Problem 2.1

In the lectures, \( \approx_E \) was defined to be the \textit{least congruence relation generated by} \( E \). What does it mean?

**Solution**

We define \( s \approx_E t \) iff \( E \cup E_\approx \models s \approx t \). In other words, \( \approx_E \) is the least relation satisfying the following properties:

1. if \( s \approx t \in E \), then \( s \approx_E t \), \hspace{1cm} (generated by \( E \))
2. \( s \approx_E s \) for all \( s \in \mathcal{T}(\mathcal{F}, \mathcal{V}) \), \hspace{1cm} (reflexivity)
3. if \( s \approx_E t \), then \( t \approx_E s \), \hspace{1cm} (symmetric)
4. if \( s \approx_E t \) and \( t \approx_E u \), then \( s \approx_E u \), \hspace{1cm} (transitivity)
5. if \( s_i \approx_E t_i \) for all \( i \in \{1, \ldots, n\} \), then \( f(s_1, \ldots, s_n) \approx_E f(t_1, \ldots, t_n) \), and \hspace{1cm} (congruence)
6. if \( s \approx_E t \), then \( s\sigma \approx_E t\sigma \) for all substitutions \( \sigma \). \hspace{1cm} (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 \( \theta \) used in every step.

**Solution**
Problem 2.3

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

1. $s \rightarrow_R t$ implies $s \approx_{E_R} t$.
2. $s \leftrightarrow^* R t$ implies $s \approx_{E_R} t$.

Solution

1. We assume $s \rightarrow_R t$
   - By definition there is $l \rightarrow r \in \mathcal{R}$, $\pi \in \mathcal{P}_s$ and a substitution $\theta$ such that $s[\pi] = l\theta$ and $t = s[\pi/r\theta]$.
   - By definition we have $l \approx r \in \mathcal{E}_R$, consequently $\mathcal{E}_R \models \forall l \approx r$
   - Then obviously $\mathcal{E}_R \models \forall l\sigma \approx r\sigma$ for all substitutions $\sigma$
     in particular $\mathcal{E}_R \models \forall l\theta \approx r\theta$, i.e., $l\theta \approx_{E_R} r\theta$.
   - Because $l\theta \approx_{E_R} r\theta$, $s[\pi] = l\theta$ and $f$-substitutivity: $s \approx_{E_R} s[\pi/r\theta] = t$
     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 $s \leftrightarrow^* R t$
   Then there is a sequence $u_1, \ldots, u_n$ of terms, with
   $$s = u_1$$
   $$t = u_n$$
   $$u_i \leftrightarrow_R u_{i+1}, \ 1 \leq i < n$$
(because $\leftrightarrow^*_{R}$ is the reflexive, transitive closure of $\leftrightarrow_R$)

We prove $\exists u_1 \approx_{\mathcal{E}_R} u_n = t$ by induction on the length $n$ of the sequence

**IB:** $n = 1$

Then $s = u_1 = t$ and $s \approx_{\mathcal{E}_R} t$, because $\approx_{\mathcal{E}_R}$ is reflexive.

**IH:** For sequences $u'_1, \ldots, u'_n$ of length $n$ it holds that $u'_1 \approx_{\mathcal{E}_R} u'_n$

**IS:** For a sequence $s = u_1 \leftrightarrow_R \cdots \leftrightarrow_R u_{n+1} = t$ of length $n + 1$:

- $u_1 \ldots u_n$ is a sequence of length $n$, so by IH:

  $s = u_1 \approx_{\mathcal{E}_R} u_n$

  $u_n \leftrightarrow_R u_{n+1}$ means either $u_n \rightarrow_R u_{n+1}$ or $u_n \leftrightarrow_R u_{n+1}$

  and by part 1: $u_n \approx_{\mathcal{E}_R} u_{n+1} = t$

Because $\approx_{\mathcal{E}_R}$ 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 terminating trs can be confluent.

For example: $R = \{ a \rightarrow b, b \rightarrow a \}$

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

\[
\begin{array}{c}
S \\
\xrightarrow[R]{} a \rightarrow_R b
\end{array}
\]

2) Let $s \uparrow_R t$

Then there exists a term $u$ such that $s \leftarrow_R u \rightarrow_R t$.

$u \rightarrow_R s$ implies that there is a sequence $v_1, \ldots, v_n$ of terms

with $v_1 = u$, $v_n = s$ and $v_i \rightarrow_R v_{i+1}$, $1 \leq i < n$.

$v_i \rightarrow_R v_{i+1}$ means:

$v_{i+1} = v_i[\pi \mapsto r]$ with $v_i[\pi] = l$ with $l = a, r = b$ or $l = b, r = a$

$(r\theta = r$ for all $\theta, \ l\theta = l$ for all $\theta)$.

Then holds $v_{i+1} \rightarrow_R v_i$ using the “opposite” rule $r \rightarrow l$

because with $v_{i+1}[\pi] = r$ (obviously) $v_i = v_{i+1}[\pi \mapsto l]$.

This means $v_i \leftarrow_R v_{i+1}$ for all $1 \leq i < n$ and $u \leftarrow_R s$.

By an analogous argument, we find $t \rightarrow_R u$.

Thus we get: $s \rightarrow_R u \leftarrow_R t$, that is $s \downarrow_R t$.

Thus $s \uparrow_R t$ implies $s \downarrow_R t$. $R$ is confluent.

### Problem 2.5

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

**Solution**

To show: $R$ is Church-Rosser iff $R$ is confluent.
We assume: $R$ is Church-Rosser, i.e., $s \leftrightarrow^* R t$ iff $s \downarrow R t$.

To show: $R$ is confluent, i.e., $s \uparrow R t$ implies $s \downarrow R t$.

Let $s \uparrow R t$.
This implies: $s \leftrightarrow R t$
By Church-Rosser, then $s \downarrow R t$.

$\Leftarrow$ We assume: $s \uparrow R t$ implies $s \downarrow R t$. (confluence)
To show: $s \leftrightarrow^* R t$ iff $s \downarrow R t$. (Church-Rosser)

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

IB: $m = 1$
with $s = u_1$, $s \downarrow R u_1$ follows immediately

IH: for an $m$ we obtain $s \downarrow R u_m$ from $s = u_1 \leftrightarrow R \ldots \leftrightarrow R u_m$

IS: For $m + 1$:
$s = u_1 \leftrightarrow^* R u_m \leftrightarrow R u_{m+1}$
By IH, there is term $a$, such that $s \to^* R a \leftrightarrow^* R u_m$

$\underline{case 1}$: $u_{m+1} \to R u_m$

Then we have: $s \to^* R a \leftrightarrow^* R u_m \leftrightarrow R u_{m+1}$
That is $s \to^* R a \leftrightarrow^* R u_{m+1}$
$\Rightarrow$ $s \downarrow R u_{m+1}$

$\underline{case 2}$: $u_m \to R u_{m+1}$
Then we have: $a \leftrightarrow^* R u_m \to^* R u_{m+1}$
By confluence, there exists $b$ with $a \to^* R b \leftrightarrow^* R u_{m+1}$.
Then $s \to^* R a \to^* R b \leftrightarrow^* R u_{m+1}$
i.e. $s \to^* R b \leftrightarrow^* R u_{m+1}$
$\Rightarrow$ $s \downarrow R u_{m+1}$

with $t = u_n$, $s \downarrow R t$ follows.
Problem 2.6

Consider the following term rewriting system:

\[ f(f(X, Y), Z) \rightarrow f(X, f(Y, Z)); \]
\[ f(X, 1) \rightarrow X. \]

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 \( s \rightarrow t \) or \( t \rightarrow s \) 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:

     \[ f^l : (m, n) \mapsto 2m + n + 1 \]
     \[ 1^l = 1 \]

     \((s > t \text{ iff } s^l > t^l)\)

   • for \( f(f(X, Y), Z) \rightarrow f(X, f(Y, Z)) \) we find

     \[ f(f(X, Y), Z)^l = 2 \cdot f(X, Y)^l + Z^l + 1 \]
     \[ = 2 \cdot (2 \cdot X^l + Y^l + 1) + Z^l + 1 \]
     \[ = 4 \cdot X^l + 2 \cdot Y^l + Z^l + 3 \]
     \[ > 2 \cdot X^l + 2 \cdot Y^l + Z^l + 2 \]
     \[ = 2 \cdot X^l + (2 \cdot Y^l + Z^l + 1) + 1 \]
     \[ = 2 \cdot X^l + f(Y, Z)^l + 1 \]
     \[ = f(X, f(Y, Z))^l \]

   • for \( f(X, 1)^l \rightarrow X \) we find

     \[ f(X, 1)^l = 2 \cdot X^l + 1^l + 1 \]
     \[ = 2 \cdot X^l + 1 + 1 \]
     \[ = 2 \cdot X^l + 2 \]
     \[ > X^l \]

   • Since a polynomial ordering is a termination ordering, the term rewriting system is terminating.
2. match 1’’ and 1’:
   1’’ \[ f(f(X'', Y''), Z'') \rightarrow f(X'', f(Y'', Z'')) \] 
   \[ (l_1 \rightarrow r_1) \]
   1’ \[ f(f(X', Y'), Z') \rightarrow f(X', f(Y', Z')) \] 
   \[ (l_2 \rightarrow r_2) \]
   \[ \text{mgu}(l_2, u) : \theta = \{ X'' \mapsto f(X', Y'), Y'' \mapsto Z' \} \]
   \[ \text{cp}1 = \langle f(f(X', Y', Z'), f(f(X', Y'), f(Z', Z'))), f(f(X', Y'), f(Z', Z')) \rangle \]
   \[ = \langle l_1 \theta, r_1 \theta \rangle \]

match 1’’ and 2’:
   1’’ \[ f(f(X'', Y''), Z'') \rightarrow f(X'', f(Y'', Z'')) \] 
   \[ (l_1 \rightarrow r_1) \]
   2’ \[ f(X', 1) \rightarrow X' \] 
   \[ (l_2 \rightarrow r_2) \]
   \[ \text{mgu}(l_2, u) : \theta = \{ X'' \mapsto X', Y'' \mapsto 1 \} \]
   \[ \text{cp}2 = \langle f(X', Z''), f(X', f(1, Z'')) \rangle \]
   \[ = \langle l_1 \theta, r_1 \theta \rangle \]

   1’’ \[ f(f(X'', Y''), Z'') \rightarrow f(X'', f(Y'', Z'')) \] 
   \[ (l_1 \rightarrow r_1) \]
   2’ \[ f(X', 1) \rightarrow X' \] 
   \[ (l_2 \rightarrow r_2) \]
   \[ \text{mgu}(l_2, u) : \theta = \{ X'' \mapsto f(X'', Y''), Z'' \mapsto 1 \} \]
   \[ \text{cp}3 = \langle f(X'', Y''), f(X'', f(Y'', 1)) \rangle \]
   \[ = \langle l_1 \theta, r_1 \theta \rangle \]

   There are no further critical pairs with the given rules.

3. Using the termination ordering from above:

   - **APPLY REDUCTIONS**

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

   \[ s_1^I = 2(2X'^I + (2Y'^I + Z'^I + 1) + 1) + Z'^I + 1 \]
   \[ = 4X'^I + 4Y'^I + 2Z'^I + Z'^I + 5 \]

   \[ t_1^I = 2(2X'^I + Y'^I + 1) + (2Z'^I + Z'^I + 1) + 1 \]
   \[ = 4X'^I + 2Y'^I + 2Z'^I + Z'^I + 4 \]

   So \( s_1 > t_1 \), we add the rule \( s_1 \rightarrow t_1 \)

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

   \[ s_2^I = 2X'^I + Z''^I + 1 \]

   \[ t_2^I = 2X'^I + (2 + Z''^I + 1) + 1 \]
   \[ = 2X'^I + Z''^I + 4 \]

   So \( t_2 > s_2 \), we add the rule \( t_2 \rightarrow s_2 \)
• $cp_3 = \langle f(X'', Y''), f(X'', f(X'', 1)) \rangle$
  
  $s_3^I = 2X''I + Y'''I + 1$
  $t_3^I = 2X''I + (2Y'''I + 1 + 1) + 1$
  
  $= 2X''I + 2Y'''I + 3$

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

Termination is preserved.

Problem 2.7

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

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

Solution

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

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

Since every pair $(s_n, s_{n+1})$ in this sequence has been generated by a rewriting step with a respective rule $l \rightarrow r$,
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 $l\sigma \rightarrow r\sigma$ of $l \rightarrow r$ 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

$$\mathcal{R} = \{ f(g(X)) \rightarrow g(X), \quad \text{(1)} $$

$$g(h(X)) \rightarrow g(X) \} \quad \text{(2)}$$

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):
\[ |f(g(X))| = |g(X)| + 3 > |g(X)| \text{ for all ground substitutions } \theta \]

For rule (2):
\[ |g(h(X))| = |g(X)| + 3 > |g(X)| \text{ for all ground substitutions } \theta \]

Thus for all rules \( l \rightarrow r \) holds that \( s > t \) iff \( s \rightarrow_R t \) and consequently, \( R \) is terminating.

**Confluence:**

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

\[
\begin{align*}
(1) & \quad f(g(X)) \rightarrow g(X) \\
(2') & \quad g(h(X')) \rightarrow g(X')
\end{align*}
\]

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

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

\[ \Rightarrow \text{ By a theorem of the lectures } R \text{ is locally confluent.} \]
\[ \Rightarrow \text{ By a theorem of the lectures } R \text{ is confluent.} \]

\[ \Rightarrow R \text{ is canonical.} \]