EXERCISE 2

Science of Computational Logic

Steffen Hölldobler, Marcos Cramer

International Masters Programme in Computational Logic — winter semester 2018/2019

Problem 2.1

In the lectures, $\approx_{\mathcal{E}}$ was defined to be the *least congruence relation generated by* $\mathcal{E}$. What does it mean?

Solution

We define $s \approx_{\mathcal{E}} t$ iff $\mathcal{E} \cup \mathcal{E}_{\approx} \models \forall s \approx t$. In other words, $\approx_{\mathcal{E}}$ is the least relation satisfying the following properties:

1. if $s \approx t \in \mathcal{E}$, then $s \approx_{\mathcal{E}} t$, *(generated by $\mathcal{E}$)*
2. $s \approx_{\mathcal{E}} s$ for all $s \in \mathcal{T}(\mathcal{F}, \mathcal{V})$, *(reflexivity)*
3. if $s \approx_{\mathcal{E}} t$, then $t \approx_{\mathcal{E}} s$, *(symmetric)*
4. if $s \approx_{\mathcal{E}} t$ and $t \approx_{\mathcal{E}} u$, then $s \approx_{\mathcal{E}} u$, *(transitivity)*
5. if $s_i \approx_{\mathcal{E}} t_i$ for all $i \in \{1, \ldots, n\}$, then $f(s_1, \ldots, s_n) \approx_{\mathcal{E}} f(t_1, \ldots, t_n)$, and *(congruence)*
6. if $s \approx_{\mathcal{E}} t$, then $s\sigma \approx_{\mathcal{E}} t\sigma$ for all substitutions σ. *(closed under substitution)*

Problem 2.2

Consider the set of clauses

$$\mathcal{F} = \{\ [p(f(Y)), q(Y), r(b)],\ [\neg p(b)],\ [\neg q(a)],\ [\neg r(a)]\ \}$$

and the equational system

$$\mathcal{E} = \{(\forall X) f(X) \approx X, a \approx b\}.$$

Show by paramodulation, resolution and factoring that $\mathcal{F} \cup \mathcal{E} \cup \mathcal{E}_{\approx}$ is unsatisfiable. Also give the mgu θ used in every step.

Solution

1)	$[p(f(Y)), q(Y), r(b)]$		
2)	$[\neg p(b)]$		
3)	$[\neg q(a)]$		
4)	$[\neg r(a)]$		
5)	$[f(X) \approx X]$		
6)	$[a \approx b]$		
7)	$[p(f(a)), r(b)]$	res(1, 3)	$\theta = \{Y_1 \mapsto a\}$
8)	$[\neg r(b)]$	pm(4, 6)	$\theta = \varepsilon$
9)	$[p(f(a))]$	res(7, 8)	$\theta = \varepsilon$
10)	$[p(a)]$	pm(9, 5)	$\theta = \{X_2 \mapsto a\}$
11)	$[p(b)]$	pm(10, 6)	$\theta = \varepsilon$
12)	$[\,]$	res(2, 11)	$\theta = \varepsilon$

Problem 2.3

Let $\mathcal{R}$ be a term rewriting system and let s and t be terms. Prove that:

1. $s \to_{\mathcal{R}} t$ implies $s \approx_{\mathcal{E}_{\mathcal{R}}} t$.
2. $s \leftrightarrow^*_{\mathcal{R}} t$ implies $s \approx_{\mathcal{E}_{\mathcal{R}}} t$.

Solution

1.
   - We assume $s \to_{\mathcal{R}} t$
   - By definition there is $l \to r \in \mathcal{R}$, $\pi \in \mathcal{P}_s$ and a substitution θ such that $s\lceil\pi\rceil = l\theta$ and $t = s\lceil\pi/r\theta\rceil$.
   - By definition we have $l \approx r \in \mathcal{E}_{\mathcal{R}}$, consequently $\mathcal{E}_{\mathcal{R}} \models \forall\ l \approx r$
   - Then obviously $\mathcal{E}_{\mathcal{R}} \models \forall l\sigma \approx r\sigma$ for all substitutions σ in particular $\mathcal{E}_{\mathcal{R}} \models \forall l\theta \approx r\theta$, i. e., $l\theta \approx_{\mathcal{E}_{\mathcal{R}}} r\theta$.
   - Because $l\theta \approx_{\mathcal{E}_{\mathcal{R}}} r\theta$, $s\lceil\pi\rceil = l\theta$ and f-substitutivity: $s \approx_{\mathcal{E}_{\mathcal{R}}} s\lceil\pi/r\theta\rceil = t$
     To be precise we would have to prove by structural induction over terms that we may substitute a subterm by an equal one.

2. We assume $s \leftrightarrow^*_{\mathcal{R}} t$
   Then there is a sequence $u_1, \ldots, u_n$ of terms, with

   $s = u_1$
   $t = u_n$
   $u_i \leftrightarrow_{\mathcal{R}} u_{i+1},\ 1 \leq i < n$

(because $\leftrightarrow^*_{\mathcal{R}}$ is the reflexive, transitive closure of $\leftrightarrow_{\mathcal{R}}$)
We prove $s = u_1 \approx_{\mathcal{E}_\mathcal{R}} u_n = t$ by induction on the length n of the sequence

<u>IB:</u> $n = 1$
Then $s = u_1 = t$ and $s \approx_{\mathcal{E}_\mathcal{R}} t$, because $\approx_{\mathcal{E}_\mathcal{R}}$ is reflexive.

<u>IH:</u> For sequences $u'_1, \ldots, u'_n$ of length n it holds that $u'_1 \approx_{\mathcal{E}_\mathcal{R}} u'_n$

<u>IS:</u> For a sequence $s = u_1 \leftrightarrow_{\mathcal{R}} \cdots \leftrightarrow_{\mathcal{R}} u_{n+1} = t$ of length $n + 1$:
$u_1 \ldots u_n$ is a sequence of length n, so by IH:

$$s = u_1 \approx_{\mathcal{E}_\mathcal{R}} u_n$$

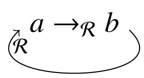
$u_n \leftrightarrow_{\mathcal{R}} u_{n+1}$ means either $u_n \rightarrow_{\mathcal{R}} u_{n+1}$ or $u_n \leftarrow_{\mathcal{R}} u_{n+1}$
and by part 1: $u_n \approx_{\mathcal{E}_R} u_{n+1} = t$
Because $\approx_{\mathcal{E}_\mathcal{R}}$ is transitive, then $s = u_1 \approx u_{n+1} = t$.

Problem 2.4

A non terminating term rewriting system can be confluent. True or false? Prove it.

Solution
A non teminating trs can be confluent.
For example: $\mathcal{R} = \{a \rightarrow b, b \rightarrow a\}$

1) is non-terminating because there is an infinite rewriting sequence:



2) Let $s \uparrow_{\mathcal{R}} t$
Then there exists a term u such that $s \leftarrow^*_{\mathcal{R}} u \rightarrow^*_{\mathcal{R}} t$.

$u \rightarrow^*_{\mathcal{R}} s$ implies that there is a sequence $v_1, \ldots, v_n$ of terms
with $v_1 = u$, $v_n = s$ and $v_i \rightarrow_{\mathcal{R}} v_{i+1},\ 1 \leq i < n$.

$v_i \rightarrow_{\mathcal{R}} v_{i+1}$ means:
$v_{i+1} = v_i\lceil \pi \mapsto r \rceil$ with $v_i\lceil \pi \rceil = l$ with $l = a, r = b$ or $l = b, r = a$
($r\theta = r$ for all θ, $l\theta = l$ for all θ) .

Then holds $v_{i+1} \rightarrow_{\mathcal{R}} v_i$ using the “opposite” rule $r \rightarrow l$
because with $v_{i+1}\lceil \pi \rceil = r$ (obviously) $v_i = v_{i+1}\lceil \pi \mapsto l \rceil$.

This means $v_i \leftarrow_{\mathcal{R}} v_{i+1}$ for all $1 \leq i < n$ and $u \leftarrow^*_{\mathcal{R}} s$.

By an analogous argument, we find $t \rightarrow^*_{\mathcal{R}} u$.
Thus we get: $s \rightarrow^*_{\mathcal{R}} u \leftarrow^*_{\mathcal{R}} t$, that is $s \downarrow_{\mathcal{R}} t$.

Thus $s \uparrow_{\mathcal{R}} t$ implies $s \downarrow_{\mathcal{R}} t$. $\mathcal{R}$ is confluent.

Problem 2.5

Prove that a term rewriting system $\mathcal{R}$ is Church-Rosser if and only if it is confluent.

Solution
<u>To show</u>: $\mathcal{R}$ is Church-Rosser iff $\mathcal{R}$ is confluent.

$\Rightarrow$ We assume: $\mathcal{R}$ is Church-Rosser, i. e., $s \leftrightarrow^*_{\mathcal{R}} t$ iff $s \downarrow_{\mathcal{R}} t$.
To show: $\mathcal{R}$ is confluent, i. e., $s \uparrow_{\mathcal{R}} t$ implies $s \downarrow_{\mathcal{R}} t$.

Let $s \uparrow_{\mathcal{R}} t$.
This implies : $s \leftrightarrow^*_{\mathcal{R}} t$
By Church-Rosser, then $s \downarrow_{\mathcal{R}} t$.

$\Leftarrow$ We assume: $s \uparrow_{\mathcal{R}} t$ implies $s \downarrow_{\mathcal{R}} t$. (confluence)
To show: $s \leftrightarrow^*_{\mathcal{R}} t$ iff $s \downarrow_{\mathcal{R}} t$. (Church-Rosser)

$\Leftarrow$ $s \downarrow_{\mathcal{R}} t$ implies $s \leftrightarrow^*_{\mathcal{R}} t$ is obvious.

$\Rightarrow$ Let $s \leftrightarrow^*_{\mathcal{R}} t$. To show: $s \downarrow_{\mathcal{R}} t$.
Then there is a sequence $s = u_1 \leftrightarrow_{\mathcal{R}} u_2 \leftrightarrow_{\mathcal{R}} \ldots \leftrightarrow_{\mathcal{R}} u_{n-1} \leftrightarrow_{\mathcal{R}} u_n = t$
By induction on the length of the sequence, we prove $s \downarrow_{\mathcal{R}} u_m$ for all m.

<u>IB:</u> $m = 1$
with $s = u_1$, $s \downarrow_{\mathcal{R}} u_1$ follows immediately

<u>IH:</u> for an m we obtain $s \downarrow_{\mathcal{R}} u_m$ from $s = u_1 \leftrightarrow_{\mathcal{R}} \ldots \leftrightarrow_{\mathcal{R}} u_m$

<u>IS:</u> For $m + 1$:
$s = u_1 \leftrightarrow^*_{\mathcal{R}} u_m \leftrightarrow_{\mathcal{R}} u_{m+1}$
By IH, there is term a, such that $s \rightarrow^*_{\mathcal{R}} a \leftarrow^*_{\mathcal{R}} u_m$

<u>case 1</u>: $u_{m+1} \rightarrow_{\mathcal{R}} u_m$
Then we have: $s \rightarrow^*_{\mathcal{R}} a \leftarrow^*_{\mathcal{R}} u_m \leftarrow_{\mathcal{R}} u_{m+1}$
That is $s \rightarrow^*_{\mathcal{R}} a \leftarrow^*_{\mathcal{R}} u_{m+1}$
$\Rightarrow$ $s \downarrow_{\mathcal{R}} u_{m+1}$

<u>case 2</u>: $u_m \rightarrow_{\mathcal{R}} u_{m+1}$
Then we have: $a \leftarrow^*_{\mathcal{R}} u_m \rightarrow^*_{\mathcal{R}} u_{m+1}$
By confluence, there exists b with $a \rightarrow^*_{\mathcal{R}} b \leftarrow^*_{\mathcal{R}} u_{m+1}$.
Then $s \rightarrow^*_{\mathcal{R}} a \rightarrow^*_{\mathcal{R}} b \leftarrow^*_{\mathcal{R}} u_{m+1}$
i. e. $s \rightarrow^*_{\mathcal{R}} b \leftarrow^*_{\mathcal{R}} u_{m+1}$
$\Rightarrow$ $s \downarrow_{\mathcal{R}} u_{m+1}$

with $t = u_n$, $s \downarrow_{\mathcal{R}} t$ follows.

Problem 2.6

Consider the following term rewriting system:

$$f(f(X,Y),Z) \to f(X,f(Y,Z));$$
$$f(X,1) \to X.$$

1. Is it terminating? Justify your answer.
2. Compute all the critical pairs, and show how you got them.
3. Can you orientate the critical pairs, i.e., add a rule $s \to t$ or $t \to s$ for each critical pair $\langle s,t \rangle$, such that termination is preserved? (If it is possible, do it . . .)

Note: When executing the completion algorithm you have to go on trying to build critical pairs with the iteratively added rules.

Solution

1.
   - Yes, it's terminating:
   - Take the following polynomial ordering:

   $$f^I : (m,n) \quad \mapsto \quad 2m+n+1$$
   $$1^I = 1$$

   $(s > t$ iff $s^I > t^I)$

   - for $f(f(X,Y),Z) \to f(X,f(Y,Z))$ we find

   $$\begin{aligned} f(f(X,Y),Z)^I &= 2 \cdot f(X,Y)^I + Z^I + 1 \\ &= 2 \cdot (2 \cdot X^I + Y^I + 1) + Z^I + 1 \\ &= 4 \cdot X^I + 2 \cdot Y^I + Z^I + 3 \\ &> 2 \cdot X^I + 2 \cdot Y^I + Z^I + 2 \\ &= 2 \cdot X^I + (2 \cdot Y^I + Z^I + 1) + 1 \\ &= 2 \cdot X^I + f(Y,Z)^I + 1 \\ &= f(X,f(Y,Z))^I \end{aligned}$$

   - for $f(X,1)^I \to X$ we find

   $$\begin{aligned} f(X,1)^I &= 2 \cdot X^I + 1^I + 1 \\ &= 2 \cdot X^I + 1 + 1 \\ &= 2 \cdot X^I + 2 \\ &> X^I \end{aligned}$$

   - Since a polynomial ordering is a termination ordering, the term rewriting system is terminating.

2. match $1''$ and $1'$:

$$1''\ )\quad f(\underbrace{f(X'',Y'')}_{u},Z'') \to f(X'',f(Y'',Z'')) \qquad (l_1 \to r_1)$$

$$1'\ )\quad \underbrace{f(f(X',Y'),Z')}_{l_2} \to f(X',f(Y',Z')) \qquad (l_2 \to r_2)$$

$\text{mgu}(l_2,u)\colon\ \theta = \{X'' \mapsto f(X',Y'), Y'' \mapsto Z'\}$

$\underline{\text{cp1}} = \langle f(f(X',f(Y',Z')),Z''),\ f(f(X',Y'),f(Z',Z''))\rangle \qquad (= \langle l_1\theta, r_1\theta\rangle)$

match $1''$ and $2'$:

$$1''\ )\quad f(\underbrace{f(X'',Y'')}_{u},Z'') \to f(X'',f(Y'',Z'')) \qquad (l_1 \to r_1)$$

$$2'\ )\quad \underbrace{f(X',1)}_{l_2} \to X' \qquad (l_2 \to r_2)$$

$\text{mgu}(l_2,u)\colon\ \theta = \{X'' \mapsto X', Y'' \mapsto 1\}$

$\underline{\text{cp2}} = \langle f(X',Z''),\ f(X',f(1,Z''))\rangle \qquad (= \langle l_1\theta, r_1\theta\rangle)$

$$1''\ )\quad \underbrace{f(f(X'',Y''),Z'')}_{u} \to f(X'',f(Y'',Z'')) \qquad (l_1 \to r_1)$$

$$2'\ )\quad \underbrace{f(X',1)}_{l_2} \to X' \qquad (l_2 \to r_2)$$

$\text{mgu}(l_2,u)\colon\ \theta = \{X' \mapsto f(X'',Y''), Z'' \mapsto 1\}$

$\underline{\text{cp3}} = \langle f(X'',Y''),\ f(X'',f(Y'',1))\rangle \qquad (= \langle l_1\theta, r_1\theta\rangle)$

There are no further critical pairs with the given rules.

3. Using the termination ordering from above:

- **APPLY REDUCTIONS**

  $\text{cp}_1 = \langle f(f(X',f(Y',Z')),Z''),\ f(f(X',Y'),f(Z',Z''))\rangle$
  $\quad = \langle s_1, t_1\rangle$

$$\begin{aligned} {s_1}^I &= 2(2X'^I + (2Y'^I + Z'^I + 1) + 1) + Z^I + 1 \\ &= 4X'^I + 4Y'^I + 2Z'^I + Z^I + 5 \\ {t_1}^I &= 2(2X'^I + Y'^I + 1) + (2Z'^I + Z^I + 1) + 1 \\ &= 4X'^I + 2Y'^I + 2Z'^I + Z^I + 4 \end{aligned}$$

  So $s_1 > t_1$, we add the rule $s_1 \to t_1$

- $\text{cp}_2 = \langle f(X',Z''),\ f(X',f(1,Z''))\rangle$
  $\quad = \langle s_2, t_2\rangle$

$$\begin{aligned} {s_2}^I &= 2X'^I + Z''^I + 1 \\ {t_2}^I &= 2X'^I + (2 + Z''^I + 1) + 1 \\ &= 2X'^I + Z''^I + 4 \end{aligned}$$

  So $t_2 > s_2$, we add the rule $t_2 \to s_2$

- $\text{cp}_3 = \langle f(X'', Y''),\ f(X'', f(X'', 1))\rangle$
  $= \langle s_3, t_3 \rangle$

$$\begin{aligned} {s_3}^I &= 2X''^I + Y''^I + 1 \\ {t_3}^I &= 2X''^I + (2Y''^I + 1 + 1) + 1 \\ &= 2X''^I + 2Y''^I + 3 \end{aligned}$$

  So $t_3 > s_3$, we add the rule $t_3 \to s_3$

Termination is preserved.

Problem 2.7

Let $\mathcal{R}$ be a term rewriting system and $>/2$ a termination ordering.

If for all rules $l \to r \in \mathcal{R}$ the relation $l > r$ holds, then $\mathcal{R}$ is terminating.

Solution

Assume that $\mathcal{R}$ is not terminating.

Then exists an infinite rewriting sequence $s_1, \dots, s_n, \dots$

Since every pair (s_n, s_{n+1}) in this sequence has been generated
by a rewriting step with a respective rule $l \to r$,
due to the conditions of a termination ordering it follows that $s_n > s_{n+1}$ holds, because

> due to the full invariance every instance $l\sigma \to r\sigma$ of $l \to r$ satisfies $l\sigma > r\sigma$,
> and due to the replacement property this $>$ is passed on to $s_n > s_{n+1}$

Thus we would get an infinite sequence $s_1 > \cdots > s_n > \cdots$ of terms
in contrast to our assumptions on $>/2$

Problem 2.8

Consider the term rewriting system

$$\begin{aligned} \mathcal{R} = \{\ & f(g(X)) \to g(X), && (1) \\ & g(h(X)) \to g(X)\ \} && (2) \end{aligned}$$

Show that $\mathcal{R}$ is canonical.

Solution

We have to show that $\mathcal{R}$ is terminating and confluent.

Termination:

We use the termination ordering on terms s given by the length of the word s .

The following holds:

For rule (1):

$|f(g(X))| = |g(X)| + 3 > |g(X)|$ for all ground substitutions θ

For rule (2):

$|g(h(X))| = |g(X)| + 3 > |g(X)|$ for all ground substitutions θ

Thus for all rules $l \to r$ holds that $s > t$ iff $s \to_{\mathcal{R}} t$

and consequently, $\mathcal{R}$ is terminating.

<u>Confluence</u>:

By matching (1), (2) we obtain the only critical pair of $\mathcal{R}$

(1) $f(\underbrace{g(X)}_{l_1}) \to g(X)$

(2') $\underbrace{g(h(X'))}_{l_2} \to g(X')$

$\theta = \text{mgu}(l_1, l_2) = \{X \to h(X')\}$ and the critical pair $\langle f(g(X')),\ g(h(X'))\rangle$

We have f(g(X')) $\xrightarrow{(1)}$ g(X') $\xleftarrow{(2)}$ g(h(X'))

$\Rightarrow$ By a thorem of the lectures $\mathcal{R}$ is locally confluent.

$\Rightarrow$ By a theorem of the lectures $\mathcal{R}$ is confluent.

$\Rightarrow$ $\mathcal{R}$ is canonical.