4.4 Critical Pairs

Showing local confluence (Sketch):

Problem: If \( t_1 \leftarrow_E t_0 \rightarrow_E t_2 \), does there exist a term \( s \) such that \( t_1 \rightarrow_E s \leftarrow_E t_2 \)?

If the two rewrite steps happen in different subtrees (disjoint redexes): yes.

If the two rewrite steps happen below each other (overlap at or below a variable position): yes.

If the left-hand sides of the two rules overlap at a non-variable position: needs further investigation.

Question:
Are there rewrite rules \( l_1 \rightarrow r_1 \) and \( l_2 \rightarrow r_2 \) such that some subterm \( l_1/p \) and \( l_2 \) have a common instance \( (l_1/p)\sigma_1 = l_2\sigma_2 \)?

Observation:
If we assume w.o.l.o.g. that the two rewrite rules do not have common variables, then only a single substitution is necessary: \( (l_1/p)\sigma = l_2\sigma \).

Further observation:
The mgu of \( l_1/p \) and \( l_2 \) subsumes all unifiers \( \sigma \) of \( l_1/p \) and \( l_2 \).

Let \( l_i \rightarrow r_i \ (i = 1, 2) \) be two rewrite rules in a TRS \( R \) whose variables have been renamed such that \( \text{var}(l_1) \cap \text{var}(l_2) = \emptyset \). (Remember that \( \text{var}(l_i) \supseteq \text{var}(r_i) \).)

Let \( p \in \text{pos}(l_1) \) be a position such that \( l_1/p \) is not a variable and \( \sigma \) is an mgu of \( l_1/p \) and \( l_2 \).

Then \( r_1\sigma \leftarrow l_1\sigma \rightarrow (l_1\sigma)[r_2\sigma]_p \).

\( \langle r_1\sigma, (l_1\sigma)[r_2\sigma]_p \rangle \) is called a critical pair of \( R \).

The critical pair is joinable (or: converges), if \( r_1\sigma \downarrow_R (l_1\sigma)[r_2\sigma]_p \).

**Theorem 4.18 (“Critical Pair Theorem”)** A TRS \( R \) is locally confluent if and only if all its critical pairs are joinable.

**Proof.** “only if”: obvious, since joinability of a critical pair is a special case of local confluence.

“if”: Suppose \( s \) rewrites to \( t_1 \) and \( t_2 \) using rewrite rules \( l_i \rightarrow r_i \in R \) at positions \( p_i \in \text{pos}(s) \), where \( i = 1, 2 \). Without loss of generality, we can assume that the two rules are variable disjoint, hence \( s/p_i = l_i\theta \) and \( t_i = s[r_i\theta]_{p_i} \).

We distinguish between two cases: Either \( p_1 \) and \( p_2 \) are in disjoint subtrees \( (p_1 \parallel p_2) \), or one is a prefix of the other (w.o.l.o.g., \( p_1 \leq p_2 \)).
Case 1: \( p_1 \parallel p_2 \).

Then \( s = s[l_1\theta]_{p_1}[l_2\theta]_{p_2} \), and therefore \( t_1 = s[r_1\theta]_{p_1}[l_2\theta]_{p_2} \) and \( t_2 = s[l_1\theta]_{p_1}[r_2\theta]_{p_2} \).

Let \( t_0 = s[r_1\theta]_{p_1}[r_2\theta]_{p_2} \). Then clearly \( t_1 \rightarrow_R t_0 \) using \( l_2 \rightarrow r_2 \) and \( t_2 \rightarrow_R t_0 \) using \( l_1 \rightarrow r_1 \).

Case 2: \( p_1 \leq p_2 \).

Case 2.1: \( p_2 = p_1q_1q_2 \), where \( l_1/q_1 \) is some variable \( x \).

In other words, the second rewrite step takes place at or below a variable in the first rule. Suppose that \( x \) occurs \( m \) times in \( l_1 \) and \( n \) times in \( r_1 \) (where \( m \geq 1 \) and \( n \geq 0 \)).

Then \( t_1 \rightarrow^*_{R} t_0 \) by applying \( l_2 \rightarrow r_2 \) at all positions \( p_1q'q_2 \), where \( q' \) is a position of \( x \) in \( r_1 \).

Conversely, \( t_2 \rightarrow^*_{R} t_0 \) by applying \( l_2 \rightarrow r_2 \) at all positions \( p_1qq_2 \), where \( q \) is a position of \( x \) in \( l_1 \) different from \( q_1 \), and by applying \( l_1 \rightarrow r_1 \) at \( p_1 \) with the substitution \( \theta' \), where \( \theta = \theta[x \mapsto (x\theta)[r_2\theta]_{p_2}] \).

Case 2.2: \( p_2 = p_1p \), where \( p \) is a non-variable position of \( l_1 \).

Then \( s/p_2 = l_2\theta \) and \( s/p_2 = (s/p_1)/p = (l_1\theta)/p = (l_1/p)\theta \), so \( \theta \) is a unifier of \( l_2 \) and \( l_1/p \).

Let \( \sigma \) be the mgu of \( l_2 \) and \( l_1/p \), then \( \theta = \tau \circ \sigma \) and \( \langle r_1\sigma, (l_1\sigma)[r_2\sigma]_p \rangle \) is a critical pair.

By assumption, it is joinable, so \( r_1\sigma \rightarrow^*_{R} v \leftarrow^*_{R} (l_1\sigma)[r_2\sigma]_p \).

Consequently, \( t_1 = s[r_1\theta]_{p_1} = s[r_1\sigma\tau]_{p_1} \rightarrow^*_{R} s[v\tau]_{p_1} \) and \( t_2 = s[r_2\theta]_{p_2} = s[(l_1\theta)[r_2\theta]_{p}]_{p_1} = s[(l_1\sigma)[r_2\sigma\tau]_p]_{p_1} = s[(l_1\sigma)[r_2\sigma\tau]_p]_{p_1} \rightarrow^*_{R} s[v\tau]_{p_1} \).

This completes the proof of the Critical Pair Theorem. \( \square \)

Note: Critical pairs between a rule and (a renamed variant of) itself must be considered – except if the overlap is at the root (i.e., \( p = \varepsilon \)).

Corollary 4.19 A terminating TRS \( R \) is confluent if and only if all its critical pairs are joinable.

Proof. By Newman’s Lemma and the Critical Pair Theorem. \( \square \)

Corollary 4.20 For a finite terminating TRS, confluence is decidable.

Proof. For every pair of rules and every non-variable position in the first rule there is at most one critical pair \( \langle u_1, u_2 \rangle \).

Reduce every \( u_i \) to some normal form \( u_i' \). If \( u_i' = u_i' \) for every critical pair, then \( R \) is confluent, otherwise there is some non-confluent situation \( u_i' \leftarrow^*_{R} u_1 \leftarrow^*_{R} s \rightarrow^*_{R} u_2 \rightarrow^*_{R} u_i' \). \( \square \)
4.5 Termination

Termination problems:

Given a finite TRS $R$ and a term $t$, are all $R$-reductions starting from $t$ terminating?

Given a finite TRS $R$, are all $R$-reductions terminating?

Proposition 4.21 Both termination problems for TRSs are undecidable in general.

Proof. Encode Turing machines using rewrite rules and reduce the (uniform) halting problems for TMs to the termination problems for TRSs. □

Consequence:
Decidable criteria for termination are not complete.

Reduction Orderings

Goal:

Given a finite TRS $R$, show termination of $R$ by looking at finitely many rules $l \to r \in R$, rather than at infinitely many possible replacement steps $s \to_R s'$.

A binary relation $\sqsubseteq$ over $T_\Sigma(X)$ is called compatible with $\Sigma$-operations, if $s \sqsubseteq s'$ implies $f(t_1, \ldots, s, \ldots, t_n) \sqsubseteq f(t_1, \ldots, s', \ldots, t_n)$ for all $f \in \Omega$ and $s, s', t_i \in T_\Sigma(X)$.

Lemma 4.22 The relation $\sqsubseteq$ is compatible with $\Sigma$-operations, if and only if $s \sqsubseteq s'$ implies $t[s]_p \sqsubseteq t[s']_p$ for all $s, s', t \in T_\Sigma(X)$ and $p \in \text{pos}(t)$.

Note: compatible with $\Sigma$-operations = compatible with contexts.

A binary relation $\sqsubseteq$ over $T_\Sigma(X)$ is called stable under substitutions, if $s \sqsubseteq s'$ implies $ss \sqsubseteq ss'$ for all $s, s' \in T_\Sigma(X)$ and substitutions $\sigma$.

A binary relation $\sqsubseteq$ is called a rewrite relation, if it is compatible with $\Sigma$-operations and stable under substitutions.

Example: If $R$ is a TRS, then $\to_R$ is a rewrite relation.

A strict partial ordering over $T_\Sigma(X)$ that is a rewrite relation is called rewrite ordering.

A well-founded rewrite ordering is called reduction ordering.

Theorem 4.23 A TRS $R$ terminates if and only if there exists a reduction ordering $\succ$ such that $l \succ r$ for every rule $l \to r \in R$. 92
Proof. “if”: $s \rightarrow_R s'$ if and only if $s = t[l\sigma]_p$, $s' = t[r\sigma]_p$. If $l \succ r$, then $l\sigma \succ r\sigma$ and therefore $t[l\sigma]_p \succ t[r\sigma]_p$. This implies $\rightarrow_R \subseteq \succ$. Since $\succ$ is a well-founded ordering, $\rightarrow_R$ is terminating.

“only if”: Define $\succ = \rightarrow^+_R$. If $\rightarrow_R$ is terminating, then $\succ$ is a reduction ordering.  

The Interpretation Method

Proving termination by interpretation:

Let $\mathcal{A}$ be a $\Sigma$-algebra; let $\succ$ be a well-founded strict partial ordering on its universe.

Define the ordering $\succ_{\mathcal{A}}$ over $T_\Sigma(X)$ by $s \succ_{\mathcal{A}} t$ iff $\mathcal{A}(\beta)(s) \succ \mathcal{A}(\beta)(t)$ for all assignments $\beta : X \rightarrow U_A$.

Is $\succ_{\mathcal{A}}$ a reduction ordering?

Lemma 4.24 $\succ_{\mathcal{A}}$ is stable under substitutions.

Proof. Let $s \succ_{\mathcal{A}} s'$, that is, $\mathcal{A}(\beta)(s) \succ \mathcal{A}(\beta)(s')$ for all assignments $\beta : X \rightarrow U_A$. Let $\sigma$ be a substitution. We have to show that $\mathcal{A}(\gamma)(s\sigma) \succ \mathcal{A}(\gamma)(s'\sigma)$ for all assignments $\gamma : X \rightarrow U_A$. Choose $\beta = \gamma \circ \sigma$, then by the substitution lemma, $\mathcal{A}(\gamma)(s\sigma) = \mathcal{A}(\beta)(s) \succ \mathcal{A}(\beta)(s') = \mathcal{A}(\gamma)(s'\sigma)$. Therefore $s\sigma \succ_{\mathcal{A}} s'\sigma$.  

A function $F : U^n_A \rightarrow U_A$ is called monotone (with respect to $\succ$), if $a \succ a'$ implies $F(b_1, \ldots, a, \ldots, b_n) \succ F(b_1, \ldots, a', \ldots, b_n)$ for all $a, a', b_i \in U_A$.

Lemma 4.25 If the interpretation $f_{\mathcal{A}}$ of every function symbol $f$ is monotone w. r. t. $\succ$, then $\succ_{\mathcal{A}}$ is compatible with $\Sigma$-operations.

Proof. Let $s \succ_{\mathcal{A}} s'$, that is, $\mathcal{A}(\beta)(s) \succ \mathcal{A}(\beta)(s')$ for all $\beta : X \rightarrow U_A$. Let $\beta : X \rightarrow U_A$ be an arbitrary assignment. Then

$$\mathcal{A}(\beta)(f(t_1, \ldots, s, \ldots, t_n)) = f_{\mathcal{A}}(\mathcal{A}(\beta)(t_1), \ldots, \mathcal{A}(\beta)(s), \ldots, \mathcal{A}(\beta)(t_n))$$

$$\succ f_{\mathcal{A}}(\mathcal{A}(\beta)(t_1), \ldots, \mathcal{A}(\beta)(s'), \ldots, \mathcal{A}(\beta)(t_n))$$

$$= \mathcal{A}(\beta)(f(t_1, \ldots, s', \ldots, t_n))$$

Therefore $f(t_1, \ldots, s, \ldots, t_n) \succ_{\mathcal{A}} f(t_1, \ldots, s', \ldots, t_n)$.  

Theorem 4.26 If the interpretation $f_{\mathcal{A}}$ of every function symbol $f$ is monotone w. r. t. $\succ$, then $\succ_{\mathcal{A}}$ is a reduction ordering.

Proof. By the previous two lemmas, $\succ_{\mathcal{A}}$ is a rewrite relation. If there were an infinite chain $s_1 \succ_{\mathcal{A}} s_2 \succ_{\mathcal{A}} \ldots$, then it would correspond to an infinite chain $\mathcal{A}(\beta)(s_1) \succ \mathcal{A}(\beta)(s_2) \succ \ldots$ (with $\beta$ chosen arbitrarily). Thus $\succ_{\mathcal{A}}$ is well-founded. Irreflexivity and transitivity are proved similarly.  

93
Polynomial Orderings

Polynomial orderings:

Instance of the interpretation method:

The carrier set $U_A$ is some subset of the natural numbers.

To every function symbol $f$ with arity $n$ we associate a polynomial $P_f(X_1, \ldots, X_n) \in \mathbb{N}[X_1, \ldots, X_n]$ with coefficients in $\mathbb{N}$ and indeterminates $X_1, \ldots, X_n$. Then we define $f_A(a_1, \ldots, a_n) = P_f(a_1, \ldots, a_n)$ for $a_i \in U_A$.

Requirement 1:

If $a_1, \ldots, a_n \in U_A$, then $f_A(a_1, \ldots, a_n) \in U_A$. (Otherwise, $A$ would not be a $\Sigma$-algebra.)

Requirement 2:

$f_A$ must be monotone (w.r.t. $\succ$).

From now on:

$U_A = \{ n \in \mathbb{N} \mid n \geq 2 \}$.

If $\text{arity}(f) = 0$, then $P_f$ is a constant $\geq 2$.

If $\text{arity}(f) = n \geq 1$, then $P_f$ is a polynomial $P(X_1, \ldots, X_n)$, such that every $X_i$ occurs in some monomial with exponent at least 1 and non-zero coefficient.

$\Rightarrow$ Requirements 1 and 2 are satisfied.

The mapping from function symbols to polynomials can be extended to terms: A term $t$ containing the variables $x_1, \ldots, x_n$ yields a polynomial $P_t$ with indeterminates $X_1, \ldots, X_n$ (where $X_i$ corresponds to $\beta(x_i)$).

Example:

$\Omega = \{ b, f, g \}$ with $\text{arity}(b) = 0$, $\text{arity}(f) = 1$, $\text{arity}(g) = 3$,

$U_A = \{ n \in \mathbb{N} \mid n \geq 2 \}$,

$P_b = 3$, $P_f(X_1) = X_1^2$, $P_g(X_1, X_2, X_3) = X_1 + X_2X_3$.

Let $t = g(f(b), f(x), y)$, then $P_t(X, Y) = 9 + X^2Y$.

If $P, Q$ are polynomials in $\mathbb{N}[X_1, \ldots, X_n]$, we write $P > Q$ if $P(a_1, \ldots, a_n) > Q(a_1, \ldots, a_n)$ for all $a_1, \ldots, a_n \in U_A$.

Clearly, $l \succ_A r$ iff $P_l > P_r$.

Question: Can we check $P_l > P_r$ automatically?
Hilbert’s 10th Problem:

Given a polynomial \( P \in \mathbb{Z}[X_1, \ldots, X_n] \) with integer coefficients, is \( P = 0 \) for some \( n \)-tuple of natural numbers?

**Theorem 4.27** Hilbert’s 10th Problem is undecidable.

**Proposition 4.28** Given a polynomial interpretation and two terms \( l, r \), it is undecidable whether \( P_l > P_r \).

**Proof.** By reduction of Hilbert’s 10th Problem. \( \square \)

One possible solution:

Test whether \( P_l(a_1, \ldots, a_n) > P_r(a_1, \ldots, a_n) \) for all \( a_1, \ldots, a_n \in \{ x \in \mathbb{R} \mid x \geq 2 \} \).

This is decidable (but very slow). Since \( U_A \subseteq \{ x \in \mathbb{R} \mid x \geq 2 \} \), it implies \( P_l > P_r \).

Another solution (Ben Cherifa and Lescanne):

Consider the difference \( P_l(X_1, \ldots, X_n) - P_r(X_1, \ldots, X_n) \) as a polynomial with real coefficients and apply the following inference system to it to show that it is positive for all \( a_1, \ldots, a_n \in U_A \):

\[
P \Rightarrow_{BCL} \top,
\]

if \( P \) contains at least one monomial with a positive coefficient and no monomial with a negative coefficient.

\[
P + cX_1^{p_1} \cdots X_n^{p_n} - dX_1^{q_1} \cdots X_n^{q_n} \Rightarrow_{BCL} P + c'X_1^{p_1} \cdots X_n^{p_n},
\]

if \( c, d > 0, p_i \geq q_i \) for all \( i \), and \( c' = c - d \cdot 2^{(q_1-p_1)+\cdots+(q_n-p_n)} \geq 0 \).

\[
P + cX_1^{p_1} \cdots X_n^{p_n} - dX_1^{q_1} \cdots X_n^{q_n} \Rightarrow_{BCL} P - d'X_1^{q_1} \cdots X_n^{q_n},
\]

if \( c, d > 0, p_i \geq q_i \) for all \( i \), and \( d' = d - c \cdot 2^{(p_1-q_1)+\cdots+(p_n-q_n)} > 0 \).

**Lemma 4.29** If \( P \Rightarrow_{BCL} P' \), then \( P(a_1, \ldots, a_n) \geq P'(a_1, \ldots, a_n) \) for all \( a_1, \ldots, a_n \in U_A \).

**Proof.** Follows from the fact that \( a_i \in U_A \) implies \( a_i \geq 2 \). \( \square \)

**Proposition 4.30** If \( P \Rightarrow_{\overline{BCL}} \top \), then \( P(a_1, \ldots, a_n) > 0 \) for all \( a_1, \ldots, a_n \in U_A \).

95
Simplification Orderings

The proper subterm ordering $\triangleright$ is defined by $s \triangleright t$ if and only if $s/p = t$ for some position $p \neq \varepsilon$ of $s$.

A rewrite ordering $\succ$ over $T_\Sigma(X)$ is called simplification ordering, if it has the subterm property: $s \triangleright t$ implies $s \succ t$ for all $s, t \in T_\Sigma(X)$.

Example:

Let $R_{\text{emb}}$ be the rewrite system $R_{\text{emb}} = \{ f(x_1, \ldots, x_n) \rightarrow x_i \mid f \in \Omega, 1 \leq i \leq n = \text{arity}(f) \}$.

Define $\triangleright_{\text{emb}} = \rightarrow^+_{R_{\text{emb}}}$ and $\succeq_{\text{emb}} = \rightarrow^*_R_{\text{emb}}$ ("homeomorphic embedding relation").

$\triangleright_{\text{emb}}$ is a simplification ordering.

Lemma 4.31 If $\succ$ is a simplification ordering, then $s \triangleright_{\text{emb}} t$ implies $s \succ t$ and $s \succeq_{\text{emb}} t$ implies $s \succeq t$.

Proof. Since $\succ$ is transitive and $\succeq$ is transitive and reflexive, it suffices to show that $s \rightarrow_{R_{\text{emb}}} t$ implies $s \succ t$. By definition, $s \rightarrow_{R_{\text{emb}}} t$ if and only if $s = s[l[\sigma]]$ and $t = s[r[\sigma]]$ for some rule $l \rightarrow r \in R_{\text{emb}}$. Obviously, $l \triangleright r$ for all rules in $R_{\text{emb}}$, hence $l \triangleright r$. Since $\succ$ is a rewrite relation, $s = s[l[\sigma]] \succ s[r[\sigma]] = t$. \qed

Goal:

Show that every simplification ordering is well-founded (and therefore a reduction ordering).

Note: This works only for finite signatures!

To fix this for infinite signatures, the definition of simplification orderings and the definition of embedding have to be modified.

Theorem 4.32 ("Kruskal’s Theorem") Let $\Sigma$ be a finite signature, let $X$ be a finite set of variables. Then for every infinite sequence $t_1, t_2, t_3, \ldots$ there are indices $j > i$ such that $t_j \succeq_{\text{emb}} t_i$. ($\succeq_{\text{emb}}$ is called a well-partial-ordering (wpo)).

Proof. See Baader and Nipkow, page 113–115. \qed
Theorem 4.33 (Dershowitz) If $\Sigma$ is a finite signature, then every simplification ordering $\succ$ on $T_\Sigma(X)$ is well-founded (and therefore a reduction ordering).

**Proof.** Suppose that $t_1 \succ t_2 \succ t_3 \succ \ldots$ is an infinite descending chain.

First assume that there is an $x \in \mathrm{var}(t_{i+1}) \setminus \mathrm{var}(t_i)$. Let $\sigma = [t_i/x]$, then $t_{i+1}\sigma \triangleright t_i\sigma = t_i$ and therefore $t_i = t_i\sigma \triangleright t_{i+1}\sigma \succeq t_i$, contradicting reflexivity.

Consequently, $\mathrm{var}(t_i) \supseteq \mathrm{var}(t_{i+1})$ and $t_i \in T_\Sigma(V)$ for all $i$, where $V$ is the finite set $\mathrm{var}(t_1)$. By Kruskal’s Theorem, there are $i < j$ with $t_i \trianglelefteq_t t_j$. Hence $t_i \preceq t_j$, contradicting $t_i \succ t_j$. \qed

There are reduction orderings that are not simplification orderings and terminating TRSs that are not contained in any simplification ordering.

Example:

Let $R = \{f(f(x)) \rightarrow f(g(f(x)))\}$.

$R$ terminates and $\rightarrow^+_R$ is therefore a reduction ordering.

Assume that $\rightarrow_R$ were contained in a simplification ordering $\succ$. Then $f(f(x)) \rightarrow_R f(g(f(x)))$ implies $f(f(x)) \triangleright f(g(f(x)))$, and $f(g(f(x))) \triangleright_{\mathrm{emb}} f(f(x))$ implies $f(g(f(x))) \succeq f(f(x))$, hence $f(f(x)) \triangleright f(f(x))$.

Recursive Path Orderings

Let $\Sigma = (\Omega, \Pi)$ be a finite signature, let $\succ$ be a strict partial ordering (“precedence”) on $\Omega$.

The lexicographic path ordering $\succ_{\mathrm{ipo}}$ on $T_\Sigma(X)$ induced by $\succ$ is defined by: $s \succ_{\mathrm{ipo}} t$ iff

1. $t \in \mathrm{var}(s)$ and $t \neq s$, or
2. $s = f(s_1, \ldots, s_m), t = g(t_1, \ldots, t_n)$, and
   a. $s_i \succeq_{\mathrm{ipo}} t$ for some $i$, or
   b. $f \triangleright g$ and $s \succ_{\mathrm{ipo}} t_j$ for all $j$, or
   c. $f = g, s \succ_{\mathrm{ipo}} t_j$ for all $j$, and $(s_1, \ldots, s_m) \triangleright_{\mathrm{exo}} (t_1, \ldots, t_n)$.

**Lemma 4.34** $s \succ_{\mathrm{ipo}} t$ implies $\mathrm{var}(s) \supseteq \mathrm{var}(t)$.

**Proof.** By induction on $|s| + |t|$ and case analysis. \qed

97