Rewriting Techniques: TD 7

11-01-2018

AProVE[1] is a system for automated termination and complexity proofs of TRSs.

Exercise 1 :
Study the termination of the TRSs from previous TDs using AProVE. For example, consider

$$\begin{aligned}
\mathtt{m}(x, \mathtt{0}) &\to 0 & \mathtt{m}(\mathtt{s}(x), \mathtt{s}(y)) &\to \mathtt{m}(x, y)\\
\mathtt{q}(\mathtt{0}, \mathtt{s}(y)) &\to 0 & \mathtt{q}(\mathtt{s}(x), \mathtt{s}(y)) &\to \mathtt{s}(\mathtt{q}(\mathtt{m}(x, y), \mathtt{s}(y)))\\
\mathtt{p}(\mathtt{0}, y) &\to y & \mathtt{p}(x, \mathtt{s}(y)) &\to \mathtt{s}(\mathtt{p}(x, y))\\
\mathtt{m}(\mathtt{m}(x, y), z) &\to \mathtt{m}(x, \mathtt{p}(y, z))
\end{aligned}$$

KBCV[2] is a tool to interactively perform the Knuth-Bendix completion procedure.

Exercise 2 :
Complete the following sets of equations using KBCV:

1. E_1 (from TD4):

$$\begin{aligned}
x \times (y + z) &= (x \times y) + (x \times z)\\
(x + y) \times z &= (x \times z) + (y \times z)
\end{aligned}$$

2. E_2:

$$\begin{aligned}
x + \mathtt{0} &= x\\
\mathtt{0} + x &= x\\
x + (-x) &= \mathtt{0}\\
(-x) + x &= \mathtt{0}\\
(x + y) + z &= x + (y + z)
\end{aligned}$$

3. E_3:

$$\begin{aligned}
x \times \mathtt{1} &= x\\
\mathtt{1} \times x &= x\\
(x \times y) \times z &= x \times (y \times z)
\end{aligned}$$

4. $E_1 \cup E_2$ and $E_2 \cup E_3$

ConCon[3] is a confluence checker for (conditional) term rewriting system.

Exercise 3 :
Study the confluence of the TRSs from previous TDs using ConCon. For example, consider

$$\begin{aligned}
\mathtt{nat} &\to \mathtt{0} : \mathtt{inc}(\mathtt{nat})\\
\mathtt{inc}(x : y) &\to s(x) : \mathtt{inc}(y)\\
\mathtt{tl}(x : y) &\to y\\
\mathtt{inc}(\mathtt{tl}(\mathtt{nat})) &\to \mathtt{tl}(\mathtt{inc}(\mathtt{nat}))
\end{aligned}$$

[1] http://aprove.informatik.rwth-aachen.de/
[2] http://cl-informatik.uibk.ac.at/software/kbcv/
[3] http://cl-informatik.uibk.ac.at/software/concon/

Two terms s and t are **joinable** (written $s \downarrow t$) w.r.t. a reduction $\to$ if there is k such that $s \to^* k \leftarrow^* t$.

A reduction $\to$ is called:

- **terminating** if there is no infinite descending chain $a_0 \to a_1 \to \dots$;
- **locally confluent** if $v_1 \leftarrow u \to v_2$ implies $v_1 \downarrow v_2$;
- **confluent** if $v_1 \leftarrow^* u \to^* v_2$ implies $v_1 \downarrow v_2$;

A pair $(A, \leq)$, where $\leq$ is a binary relation on the set A, is a **well quasi-ordering** (wqo) if $\leq$:

- is a *quasi-order*, i.e. $\leq$ is reflexive and transitive;
- is *well-founded*, i.e. there are no infinite strictly decreasing sequences $a_0 > a_1 > a_2 > \dots$ in A;
- does not have *infinite anti-chains*, i.e. it does not exists an infinite subset I of A such that for each $a, b \in I$, $a \not\leq b$ and $b \not\leq a$.

Exercise 4 :
Which of the following are true? Give a justification or a counter-example.

1. Every locally confluent TRS is confluent.
2. Every confluent TRS is terminating.
3. If $\leq$ is a wqo, from every infinite sequence it is possible to extract an infinite increasing subsequence.
4. If $\mathcal{R}$ is a non-terminating TRS then there are terms u, v such that $u \to^*_{\mathcal{R}} v$ and $u \trianglelefteq v$ (where $\trianglelefteq$ is the sub-term relation).
5. If $\mathcal{R}$ is terminating TRS, then $\to^*_{\mathcal{R}}$ is a wqo on $T(\mathcal{F})$.

Solution:

(1) False. Consider for instance $\mathcal{R}_2$ from the solution of Exercise 4.3 of TD5.

(2) False. Consider the TRS $\{a \to a\}$.

(3) True, since $\leq$ is well-founded.

(4) True. Let $u_1 \to_{\mathcal{R}} u_2 \to_{\mathcal{R}} \cdots \to_{\mathcal{R}} u_n \to_{\mathcal{R}} \dots$ be an infinite sequence of rewriting. We may assume that all u_i are ground (replace all variables with a constant). Since $\trianglelefteq$ is a wqo on $T(\mathcal{F})$ for finite $\mathcal{F}$, there are no infinite anti-chains and therefore $u_i \trianglelefteq u_j$ holds for two indices $i < j$.

(5) False. Consider $\mathcal{R}$ empty. A sequence $\mathtt{a}, \mathtt{f}(\mathtt{a}), \mathtt{f}(\mathtt{f}(\mathtt{a})), \dots$ of distinct terms is an infinite anti-chain.

Exercise 5 :
Let $\mathcal{R}_1$ and $\mathcal{R}_2$ be two confluent TRS such that $\leftarrow_{\mathcal{R}_2} \circ \to_{\mathcal{R}_1} \subseteq \to_{\mathcal{R}_1} \circ \leftarrow_{\mathcal{R}_2}$.

1. Prove that $\leftarrow^*_{\mathcal{R}_1} \circ \to^*_{\mathcal{R}_1 \cup \mathcal{R}_2} \subseteq \to^*_{\mathcal{R}_1 \cup \mathcal{R}_2} \circ \leftarrow^*_{\mathcal{R}_1 \cup \mathcal{R}_2}$
2. Show that $\mathcal{R}_1 \cup \mathcal{R}_2$ is confluent.

Solution:

(1) Assume $u \leftarrow^*_{\mathcal{R}_1} t \to^n_{\mathcal{R}_1 \cup \mathcal{R}_2} v$. We prove the result by induction on n. If $n = 0$, this is trivial: $t = v \to^*_{\mathcal{R}_1} u$. Otherwise, there are two cases.

- the first step is a reduction by $\mathcal{R}_1$:

$$u \leftarrow^*_{\mathcal{R}_1} t \to_{\mathcal{R}_1} t' \to^{n-1}_{\mathcal{R}_1 \cup \mathcal{R}_2} v$$

  By confluence of $\mathcal{R}_1$, $u \to^*_{\mathcal{R}_1} u' \leftarrow^*_{\mathcal{R}_1} t' \to^{n-1}_{\mathcal{R}_1 \cup \mathcal{R}_2} v$ and it is sufficient to apply the induction hypothesis.

- the first step is a reduction by $\mathcal{R}_2$:

$$u \leftarrow^{k}_{\mathcal{R}_1} t \rightarrow_{\mathcal{R}_2} t' \rightarrow^{n-1}_{\mathcal{R}_1\cup\mathcal{R}_2} v$$

  Then, by induction on k, thanks to the inclusion $\leftarrow_{\mathcal{R}_2} \circ \rightarrow_{\mathcal{R}_1} \subseteq \rightarrow_{\mathcal{R}_1} \circ \leftarrow_{\mathcal{R}_2}$, it holds $u \rightarrow_{\mathcal{R}_2} \circ \leftarrow^{k}_{\mathcal{R}_1} t'$. We may again apply the induction hypothesis.

(2) From the previous question, by symmetry $\leftarrow_{\mathcal{R}_1\cup\mathcal{R}_2} \circ \rightarrow^{*}_{\mathcal{R}_1\cup\mathcal{R}_2} \subseteq \rightarrow^{*}_{\mathcal{R}_1\cup\mathcal{R}_2} \circ \leftarrow^{*}_{\mathcal{R}_1\cup\mathcal{R}_2}$. Hence $\mathcal{R}_1 \cup \mathcal{R}_2$ is semi-confluent and therefore confluent.

A **conditional term rewriting system** (CTRS) $\mathcal{R}$ is a set of rules of the form $\ell \to r \Leftarrow C$ where are terms of a given signature and C is a sequence $a_1 \approx b_1, \ldots, a_k \approx b_k$ of equations between terms.

The rewrite relation $\rightarrow_{\mathcal{R}}$ associated with $\mathcal{R}$ is formally defined as the union of a series of approximations $\rightarrow_{\mathcal{R}_i}$, where

- $\mathcal{R}_0 = \emptyset$,
- $\mathcal{R}_{i+1} = \{\ell\sigma \to r\sigma \mid \ell \to r \Leftarrow C \text{ in } \mathcal{R} \text{ and } a\sigma \rightarrow^{*}_{\mathcal{R}_i} b\sigma \text{ for all } a \approx b \text{ in } C\}$

It holds that $s \rightarrow_{\mathcal{R}} t$ whenever there exists a position $p \in \mathrm{Pos}(s)$, a rule $\ell \to r \Leftarrow c$ in $\mathcal{R}$ and a substitution σ such that $s|_p = \ell\sigma$, $t = s[r\sigma]_p$ and for all $a \approx b \in C$ it holds that $a\sigma \rightarrow^{*}_{\mathcal{R}} b\sigma$.

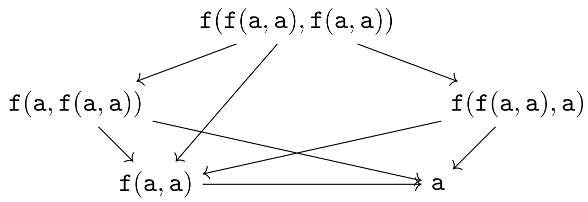
Exercise 6 :
Consider the following CTRS $\mathcal{R}_1$:

$$\begin{aligned} \mathtt{f}(x,y) &\to x \ \Leftarrow x \approx k,\ z \approx k,\ z \approx k',\ y \approx k' \\ \mathtt{f}(x,y) &\to y \ \Leftarrow x \approx k,\ z \approx k,\ z \approx k',\ y \approx k' \end{aligned}$$

with function symbol $\mathtt{f}/2$ and constants $\mathtt{a}$, $\mathtt{b}$, $\mathtt{0}$, $\mathtt{1}$.

1. Show the reduction graph of $\mathtt{f}(\mathtt{f}(\mathtt{a},\mathtt{a}),\mathtt{f}(\mathtt{a},\mathtt{a}))$.
2. Is $\mathcal{R}_1$ locally confluent? *(hint: study it w.r.t. the one-rule TRS $\mathtt{f}(x,x) \to x$)*
3. Define a locally confluent (C)TRS $\mathcal{R}_2$ with the same signature $\{\mathtt{a}/0, \mathtt{b}/0, \mathtt{0}/0, \mathtt{1}/0, \mathtt{f}/2\}$ of $\mathcal{R}_1$, such that $\mathcal{R}_1 \cup \mathcal{R}_2$ is not locally confluent.

Solution:
(1)



(2) Yes. Let $\mathcal{R} = \{\mathtt{f}(x,x) \to x\}$. Clearly, $\rightarrow_{\mathcal{R}} \subseteq \rightarrow_{\mathcal{R}_1}$. Conversely, if $s \rightarrow_{\mathcal{R}_1} t$ then we obtain $s \downarrow_{\mathcal{R}} t$ by a straightforward induction on the depth of $s \rightarrow_{\mathcal{R}_1} t$ (which is well-founded since $\mathcal{R}_1$ is terminating). The local confluence of $\mathcal{R}_1$ then follows from the local confluence of $\mathcal{R}$.

(3) Consider the following TRS $\mathcal{R}_2$:

$$\begin{gathered} \mathtt{a} \to \mathtt{b} \\ \mathtt{b} \to \mathtt{a} \\ \mathtt{a} \to \mathtt{0} \\ \mathtt{b} \to \mathtt{1} \end{gathered}$$

This TRS has already been considered multiple times (e.g. TD 5) and is a standard example of a TRS which is locally confluent but not confluent. To show that $\mathcal{R}_1 \cup \mathcal{R}_2$ is not locally confluent it is sufficient to notice that $\mathtt{0} \leftarrow_{\mathcal{R}_1\cup\mathcal{R}_2} \mathtt{f}(\mathtt{0},\mathtt{1}) \rightarrow_{\mathcal{R}_1\cup\mathcal{R}_2} \mathtt{1}$ since $\mathtt{0} \approx \mathtt{0}$, $\mathtt{b} \approx \mathtt{0}$, $\mathtt{b} \approx \mathtt{1}$ and $\mathtt{1} \approx \mathtt{1}$ whereas $\mathtt{0}$ and $\mathtt{1}$ do not have common reduct.

A **completion procedure** is a program that accepts as input a finite set of identities E_0 and a reduction order $>$, and generate a (finite or infinite) sequence (called run) $(E_0, R_0), (E_1, R_1), (E_2, R_2), \ldots$ where $R_0 = \emptyset$, by applying the rules:

$$\frac{E, R \quad s \leftarrow_R u \rightarrow_R t}{E \cup \{s = t\}, R}\ \text{Deduce} \qquad\qquad \frac{E \cup \{s \doteq t\}, R \quad s > t}{E, R \cup \{s \rightarrow t\}}\ \text{Orient}$$

$$\frac{E \cup \{s = s\}, R}{E, R}\ \text{Delete} \qquad\qquad \frac{E \cup \{s \doteq t\}, R \quad s \rightarrow_R u}{E, R \cup \{u \rightarrow t\}}\ \text{Simplify-Id}$$

$$\frac{E, R \cup \{s \rightarrow t\} \quad t \rightarrow_R u}{E, R \cup \{s \rightarrow u\}}\text{R-Simplify} \qquad\qquad \frac{E, R \cup \{s \rightarrow t\} \quad s \overset{\sqsupset}{\rightarrow}_R u}{E \cup \{u = t\}, R}\text{L-Simplify}$$

where $s \doteq t$ if and only if $s = t$ or $t = s$, whereas $s \overset{\sqsupset}{\rightarrow}_R u$ is used to express that s is reduced to u by a rule $l \rightarrow r$ of R such that each sub-term of l is not an instance of s. A special case of *Deduce* is to apply it only if (s, t) is a critical pair. Most completion procedures use the rule *Deduce* only in this way. The goal of these procedures is to transform an initial pair $(E_0, \emptyset)$ into a pair $(\emptyset, \mathcal{R})$ such that $\mathcal{R}$ is a convergent TRS equivalent to E_0.

Exercise 7 :
Consider the single equation $\mathtt{I}(x) \times (x \times y) = y$. Compute a convergent TRS for the equational theory defined by this equation (without using KBCV!).

Solution:

For this Exercise, we will just use the rules *Orient* and *Deduce*, as follows:

1. Update R by using *Orient* on an element of E,
2. Check for a critical pair (s, t) in R s.t. s are t are not joinable w.r.t. R.
   - if (s, t) exists, then R is not locally confluent. *Deduce* $s = t$ (which is added to E).
   - if (s, t) does not exists, R is locally confluent.
3. if E is empty, terminate. Otherwise, go to (1).

Let $E_0 = \{\mathtt{I}(x) \times (x \times y) = y\}$ and $R_0 = \emptyset$. By applying the *Orient* rule we obtain $E_1 = \emptyset$ and $R_1 = \{\mathtt{I}(x) \times (x \times y) \rightarrow y\}$. The only critical peak in R_1 is $\mathtt{I}(\mathtt{I}(x)) \times (\mathtt{I}(x) \times (x \times y))$ with critical pair $(\mathtt{I}(\mathtt{I}(x)) \times y, x \times y)$. R_1 is not locally confluent. By applying *Deduce* we obtain $E_2 = \{\mathtt{I}(\mathtt{I}(x)) \times y = x \times y\}$ and $R_2 = R_1$. By orienting the new identity we obtain $E_3 = \emptyset$ and

$$R_3 = \{\mathtt{I}(x) \times (x \times y) \rightarrow y,\ \mathtt{I}(\mathtt{I}(x)) \times y \rightarrow x \times y\}$$

which has a new critical peak $\mathtt{I}(\mathtt{I}(x)) \times (\mathtt{I}(x) \times y)$. R_3 is not locally confluent. Therefore, we apply *Deduce* to the critical pair $(x \times (\mathtt{I}(x) \times y, y)$ of this new critical peak and obtain $E_4 = \{x \times (\mathtt{I}(x) \times y = y\}$ and $R_4 = R_3$.
We now apply *Orient* and obtain $E_5 = \emptyset$ and

$$R_5 = \{\mathtt{I}(x) \times (x \times y) \rightarrow y,\ \mathtt{I}(\mathtt{I}(x)) \times y \rightarrow x \times y,\ x \times (\mathtt{I}(x) \times y \rightarrow y\}$$

It's easy to prove that R_5 is a convergent TRS. Termination is trivial, whereas confluence follows by Newman's Lemma from its local confluency, which holds since all of its critical pairs are joinable. For example, consider the critical peak $x \times (\mathtt{I}(x) \times (\mathtt{I}(\mathtt{I}(x)) \times y))$ which is associated with the following diagram

$$\begin{tikzcd} & x \times (\mathtt{I}(x) \times (\mathtt{I}(\mathtt{I}(x)) \times y)) \arrow[dl] \arrow[dr] & \\ \mathtt{I}(\mathtt{I}(x)) \times y \arrow[rr] & & x \times y \end{tikzcd}$$

Let $\mathtt{status}(f) \in \{\text{mul}, \text{lex}\}$ (i.e. multiset order or lexicographic order) a *status* function on Σ and let $>$ be a strict order on Σ. The **recursive path order** $>_{\text{rpo}}$ on $T(\Sigma, V)$ induced by $>$ is defined as follows. $s >_{\text{rpo}} t$ if and only if one of the following holds:

1. t is a variable appearing in s and $s \neq t$, or

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

2. there exists $i \in [1, m]$ such that $s_i \geq_{\text{rpo}} t$, or
3. $f > g$ and $s >_{\text{rpo}} t_j$ for all $j \in [1, n]$, or
4. $f = g$, for all $j \in [1, n]$ it holds $s >_{\text{rpo}} t_j$ and $(s_1, \ldots, s_m)(>_{\text{rpo}})_{\mathtt{status}(f)}(t_1, \ldots, t_m)$.

Let $>$ be a strict order on Σ and $w : \Sigma \cup V \to \mathbb{R}_0^+$ be a weight function $w : \Sigma \cup V \to \mathbb{R}_0^+$. The **Knuth-Bendix order** (KBO) $>_{\text{kbo}}$ on $T(\Sigma, V)$ induced by $>$ and w is defined as follows: for $s, t \in T(\Sigma, V)$ we have $s >_{\text{kbo}} t$ if and only if $|s|_x \geq |t|_x$ for all $x \in V$ and $w(s) \geq w(t)$. Moreover, if $w(s) = w(t)$ then one of the following properties must hold:

1. There are a unary function f, $x \in V$ and $n \in \mathbb{N}^{\geq 1}$ s.t. $s = f^n(x)$ and $t = x$, or
2. there exist function symbols f, g s.t. $f > g$ and $s = f(s_1, \ldots, s_m)$ and $t = g(t_1, \ldots, t_n)$, or
3. there exist a function symbol f such that $s = f(s_1, \ldots, s_m)$, $t = f(t_1, \ldots, t_m)$ and

$$(s_1, \ldots, s_m)(>_{\text{kbo}})_{\text{lex}}(t_1, \ldots, t_m).$$

A weight function $w : \Sigma \cup V \to \mathbb{R}_0^+$ is called **admissible** if and only if it satisfy the following properties w.r.t. a strict order $>$:

1. There exists $w_0 \in \mathbb{R}_0^+ \setminus \{0\}$ s.t. $w(x) = w_0$ for all $x \in V$ and $w(c) \geq w_0$ for all constants $c \in \Sigma$.
2. If $f \in \Sigma$ is a unary function symbol of weight $w(f) = 0$ then f is the greatest element in Σ, i.e. $f \geq g$ for all $g \in \Sigma$.

A **polynomial interpretation on integers** is the following:

- a subset A of $\mathbb{N}$;
- for every symbol f of arity n, a polynomial $\mathtt{P}_f \in \mathbb{N}[X_1, \ldots, X_n]$;
- for every $a_1, \ldots, a_n \in A$, $\mathtt{P}_f(a_1, \ldots, a_n) \in A$;
- for every $a_1, \ldots, a_i > a'_i, \ldots, a_n \in A$, $\mathtt{P}_f(a_1, \ldots, a_i, \ldots, a_n) > \mathtt{P}_f(a_1, \ldots, a'_i, \ldots, a_n)$;

Then $(A, (\mathtt{P}_f)_f, >)$ is a well-founded monotone algebra.

Exercise 8 :
Let $\mathcal{R}$ be the following TRS:

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

1. Show that the termination of $\mathcal{R}$ cannot be proved with RPO or KBO.
2. Show that $\mathcal{R}$ terminates by defining a suitable polynomial interpretation over integers.

Solution:

(1) KBO cannot be used since $|\mathtt{f}(y, \mathtt{f}(x, z))|_x < |\mathtt{f}(x, x)|_x$ and therefore the condition "$|s|_x \geq |t|_x$ for all $x \in V$" is violated. For RPO, if we consider $\mathtt{status}(\mathtt{f}) = \text{lex}$ then $y >_{\text{rpo}} x$ (from the second rule) does not holds, whereas $\{\!|\mathtt{f}(x, y), z|\!\}(>_{\text{rpo}})_{\text{mul}}\{\!|x, \mathtt{f}(y, z)|\!\}$ does not holds when we consider $\mathtt{status}(\mathtt{f}) = \text{mul}$.

(2) We consider $A = \mathbb{N} \setminus \{0, 1, 2\}$ and $P_{\mathtt{f}} = X^2 + XY$. It holds that

$$P_{\mathtt{f}(\mathtt{f}(x,y),z)} = X^4 + 2X^3Y + X^2y^2 + X^2Z + XYZ > X^2 + Y^2X + XYZ = P_{\mathtt{f}(x,\mathtt{f}(y,z))}$$
$$P_{\mathtt{f}(y,\mathtt{f}(x,z))} = Y^2 + X^2Y + XZ > 2X^2 = P_{\mathtt{f}(x,x)}$$