Certification of Classical Confluence Results for Left-Linear Term Rewrite Systems

Julian Nagele Aart Middeldorp

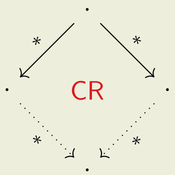
Department of Computer Science
University of Innsbruck

ITP 2016 August 23, 2016

Rewriting

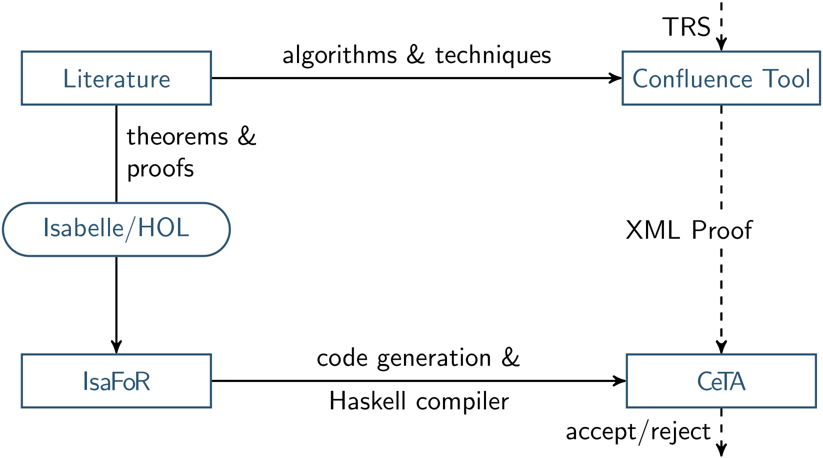
- simple computational model for equational reasoning
- widely used in proof assistants, functional programming,...
- this talk: untyped first-order term rewriting

Confluence Criteria



Knuth and Bendix, orthogonality, strongly/parallel/development closed critical pairs, decreasing diagrams (rule labeling), parallel and simultaneous critical pairs, divide and conquer techniques (commutation, layer preservation, order-sorted decomposition), decision procedures, depth/weight preservation, reduction-preserving completion, Church-Rosser modulo, relative termination and extended critical pairs, non-confluence techniques (tcap, tree automata, interpretation), ...

Reliable Automatic Confluence Analysis



Critical Pairs

Definition

$\rightarrow$ is strongly confluent if $\leftarrow \cdot \rightarrow \ \subseteq \rightarrow^* \cdot {}^=\!\!\leftarrow$

Definition

critical overlap $(\ell_1 \rightarrow r_1, C, \ell_2 \rightarrow r_2)_\mu$ consists of

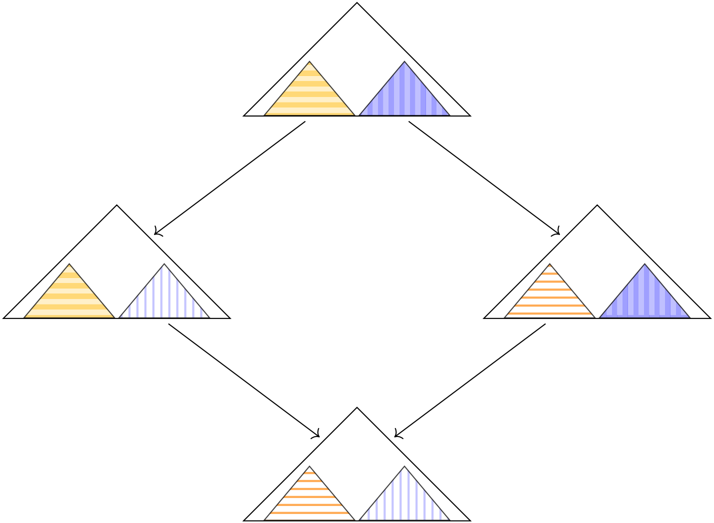
- (variable disjoint variants of) rules $\ell_1 \rightarrow r_1$, $\ell_2 \rightarrow r_2$
- context C, such that $\ell_2 = C[\ell']$ with $\ell' \notin \mathcal{V}$ and $\mathrm{mgu}(\ell_1, \ell') = \mu$

then $C\mu[r_1\mu] \leftarrow\!\rtimes\!\rightarrow r_2\mu$ is critical pair

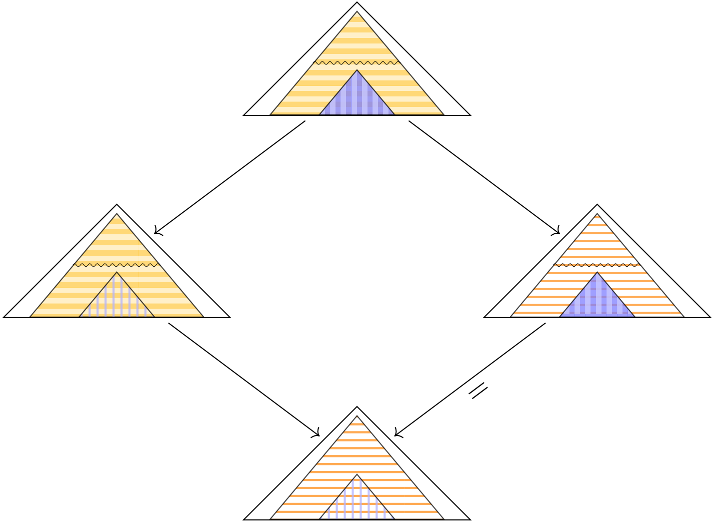
Theorem (Huet)

If TRS $\mathcal{R}$ is linear and $s \rightarrow^= \cdot {}^*\!\!\leftarrow t$ and $s \rightarrow^* \cdot {}^=\!\!\leftarrow t$ for all $t \leftarrow\!\rtimes\!\rightarrow s$ then $\rightarrow_\mathcal{R}$ is strongly confluent

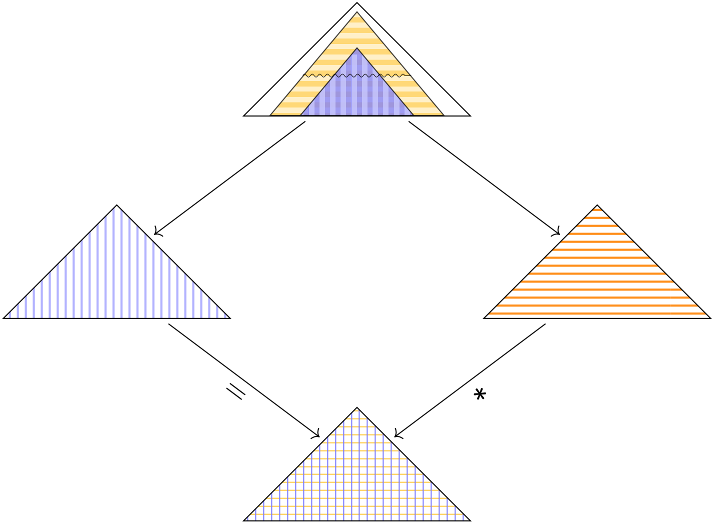
Proof by Picture



Proof by Picture



Proof by Picture



Critical Pairs

Example

- TRS $\mathcal{R}$

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

- 4 non-trivial critical pairs

$$\mathsf{f}(\mathsf{f}(x,\mathsf{f}(y,z)),v) \leftarrow\!\rtimes\!\rightarrow \mathsf{f}(\mathsf{f}(x,y),\mathsf{f}(z,v)) \qquad \mathsf{f}(x,\mathsf{f}(y,z)) \leftarrow\!\rtimes\!\rightarrow \mathsf{f}(z,\mathsf{f}(x,y))$$
$$\mathsf{f}(z,\mathsf{f}(x,y)) \leftarrow\!\rtimes\!\rightarrow \mathsf{f}(x,\mathsf{f}(y,z)) \qquad \mathsf{f}(\mathsf{f}(y,x),z) \leftarrow\!\rtimes\!\rightarrow \mathsf{f}(x,\mathsf{f}(y,z))$$

- are strongly closed, hence $\mathcal{R}$ is (strongly) confluent

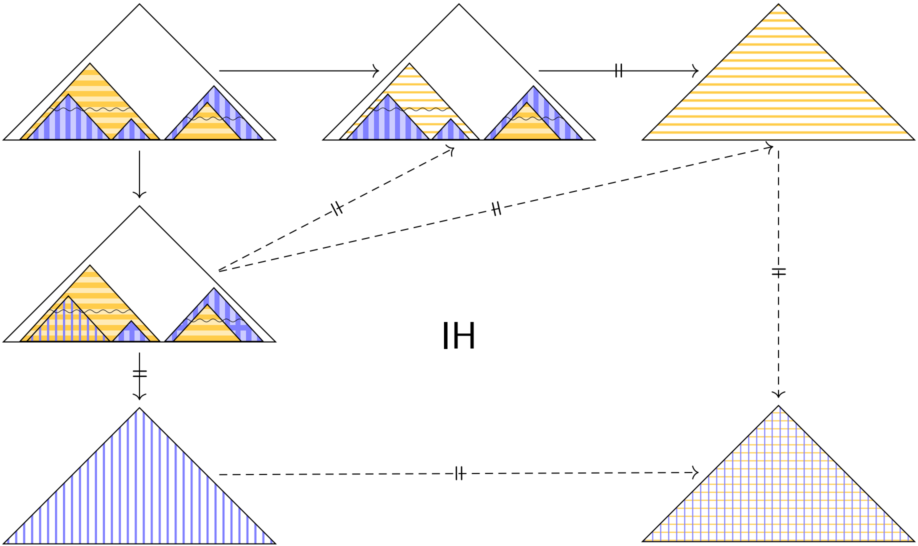
Remark

Right-linearity is a rather unnatural restriction

Theorem (Huet)

If $\mathcal{R}$ is left-linear and $s \mathrel{+\!\!\!\!\twoheadrightarrow} t$ for all $s \leftarrow\!\rtimes\!\rightarrow t$ then $\mathrel{+\!\!\!\!\twoheadrightarrow}$ has the diamond property

Proof by Picture



Parallel Rewriting and Measuring Overlap

Definitions (Huet)

- $s \xrightarrow[\Vert]{\{p_1,\ldots,p_n\}} t$ if $p_i \parallel p_j$ for $i \neq j$ and $s|_{p_i} \to^\epsilon t|_{p_i}$ for all $1 \leqslant i,j \leqslant n$
- overlap of peak is $\blacktriangle_{\mathsf{H}}\left(\xleftarrow[\Vert]{P_1} s \xrightarrow[\Vert]{P_2}\right) = \sum_{q \in Q} |s|_q|$ where
- $Q = \{p_1 \in P_1 \mid \exists p_2 \in P_2.\, p_2 \leqslant p_1\} \cup \{p_2 \in P_2 \mid \exists p_1 \in P_1.\, p_1 \leqslant p_2\}$

- book keeping required by sets of positions and reasoning about $\blacktriangle_{\mathsf{H}}$ in Isabelle became convoluted, inelegant, and in the end unmanageable

Definitions (Toyama)

- $C[s_1,\ldots,s_n] \xrightarrow[\Vert]{s_1,\ldots,s_n} C[t_1,\ldots,t_n]$ if $s_i \to^\epsilon t_i$ for all $1 \leqslant i \leqslant n$
- overlap of peak is $\blacktriangle_{\mathsf{T}}\left(\xleftarrow[\Vert]{t_1,\ldots,t_n} s \xrightarrow[\Vert]{u_1,\ldots,u_m}\right) = \sum_{s \in S} |s|$ where
- $S = \{u_i \mid \exists t_j.\, u_i \trianglelefteq t_j\} \cup \{t_j \mid \exists u_i.\, t_j \trianglelefteq u_i\}$

Example

- TRS $\mathcal{R}$

$$\mathsf{f}(\mathsf{a},\mathsf{a},\mathsf{b},\mathsf{b}) \to \mathsf{f}(\mathsf{c},\mathsf{c},\mathsf{c},\mathsf{c}) \qquad \mathsf{a} \to \mathsf{b} \qquad \mathsf{a} \to \mathsf{c} \qquad \mathsf{b} \to \mathsf{a} \qquad \mathsf{b} \to \mathsf{c}$$

- peak after closing critical pair

$$\begin{array}{ccc}
\mathsf{f}(\mathsf{a},\mathsf{a},\mathsf{b},\mathsf{b}) & \longrightarrow & \mathsf{f}(\mathsf{c},\mathsf{c},\mathsf{c},\mathsf{c}) \\
\downarrow & \nearrow_{\parallel} & \\
\mathsf{f}(\mathsf{b},\mathsf{a},\mathsf{b},\mathsf{b}) & & \\
\downarrow^{*}_{\parallel} & & \\
\mathsf{f}(\mathsf{b},\mathsf{b},\mathsf{a},\mathsf{a}) & &
\end{array}$$

- $\blacktriangle_{\mathsf{T}}\left(\xleftarrow[\parallel]{\mathsf{a,a,b,b}} \mathsf{f}(\mathsf{a},\mathsf{a},\mathsf{b},\mathsf{b}) \xrightarrow[\parallel]{\mathsf{f(a,a,b,b)}}\right) = 2$ since $S = \{\mathsf{a},\mathsf{b}\} \cup \varnothing$
- $\blacktriangle_{\mathsf{T}}\left(\xleftarrow[\parallel]{\mathsf{a,b,b}} \mathsf{f}(\mathsf{b},\mathsf{a},\mathsf{b},\mathsf{b}) \xrightarrow[\parallel]{\mathsf{b,a,b,b}}\right) = 2$ since $S = \{\mathsf{a},\mathsf{b}\} \cup \{\mathsf{a},\mathsf{b}\}$

Measuring Overlap in IsaFoR

Definition

Overapproximation of overlap between two parallel steps is multiset defined by

$$\blacktriangle\left(\xleftarrow[\Vert]{\Box,a} s \xrightarrow[\Vert]{\Box,b}\right) = \{s\}$$

$$\blacktriangle\left(\xleftarrow[\Vert]{C,a_1,\ldots,a_c} s \xrightarrow[\Vert]{\Box,b}\right) = \{a_1,\ldots,a_c\}$$

$$\blacktriangle\left(\xleftarrow[\Vert]{\Box,a} s \xrightarrow[\Vert]{D,b_1,\ldots,b_d}\right) = \{b_1,\ldots,b_d\}$$

$$\blacktriangle\left(\xleftarrow[\Vert]{f(C_1,\ldots,C_n),\overline{a}} f(s_1,\ldots,s_n) \xrightarrow[\Vert]{f(D_1,\ldots,D_n),\overline{b}}\right) = \bigcup_{i=1}^{n} \blacktriangle\left(\xleftarrow[\Vert]{C_i,\overline{a}_i} s_i \xrightarrow[\Vert]{D_i,\overline{b}_i}\right)$$

where $\overline{a}_1,\ldots,\overline{a}_n = \overline{a}$ and $\overline{b}_1,\ldots,\overline{b}_n = \overline{b}$ are partitions of $\overline{a}$ and $\overline{b}$ such that length of $\overline{a}_i$ and $\overline{b}_i$ matches number of holes in C_i and D_i for all $1 \leqslant i \leqslant n$

- compare multisets using multiset extension of superterm relation $\rhd_{\mathsf{mul}}$
- $\rhd_{\mathsf{mul}}$ is well-founded

Example

Applying this definition for the two peaks from before yields

$$\blacktriangle\left(\xleftarrow[\Vert]{\mathsf{f}(\square,\square,\square,\square),\mathsf{a},\mathsf{a},\mathsf{b},\mathsf{b}} \mathsf{f}(\mathsf{a},\mathsf{a},\mathsf{b},\mathsf{b}) \xrightarrow[\Vert]{\square,\mathsf{f}(\mathsf{a},\mathsf{a},\mathsf{b},\mathsf{b})}\right) = \{\mathsf{a},\mathsf{a},\mathsf{b},\mathsf{b}\}$$

$$\blacktriangle\left(\xleftarrow[\Vert]{\mathsf{f}(\mathsf{b},\square,\square,\square),\mathsf{a},\mathsf{b},\mathsf{b}} \mathsf{f}(\mathsf{b},\mathsf{a},\mathsf{b},\mathsf{b}) \xrightarrow[\Vert]{\mathsf{f}(\square,\square,\square,\square),\mathsf{b},\mathsf{a},\mathsf{b},\mathsf{b}}\right) = \{\mathsf{a},\mathsf{b},\mathsf{b}\}$$

and $\{\mathsf{a},\mathsf{a},\mathsf{b},\mathsf{b}\} \rhd_{\mathsf{mul}} \{\mathsf{a},\mathsf{b},\mathsf{b}\}$

Lemma

- $\blacktriangle\left(\xleftarrow[\Vert]{C,\bar{a}} s \xrightarrow[\Vert]{D,\bar{b}}\right) = \blacktriangle\left(\xleftarrow[\Vert]{D,\bar{b}} s \xrightarrow[\Vert]{C,\bar{a}}\right)$
- $\blacktriangle\left(\xleftarrow[\Vert]{C_i,\bar{a}_i} s_i \xrightarrow[\Vert]{D_i,\bar{b}_i}\right) \subseteq \blacktriangle\left(\xleftarrow[\Vert]{f(C_1,\ldots,C_n),\bar{a}} f(s_1,\ldots,s_n) \xrightarrow[\Vert]{f(D_1,\ldots,D_n),\bar{b}}\right)$
- $\{a_1,\ldots,a_c\} \rhd^{=}_{\mathsf{mul}} \blacktriangle\left(\xleftarrow[\Vert]{C,a_1,\ldots,a_c} s \xrightarrow[\Vert]{D,\bar{b}}\right)$

Almost Parallel Closed Critical Pairs

Theorem (Toyama)

If $\mathcal{R}$ is left-linear, $t \mathrel{+\!\!\!\!\!\!\rightarrow} s$ for all inner critical pairs $t \leftarrow\!\rtimes\!\rightarrow s$, and $t \mathrel{+\!\!\!\!\!\!\rightarrow} \cdot\, {}^*\!\!\leftarrow s$ for all overlays $t \leftarrow\!\bowtie\!\rightarrow s$ then $\mathrel{+\!\!\!\!\!\!\rightarrow}$ is strongly confluent

Proof (Adaptations)

- $t \xleftarrow{C,\bar{a}} s \xrightarrow{D,\bar{b}} u$
- show $t \mathrel{+\!\!\!\!\!\!\rightarrow}^* \cdot \leftarrow\!\!\!\!\!\!+ \; u$ and $u \mathrel{+\!\!\!\!\!\!\rightarrow}^* \cdot \leftarrow\!\!\!\!\!\!+ \; t$
- if $C = D = \Box$ then assumption for overlays applies
- other cases remain (almost) the same

Remark

- incorporating Toyama's extension to commutation is straightforward

Certification and Experiments

CeTA

- CeTA computes critical pairs
- and checks linearity and joining conditions
- only information required in certificate: bound on length of $\to^*$

CSI on 277 TRSs in Confluence Problem Database

	SC	PC	SC+PC	full
yes	38	21	41	110
no	0	0	0	48
maybe	239	256	236	119

Development Closed Critical Pairs

Theorem (van Oostrom)

If $\mathcal{R}$ is left-linear and $t \twoheadrightarrow\!\!\!\!\!\circ\; s$ for all critical peaks $t \leftarrow\!\rtimes\!\rightarrow s$ then $\twoheadrightarrow\!\!\!\!\!\circ$ has the diamond property

- nesting of steps makes describing $\twoheadrightarrow\!\!\!\!\!\circ$ harder
- need to split off single steps on both sides and combine closing step with remainder
- due to nesting of redexes this needs non-trivial reasoning about residuals
- need to split off "innermost" overlap to get decrease in measure
- notion of overlap does not carry over

Summary

- formalization of two classical confluence results
- strongly closed was straightforward
- (almost) parallel closed was much more involved

Main differences to Paper Proof

- multihole contexts for describing parallel steps
- notion of overlap: collect overlapping redexes in multiset, compare with $\rhd_{\mathsf{mul}}$

- future work: development closed
- harder future work: apply to higher-order rewriting