered Completion: Example

$$
\begin{aligned}
E_{19} &= \emptyset \\
R_{19} &= \{(x \cdot y) \cdot z \to x \cdot (y \cdot z),\ x \cdot e \to x,\ x \cdot i(x) \to e,\ x \cdot x \to e, \\
&\quad x_1 \cdot (e \cdot x_2) \to x_1 \cdot x_2,\ i(e) \to e,\ x_1 \cdot (i(x_1) \cdot x_2) \to e \cdot x_2, \\
&\quad e \cdot i(x) \to x\}
\end{aligned}
$$

Apply DEDUCE to $x_1 \cdot (e \cdot x_2) \to x_1 \cdot x_2$ and $e \cdot i(x) \to x$ with the overlapping term $x_1 \cdot (e \cdot i(x_2))$ and then ORIENT:

$$
\begin{aligned}
E_{21} &= \emptyset \\
R_{21} &= \{(x \cdot y) \cdot z \to x \cdot (y \cdot z),\ x \cdot e \to x,\ x \cdot i(x) \to e,\ x \cdot x \to e, \\
&\quad x_1 \cdot (e \cdot x_2) \to x_1 \cdot x_2,\ i(e) \to e,\ x_1 \cdot (i(x_1) \cdot x_2) \to e \cdot x_2, \\
&\quad e \cdot i(x) \to x,\ x_1 \cdot i(x_2) \to x_1 \cdot x_2\}
\end{aligned}
$$

Proving by Ordered Completion: Example

$$E_{21} = \emptyset$$

$$R_{21} = \{(x \cdot y) \cdot z \to x \cdot (y \cdot z),\ x \cdot e \to x,\ x \cdot i(x) \to e,\ x \cdot x \to e,$$
$$x_1 \cdot (e \cdot x_2) \to x_1 \cdot x_2,\ i(e) \to e,\ x_1 \cdot (i(x_1) \cdot x_2) \to e \cdot x_2,$$
$$e \cdot i(x) \to x,\ x_1 \cdot i(x_2) \to x_1 \cdot x_2\}$$

Applying Collapse, Simplification, and Delete, we get rid of $x \cdot i(x) \to e$:

$$E_{24} = \emptyset$$

$$R_{24} = \{(x \cdot y) \cdot z \to x \cdot (y \cdot z),\ x \cdot e \to x,\ x \cdot x \to e,$$
$$x_1 \cdot (e \cdot x_2) \to x_1 \cdot x_2,\ i(e) \to e,\ x_1 \cdot (i(x_1) \cdot x_2) \to e \cdot x_2,$$
$$e \cdot i(x) \to x,\ x_1 \cdot i(x_2) \to x_1 \cdot x_2\}$$

Proving by Ordered Completion: Example

$$E_{24} = \emptyset$$

$$R_{24} = \{(x \cdot y) \cdot z \to x \cdot (y \cdot z),\ x \cdot e \to x,\ x \cdot x \to e,$$
$$x_1 \cdot (e \cdot x_2) \to x_1 \cdot x_2,\ i(e) \to e,\ x_1 \cdot (i(x_1) \cdot x_2) \to e \cdot x_2,$$
$$e \cdot i(x) \to x,\ x_1 \cdot i(x_2) \to x_1 \cdot x_2\}$$

Applying COLLAPSE and ORIENT, we replace $e \cdot i(x) \to x$ with $e \cdot x \to x$:

$$E_{26} = \emptyset$$

$$R_{26} = \{(x \cdot y) \cdot z \to x \cdot (y \cdot z),\ x \cdot e \to x,\ x \cdot x \to e,$$
$$x_1 \cdot (e \cdot x_2) \to x_1 \cdot x_2,\ i(e) \to e,\ x_1 \cdot (i(x_1) \cdot x_2) \to e \cdot x_2,$$
$$e \cdot x \to x,\ x_1 \cdot i(x_2) \to x_1 \cdot x_2\}$$

Proving by Ordered Completion: Example

$$E_{26} = \emptyset$$

$$R_{26} = \{(x \cdot y) \cdot z \to x \cdot (y \cdot z),\ x \cdot e \to x,\ x \cdot x \to e,$$
$$x_1 \cdot (e \cdot x_2) \to x_1 \cdot x_2,\ i(e) \to e,\ x_1 \cdot (i(x_1) \cdot x_2) \to e \cdot x_2,$$
$$e \cdot x \to x,\ x_1 \cdot i(x_2) \to x_1 \cdot x_2\}$$

Applying COLLAPSE and DELETE, we get rid of $x_1 \cdot (e \cdot x_2) \to x_1 \cdot x_2$:

$$E_{28} = \emptyset$$

$$R_{28} = \{(x \cdot y) \cdot z \to x \cdot (y \cdot z),\ x \cdot e \to x,\ x \cdot x \to e,$$
$$i(e) \to e,\ x_1 \cdot (i(x_1) \cdot x_2) \to e \cdot x_2,$$
$$e \cdot x \to x,\ x_1 \cdot i(x_2) \to x_1 \cdot x_2\}$$

Proving by Ordered Completion: Example

$$E_{28} = \emptyset$$

$$\begin{aligned} R_{28} = \{&(x \cdot y) \cdot z \to x \cdot (y \cdot z),\ x \cdot e \to x,\ x \cdot x \to e, \\ &i(e) \to e,\ x_1 \cdot (i(x_1) \cdot x_2) \to e \cdot x_2, \\ &e \cdot x \to x,\ x_1 \cdot i(x_2) \to x_1 \cdot x_2\} \end{aligned}$$

Apply DEDUCE to $e \cdot x \to x$ and $x_1 \cdot i(x_2) \to x_1 \cdot x_2$ with the overlapping term $e \cdot i(x_2)$:

$$E_{29} = \{i(x_1) \doteq e \cdot x_2\}$$

$$\begin{aligned} R_{29} = \{&(x \cdot y) \cdot z \to x \cdot (y \cdot z),\ x \cdot e \to x,\ x \cdot x \to e, \\ &i(e) \to e,\ x_1 \cdot (i(x_1) \cdot x_2) \to e \cdot x_2, \\ &e \cdot x \to x,\ x_1 \cdot i(x_2) \to x_1 \cdot x_2\} \end{aligned}$$

Proving by Ordered Completion: Example

$$E_{29} = \{i(x_2) \doteq e \cdot x_2\}$$

$$R_{29} = \{(x \cdot y) \cdot z \to x \cdot (y \cdot z),\ x \cdot e \to x,\ x \cdot x \to e,$$
$$i(e) \to e,\ x_1 \cdot (i(x_1) \cdot x_2) \to e \cdot x_2,$$
$$e \cdot x \to x,\ x_1 \cdot i(x_2) \to x_1 \cdot x_2\}$$

Apply SIMPLIFICATION to $i(x_1) \doteq e \cdot x_2$ with $e \cdot x \to x$ and then ORIENT:

$$E_{31} = \emptyset$$

$$R_{31} = \{(x \cdot y) \cdot z \to x \cdot (y \cdot z),\ x \cdot e \to x,\ x \cdot x \to e,$$
$$i(e) \to e,\ x_1 \cdot (i(x_1) \cdot x_2) \to e \cdot x_2,$$
$$e \cdot x \to x,\ x_1 \cdot i(x_2) \to x_1 \cdot x_2,\ i(x) \to x\}$$

Proving by Ordered Completion: Example

$$E_{31} = \emptyset$$

$$\begin{aligned} R_{31} = \{ & (x \cdot y) \cdot z \to x \cdot (y \cdot z),\ x \cdot e \to x,\ x \cdot x \to e, \\ & i(e) \to e,\ x_1 \cdot (i(x_1) \cdot x_2) \to e \cdot x_2, \\ & e \cdot x \to x,\ x_1 \cdot i(x_2) \to x_1 \cdot x_2,\ i(x) \to x \} \end{aligned}$$

Apply COLLAPSE and DELETE, we get rid of $i(e) \to e$:

$$E_{33} = \emptyset$$

$$\begin{aligned} R_{33} = \{ & (x \cdot y) \cdot z \to x \cdot (y \cdot z),\ x \cdot e \to x,\ x \cdot x \to e, \\ & x_1 \cdot (i(x_1) \cdot x_2) \to e \cdot x_2,\ e \cdot x \to x, \\ & x_1 \cdot i(x_2) \to x_1 \cdot x_2,\ i(x) \to x \} \end{aligned}$$

Proving by Ordered Completion: Example

$$
\begin{aligned}
E_{33} &= \emptyset \\
R_{33} &= \{(x \cdot y) \cdot z \to x \cdot (y \cdot z),\ x \cdot e \to x,\ x \cdot x \to e, \\
&\quad x_1 \cdot (i(x_1) \cdot x_2) \to e \cdot x_2,\ e \cdot x \to x, \\
&\quad x_1 \cdot i(x_2) \to x_1 \cdot x_2,\ i(x) \to x\}
\end{aligned}
$$

Applying COMPOSITION, we replace $x_1 \cdot (i(x_1) \cdot x_2) \to e \cdot x_2$ by $x_1 \cdot (i(x_1) \cdot x_2) \to x_2$:

$$
\begin{aligned}
E_{34} &= \emptyset \\
R_{34} &= \{(x \cdot y) \cdot z \to x \cdot (y \cdot z),\ x \cdot e \to x,\ x \cdot x \to e, \\
&\quad x_1 \cdot (i(x_1) \cdot x_2) \to x_2,\ e \cdot x \to x, \\
&\quad x_1 \cdot i(x_2) \to x_1 \cdot x_2,\ i(x) \to x\}
\end{aligned}
$$

Proving by Ordered Completion: Example

$$E_{34} = \emptyset$$

$$\begin{aligned} R_{34} = \{ & (x \cdot y) \cdot z \to x \cdot (y \cdot z),\ x \cdot e \to x,\ x \cdot x \to e, \\ & x_1 \cdot (i(x_1) \cdot x_2) \to x_2,\ e \cdot x \to x, \\ & x_1 \cdot i(x_2) \to x_1 \cdot x_2,\ i(x) \to x \} \end{aligned}$$

Applying SIMPLIFICATION and ORIENT, we replace $x_1 \cdot (i(x_1) \cdot x_2) \to x_2$ by $x_1 \cdot (x_1 \cdot x_2) \to x_2$:

$$E_{36} = \emptyset$$

$$\begin{aligned} R_{36} = \{ & (x \cdot y) \cdot z \to x \cdot (y \cdot z),\ x \cdot e \to x,\ x \cdot x \to e, \\ & x_1 \cdot (x_1 \cdot x_2) \to x_2,\ e \cdot x \to x, \\ & x_1 \cdot i(x_2) \to x_1 \cdot x_2,\ i(x) \to x \} \end{aligned}$$

Proving by Ordered Completion: Example

$$E_{36} = \emptyset$$

$$\begin{aligned} R_{36} = \{ & (x \cdot y) \cdot z \to x \cdot (y \cdot z),\ x \cdot e \to x,\ x \cdot x \to e, \\ & x_1 \cdot (i(x_1) \cdot x_2) \to x_2,\ e \cdot x \to x, \\ & x_1 \cdot i(x_2) \to x_1 \cdot x_2,\ i(x) \to x \} \end{aligned}$$

Apply DEDUCE to $(x \cdot y) \cdot z \to x \cdot (y \cdot z)$ and $x \cdot x \to e$ with the overlapping term $(x_1 \cdot x_2) \cdot (x_1 \cdot x_2)$, then ORIENT:

$$E_{37} = \emptyset$$

$$\begin{aligned} R_{37} = \{ & (x \cdot y) \cdot z \to x \cdot (y \cdot z),\ x \cdot e \to x,\ x \cdot x \to e, \\ & x_1 \cdot (x_1 \cdot x_2) \to x_2,\ e \cdot x \to x,\ x_1 \cdot i(x_2) \to x_1 \cdot x_2, \\ & i(x) \to x,\ x_1 \cdot (x_2 \cdot (x_1 \cdot x_2)) \to e \} \end{aligned}$$

Proving by Ordered Completion: Example

$$E_{37} = \emptyset$$

$$\begin{aligned} R_{37} = \{&(x \cdot y) \cdot z \to x \cdot (y \cdot z),\ x \cdot e \to x,\ x \cdot x \to e,\\ &x_1 \cdot (x_1 \cdot x_2) \to x_2,\ e \cdot x \to x,\ x_1 \cdot i(x_2) \to x_1 \cdot x_2,\\ &i(x) \to x,\ x_1 \cdot (x_2 \cdot (x_1 \cdot x_2)) \to e\} \end{aligned}$$

Apply DEDUCE to $x_1 \cdot (x_1 \cdot x_2) \to x_2$ and $x_1 \cdot (x_2 \cdot (x_1 \cdot x_2)) \to e$ with the overlapping term $x_1 \cdot (x_1 \cdot (x_2 \cdot (x_1 \cdot x_2)))$, then ORIENT:

$$E_{39} = \emptyset$$

$$\begin{aligned} R_{39} = \{&(x \cdot y) \cdot z \to x \cdot (y \cdot z),\ x \cdot e \to x,\ x \cdot x \to e,\\ &x_1 \cdot (x_1 \cdot x_2) \to x_2,\ e \cdot x \to x,\ x_1 \cdot i(x_2) \to x_1 \cdot x_2,\\ &i(x) \to x,\ x_1 \cdot (x_2 \cdot (x_1 \cdot x_2)) \to e,\ x_2 \cdot (x_1 \cdot x_2) \to x_1 \cdot e\} \end{aligned}$$

Proving by Ordered Completion: Example

$$E_{39} = \emptyset$$

$$\begin{aligned} R_{39} = \{&(x \cdot y) \cdot z \to x \cdot (y \cdot z),\ x \cdot e \to x,\ x \cdot x \to e, \\ &x_1 \cdot (x_1 \cdot x_2) \to x_2,\ e \cdot x \to x,\ x_1 \cdot i(x_2) \to x_1 \cdot x_2, \\ &i(x) \to x,\ x_1 \cdot (x_2 \cdot (x_1 \cdot x_2)) \to e,\ x_2 \cdot (x_1 \cdot x_2) \to x_1 \cdot e\} \end{aligned}$$

Apply COMPOSITION to $x_2 \cdot (x_1 \cdot x_2) \to x_1 \cdot e$ with $x \cdot e \to x$:

$$E_{40} = \emptyset$$

$$\begin{aligned} R_{40} = \{&(x \cdot y) \cdot z \to x \cdot (y \cdot z),\ x \cdot e \to x,\ x \cdot x \to e, \\ &x_1 \cdot (x_1 \cdot x_2) \to x_2,\ e \cdot x \to x,\ x_1 \cdot i(x_2) \to x_1 \cdot x_2, \\ &i(x) \to x,\ x_1 \cdot (x_2 \cdot (x_1 \cdot x_2)) \to e,\ x_2 \cdot (x_1 \cdot x_2) \to x_1\} \end{aligned}$$

Proving by Ordered Completion: Example

$$E_{41} = \emptyset$$

$$\begin{aligned} R_{41} = \{ & (x \cdot y) \cdot z \to x \cdot (y \cdot z),\ x \cdot e \to x,\ x \cdot x \to e, \\ & x_1 \cdot (x_1 \cdot x_2) \to x_2,\ e \cdot x \to x,\ x_1 \cdot i(x_2) \to x_1 \cdot x_2, \\ & i(x) \to x,\ x_1 \cdot (x_2 \cdot (x_1 \cdot x_2)) \to e,\ x_2 \cdot (x_1 \cdot x_2) \to x_1 \} \end{aligned}$$

Apply DEDUCE to $x_1 \cdot (x_1 \cdot x_2) \to x_2$ and $x_2 \cdot (x_1 \cdot x_2) \to x_1$ with the overlapping term $x_2 \cdot (x_2 \cdot (x_1 \cdot x_2))$:

$$E_{42} = \{ x_1 \cdot x_2 \doteq x_2 \cdot x_1 \}$$

$$\begin{aligned} R_{42} = \{ & (x \cdot y) \cdot z \to x \cdot (y \cdot z),\ x \cdot e \to x,\ x \cdot x \to e, \\ & x_1 \cdot (x_1 \cdot x_2) \to x_2,\ e \cdot x \to x,\ x_1 \cdot i(x_2) \to x_1 \cdot x_2, \\ & i(x) \to x,\ x_1 \cdot (x_2 \cdot (x_1 \cdot x_2)) \to e,\ x_2 \cdot (x_1 \cdot x_2) \to x_1 \cdot e \} \end{aligned}$$

Proving by Ordered Completion: Example

$$E_{42} = \{x_1 \cdot x_2 \doteq x_2 \cdot x_1\}$$

$$\begin{aligned} R_{42} = \{&(x \cdot y) \cdot z \to x \cdot (y \cdot z),\ x \cdot e \to x,\ x \cdot x \to e, \\ &x_1 \cdot (x_1 \cdot x_2) \to x_2,\ e \cdot x \to x,\ x_1 \cdot i(x_2) \to x_1 \cdot x_2, \\ &i(x) \to x,\ x_1 \cdot (x_2 \cdot (x_1 \cdot x_2)) \to e,\ x_2 \cdot (x_1 \cdot x_2) \to x_1 \cdot e\} \end{aligned}$$

The equation $x_1 \cdot x_2 \doteq x_2 \cdot x_1$ joins the goal $a \cdot b \doteq b \cdot a$. Hence, the goal is proved.

Superposition Calculus with Ordering and Selection

Back to general clauses.

$\doteq$ the only predicate.

A well-behaves selection function wrt $\succ$:

- If only positive literals are selected in C, then all maximal (wrt $\succ$) literals in C are selected.

Superposition Calculus with Ordering and Selection

Back to general clauses.

$\doteq$ the only predicate.

A well-behaves selection function wrt $\succ$:

- If only positive literals are selected in C, then all maximal (wrt $\succ$) literals in C are selected.

Comparison between literals. Assume $l \succeq r$ and $s \succeq t$. Then

- If $l \succ s$, then $l \not\doteq r \succ l \doteq r \succ s \not\doteq t \succ s \doteq t$.
- If $l = s$, then $l \not\doteq r \succ s \doteq t$ and $s \not\doteq t \succ l \doteq r$,

Superposition Calculus with Ordering and Selection

Superposition:

$$\frac{\underline{l \doteq r} \vee C \qquad \underline{s[l'] \doteq t} \vee D}{\sigma(s[r] \doteq t \vee C \vee D)},$$

$$\frac{\underline{l \doteq r} \vee C \qquad \underline{s[l'] \not\doteq t} \vee D}{\sigma(s[r] \not\doteq t \vee C \vee D)}$$

Superposition Calculus with Ordering and Selection

Superposition:

$$\frac{\underline{l \doteq r} \lor C \qquad \underline{s[l'] \doteq t} \lor D}{\sigma(s[r] \doteq t \lor C \lor D)},$$

$$\frac{\underline{l \doteq r} \lor C \qquad \underline{s[l'] \not\doteq t} \lor D}{\sigma(s[r] \not\doteq t \lor C \lor D)}$$

where

- $\sigma = mgu(l, l')$,
- $l' \notin \mathcal{V}$,
- $\sigma(r) \not\succeq \sigma(l)$,
- $\sigma(t) \not\succeq \sigma(s[l'])$.

Superposition Calculus with Ordering and Selection

Equality resolution:

$$\frac{\underline{s \doteq t} \lor C}{\sigma(C)}, \qquad \text{where } \sigma = mgu(s,t).$$

Equality factoring:

$$\frac{\underline{l \doteq r} \lor l' \doteq r' \lor C}{\sigma(l \doteq r \lor r \not\doteq r' \lor C)},$$

Superposition Calculus with Ordering and Selection

Equality resolution:

$$\frac{\underline{s \doteq t} \lor C}{\sigma(C)}, \qquad \text{where } \sigma = mgu(s, t).$$

Equality factoring:

$$\frac{\underline{l \doteq r} \lor l' \doteq r' \lor C}{\sigma(l \doteq r \lor r \not\doteq r' \lor C)},$$

where

- $\sigma = mgu(l, l')$, $\sigma(r) \not\succeq \sigma(l)$, $\sigma(r') \not\succeq \sigma(l')$, $\sigma(r') \not\succeq \sigma(r)$,

The superposition calculus with ordering and selection is refutationally complete.