Certification of Completion-Based Infeasibility Proofs

Teppei Saito **René Thiemann**

February 22, 2024

completion-based infeasibility provers: Moca, Mædmax (ConCon), Toma

Moca (developed by Ōi) solves 48 COPS problems including

$$\#\{809, 853, 857, 882, 905, 908, 930\}$$

which are only solved by Moca

table of contents:

1. unraveling for infeasibility (using #908)
2. ground completeness/joinability for infeasibility (using #853)

Unraveling for Infeasibility

Definition (infeasibility problem)

specification of infeasibility problem is as follows

- input: conditional (oriented) TRS $\mathcal{R}$ and queries $s_1 \to^* t_1, \ldots, s_n \to^* t_n$
- output: whether there is a substitution σ s.t. $s_1\sigma \to^*_{\mathcal{R}} t_1\sigma, \ldots, s_n\sigma \to^*_{\mathcal{R}} t_n\sigma$

problem is called infeasible if there is no such σ

framework of completion-based infeasibility provers:

1. turn query into ground one (lift query into conditional rule)
2. unravel CTRS into pure equations
3. solve word problem by completion (e.g., Knuth–Bendix completion)

Step 1: Turn Query into Ground One

Proposition

for fresh symbols T and F, the following statements are equivalent

- $s_1 \to^* t_1, \ldots, s_n \to^* t_n$ *is infeasibile under CTRS* $\mathcal{R}$
- $T \to^* F$ *is infeasible under* $\mathcal{R} \cup \{T \to F \Longleftarrow s_1 \to^* t_1, \ldots, s_n \to^* t_n\}$

remarks

- grounding query is essential for final step (refutation by completion)
- one can virtually apply rule-inlining by Sternagels (CADE 2017) to query

Example: Apply Step 1 to COPS#908 (ARI#763)

query $x < \mathsf{min}(y) \to^* \mathsf{true},\ x < \mathsf{min}(y) \to^* \mathsf{false}$ under CTRS $\mathcal{R}$

$$\begin{aligned} x < 0 &\to \mathsf{false} \\ 0 < \mathsf{s}(y) &\to \mathsf{true} \\ \mathsf{s}(x) < \mathsf{s}(y) &\to x < y \\ \mathsf{min}(\mathsf{cons}(x, \mathsf{nil})) &\to x \\ \mathsf{min}(\mathsf{cons}(x, xs)) &\to x && \Longleftarrow && x < \mathsf{min}(xs) \to^* \mathsf{true} \\ \mathsf{min}(\mathsf{cons}(x, xs)) &\to \mathsf{min}(xs) && \Longleftarrow && x < \mathsf{min}(xs) \to^* \mathsf{false} \end{aligned}$$

is transformed into new query $\mathsf{T} \to^* \mathsf{F}$ under CTRS

$$\mathcal{R} \cup \{\mathsf{T} \to \mathsf{F} \Longleftarrow x < \mathsf{min}(y) \to^* \mathsf{true},\ x < \mathsf{min}(y) \to^* \mathsf{false}\}$$

Step 2: Unraveling

Definition (Marchiori 2005; Claessen and Smallbone 2018; Ōi 2020)

unraveling $\mathbb{U}$ maps each rule $\ell \to r \Longleftarrow s_1 \to^* t_1, \ldots, s_n \to^* t_n$ into either

- $\{\ell \to r\}$, or
- $\{\ell \to U(s_1, \ldots, s_n, \vec{x}),\ U(t_1, \ldots, t_n, \vec{x}) \to r\}$

where U is function symbol and $\vec{x}$ are variables

Proposition

$\to_{\mathcal{R}} \subseteq \to^+_{\mathbb{U}(\mathcal{R})}$ *for all CTRSs* $\mathcal{R}$ *and unravelings* $\mathbb{U}$, *where* $\mathbb{U}(\mathcal{R}) = \bigcup_{\rho \in \mathcal{R}} \mathbb{U}(\rho)$

we may choose same U for different rules, or ignore conditions

Example: Unraveling COPS#908 (Failure)

part of conditional rules:

$$\begin{aligned} \mathsf{min}(\mathsf{cons}(x, xs)) &\to x && \Longleftarrow && x < \mathsf{min}(xs) \to^* \mathsf{true} \\ \mathsf{min}(\mathsf{cons}(x, xs)) &\to \mathsf{min}(xs) && \Longleftarrow && x < \mathsf{min}(xs) \to^* \mathsf{false} \end{aligned}$$

use U_1 and $[x, xs]$ for the first, and U_2 and $[x, xs]$ for the second

$$\begin{aligned} \mathsf{min}(\mathsf{cons}(x, xs)) &\to \mathsf{U}_1(x < \mathsf{min}(xs), x, xs) && \mathsf{U}_1(\mathsf{true}, x, xs) \to x \\ \mathsf{min}(\mathsf{cons}(x, xs)) &\to \mathsf{U}_2(x < \mathsf{min}(xs), x, xs) && \mathsf{U}_2(\mathsf{false}, x, xs) \to \mathsf{min}(xs) \end{aligned}$$

but Moca fails in the next step (or fails to find complete presentation)

Example: Unraveling COPS#908 (Ōi's Refinement)

part of conditional rules:

$$\mathsf{min}(\mathsf{cons}(x, xs)) \to x \quad \Longleftarrow \quad x < \mathsf{min}(xs) \to^* \mathsf{true}$$
$$\mathsf{min}(\mathsf{cons}(x, xs)) \to \mathsf{min}(xs) \quad \Longleftarrow \quad x < \mathsf{min}(xs) \to^* \mathsf{false}$$

use U_1 and $[x, xs]$ for the first, and same U_1 and $[x, xs]$ for the second

$$\mathsf{min}(\mathsf{cons}(x, xs)) \to \mathsf{U}_1(x < \mathsf{min}(xs), x, xs) \qquad \mathsf{U}_1(\mathsf{true}, x, xs) \to x$$
$$\mathsf{min}(\mathsf{cons}(x, xs)) \to \mathsf{U}_1(x < \mathsf{min}(xs), x, xs) \qquad \mathsf{U}_1(\mathsf{false}, x, xs) \to \mathsf{min}(xs)$$

then Moca succeeds on transformed problem afterwards

Step 3: Disproof by Completion

at this point we have ground query $s \to^* t$ and TRS $\mathcal{R}$

Proposition

$s \to^* t$ is infeasible if there is confluent $\mathcal{S}$ with $\mathcal{R} \subseteq \leftrightarrow^*_{\mathcal{S}}$ and s, t not $\mathcal{S}$-joinable

Proof.

$s\sigma = s \to^*_{\mathcal{R}} t = t\sigma \implies s \leftrightarrow^*_{\mathcal{S}} t \implies s$ and t are joinable $\lightning$

remarks

- equivalence $\leftrightarrow^*_{\mathcal{R}} = \leftrightarrow^*_{\mathcal{S}}$ is unnecessary (Moca further exploits this fact)
- we can use any completion (Knuth–Bendix/maximal/with termination tool)

Demo and Summary of Part 1

demo!

framework of completion-based infeasibility provers:

1. turn query into ground one (lift query into conditional rule)
2. unravel CTRS into pure equations
3. solve word problem by completion (e.g., Knuth–Bendix completion)

Ground-Completeness/Joinability

Solving Word Problem by Ordered Completion

observation: goal is ground in the last step (for solving word problem)

let $\mathcal{E}$ be equations and $>$ reduction order

Definition (ordered rewrite system or OTRS)

$\mathcal{E}_> = \{\ell\sigma \to r\sigma \mid \ell \approx r \in \mathcal{E} \cup \mathcal{E}^{-1}, \ell\sigma > r\sigma\}$

let $s \to^* t$ be ground query and $\mathcal{R}$ TRS (maybe violating variable condition)

Proposition

$s \to^* t$ is infeasible if $\mathcal{E}_>$ is ground-confluent, $\mathcal{R} \subseteq \leftrightarrow^*_{\mathcal{E}_>}$ and s, t are not joinable

remark: extended critical pair lemma is nice characterization of ground-confluence

Moca completely ignores condition parts of COPS#853 (ARI#709)

$$
\begin{aligned}
x < 0 &\to \mathsf{false} \\
0 < \mathsf{s}(y) &\to \mathsf{true} \\
\mathsf{s}(x) < \mathsf{s}(y) &\to x < y \\
\mathsf{app}(\mathsf{nil}, ys) &\to ys \\
\mathsf{app}(x : xs, ys) &\to x : \mathsf{app}(xs, ys) \\
\mathsf{split}(x, \mathsf{nil}) &\to \mathsf{nil} \\
\mathsf{split}(x, y : ys) &\to \mathsf{pair}(xs, y : zs) && \Longleftarrow \mathsf{split}(x, ys) \to^* \mathsf{pair}(xs, zs), \ldots \\
\mathsf{split}(x, y : ys) &\to \mathsf{pair}(y : xs, zs) && \Longleftarrow \mathsf{split}(x, ys) \to^* \mathsf{pair}(xs, zs), \ldots \\
\mathsf{qs}(\mathsf{nil}) &\to \mathsf{nil} \\
\mathsf{qs}(x : xs) &\to \mathsf{app}(\mathsf{qs}(ys), x : \mathsf{qs}(zs)) && \Longleftarrow \mathsf{split}(x, xs) \to^* \mathsf{pair}(ys, zs)
\end{aligned}
$$

but successfully finds ground-confluent OTRS $\mathcal{E}_>$ (!?)

$\mathcal{E}_>$: OTRS with $>$ ground-total

Theorem (Martin and Nipkow 1990)

$\mathcal{E}_>$ is ground-confluent iff all extended critical pairs are ground-joinable

remark: ground-confluence of TRS is different from that of OTRS

Martin and Nipkow's testing for checking ground-joinability of $s \approx t$ w.r.t $\mathcal{E}_>$

1. enumerate all possible orderings π of variables in s, t
2. extend ordering $>$ to $>^\pi$ (closure operation)
3. test ground-joinability of $s \approx t$ w.r.t $\mathcal{E}_{>^\pi}$

remark

- closure operation need be defined for each ordering (e.g. KBO/LPO closure)
- required properties of closure operation are described in axiomatic way

34 of 48 proofs by Moca are already certified by CeTA, including

COPS#{809, 853, 857, 882, 905, 908, 930}

done

- formalized unraveling for infeasibility (Réne)
- (ground-)completion (Christian Sternagel and Sarah Winkler)
  - (extended) critical pair lemma
  - Martin and Nipkow's method for ground-joinability
  - KBO closure for Martin and Nipkow's method
- putting everything together (certification interface, certificate generation)

todo: LPO closure for COPS#{809, 853, 857, 930} (in March)

Comments by Audience

- NN: Ōi's refinement was already observed by Gmeiner, Nishida and Gramlich (WST 2013)
- NN: ConCon's tree automata approach also completely ignores conditions
- NH: simulating TCAP by completion-based approach?
- RT: partial unraveling (leaving some conditions) could be useful?