Chapter 2

Basic definitions

2.1 Terms and substitutions

2.2 Term Rewriting systems

A term rewriting system \( \mathcal{R} \) is a set of pairs of terms in \( T(F, X) \). Its members are typically written \( l \to r \)

The following relations are defined on \( T(F, X) \).

- \( s \xrightarrow{p \sigma}{l \to r} t \) if \( s|_p = l \sigma \) and \( t = s[r \sigma]_p \)
- \( s \xrightarrow{l \to r} t \) if there is a position \( p \in \text{Pos}(s) \) and a substitution \( \sigma \) such that \( s \xrightarrow{p \sigma}{l \to r} t \).
- \( s \xrightarrow{l \to r} t \) if there is a rule \( l \to r \in \mathcal{R} \) such that \( s \xrightarrow{l \to r} t \)
- \( \xleftarrow{\mathcal{R}} = \xrightarrow{\mathcal{R}} \cup \xleftarrow{\mathcal{R}} \)
- \( \xrightarrow{\mathcal{R}} \cup \xleftarrow{\mathcal{R}} = \mathcal{R} \cup \mathcal{R} \)
- \( \xrightarrow{\mathcal{R}} = \bigcup_{n=0}^{+\infty} \xrightarrow{n}{\mathcal{R}} \) where \( \xrightarrow{0}{\mathcal{R}} \) is the identity and \( \xrightarrow{n+1}{\mathcal{R}} = \xrightarrow{n}{\mathcal{R}} \circ \xrightarrow{n}{\mathcal{R}} \).

Example 1

\[
\begin{align*}
(r_1) & \quad \text{dec} \left( \text{enc}(x, y), y \right) \to x \\
(r_2) & \quad \pi_1 \left( \langle x, y \rangle \right) \to x \\
(r_3) & \quad \pi_2 \left( \langle x, y \rangle \right) \to y \\
\text{dec} \left( \pi_1 \left( \langle a, b \rangle \right), a \right) & \xrightarrow{\epsilon \{ x \to \pi_1 \left( \langle a, b \rangle \rangle ; y \to a \}} r_1 \pi_1 \left( \langle a, b \rangle \right)
\end{align*}
\]
Definition 1 A term rewriting system $R$ is terminating if there is no infinite sequence $\{s_i\}_{i \in \mathbb{N}}$ such that, for every $i$, $s_i \xrightarrow{R} s_{i+1}$.

Note that this definition corresponds to universal termination and strong normalization; we may start from an arbitrary term and the reductions take place at any position, using any rule.

Exercice 1
Give an example of a finite TRS $R$, which is not terminating and such that, for every term $t$, there is a term $u$ such that $t \xrightarrow{R} u$ and $u$ cannot be reduced by $R$.

Exercice 2
Give an example of a finite TRS which
1. is not terminating
2. each rule alone is a terminating system
3. for any term $t$ and any position $p$ of $t$, at most one rule can be applied at position $p$ in $t$

Theorem 1 Termination is undecidable for finite term rewriting systems.

Proof:
We reduce the Post Correspondance Problem. Let $(u_1, \ldots, u_n), (v_1, \ldots, v_n)$ be an instance of PCP, where $u_i, v_i \in \Sigma^*$.

We consider the set of symbols $F = \{0(0), f(4)\} \cup \{a(1) \mid a \in \Sigma\}$. If $u \in \Sigma^*$ and $t \in T(F, X)$, we write $\overline{u}(t)$ the term defined by induction on $u$: $\overline{e}(t) = t$, $\overline{a}(t) = a(\overline{a}(t))$. $\overline{u}(t)$ is defined by induction on $u$: $\overline{e}(t) = t$, $\overline{u}(t) = \overline{u}(a(t))$.

We let $R$ be the rewrite system containing the rules
\[
\begin{align*}
(r_1) & \quad f(\overline{u}_i(x), \overline{v}_1(y), x_1, y_1) \rightarrow f(x, y, \overline{u}_i(x), \overline{v}_1(y_1)) \quad \text{For every pair } (u_i, v_i) \\
(r_2) & \quad f(x, y, a(z), a(z)) \rightarrow f(a(x), a(y), z, z) \quad \text{For every letter } a
\end{align*}
\]

We claim that PCP has a solution iff $R$ is not terminating.

If PCP has a solution $u_{i_1} \cdots u_{i_k} = v_{i_1} \cdots v_{i_k} = w$, then
\[
f(u_{i_1} \cdots u_{i_k}(0), v_{i_1} \cdots v_{i_k}(0), 0, 0) \xrightarrow{r_1} \cdots \xrightarrow{r_1} f(0, 0, \overline{u}_{i_1} \cdots \overline{u}_{i_k}(0), \overline{v}_{i_1} \cdots \overline{v}_{i_k}(0))
\]
and
\[
f(0, 0, \overline{w}(0), \overline{w}(0)) \xrightarrow{r_2} f(\overline{w}(0), \overline{w}(0), 0, 0) = f(\overline{u_i} \cdots \overline{u_k}(0), \overline{v_i} \cdots \overline{v_k}(0), 0, 0)
\]

Hence \( \mathcal{R} \) is not terminating.

**If \( \mathcal{R} \) is not terminating**, consider a term \( t \) from which there is an infinite reduction sequence.

\[
t \xrightarrow{p_1, \sigma_1} t_1 \cdots \xrightarrow{p_n, \sigma_n} t_n \cdots
\]

We first note that the number of occurrences of \( f \) in \( t_i \) (written \( \#f(t_i) \)) is constant along the sequence since the rewriting rules in \( \mathcal{R} \) do not erase nor duplicate variables:

\[
\#f(u[l\sigma]_p) = \#f(u[0]_p) + \#f(l) + \sum_{x \in \text{Var}(l)} \#f(x\sigma) = \#f(u[0]_p) + \#f(r) + \sum_{x \in \text{Var}(r)} \#f(x\sigma) = \#f(u[r\sigma]_p)
\]

Now, we prove, by induction on \( \#f(t), |t| \) (where \( |t| \) is the size of the term \( t \)) that there is an infinite reduction sequence

\[
s_1 \xrightarrow{\cdot} s_2 \cdots \xrightarrow{\cdot} s_n \xrightarrow{\cdot}
\]

in which all reductions take place at the root position.

If \( \#f(t) = 0 \), there is nothing to prove.

If \( t = a(t') \) for some \( a \in \Sigma \), then \( p_i = 1 \cdot p'_i \) for all \( i \) and

\[
t|_1 \xrightarrow{p'_1, \sigma_1} \cdots t_n|_1 \xrightarrow{p'_n, \sigma_n} \cdots
\]

and we can apply the induction hypothesis to \( t|_1 \), whose size is strictly smaller than the size of \( t \).

If \( t = f(\alpha, \beta, \gamma, \delta) \). Then, for every \( i \), \( t_i = f(\alpha_i, \beta_i, \gamma_i, \delta_i) \). Consider again two cases: either \( \{ i \in \mathbb{N} | p_i = \epsilon \} \) is infinite or not.

**Case 1: \( \{ i \in \mathbb{N} | p_i = \epsilon \} \) is finite**. Let \( i_0 \) be the maximum of this set. Then, for \( i > i_0 \), \( p_i > \epsilon \). Therefore, one of the four sets \( \{ p_i | i > i_0 \} \cap j.\mathbb{N}^* \) for \( j = 1, 2, 3, 4 \) is infinite: we can extract an infinite sequence

\[
t_{m_1}|_j \xrightarrow{\mathcal{R}} \cdots t_{m_n}|_j \xrightarrow{\mathcal{R}} \cdots
\]

and \( \#f(t_{m_1}|_j) < \#f(t) \); we can apply the induction hypothesis.
**Case 2:** \( \{ i \in \mathbb{N} \mid p_i = \epsilon \} \) is infinite. Consider the morphism \( \rho \) such that, \( \rho(a(t)) = a(\rho(t)) \) for \( a \in \Sigma \) and \( \rho(f(s_1, \ldots, s_4)) = 0 \). Thanks to the definition of \( \mathcal{R} \), if \( s \xrightarrow{\mathcal{R}} s' \), then \( \rho(s) = \rho(s') \).

We let \( \rho' \) be the mapping defined by \( \rho'(a(t)) = \rho(a(t)) \) and \( \rho'(f(s_1, s_2, s_3, s_4)) = f(\rho(s_1), \rho(s_2), \rho(s_3), \rho(s_4)) \). Let us show that, for every \( i \), either \( t_i \xrightarrow{\rho'} t_{i+1} \), in which case \( \rho'(t_i) \xrightarrow{\mathcal{R}} \rho'(t_{i+1}) \) or else \( \rho'(t_i) = \rho'(t_{i+1}) \).

Indeed, by definition of \( \mathcal{R} \), \( \rho'(l\sigma) = l\sigma' \) where \( x\sigma' = \rho(x\sigma) \) for every variable \( x \). Hence, if \( t_i = l\sigma_i \), then \( \rho'(t_i) = l\sigma'_i \xrightarrow{\mathcal{R}} r\sigma'_i = t_{i+1} \). If \( t_i \xrightarrow{\mathcal{R}} t_{i+1} \), then, for \( j = 1, 2, 3, 4 \), \( \rho(t_{i,j}) = \rho(t_{i+1,j}) \), hence \( \rho'(t_i) = \rho'(t_{i+1}) \).

Therefore, if \( t_{i_k} \) is the subsequence of terms such that \( t_{i_k} \xrightarrow{\rho'} t_{i_{k+1}} \), then \( \rho'(t_{i_k}) \xrightarrow{\mathcal{R}} \rho'(t_{i_{k+1}}) \) and \( \rho'(t_{i_k}) \xrightarrow{\mathcal{R}} \rho'(t_{i_{k+1}}) \)...

We are left now to consider the case where all \( p_i = \epsilon \).

Consider the two interpretations: \( I_1(t_i) = (|\alpha_i|, |\beta_i|, |\gamma_i|, |\delta_i|)_{\text{lex}} \) and \( I_2(t_i) = (|\delta_i|, |\gamma_i|, |\beta_i|, |\alpha_i|)_{\text{lex}} \). The lexicographic ordering on \( \mathbb{N}^4 \) is well-founded and, if \( s \xrightarrow{r_1^i} s' \), then \( I_1(s) > I_1(s') \) and, if \( s \xrightarrow{r_2^i} s' \), then \( I_2(s) > I_2(s') \). It follows that there is no infinite reduction sequence using the rules \( r_1^i \) only, nor using the rules \( r_2^i \) only. In other words, the infinite reduction sequence must switch infinitely often between the \( r_1 \) rules and the \( r_2 \) rules. Therefore, there is a subsequence

\[
\begin{align*}
f(u, v, a(w), a(w)) & \xrightarrow{r_2^i} f(a(u), a(v), w, w) \\
& \xrightarrow{r_1^i} f(u'_1, v'_1, u_{1k}(w), v_{1k}(w)) \\
& \cdots \\
& \xrightarrow{r_1^i} f(u'_k, v'_k, u_{i_1} \cdots u_{i_k}(w), v_{i_1} \cdots v_{i_k}(w)) \\
& \xrightarrow{r_2^i} \cdots
\end{align*}
\]

But applying a rule \( r_2^i \) at position \( \epsilon \) to \( f(u'_k, v'_k, u_{i_1} \cdots u_{i_k}(w), v_{i_1} \cdots v_{i_k}(w)) \) requires \( u_{i_1} \cdots u_{i_k}(w) = v_{i_1} \cdots v_{i_k}(w) \), which implies \( u_{i_1} \cdots u_{i_k} = v_{i_1} \cdots v_{i_k} \); there is a solution to PCP.