universität innsbruck

Church–Rosser Modulo for Left-Linear TRSs Revisited

IWC 2023

Johannes Niederhauser, Nao Hirokawa, Aart Middeldorp

Outline

Huet's Result

consider equational theory $\mathcal{B}$ (e.g. AC)

Lemma (Huet, JACM 1980)

- consider left-linear and $\mathcal{B}$-terminating TRSs $\mathcal{R}$
- $\mathcal{R}$ is CR modulo $\mathcal{B}$ $\iff$ $\mathsf{CP}(\mathcal{R}) \cup \mathsf{CP}^{\pm}(\mathcal{R}, \mathcal{B}^{\pm}) \subseteq \downarrow^{\sim}_{\mathcal{R}}$

known facts (shown later):

- left-linearity of $\mathcal{R}$ is crucial
- termination modulo $\mathcal{B}$ of $\mathcal{R}$ is also crucial

Lemma (Kapur et al., JSC 1988)

terminating TRSs $\mathcal{R}$ are confluent $\iff$ $\mathsf{PCP}(\mathcal{R}) \subseteq \downarrow_{\mathcal{R}}$

question: can we replace $\mathsf{CP}(\mathcal{R}) \cup \mathsf{CP}^{\pm}(\mathcal{R}, \mathcal{B}^{\pm})$ by $\mathsf{PCP}(\mathcal{R}) \cup \mathsf{PCP}^{\pm}(\mathcal{R}, \mathcal{B}^{\pm})$?

Running Example

Example

- TRS $\mathcal{R}$ consists of the rules

$$\mathsf{f}(\mathsf{a}+x) \to x \quad \mathsf{f}(x+\mathsf{a}) \to x \quad \mathsf{f}(\mathsf{b}+x) \to x \quad \mathsf{f}(x+\mathsf{b}) \to x \quad \mathsf{a} \to \mathsf{b}$$

- $\mathcal{B} = \{x + y \approx y + x\}$
- critical peaks of the form $t \; {}_{\mathcal{R}}^{p}\!\leftarrow s \to_{\mathcal{R}}^{\epsilon} u$:

$$\begin{array}{cccccc}
\underline{\mathsf{f}(\mathsf{a}+\mathsf{a})} & \underline{\mathsf{f}(\mathsf{a}+\mathsf{b})} & \underline{\mathsf{f}(\mathsf{b}+\mathsf{a})} & \underline{\mathsf{f}(\mathsf{b}+\mathsf{b})} & \mathsf{f}(\underline{\mathsf{a}}+x) & \mathsf{f}(x+\underline{\mathsf{a}}) \\
\swarrow \;\; \searrow & \swarrow \;\; \searrow & \swarrow \;\; \searrow & \swarrow \;\; \searrow & \swarrow \;\; \searrow & \swarrow \;\; \searrow \\
\mathsf{a} \quad\quad \mathsf{a} & \mathsf{a} \quad\quad \mathsf{b} & \mathsf{a} \quad\quad \mathsf{b} & \mathsf{b} \quad\quad \mathsf{b} & \mathsf{f}(\mathsf{b}+x) \quad x & \mathsf{f}(x+\mathsf{b}) \quad x
\end{array}$$

- $\mathrm{PCP}(\mathcal{R}) = \{\mathsf{b} \approx \mathsf{b}, \mathsf{f}(\mathsf{b}+x) \approx x, \mathsf{f}(x+\mathsf{b}) \approx x\}$

Running Example

Example (cont'd)

- TRS $\mathcal{R}$ consists of the rules

$$\mathsf{f}(\mathsf{a}+x) \to x \qquad \mathsf{f}(x+\mathsf{a}) \to x \qquad \mathsf{f}(\mathsf{b}+x) \to x \qquad \mathsf{f}(x+\mathsf{b}) \to x \qquad \mathsf{a} \to \mathsf{b}$$

- $\mathcal{B} = \{x+y \approx y+x\}$
- critical peaks of the forms $t \;{}_{\mathcal{R}}^{p}\!\leftarrow s \leftrightarrow_{\mathcal{B}}^{\epsilon} u$ and $t \leftrightarrow_{\mathcal{B}}^{p} s \to_{\mathcal{R}}^{\epsilon} u$:

$$\begin{array}{ccc} & \mathsf{f}(\underline{\mathsf{a}+x}) & \\ \swarrow & & \searrow \\ \mathsf{f}(x+\mathsf{a}) & & x \end{array} \qquad \begin{array}{ccc} & \mathsf{f}(\underline{x+\mathsf{a}}) & \\ \swarrow & & \searrow \\ \mathsf{f}(\mathsf{a}+x) & & x \end{array} \qquad \begin{array}{ccc} & \mathsf{f}(\underline{\mathsf{b}+x}) & \\ \swarrow & & \searrow \\ \mathsf{f}(x+\mathsf{b}) & & x \end{array} \qquad \begin{array}{ccc} & \mathsf{f}(\underline{x+\mathsf{b}}) & \\ \swarrow & & \searrow \\ \mathsf{f}(\mathsf{b}+x) & & x \end{array}$$

- $\mathsf{PCP}^{\pm}(\mathcal{R},\mathcal{B}^{\pm}) = \{\mathsf{f}(\mathsf{b}+x) \approx x, \mathsf{f}(x+\mathsf{b}) \approx x\}$

Outline

Critical Pairs

Definition

- $\mathrm{CP}(\mathcal{R})$ is the set of critical pairs in $\mathcal{R}$
- $\mathrm{PCP}(\mathcal{R})$ only considers critical peaks

$$t \xleftarrow[\mathcal{R}]{p} s \xrightarrow[\mathcal{R}]{\epsilon} u$$

where all proper subterms of $s|_p$ are irreducible
- $\mathrm{CP}(\mathcal{R}_1, \mathcal{R}_2)$ denotes CPs which originate from critical peaks of the form

$$t \;{}_{\mathcal{R}_1}^{\;p}\!\!\leftarrow s \to_{\mathcal{R}_2}^{\epsilon} u$$

Church–Rosser Modulo Property

consider equational theory $\mathcal{B}$ where $\mathcal{V}\text{ar}(\ell) = \mathcal{V}\text{ar}(r)$ for all $\ell \approx r \in \mathcal{B}$

Definition

TRS $\mathcal{R}$ is Church–Rosser (CR) modulo $\mathcal{B}$ if $(\leftrightarrow_{\mathcal{B}} \cup {}_{\mathcal{R}}\!\leftarrow \cup \rightarrow_{\mathcal{R}})^* \subseteq \rightarrow_{\mathcal{R}}^* \cdot \sim_{\mathcal{B}} \cdot {}_{\mathcal{R}}^{*}\!\leftarrow$

Notation

- $\sim_{\mathcal{B}} = \leftrightarrow_{\mathcal{B}}^*$
- $\downarrow_{\mathcal{R}}^{\sim} = \rightarrow_{\mathcal{R}}^* \cdot \sim_{\mathcal{B}} \cdot {}_{\mathcal{R}}^{*}\!\leftarrow$
- $\mathcal{B}^{\pm} = \mathcal{B} \cup \{r \approx \ell \mid \ell \approx r \in \mathcal{B}\}$
- $\mathrm{CP}^{\pm}(\mathcal{R}_1, \mathcal{R}_2) = \mathrm{CP}(\mathcal{R}_1, \mathcal{R}_2) \cup \mathrm{CP}(\mathcal{R}_2, \mathcal{R}_1)$
- $\mathrm{PCP}^{\pm}(\mathcal{R}, \mathcal{B})$ restricts $\mathrm{CP}^{\pm}(\mathcal{R}, \mathcal{B})$ to prime critical pairs where irreducibility is always checked with respect to $\mathcal{R}$

Huet's Result (again)

Lemma (Huet, JACM 1980)

- consider left-linear and $\mathcal{B}$-terminating TRSs $\mathcal{R}$
- $\mathcal{R}$ is CR modulo $\mathcal{B}$ $\iff$ $\mathsf{CP}(\mathcal{R}) \cup \mathsf{CP}^{\pm}(\mathcal{R}, \mathcal{B}^{\pm}) \subseteq \downarrow^{\sim}_{\mathcal{R}}$

Example

- consider TRS $\mathcal{R}$ consisting of single rule $\mathsf{f}(x, x) \to x$
- additional AC symbol $+$
- $x + y \ {}_{\mathcal{R}}\!\leftarrow \ \mathsf{f}(x + y, x + y) \sim_{\mathsf{AC}} \mathsf{f}(x + y, y + x)$
- $\mathsf{CP}(\mathcal{R}) = \mathsf{CP}^{\pm}(\mathcal{R}, \mathsf{AC}^{\pm}) = \varnothing$
- $x + y \downarrow^{\sim}_{\mathcal{R}} \mathsf{f}(x + y, y + x)$ does not hold

question: can we replace $\mathsf{CP}(\mathcal{R}) \cup \mathsf{CP}^{\pm}(\mathcal{R}, \mathcal{B}^{\pm})$ by $\mathsf{PCP}(\mathcal{R}) \cup \mathsf{PCP}^{\pm}(\mathcal{R}, \mathcal{B}^{\pm})$?

Outline

1. Introduction
2. Preliminaries
3. **Peak-and-Cliff Decreasingness**
4. Prime Critical Pairs
5. Conclusion

Peak-And-Cliff Decreasingness

Definition

- $\mathcal{A} = \langle A, \{\to_\alpha\}_{\alpha \in I} \rangle$ is an ARS
- $\sim\ = (\bigcup_{\alpha \in I} \vdash\!\dashv_\alpha)^*$ is an equivalence relation on A
- $\Leftrightarrow\ =\ \sim \cup \leftarrow \cup \to$

$\mathcal{A}$ is peak-and-cliff decreasing if there is a well-founded order $>$ on I s.t. $\forall\, \alpha, \beta \in I$

$$_\alpha\!\leftarrow \cdot \to_\beta \;\subseteq\; \xLeftrightarrow[\vee\alpha\beta]{*} \qquad\qquad _\alpha\!\leftarrow \cdot \vdash\!\dashv_\beta \;\subseteq\; \xLeftrightarrow[\vee\alpha]{*} \cdot \xleftarrow[\beta]{=}$$

here $\vee\alpha\beta = \{\gamma \in I \mid \alpha > \gamma$ or $\beta > \gamma\}$, $\to_J = \bigcup_{\gamma \in J} \to_\gamma$ and $\vee\alpha\alpha = \vee\alpha$

- based on peak decreasingness (Hirokawa et al., LMCS 2019)
- introduced in our recent paper on left-linear AC completion (CADE 2023)

Peak-And-Cliff Decreasingness (cont'd)

Theorem

if $\mathcal{A}$ is peak-and-cliff decreasing then $\mathcal{A}$ is CR modulo $\sim$

Proof Sketch

- $\Leftrightarrow^* \subseteq \downarrow^\sim \cup \Leftrightarrow^* \cdot \leftarrow \cdot \rightarrow \cdot \Leftrightarrow^* \cup \Leftrightarrow^* \cdot \vdash\!\dashv \cdot \rightarrow \cdot \Leftrightarrow^* \cup \Leftrightarrow^* \cdot \leftarrow \cdot \vdash\!\dashv \cdot \Leftrightarrow^*$
- conversion C gives rise to multiset M_C of labels
- well-founded order $>$ on labels by peak-and-cliff decreasingness
- induction on $>_{\mathsf{mul}}$
- replace conversions C of the from

$$_{\alpha}\!\leftarrow \cdot \rightarrow_{\beta} \quad \text{or} \quad _{\alpha}\!\leftarrow \cdot \vdash\!\dashv_{\beta} \quad \text{or} \quad \vdash\!\dashv_{\beta} \cdot \rightarrow_{\alpha}$$

by conversions C' where $M_C >_{\mathsf{mul}} M_{C'}$ □

Source Decreasingness Modulo

Definition

- ARS $\mathcal{A} = \langle A, \to \rangle$, equivalence relation $\sim \; = \; \vdash\!\dashv^*$ on A
- well-founded order $>$ where $\sim \cdot > \cdot \sim \; \subseteq \; >$
- $b \xrightarrow{a} c$ ($b \overset{a}{\vdash\!\dashv} c$) if $b \to c$ ($b \vdash\!\dashv c$) and $b \sim a$
- $b \xleftrightarrow[\vee a]{*} c$ if all steps are labeled by a smaller element than a

$\mathcal{A}$ is source decreasing modulo $\sim$ if for all $a \in A$

$$\leftarrow a \rightarrow \; \subseteq \; \xleftrightarrow[\vee a]{*} \qquad\qquad \leftarrow a \vdash\!\dashv \; \subseteq \; \xleftrightarrow[\vee a]{*} \cdot \xleftarrow[a]{=}$$

Corollary

if $\mathcal{A}$ is source decreasing modulo $\sim$ then $\mathcal{A}$ is CR modulo $\sim$

Outline

Prime Critical Pairs

Definition

- consider TRS $\mathcal{R}$ and terms s, t and u
- $t \nabla_s u$ if $s \to_{\mathcal{R}}^{+} t$, $s \to_{\mathcal{R}}^{+} u$, and $t \downarrow_{\mathcal{R}} u$ or $t \leftrightarrow_{\mathsf{PCP}(\mathcal{R})} u$
- $t \nabla_s^{\sim} u$ if $s \to_{\mathcal{R}}^{+} t$, $s \sim u$ and $t \downarrow_{\mathcal{R}}^{\sim} u$ or $t \leftrightarrow_{\mathsf{PCP}^{\pm}(\mathcal{R},\mathcal{B}^{\pm})} u$

Lemma

consider a left-linear TRS $\mathcal{R}$

1. if $t \;{}_{\mathcal{R}}\!\leftarrow s \to_{\mathcal{R}} u$ then $t \nabla_s^2 u$
2. if $t \;{}_{\mathcal{R}}\!\leftarrow s \leftrightarrow_{\mathcal{B}} u$ then $t \nabla_s \cdot \nabla_s^{\sim} u$

Main Result

Theorem

- consider left-linear and $\mathcal{B}$-terminating TRSs $\mathcal{R}$
- $\mathcal{R}$ is CR modulo $\mathcal{B}$ $\iff$ $\mathsf{PCP}(\mathcal{R}) \cup \mathsf{PCP}^{\pm}(\mathcal{R}, \mathcal{B}^{\pm}) \subseteq {\downarrow}^{\sim}_{\mathcal{R}}$

Proof Sketch ($\Longleftarrow$)

- show source decreasingness modulo $\sim$ with $> \; = \; \to^{+}_{\mathcal{R}/\mathcal{B}}$
- proof for local peaks like in (Hirokawa et al., LMCS 2019)
- consider arbitrary local cliff $t \;{}_{\mathcal{R}}{\leftarrow}\; s \leftrightarrow_{\mathcal{B}} u$
- $t \downarrow^{\sim}_{\mathcal{R}} v \downarrow^{\sim}_{\mathcal{R}} u$ by previous lemma and assumption
- $s > t, v$ and $s \sim u$
- source decreasingness modulo $\sim$ follows from choice of $>$ $\square$

Running Example

Example

- TRS $\mathcal{R}$ consists of the rules

$$\mathsf{f}(\mathsf{a}+x) \to x \quad \mathsf{f}(x+\mathsf{a}) \to x \quad \mathsf{f}(\mathsf{b}+x) \to x \quad \mathsf{f}(x+\mathsf{b}) \to x \quad \mathsf{a} \to \mathsf{b}$$

- $\mathcal{B} = \{x + y \approx y + x\}$
- $\mathrm{PCP}(\mathcal{R}) = \{\mathsf{b} \approx \mathsf{b}, \mathsf{f}(\mathsf{b}+x) \approx x, \mathsf{f}(x+\mathsf{b}) \approx x\}$
- $\mathrm{PCP}^{\pm}(\mathcal{R}, \mathcal{B}^{\pm}) = \{\mathsf{f}(\mathsf{b}+x) \approx x, \mathsf{f}(x+\mathsf{b}) \approx x\}$
- $\mathcal{R}/\mathcal{B}$ is terminating
- $\mathrm{PCP}(\mathcal{R}) \cup \mathrm{PCP}^{\pm}(\mathcal{R}, \mathcal{B}^{\pm}) \subseteq \downarrow^{\sim}_{\mathcal{R}}$
- $\mathcal{R}$ is CR modulo $\mathcal{B}$ by previous theorem

Termination Modulo AC is Needed

Example

- $+$ is AC symbol, TRS $\mathcal{R}$ consists of rules

$$
\begin{aligned}
(a+a)+b &\to a+(a+b) & \qquad (a+b)+a &\to a+(a+b) \\
(b+a)+a &\to a+(a+b) & \qquad b+(a+a) &\to c \\
a+(a+b) &\to b+(a+a) & \qquad a+(b+a) &\to d \\
a+(a+b) &\to a+(b+a) & &
\end{aligned}
$$

- $\mathrm{PCP}(\mathcal{R}) \subseteq \downarrow^{\sim}_{\mathcal{R}}$
- for $\mathrm{PCP}^{\pm}(\mathcal{R}, \mathrm{AC}^{\pm})$ it suffices to consider $\ell \to r \in \mathcal{R}$ with $r = c, d$

Termination Modulo AC is Needed

Example (cont'd)

- add these rules to $\mathcal{R}$:

$$\mathsf{b} + ((\mathsf{a} + \mathsf{a}) + x) \to (\mathsf{b} + (\mathsf{a} + \mathsf{a})) + x \qquad (x + \mathsf{b}) + (\mathsf{a} + \mathsf{a}) \to x + (\mathsf{b} + (\mathsf{a} + \mathsf{a}))$$

$$\mathsf{a} + ((\mathsf{b} + \mathsf{a}) + x) \to (\mathsf{a} + (\mathsf{b} + \mathsf{a})) + x \qquad (x + \mathsf{a}) + (\mathsf{b} + \mathsf{a}) \to x + (\mathsf{a} + (\mathsf{b} + \mathsf{a}))$$

- $\mathsf{PCP}(\mathcal{R}) \cup \mathsf{PCP}^{\pm}(\mathcal{R}, \mathsf{AC}^{\pm}) \subseteq \downarrow^{\sim}_{\mathcal{R}}$
- termination of $\mathcal{R}$ is confirmed by $\mathsf{T_TT_2}$
- $\mathsf{a} + (\mathsf{a} + \mathsf{b}) \to_{\mathcal{R}} \mathsf{a} + (\mathsf{b} + \mathsf{a}) \sim_{\mathsf{AC}} \mathsf{a} + (\mathsf{a} + \mathsf{b})$
- $\mathcal{R}$ is not AC terminating
- $\mathsf{c} \Leftrightarrow^* \mathsf{d}$ but not $\mathsf{c} \downarrow^{\sim}_{\mathcal{R}} \mathsf{d}$
- $\mathcal{R}$ is not CR modulo AC

Outline

Conclusion

- strengthened result by Huet to prime critical pairs
- used in our recent paper on left-linear AC completion
- proof via an adaptation of peak decreasingness
- fewer critical pairs to consider in practice
- termination modulo $\mathcal{B}$ is necessary when $\mathcal{B} = \text{AC}$
- our counterexample is based on Example 4.1.8 from (Avenhaus 1995) which uses an ARS
- **open question:** is there a counterexample where $\sim_{\mathcal{B}} \cap \rightarrow_{\mathcal{R}} = \varnothing$?