Lecture notes on rewriting theory  
Lecture 5  
Frédéric Blanqui (INRIA)  
19 September 2016, last revised on 8 January 2020

1 Confluence of orthogonal systems

We have already seen that there are locally confluent relations that are non-confluent. This is still so even though \( R \) has no critical pair as shown by the following example due to Huet:

\[
\begin{align*}
f \ x \ x & \rightarrow a \\
f \ x \ (g \ x) & \rightarrow b \\
c & \rightarrow g \ c
\end{align*}
\]

This system has no critical pair, so it is locally confluent, but it is not confluent since \( a \leftarrow f \ c \ c \rightarrow f \ c \ (g \ c) \rightarrow b. \)

On the other hand, if \( R \) is also left-linear (for every rule \( l \rightarrow r \in R \), \( l \) is linear), then it is confluent (even though it does not terminate), a result due to Huet [1] that is very useful since, in many programming languages (e.g. OCaml, Haskell), the operational semantics is an orthogonal rewrite system (Huet’s result is about rewriting on first-order terms but has been later extended to rewriting on \( \lambda \)-terms too).

**Definition 1** A rewrite system is orthogonal if it is left-linear and has no critical pair.

**Theorem 1** Orthogonal rewrite systems are confluent.

Proof. The idea of the proof is to introduce a new relation, \( \rightarrow_R \), allowing rewriting of several subterms at the same time if they are at disjoint positions, that is, \( \rightarrow_R \) is the smallest reflexive stable relation containing \( R \) and such that \( f^i \xrightarrow{\rightarrow_R} f^i u \) whenever, for all \( i, t_i \xrightarrow{\rightarrow_R} u_i \). Hence, \( \rightarrow_R \subseteq \rightarrow_R \subseteq \rightarrow_R^{*} \) and \( \rightarrow_R \) is confluent whenever \( \rightarrow_R \) is confluent. We now prove that \( \leftarrow_R \rightarrow_R \subseteq \rightarrow_R \rightarrow_R^{*} \), by induction on the definition of \( \leftarrow_R \). Assume that \( t_1 \xleftarrow{\leftarrow_R} t \xrightarrow{\rightarrow_R} t_2 \).

- Case \( t_1 = t \) or \( t_2 = t \). Immediate.
2 Basic definitions and results

Lemma 1 (Newman, 1942, [3]) If \( R \) is terminating and locally confluent, then \( R \) is confluent.

Proof. By well-founded induction on \( R \). Assume that \( tR^*u_i, i \in \{1, 2\} \). If \( t = u_1 \) or \( t = u_2 \), then we are done. Otherwise, for all \( i \), there is \( t_i \) such that \( tR_i R^*u_i \). By local confluence, there is \( u \) such that, for all \( i \), \( t_i R^*u \). Now, by induction hypothesis, there is \( v \) such that \( uR^*v \) and \( uR^*v \). And since \( t_2 R^*uR^*v \), by induction hypothesis again, there is \( w \) such that \( u_2 R^*w \) and \( vR^*w \).

Remark:

Lemma 2 If \( M >_{\text{mul}} N \) and \( P \subseteq >_{\text{mul}} (M) \implies (N) \), then \( M >_{\text{mul}} N + P \).

Proof. Assume that \( M = Z + X, N = Z + Y, X \neq \emptyset \) and \( Y \subseteq >_{\text{mul}} (X) \). The result holds since \( P \subseteq >_{\text{mul}} (Z + X) = >_{\text{mul}} (Z + Y) = >_{\text{mul}} (X) \implies (Z + Y) \subseteq >_{\text{mul}} (X) \).
3 Confluence by locally decreasing diagrams

Decreasing diagrams is a powerful confluence technique introduced by van Oostrom in 1992 (see section 2.3 in [3] or [4]), that generalizes Newman’s lemma and is complete for cofinal, countable or normalizing relations.

The idea is to label rewrite steps into a well-founded domain \((I, \succ)\), extend \(\succ\) into a well-founded relation \(\succ_{lm}\) on \(I^*\), and check that every local peak satisfies some property wrt \(\leq_{lm}\).

Labeling rewrite steps allows to represent rewrite sequences by words.

**Definition 2 (Lexicographic maximum order)** Given a strict order \(<\) on a set \(I\), the lexicographic maximum order is the relation \(<_{lm}\) on \(I^*\) such that \(a <_{lm} b\) iff \(|a| <_{mul} |b|\) where \(||\) is recursively defined as follows:

- \(|\varepsilon| = \emptyset\)
- \(|ia| = [i] + (|a|/\{i\})\)

where \([i]\) is the multiset with one occurrence of \(i\) and \(M/S = M - \succ(S)\) is the multiset obtained by removing in \(M\) every occurrence of an element smaller than an element of \(S\).

**Example:** \(|132343| = [1, 3, 3, 4]\) and \(|211| = [2]\).

In the following, we simply write \(\leq\) instead of \(\leq_{lm}\), and \(a\) instead of \(|a|\).

**Lemma 3** • If \(\succ\) is a (well-founded) order, then \(\succ_{lm}\) is a (well-founded) order.

- \(ab = a + b/a\)

**Proof.**

- Since \(\succ_{lm} \subseteq \succ_{mul}\).
- By induction on \(a:\)
  - \(\varepsilon b = b = \varepsilon + b/\varepsilon\).
  - \((ia)b = i(ab) = i + ab/i = i + (a + b/a)/i = i + a/i + b/ia = ia + b/ia\).

We then measure the size of a peak by the multiset \(a + b\).

We now prove that inner peaks are strictly smaller than outer peaks if the inner diagram is decreasing:

**Definition 3 (Decreasing diagram)** A diagram \((a, b, b', a')\) representing
is decreasing if $b'/a \leq b$ and $a'/b \leq a$.

**Lemma 4** If $(a, b, b', a')$ is a decreasing diagram with $b \neq \varepsilon$ then, for all $c$, $a' + c < a + bc$ and $c + b' < ac + b$.

**Proof.** $a' + c = (a' + c)\cap > (b) + (a' + c)/b < b + a'/b + c/b \leq b + a + c/b = a + bc$, and $c + b' = (c + b')\cap > (a) + (c + b')/a < a + c/a + b = ac + b$.

We now prove that horizontal and vertical compositions preserve decreasingness:

**Lemma 5** • If $(a, b, b', a')$ and $(a', c, c', a'')$ are decreasing, then $(a, bc, b', a'')$ is decreasing.

• If $(a, b, b', a')$ and $(c, b', b'', c')$ are decreasing, then $(ac, b, b'' , a'c')$ is decreasing.

**Proof.** We give the proof for horizontal composition only. The proof for vertical composition is similar.

• We prove that $a''/bc \leq a$.
  
  $a''/bc = (a''/c)/b \leq a'/b \leq a$. 

4
We prove that $b'c'/a \leq bc = b + c/b$.

Now, $b'/a + (c'/ab') \cap > (b) \leq b$ by Lemma 2 since $b'/a \leq b$ and $(c'/ab') \cap > (b) = (c' \cap > (b))/ab' = (c' \cap > (b))/(a + b'/a) \subseteq > (b) - > (b/a)$. Moreover, $c'/ab'b \leq c'/ba'$ since $ba' = b + a'/b \leq b + a \subseteq b'ab$, and $c'/ba' = (c'/a')/b \leq c/b$. Hence, $b'c'/a \leq b + c/b = bc$. ■

Theorem 2 (van Oostrom, 1992, [4]) Let $(\rightarrow_i)_{i \in I}$ and $(\rightarrow_j)_{j \in J}$ be two families of relations on a set $A$, and $> b$ a well-founded order on $I \cup J$. The relations $\rightarrow_I = \bigcup_{i \in I} \rightarrow_i$ and $\rightarrow_J = \bigcup_{j \in J} \rightarrow_j$ commute if, for all $i \in I$ and $j \in J$, there is a decreasing diagram $(i, j, a, b)$, that is, by definition of the lexicographic maximum order:

![Diagram](https://via.placeholder.com/150)

Proof. The proof is similar to the one of Newman’s lemma (Lemma 1). We prove that every peak $(a, b)$ can be closed by a decreasing diagram $(a, b', a')$, by induction on the well-founded relation $>$ such that $(a, b) > (c, d)$ if $|a| + |b| >_{\text{lm}} |c| + |d|$. Assume that we have a peak $(ia, jb)$:

![Diagram](https://via.placeholder.com/150)

By assumption, there is a decreasing diagram $(i, j, c, d)$. By Lemma 5, $d + b < i + jb \leq ia + jb$. Hence, by induction hypothesis, there is a decreasing diagram...
(d, b, b', d'). Since horizontal composition preserves decreasingness, (i, jb, cb', d') is decreasing. By Lemma 5, a + cb' < ia + jb. Hence, by induction hypothesis, there is a decreasing diagram (a, cb', e, a'). Therefore, there is a diagram (ia, jb, e, d'a'). Moreover, since vertical composition preserves decreasingness, this diagram is decreasing too.

We are now going to prove that this technique is complete for countable or weakly normalizing relations.

Definition 4 (Locally-decreasing-diagram property) A relation $\rightarrow$ has the locally-decreasing-diagram property if there is a well-founded domain $(I, >)$ such that $\rightarrow = \bigcup_{i \in I} \rightarrow_i$ and, for all $i, j \in I$, there are $a, b \in I^*$ such that $(i, j, a, b)$ is decreasing.

Definition 5 (Cofinality property) A relation $\rightarrow$ has the cofinality property if, for all $t$, there is a (finite or infinite) rewrite sequence $t = t_0 \rightarrow t_1 \rightarrow \ldots$ such that, for all $u$, if $t \rightarrow^* u$, then there is $k$ such that $u \rightarrow^* t_k$.

Remark: this notion comes from order theory where a subset $X$ of a poset $(Y, \leq)$ is cofinal if, for all $y \in Y$, there is $x \in X$ such that $y \leq x$. Here, $Y = \rightarrow^* (t)$, $\leq = = \rightarrow^*$ and $X = \{t_k\}$.

Lemma 6 (Klop, 1980, [2]) If $\rightarrow$ has the cofinality property, then $\rightarrow$ is confluent.

Proof. Assume that $\rightarrow$ has the cofinality property, $t \rightarrow^* u$ and $t \rightarrow^* v$. Then, there is $k_u$ and $k_v$ such that $u \rightarrow^* t_{k_u}$ and $v \rightarrow^* t_{k_v}$. Wlog. we can assume that $k_u \leq k_v$. Therefore, $t_{k_u} \rightarrow^* t_{k_v}$.

Theorem 3 (Klop, 1980, [2]) If $\rightarrow$ is confluent and countable, then $\rightarrow$ has the cofinality property.

Proof. Assume now that $\rightarrow$ is confluent and countable. Since $\rightarrow$ is countable, there is an enumeration $a_0, a_1, \ldots$ of all the reducts of $t$. Wlog we can take $a_0 = t$. Then, let $s_0 = a_0 = t$ and, for all $k$, let $s_{k+1}$ be a common reduct of $s_k$ and $a_{k+1}$. It exists since $\rightarrow$ is confluent and both $s_k$ and $a_{k+1}$ are reducts of $t$. Note that, for all $k$, $a_k \rightarrow^* s_k \rightarrow^* s_{k+1}$. Hence, $(s_k)_k$ is a sequence of $\rightarrow^*$ steps. Let $(t_k)_k$ be the underlying sequence of $\rightarrow$ steps. Now, one can easily check that, for all $u$, if $t \rightarrow^* u$, then there is $k$ such that $u \rightarrow^* t_k$. Indeed, if $t \rightarrow^* u$, then $u = a_i$ for some $i$. Therefore, $u \rightarrow^* s_i = t_k$ for some $k$.

As remarked by van Oostrom, Klop’s condition of countability can be replaced by weak normalization:

Lemma 7 If $\rightarrow$ is confluent and weakly normalizing, then $\rightarrow$ has the cofinality property.

Proof. For $(t_k)_k$, take any sequence from $t$ to its normal form $v$. If $t \rightarrow^* u$ then, by confluence, $u \rightarrow^* v$. ■
Lemma 8 If \((\rightarrow_k)_{k \in K}\) is a family of pairwise disjoint relations having the locally-decreasing-diagram property, then \(\bigcup_{k \in K} \rightarrow_k\) has the locally-decreasing-diagram property.

Proof. Take \(I = \bigcup_{k \in K} I_k\) and \(< = \bigcup_{k \in K} <_k\) with \((I_k,<_k)\) the label set of \(\rightarrow_k\).

Lemma 9 If \(\rightarrow\) has the cofinality property then, for all \(t\), there is a rewrite sequence \(t = t_0 \rightarrow t_1 \rightarrow \ldots\) such that the \(t_k\)'s are pairwise distinct.

Proof. Assume that \(a\) occurs infinitely often in \((t_k)_k\). Then, every reduct of \(t\) rewrites to \(a\) and we can take \([a]\) itself as cofinal rewrite sequence. Otherwise, let \(a_0 = t\) and, for all \(k\), let \(a_{k+1}\) be the reduct in \((t_k)_k\) following the last occurrence of \(a_k\).

Theorem 4 (Van Oostrom, 1994, [5]) If \(\rightarrow\) has the cofinality property, then \(\rightarrow\) has the locally-decreasing-diagram property.

Proof. By the previous modularity lemma, it is enough to prove the theorem for the restriction of \(\rightarrow\) to the equivalence class modulo \(\leftrightarrow^*\) of some element \(t\). Let \(t = t_0 \rightarrow \ldots\) be the rewrite sequence made of pairwise distinct elements given by cofinality.

We label a step \(a \rightarrow b\) by:

- 0 if there is \(k\) such that \(a = t_k\) and \(b = t_{k+1}\),
- \(i + 1\) if there is no such \(k\) and \(i\) is the minimum number of rewrite steps necessary to reach some \(t_k\) from \(b\) (\(i\) exists since \(b \leftrightarrow^* t\); thus, by confluence, there is \(u\) such that \(b \rightarrow^* u\) and \(t \rightarrow^* u\); thus, by cofinality, there is \(k\) such that \(u \rightarrow^* t_k\).

We now prove that, for all \(i, j \in \mathbb{N}\), there are words \(p, q\) over \(\mathbb{N}\) such that \((i, j, p, q)\) is decreasing. Assume that \(a \rightarrow_i b\) and \(a \rightarrow_j c\).

If \(i = j = 0\), then there are \(k\) and \(l\) such that \(a = t_k = t_l\), \(b = t_{k+1}\) and \(c = t_{l+1}\). Since the \(t_i\)'s are pairwise distinct, \(k = l\) and \(b = c\). So, the diagram is decreasing.

If \(i > 0\) and \(j > 0\) then, there are \(k\) and \(l\) such that \(b \rightarrow_{i-1} \ldots \rightarrow_1 t_k\) and \(c \rightarrow_{j-1} \ldots \rightarrow_1 t_l\). If \(k \leq l\), then \(t_k \rightarrow_0 \rightarrow_1 t_l\) and the diagram is decreasing since \((i-1)\ldots(1)0^{l-k}/i \leq j\) and \((j-1)\ldots(1)/j \leq i\). Otherwise, \(t_l \rightarrow_0 \rightarrow_1 t_k\) and the diagram is decreasing too.

If \(i = 0\) and \(j > 0\) then, there is \(k\) such that \(a = t_k\), \(b = t_{k+1}\) and \(c \rightarrow t_{j-1} \ldots \rightarrow_1 t_l\). If \(k + 1 \leq l\), then \(t_{k+1} \rightarrow_0 t_k \rightarrow_0 \ldots \rightarrow_1 t_l\) and the diagram is decreasing since \(0^{l-k-1}/0 \leq j\) and \((j-1)\ldots(1)/j \leq 0\). Otherwise, \(l < k + 1\) and \(t_l \rightarrow_{k+1-l} t_{k+1}\) and the diagram is decreasing too since \(\varepsilon/0 \leq j\) and \((j-1)\ldots(1)0^{k+1-l}/j \leq 0\).

The case \(i > 0\) and \(j = 0\) is similar by symmetry.
References


