Term Rewriting Systems

Franz Baader
Theoretical Computer Science
TU Dresden
Germany

1. Motivation and basic definitions and results.
2. Equational Problems: the word problem and term rewriting
3. Termination of term rewriting systems
4. Confluence of term rewriting systems
5. Completion of term rewriting systems

Dresden

Termination

definition and undecidability

The TRS R is terminating iff $\to_R$ is terminating, i.e., there is no infinite reduction chain

$$t_0 \to_R t_1 \to_R t_2 \to_R t_3 \to_R \cdots$$

Theorem (undecidability of termination)

> The following problem is in general undecidable:
>
> Given: A finite TRS R.
>
> Question: Is R terminating or not?

Proof by reduction of the uniform halting problem for Turing machines.

Dresden

A decidable special case

right-ground TRS

A term rewriting system R is called right-ground iff the right-hand sides of rules in R are ground terms, i.e. do not contain variables.

Lemma

> Let R be a finite right-ground TRS. Then the following statements are equivalent:
>
> 1. R does not terminate.
> 2. There exist a rule $l \to r \in R$ and a term t such that $r \xrightarrow{+}_R t$ and t contains r as a subterm.

Proof:

$(2 \Rightarrow 1)$ is trivial: if $r \xrightarrow{+}_R t$ and $t|_p = r$, then

$$r \xrightarrow{+}_R t = t[r]_p \xrightarrow{+}_R t[t]_p = t[t[r]_p]_p \xrightarrow{+}_R \cdots$$

Dresden

$(1 \Rightarrow 2)$ by induction on the cardinality of R.

If R is empty, then (1) is trivially false.

$|R| > 0$ and consider an infinite reduction

$$t_1 \to_R t_2 \to_R t_3 \to_R \cdots$$

(i) Without loss of generality, we may assume that at least one of these reductions occurs at position ϵ.

(ii) This means that there exist an index i, a rule $l \to r \in R$, and a substitution σ such that $t_i = \sigma(l)$ and $t_{i+1} = \sigma(r) = r$.

Consequently, there is an infinite reduction

$$r \to_R t_{i+2} \to_R t_{i+3} \to_R \cdots$$

- Case a: the rule $l \to r$ is not used.

  $R - \{l \to r\}$ does not terminate. Apply induction!

- Case b: the rule $l \to r$ is used.

  There exists $j \geq 2$ such that r occurs in t_{i+j}, which shows (2).

Dresden

Theorem

For finite right-ground term rewriting systems, termination is a decidable property.

Proof:

Consider all right-hand sides $r_1, \ldots, r_n$, and simultaneously generate all reduction sequences of increasing length starting with these right-hand sides:

Either one detects a cycle as described in the lemma (R is not terminating),

or the process of generating these reductions terminates (R is terminating).

Dresden

Reduction orders

a tool for proving termination

Goal: define a class of strict orders $>$ on terms such that

$$l > r \quad \text{for all} \quad (l \to r) \in R$$

implies termination of R.

Definition

A strict order $>$ on $T(\Sigma, V)$ is called a reduction order iff it is

1. compatible with Σ-operations:
$$s_1 > s_2 \;\Rightarrow f(\ldots, s_1, \ldots) > f(\ldots, s_2, \ldots)$$
2. closed under substitutions:
$$s_1 > s_2 \;\Rightarrow\; \sigma(s_1) > \sigma(s_2)$$
3. well-founded

Dresden

Example

The strict order $>$ on $T(\Sigma, V)$ that is defined by

$s > t$ iff $|s| > |t|$

is well-founded and compatible with Σ-operations.

It is not a reduction order since it need not be closed under substitutions:

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

but for the substitution $\sigma := \{y \mapsto f(x,x)\}$ we have

$$\begin{aligned} |\sigma(f(f(x,x),y))| &= |f(f(x,x),f(x,x))| = 7, \\ |\sigma(f(y,y))| &= |f(f(x,x),f(x,x))| = 7. \end{aligned}$$

In contrast:

$$s > t \text{ iff } |s| > |t| \text{ and, for all } x \in V,\ |s|_x \geq |t|_x$$

defines a reduction order.

Dresden

Theorem

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

Proof:

(1) Assume that R terminates.

In this case, $\xrightarrow{+}_R$ itself is a reduction order,

which obviously satisfies $l \xrightarrow{+}_R r$ for all $l \to r \in R$.

(2) $l > r$ implies $t[\sigma(l)]_p > t[\sigma(r)]_p$.

Thus $s_1 \to_R s_2$ implies $s_1 > s_2$,

and well-foundedness of $>$ shows that there cannot be an infinite chain

$$s_1 \to_R s_2 \to_R s_3 \cdots$$

Dresden

Example

The TRS

$$R := \{f(x, f(y,x)) \to f(x,y),\;\; f(x,x) \to x\}$$

is terminating.

For the reduction order defined as

$$s > t \text{ iff } |s| > |t| \text{ and, for all } x \in V, |s|_x \geq |t|_x$$

we have

$$f(x, f(y,x)) > f(x,y),\;\; f(x,x) > x.$$

The TRS

$$R \cup \{f(f(x,y),z) \to f(x, f(y,z))\}$$

is also terminating, but this cannot be shown with the above reduction order since

$$f(f(x,y),z) \not> f(x, f(y,z)).$$

Dresden

Methods for constructing reduction orders:

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

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

Dresden

Polynomial orders

interpret function symbols by polynomials

Definition (polynomial interpretation)

A polynomial interpretation $\mathcal{P}$ of a signature Σ is defined by

- a non-empty carrier set $A \subseteq \mathbb{N} - \{0\}$,
- polynomials $P_f(X_1, \ldots, X_n) \in \mathbb{N}[X_1, \ldots, X_n]$ associated with every $f \in \Sigma^{(n)}$ such that $a_1, \ldots, a_n \in A$ implies $P_f(a_1, \ldots, a_n) \in A$.

Example

$\Sigma = \{\oplus, \odot\}$ consists of two binary function symbols, and $A := \mathbb{N} - \{0, 1\}$.

$$P_\oplus := 2X + Y + 1$$
$$P_\odot := XY$$

Dresden

A given polynomial interpretation also associates a polynomial P_t with every term t:

The polynomial interpretation from above associates the term $t = x \odot (x \oplus y)$ with the polynomial

$$\begin{aligned} P_t &= P_\odot(X, P_\oplus(X,Y)) \\ &= X(2X + Y + 1) \\ &= 2X^2 + XY + X. \end{aligned}$$

$$P_\oplus := 2X + Y + 1 \qquad P_\odot := XY$$

Definition (polynomial order)

The polynomial interpretation $\mathcal{P}$ of the signature Σ induces the following polynomial order $>_\mathcal{P}$ on $T(\Sigma, V)$:

$$s >_\mathcal{P} t \text{ iff } P_s(a_1, \ldots, a_n) > P_t(a_1, \ldots, a_n) \text{ for all } a_1, \ldots, a_n \text{ in } A$$

Dresden

Definition (Monotony)

We call a polynomial $P(X_1, \ldots, X_n) \in \mathbb{N}[X_1, \ldots, X_n]$ a monotone polynomial iff it depends on all its indeterminates.

A monotone polynomial interpretation is a polynomial interpretation in which all function symbols are associated with monotone polynomials.

$P_\oplus(X,Y) = 2X + Y + 1$

$P_\odot(X,Y) = XY$

~~$Q(X,Y) = X^2$~~

Theorem

The relation $>_\mathcal{P}$ induced by a monotone polynomial interpretation $\mathcal{P}$ is a reduction order.

Dresden

Example

The polynomial order induced by

$A := \mathbb{N} - \{0,1\}$, $P_\oplus = 2X + Y + 1$, and $P_\odot = XY$

can be used to show termination of

$$R := \{x \odot (y \oplus z) \rightarrow (x \odot y) \oplus (x \odot z)\}$$

The polynomial P_l associated with $l := x \odot (y \oplus z)$ is

$$X(2Y + Z + 1) = 2XY + XZ + X,$$

and the polynomial P_r associated with $r := (x \odot y) \oplus (x \odot z)$ is

$$2XY + XZ + 1.$$

Since all elements of A are greater than 1, we have $l >_\mathcal{P} r$.

Dresden

Theorem

The following problem is in general undecidable:

Given: A polynomial interpretation $\mathcal{P}$ and terms s, t.

Question: Does $s >_\mathcal{P} t$ hold or not?

This is an easy consequence of the undecidability of Hilbert's 10th Problem :

Given: A polynomial $P \in \mathbb{Z}[X_1, \ldots, X_n]$ in n indeterminates with integer coefficients.

Question: Is there an n-tuple of non-negative integers for which the polynomial P is 0?

Dresden

Simplification orders

construct reduction orders > for which "s > t?" is decidable

Definition

A strict order $>$ on $T(\Sigma, V)$ is called a simplification order iff it

1. is compatible with Σ-operations:

$$s_1 > s_2 \;\Rightarrow f(\ldots, s_1, \ldots) > f(\ldots, s_2, \ldots)$$

2. is closed under substitutions:

$$s_1 > s_2 \;\Rightarrow\; \sigma(s_1) > \sigma(s_2)$$

3. satisfies the subterm property:

for all terms $t \in T(\Sigma, V)$ and all positions $p \in \mathcal{P}os(t) - \{\epsilon\}$,

$$t > t|_p$$

In the context of the other two properties, the subterm property can be replaced by the following simpler property:

$$f(x_1, \ldots, x_i, \ldots, x_n) > x_i$$

Dresden

Theorem

Let Σ be a finite signature.

Every simplification order on $T(\Sigma, V)$ is a reduction order.

The proof of this theorem depends on Kruskal's theorem for the homeomorphic embedding relation.

Definition

The homeomorphic embedding $\trianglerighteq_{emb}$ is defined as the reduction relation $\xrightarrow{*}_{R_{emb}}$ induced by the rewrite system

$$R_{emb} := \{f(x_1, \ldots, x_n) \to x_i \mid n \geq 1, f \in \Sigma^{(n)}, 1 \leq i \leq n\}.$$

Since R_{emb} is obviously terminating, $\trianglerighteq_{emb}$ is a well-founded partial order.

Well-foundedness of $\trianglerighteq_{emb}$ is not enough to prove the theorem!

Definition

A partial order $\succeq$ on a set A is a well-partial-order (wpo) iff for every infinite sequence

$$a_1, a_2, a_3, \ldots$$

of elements of A there exist indices $i < j$ such that $a_i \preceq a_j$.

In addition to prohibiting infinite descending chains, wpos also disallow infinite anti-chains, i.e., infinite sets of incomparable elements.

Theorem (Kruskal)

If Σ and X are finite, then $\trianglerighteq_{emb}$ is a wpo on $T(\Sigma, X)$.

Lemma

Let $>$ be a simplification order on $T(\Sigma, V)$, and let $s, t \in T(\Sigma, V)$ be terms. Then

$$s \trianglerighteq_{emb} t \text{ implies } s \geq t.$$

Proof:

Since $>$ satisfies the subterm property, we have

$$f(x_1, \ldots, x_i, \ldots, x_n) > x_i$$

for all $n \geq 1, f \in \Sigma^{(n)}, 1 \leq i \leq n$.

This shows $R_{emb} \subseteq >$.

Since $\geq$ is reflexive and transitive as well as closed under substitutions and compatible with Σ-operations, this implies

$$\trianglerighteq_{emb} = \xrightarrow{*}_{R_{emb}} \subseteq \geq.$$

Theorem

Let Σ be a finite signature.

Every simplification order on $T(\Sigma, V)$ is a reduction order.

Proof:

Assume that $>$ is a simplification order on $T(\Sigma, V)$, and that

$$t_1 > t_2 > t_3 > \cdots$$

is an infinite chain in $T(\Sigma, V)$.

1. For the finite set $X := \mathcal{V}ar(t_1)$, all terms in the sequence $t_1, t_2, t_3, \ldots$ belong to $T(\Sigma, X)$.

   Assume $x \in \mathcal{V}ar(t_i) - X$ and let $\sigma := \{x \mapsto t_1\}$.

   Then $t_1 = \sigma(t_1) > \sigma(t_i) \geq t_1$.

2. Since Σ and X are finite, Kruskal's Theorem implies that there exist $i < j$ such that $t_i \trianglelefteq_{emb} t_j$.

   The lemma yields $t_i \leq t_j$, which is a contradiction since we know that $t_i > t_{i+1} > \cdots > t_j$.

Definition (lexicographic path order)

Let Σ be a finite signature and $>$ be a strict order on Σ.

The lexicographic path order on $T(\Sigma, V)$ induced by $>$ is defined as follows:

$s >_{lpo} t$ iff

(LPO1) $t \in \mathcal{V}ar(s)$ and $s \neq t$, or

(LPO2) $s = f(s_1, \dots, s_m), t = g(t_1, \dots, t_n)$, and

(LPO2a) there exists $i, 1 \leq i \leq m$, with $s_i \geq_{lpo} t$, or

(LPO2b) $f > g$ and $s >_{lpo} t_j$ for all $j, 1 \leq j \leq n$, or

(LPO2c) $f = g$, $s >_{lpo} t_j$ for all $j, 1 \leq j \leq n$, and there exists $i, 1 \leq i \leq m$, such that $s_1 = t_1, \dots, s_{i-1} = t_{i-1}$ and $s_i >_{lpo} t_i$.

Dresden

Example

$\Sigma = \{f, i, e\}$, where f is binary, i is unary, and e is a constant.

$$i > f > e$$

- $f(x, e) >_{lpo} x$ by (LPO1).
- $i(e) >_{lpo} e$ by (LPO2a)
  since we have $e \geq_{lpo} e$.
- $i(f(x, y)) >_{lpo} f(i(y), i(x))$ by (LPO2b)
  since $i > f$ and, by (LPO2c),
  $i(f(x, y)) >_{lpo} i(y)$ and $i(f(x, y)) >_{lpo} i(x)$.
  The preconditions for case (LPO2c) are satisfied since we have
  $i(f(x, y)) >_{lpo} y$, $i(f(x, y)) >_{lpo} x$ and $f(x, y) >_{lpo} y$, $f(x, y) >_{lpo} x$
  by (LPO1).

Dresden

Theorem

For any strict order $>$ on Σ, the induced lexicographic path order $>_{lpo}$ is a simplification order on $T(\Sigma, V)$.

Application of this method for showing termination can be automated:

Proposition

Let Σ be a finite signature, $s, t \in T(\Sigma, V)$, and R a finite term rewriting system over $T(\Sigma, V)$.

1. For a given lexicographic path order, $s >_{lpo} t$ can be decided in time polynomial in the size of s, t.

2. The question of whether termination of R can be shown using some lexicographic path order on $T(\Sigma, V)$ is an NP-complete problem.

Dresden