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 $T(\mathcal{F}, X)$. Its members are typically written $l \to r$

The following relations are defined on $T(\mathcal{F}, X)$.

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

Example 1

$$\begin{array}{lrcl} (r_1) & \mathtt{dec}(\mathtt{enc}(x, y), y) & \to & x \\ (r_2) & \pi_1(\langle x, y \rangle) & \to & x \\ (r_3) & \pi_2(\langle x, y \rangle) & \to & y \end{array}$$

$$\mathtt{dec}(\mathtt{enc}(\pi_1(\langle a, b \rangle), a), a) \xrightarrow[r_1]{\epsilon, \{x \mapsto \pi_1(\langle a, b \rangle); y \mapsto a\}} \pi_1(\langle a, b \rangle)$$

Definition 1 *A term rewriting system* $\mathcal{R}$ *is* terminating *if there is no infinite sequence* $\{s_i\}_{i\in\mathbb{N}}$ *such that, for every* i, $s_i \xrightarrow[\mathcal{R}]{} s_{i+1}$.

Note that this definition corresponds to *universall 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 $\mathcal{R}$, which is not terminating and such that, for every term t, there is a term u such that $t \xrightarrow[\mathcal{R}]{*} u$ and u cannot be reduced by $\mathcal{R}$.

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 $\mathcal{F} = \{0(0), f(4)\} \cup \{a(1) \mid a \in \Sigma\}$. If $u \in \Sigma^*$ and $t \in T(\mathcal{F}, X)$, we write $\overline{u}(t)$ the term defined by induction on u: $\overline{\epsilon}(t) = t$, $\overline{au}(t) = a(\overline{u}(t))$. $\widetilde{u}(t)$ is defined by induction on u: $\widetilde{\epsilon}(t) = t$, $\widetilde{au}(t) = \widetilde{u}(a(t))$.

We let $\mathcal{R}$ be the rewrite system containing the rules

$$\left\{\begin{array}{llcll} (r_1^i) & f(\widetilde{u_i}(x), \widetilde{v_i}(y), x_1, y_1) & \to & f(x, y, \overline{u_i}(x_1), \overline{v_i}(y_1)) & \text{For every pair } (u_i, v_i) \\ (r_2^a) & f(x, y, a(z), a(z)) & \to & f(a(x), a(y), z, z) & \text{For every letter } a \end{array}\right.$$

We claim that PCP has a solution iff $\mathcal{R}$ is not terminating.

If PCP has a solution $u_{i_1}\cdots u_{i_k} = v_{i_1}\cdots v_{i_k} = w$, then

$$f(\widetilde{u_{i_1}\cdots u_{i_k}}(0), \widetilde{v_{i_1}\cdots v_{i_k}}(0), 0, 0) \xrightarrow[r_1^{i_k}]{} \cdots \xrightarrow[r_1^{i_1}]{} f(0, 0, \overline{u_{i_1}\cdots u_{i_k}}(0), \overline{v_{i_1}\cdots v_{i_k}}(0))$$

and

$$f(0,0,\overline{w}(0),\overline{w}(0)) \xrightarrow[r_2]{*} f(\widetilde{w}(0),\widetilde{w}(0),0,0) = f(u_{\widetilde{i_1} \cdots u_{i_k}}(0), v_{\widetilde{i_1} \cdots v_{i_k}}(0),0,0)$$

Hence $\mathcal{R}$ is not terminating.

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

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

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

$$\begin{array}{rcl} \#_f(u[l\sigma]_p) & = & \#_f(u[0]_p) + \#_f(l) + \sum_{x \in Var(l)} \#_f(x\sigma) \\ & = & \#_f(u[0]_p) + \#_f(r) + \sum_{x \in Var(r)} \#_f(x\sigma) \\ & = & \#_f(u[r\sigma]_p) \end{array}$$

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

$$s_1 \xrightarrow{\epsilon} s_2 \cdots \xrightarrow{\epsilon} s_n \xrightarrow{\epsilon}$$

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

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

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 $\{i \in \mathbb{N} \mid p_i = \epsilon\}$ is infinite or not.

Case 1: $\{i \in \mathbb{N} \mid p_i = \epsilon\}$ 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 $\{p_i \mid i > i_0\} \cap j.\mathbb{N}^*$ for $j = 1,2,3,4$ is infinite: we can extract an infinite sequence

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

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 ρ 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 ρ' 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 $t_i \xrightarrow{\epsilon} t_{i+1}$, in which case $\rho'(t_i) \xrightarrow{\epsilon} \rho'(t_{i+1})$ or else $\rho'(t_i) = \rho'(t_{i+1})$.

Indeed, by definition of $\mathcal{R}$, $\rho'(l\sigma) = l\sigma^\rho$ where $x\sigma^\rho = \rho(x\sigma)$ for every variable x. Hence, if $t_i = l\sigma_i$, then $\rho'(t_i) = l\sigma_i^\rho \xrightarrow{\epsilon} r\sigma_i^\rho = t_{i+1}$. If $t_i \xrightarrow[t_{i+1}]{\neq\epsilon}$, 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 $t_{i_k} \xrightarrow[\mathcal{R}]{\epsilon} t_{i_k+1}$, then

$$\rho'(t_{i_1}) \xrightarrow[\mathcal{R}]{\epsilon} \rho'(t_{i_2}) \xrightarrow[\mathcal{R}]{\epsilon} \cdots \xrightarrow[\mathcal{R}]{\epsilon} \rho'(t_{i_k}) \xrightarrow[\mathcal{R}]{\epsilon} \cdots$$

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

Consider the two interpretations: $I_1(t_i) = (|\alpha_i|, |\beta_i|, |\gamma_i|, |\delta_i|)_{lex}$ and $I_2(t_i) = (|\delta_i|, |\gamma_i|, |\beta_i|, |\alpha_i|)_{lex}$. The lexicographic ordering on $\mathbb{N}^4$ is well-founded and, if $s \xrightarrow[r_1^i]{\epsilon} s'$, then $I_1(s) > I_1(s')$ and, if $\xrightarrow[r_2^a]{\epsilon} s'$, 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^a only. In other words, the infinite reduction sequence must swicth infinitely often between the r_1 rules and the r_2 rules. Therefore, there is a subsequence

$$\begin{array}{lcl}
f(u, v, a(w), a(w)) & \xrightarrow[r_2]{} & f(a(u), a(v), w, w) \\
 & \xrightarrow[r_1^{i_k}]{\epsilon} & f(u'_1, v'_1, \overline{u_{i_k}}(w), \overline{v_{i_k}}(w)) \\
 & \cdots & \\
 & \xrightarrow[r_1^{i_1}]{\epsilon} & f(u'_k, v'_k, \overline{u_{i_1} \cdots u_{i_k}}(w), \overline{v_{i_1} \cdots v_{i_k}}(w)) \\
 & \xrightarrow[r_2^a]{\epsilon} & \cdots
\end{array}$$

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