Ground Confluence Proof with Pattern Complementation

IWC 2016, obergurgle

Takahito Aoto (Niigata University)
Yoshihito Toyama (Tohoku University)

Outline:

1. Proving Ground Confluence by Rewriting Induction
2. GCR Proof with Pattern Complementation

Ground Confluence (GCR)

$$
\begin{tikzcd}
 & \bullet \arrow[dl, "*"'] \arrow[dr, "*"] & \\
\bullet \arrow[dr, dotted, "*"'] & & \bullet \arrow[dl, dotted, "*"] \\
 & \bullet &
\end{tikzcd}
$$

on ground terms

for any ground term s_g, t_g, u_g ***such that*** $t_g \overset{*}{\leftarrow}_{\mathcal{R}} s_g \overset{*}{\rightarrow}_{\mathcal{R}} u_g$, ***there exists a ground term*** v_g ***such that*** $t_g \overset{*}{\rightarrow}_{\mathcal{R}} v_g \overset{*}{\leftarrow}_{\mathcal{R}} u_g$.

Rewriting Induction

Rewriting induction [Reddy, 1990] is a method to prove *inductive theorems*.

Inductive theorems

An equation $s \doteq t$ is an inductive theorem of $\mathcal{R}$

$(\mathcal{R} \models_{ind} s \doteq t)$

$\Leftrightarrow$ For any ground substitution σ_g, $s\sigma_g \overset{*}{\leftrightarrow}_{\mathcal{R}} t\sigma_g$

($\Leftrightarrow$ $s \doteq t$ is valid on the initial model of $\mathcal{R}$)

Theorem. [Reddy, 1990]

Suppose $\mathcal{R}$: SN, QR. Let $>$ be a reduction order with $\mathcal{R} \subseteq >$. If $\langle E, \emptyset \rangle \overset{*}{\rightsquigarrow}_{RI} \langle \emptyset, H \rangle$ then $\mathcal{R} \models_{ind} E$.

Here, $\mathcal{R}$: QR $\overset{\text{def}}{\Leftrightarrow}$ any ground basic term is reducible.

Rewriting Induction

Rewriting induction [Reddy, 1990] is a method to prove *inductive theorems*.

<u>Inductive theorems</u>

An equation $s \doteq t$ is an inductive theorem of $\mathcal{R}$

$(\mathcal{R} \models_{ind} s \doteq t)$

$\Leftrightarrow$ For any ground substitution σ_g, $s\sigma_g \overset{*}{\leftrightarrow}_{\mathcal{R}} t\sigma_g$

($\Leftrightarrow$ $s \doteq t$ is valid on the initial model of $\mathcal{R}$)

<u>Theorem.</u>

Suppose $\mathcal{R}$: SN, QR. Let $>$ be a reduction order with $\mathcal{R} \subseteq >$. If $\langle \mathrm{CP}(\mathcal{R}), \emptyset \rangle \overset{*}{\rightsquigarrow}_{RI} \langle \emptyset, H \rangle$ then $\mathcal{R}$: GCR.

Here, $\mathcal{R}$: QR $\overset{\text{def}}{\Leftrightarrow}$ any ground basic term is reducible.

(Basic) Rewriting Induction

Input: a TRS $\mathcal{R}$

a reduction order $>$ such that $\mathcal{R} \subseteq >$

a set E_0 of equations

Inference rules: (starting from $\langle E_0, \emptyset \rangle$)

Expand

$$\frac{\langle E \uplus \{s \doteq t\}, \quad H \rangle}{\langle E \cup \mathrm{Expd}_u(s,t), \quad H \cup \{s \to t\} \rangle} \; s > t, u \in \mathcal{B}(s)$$

Simplify

$$\frac{\langle E \uplus \{s \doteq t\}, \quad H \rangle}{\langle E \cup \{s' \doteq t\}, \quad H \rangle} \quad s \to_{\mathcal{R} \cup H} s'$$

Delete

$$\frac{\langle E \uplus \{s \doteq s\}, \quad H \rangle}{\langle E, \quad H \rangle}$$

Expand Rule

Expand

$$\frac{\langle E \cup \{s \doteq t\}, \quad H\rangle}{\langle E \cup \mathrm{Expd}_u(s,t), \quad H \cup \{s \to t\}\rangle}\ s > t, u \in \mathcal{B}(s)$$

$\mathcal{B}(s)$: **a set of** ***basic*** **subterms of** s

subterms of the form $f(c_1, \ldots, c_n)$

with $f \in \mathcal{D} = \{l(\epsilon) \mid l \to r \in \mathcal{R}\}$

and constructor terms $c_1, \ldots, c_n \in \mathrm{T}(\mathcal{C}, \mathcal{V})$**.**

Expand Rule

Expand

$$\frac{\langle E \cup \{s \doteq t\},\quad H\rangle}{\langle E \cup \mathrm{Expd}_u(s,t),\quad H \cup \{s \to t\}\rangle}\ s > t, u \in \mathcal{B}(s)$$

$\mathcal{B}(s)$: a set of *basic* subterms of s

subterms of the form $f(c_1, \ldots, c_n)$
with $f \in \mathcal{D} = \{l(\epsilon) \mid l \to r \in \mathcal{R}\}$
and constructor terms $c_1, \ldots, c_n \in \mathrm{T}(\mathcal{C}, \mathcal{V})$.

$$\mathrm{Expd}_u(s,t) = \{C[r]\sigma \doteq t\sigma \mid s = C[u], \sigma = \mathrm{mgu}(u,l), \\ l \to r \in \mathcal{R}\}$$

lhs-expansion (narrowing) of the equation $s \doteq t$

$$C[r]\sigma \leftarrow_{\mathcal{R}} C[l]\sigma = C[u]\sigma = s\sigma \doteq t\sigma$$

Example

$$\mathcal{R}\begin{cases} +(0,0) & \to & 0 \\ +(\mathsf{s}(x),y) & \to & \mathsf{s}(+(x,y)) \\ +(x,\mathsf{s}(y)) & \to & \mathsf{s}(+(y,x)) \end{cases}$$

$$\begin{array}{ll}
 & \langle \{\mathsf{s}(+(x,\mathsf{s}(y))) \doteq \mathsf{s}(+(y,\mathsf{s}(x))\},\ \emptyset\rangle \\
\overset{*}{\leadsto}{}^{s} & \langle \{\mathsf{s}(\mathsf{s}(+(y,x))) \doteq \mathsf{s}(\mathsf{s}(+(x,y)))\},\ \emptyset\rangle \\
\leadsto^{e} & \langle \{\mathsf{s}(\mathsf{s}(0)) \doteq \mathsf{s}(\mathsf{s}(0)),\ \mathsf{s}(\mathsf{s}(\mathsf{s}(+(y',x)))) \doteq \mathsf{s}(\mathsf{s}(+(x,\mathsf{s}(y')))), \\
 & \qquad \mathsf{s}(\mathsf{s}(\mathsf{s}(+(x',y)))) \doteq \mathsf{s}(\mathsf{s}(+(\mathsf{s}(x'),y)))\}, \\
 & \ \{\mathsf{s}(\mathsf{s}(+(y,x))) \to \mathsf{s}(\mathsf{s}(+(x,y)))\}\rangle \\
\overset{*}{\leadsto}{}^{s} & \langle \{\mathsf{s}(\mathsf{s}(0)) \doteq \mathsf{s}(\mathsf{s}(0)),\ \mathsf{s}(\mathsf{s}(\mathsf{s}(+(y',x)))) \doteq \mathsf{s}(\mathsf{s}(\mathsf{s}(+(y',x)))), \\
 & \qquad \mathsf{s}(\mathsf{s}(\mathsf{s}(+(x',y)))) \doteq \mathsf{s}(\mathsf{s}(\mathsf{s}(+(x',y))))\}, \\
 & \ \{\mathsf{s}(\mathsf{s}(+(y,x))) \to \mathsf{s}(\mathsf{s}(+(x,y)))\}\rangle \\
\overset{*}{\leadsto}{}^{d} & \langle \emptyset,\ \{\mathsf{s}(\mathsf{s}(+(y,x))) \to \mathsf{s}(\mathsf{s}(+(x,y)))\}\rangle
\end{array}$$

Advanced RI System for GCR

Expand

$$\frac{\langle E \uplus \{s \doteq t\}, \quad H\rangle}{\langle E \cup \{s'_i \doteq t_i\}_i, \quad H \cup \{s \to t\}\rangle} \quad \begin{array}{l} u \in \mathcal{B}(s), \cancel{s \succ t} \\ \{s_i \to t_i\}_i = \mathrm{Expd}_u(s,t), \\ s_i \to_{(H \cup H^{-1})^{\succsim}} s'_i \end{array}$$

Simplify

$$\frac{\langle E \uplus \{s \doteq t\}, \quad H\rangle}{\langle E \cup \{s' \doteq t\}, \quad H\rangle} \quad s \to_{\mathcal{R} \cup H^{\succ}} \circ \to_{(H \cup H^{-1})^{\succsim}} s'$$

Delete

$$\frac{\langle E \uplus \{s \doteq t\}, \quad H\rangle}{\langle E, \quad H\rangle} \; s \overset{=}{\leftrightarrow}_H t$$

Theorem. [Aoto&Toyama, 2016]

Suppose $\mathcal{R}$: SN, QR. Let $\succsim$ be a reduction quasi-order with $\mathcal{R} \subseteq \succ$. If $\langle \mathrm{CP}(\mathcal{R}), \emptyset\rangle \overset{*}{\rightsquigarrow} \langle \emptyset, H\rangle$ then $\mathcal{R}$: GCR.

GCR Proving Procedure

Step 1. Compute (possibly multiple) candidates for the partition $\mathcal{F} = \mathcal{D} \uplus \mathcal{C}$ of function symbols. (Our system includes more general non-free constructor case.)

Step 2. Compute (possibly multiple) candidates for (strongly) quasi-reducible $\mathcal{R}_0 \subseteq \mathcal{R}$.

Step 3. Find a reduction quasi-order $\succsim$ such that $\mathcal{R}_0 \subseteq \succ$.

Step 4. Run RI for GCR of $\mathcal{R}_0$ with $\succsim$.

Step 5. Run RI for proving $\mathcal{R}_0 \models_{ind} (\mathcal{R} \setminus \mathcal{R}_0)$.

Step 6. Return `YES` if it succeeds in steps 4 & 5.

GCR Proving Procedure

Step 1. Compute (possibly multiple) candidates for the partition $\mathcal{F} = \mathcal{D} \uplus \mathcal{C}$ of function symbols. (Our system includes more general non-free constructor case.)

Step 2. Compute (possibly multiple) candidates for (strongly) quasi-reducible $\mathcal{R}_0 \subseteq \mathcal{R}$.

Step 3. Find a reduction quasi-order $\succsim$ such that $\mathcal{R}_0 \subseteq \succ$.

Step 4. Run RI for GCR of $\mathcal{R}_0$ with $\succsim$.

Step 5. Run RI for proving $\mathcal{R}_0 \models_{ind} (\mathcal{R} \setminus \mathcal{R}_0)$.

Step 6. Return YES if it succeeds in steps 4 & 5.

GCR Proving Procedure

Step 1. Compute (possibly multiple) candidates for the partition $\mathcal{F} = \mathcal{D} \uplus \mathcal{C}$ of function symbols. (Our system includes more general non-free constructor case.)

Step 2. Compute (possibly multiple) candidates for (strongly) quasi-reducible $\mathcal{R}_0 \subseteq \mathcal{R}$.

Step 3. Find a reduction quasi-order $\succsim$ such that $\mathcal{R}_0 \subseteq \succ$.

Step 4. Run RI for GCR of $\mathcal{R}_0$ with $\succsim$.

Step 5. Run RI for proving $\mathcal{R}_0 \models_{ind} (\mathcal{R} \setminus \mathcal{R}_0)$.

Step 6. Return `YES` if it succeeds in steps 4 & 5.

Our procedure requires $\mathcal{R}_0 \subseteq \mathcal{R}$ with SN, QR.

Outline:

1. **Proving Ground Confluence by Rewriting Induction**
2. **GCR Proof with Pattern Complementation**

Failure of GCR Proving

Example. (from Cops 128)
Let $\mathcal{F} = \{+ : \mathsf{Nat} \times \mathsf{Nat} \to \mathsf{Nat}, \mathsf{s} : \mathsf{Nat} \to \mathsf{Nat}, 0 : \mathsf{Nat}\}$
and

$$\mathcal{R} = \left\{ \begin{array}{lcll} +(0, y) & \to & y & (a) \\ +(x, \mathsf{s}(y)) & \to & \mathsf{s}(+(x, y)) & (b) \\ +(x, y) & \to & +(y, x) & (c) \end{array} \right\}$$

Then there exists no quasi-reducible and terminating subsets of $\mathcal{R}$.

Note $+(\mathrm{s}(0), 0) \in \mathrm{NF}(\{(a), (b)\})$

Our Idea

A natural candidate of quasi-reducible terminating $\mathcal{R}_0$:

$$\mathcal{R}_0 = \left\{ \begin{array}{lcll} +(0, y) & \to & y & (a) \\ +(\mathsf{s}(x), y) & \to & \mathsf{s}(+(x, y)) & (b') \end{array} \right\}$$

Validity of the rewrite rule (b'):

$$\begin{array}{rl} +(\mathsf{s}(x), y) \to_{(c)} +(y, \mathsf{s}(x)) & \to_{(b)} \mathsf{s}(+(y, x)) \\ & \to_{(c)} \mathsf{s}(+(x, y)) \end{array}$$

How we compute missing patterns?

$\Rightarrow$ **Pattern Complementation Algorithm**

[Lazrek & Lescanne & Thiel, 1990]

Complement of linear substitution

A **complement** $C(t)$ **of** $t \in \mathrm{T}_L(\mathcal{C}, \mathcal{V})$ **(linear constr. term):**

$$\begin{array}{rcl} C(x) & = & \emptyset \\ C(c(t_1, \ldots, t_n)) & = & \{c'(x_1, \ldots, x_n) \mid c \neq c' \in \mathcal{C}\} \\ & & \cup \bigcup_{1 \leq k \leq n} \{c(t_1, \ldots, t_{k-1}, v, x_{k+1}, \ldots) \mid v \in C(t_k)\} \end{array}$$

Then $\mathrm{T}(\mathcal{C}) \setminus \mathrm{Inst}(t) = \bigcup_{v \in C(t)} \mathrm{Inst}(v)$ **where**

$$\mathrm{Inst}(v) = \{v\sigma_{gc} \mid \sigma_{gc}{:}\mathcal{V} \to \mathrm{T}(\mathcal{C})\}$$

A **complement** $C(\sigma)$ **of linear** $\sigma : \mathcal{V} \to \mathrm{T}(\mathcal{C}, \mathcal{V})$**:**

$$\begin{array}{rcl} C(\sigma) & = & \{\rho : \mathcal{V} \to \mathrm{T}(\mathcal{C}, \mathcal{V}) \mid \mathrm{dom}(\rho) = \mathrm{dom}(\sigma), \\ & & \rho(x) \in C(\sigma(x)) \cup \{\sigma(x)\}, \rho \neq \sigma\} \end{array}$$

Pattern Complementation

Let $P, Q \subseteq \mathrm{T}_{LB}(\mathcal{D}, \mathcal{C}, \mathcal{V})$ **(i.e. sets of linear basic terms)**
P **is a complement of** Q **if** $\mathrm{Inst}(P) \uplus \mathrm{Inst}(Q) = \mathrm{T}_B(\mathcal{D}, \mathcal{C})$
where $\mathrm{Inst}(P) = \{p\sigma_{gc} \mid p \in P, \sigma_{gc} : \mathcal{V} \to \mathrm{T}(\mathcal{C})\}$

Subtraction on patterns $P \ominus Q$**:**

$$P \ominus Q = \begin{cases} P_s \ominus Q_t & \textbf{if } \exists s \in P, t \in Q, \sigma = \mathrm{mgu}(s, t) \\ P & \textbf{otherwise} \end{cases}$$

where $P_s = (P \setminus \{s\}) \cup \{s\rho \mid \rho \in C(\sigma), s\rho \neq s\sigma\}$
$Q_t = (Q \setminus \{t\}) \cup \{t\rho \mid \rho \in C(\sigma), t\rho \neq t\sigma\}$

Complement $C(P)$ **of a pattern** P**:**

$$C(P) = \{f(x_1, \ldots, x_n) \mid f \in \mathcal{D}\} \ominus P$$

New Procedure

Step 1. Compute (possibly multiple) candidates for the partition $\mathcal{F} = \mathcal{D} \uplus \mathcal{C}$ of function symbols.

Step 2. Find left-linear $\mathcal{R}_0 \subseteq \mathcal{R}$ and a reduction quasi-order $\succsim$ such that $\mathcal{R}_0 \subseteq \succ$.

Step 3. Compute complement $\{p_i\}_i$ of $lhs(\mathcal{R}_0)$. For each i, find p'_i such that $p_i \xrightarrow{*}_{\mathcal{R}} p'_i$ and $p \succ p'_i$. Let $\mathcal{R}_1 = \mathcal{R}_0 \cup \{p_i \to p'_i\}_i$.

Step 4. Run RI for GCR of $\mathcal{R}_1$ with $\succsim$.

Step 5. Run RI for proving $\mathcal{R}_1 \models_{ind} (\mathcal{R} \setminus \mathcal{R}_0)$.

Step 6. Return YES if it succeeds in steps 4 & 5.

Experiments by AGCP

problem	added equation(s)	steps		
		#1	#2	#3
Cops 128	$+(\mathsf{s}(x), 0) \to \mathsf{s}(x)$	$\times$	$\checkmark$	$\checkmark$
Cops 130	$\left\{ \begin{array}{l} \mathsf{and3}(\mathsf{F}, \mathsf{T}, \mathsf{T}) \to \mathsf{F} \\ \mathsf{and3}(\mathsf{F}, \mathsf{F}, \mathsf{T}) \to \mathsf{F} \\ \mathsf{and3}(\mathsf{T}, \mathsf{F}, \mathsf{T}) \to \mathsf{F} \end{array} \right\}$	$\times$	$\times$	$\checkmark$
Cops 133	$+(0, \mathsf{s}(x)) \to \mathsf{s}(x)$	$\times$	$\checkmark$	$\checkmark$
Cops 137	$\mathsf{max}(0, \mathsf{s}(y)) \to \mathsf{s}(y)$	$\times$	$\checkmark$	$\checkmark$
Cops 140	$+(\mathsf{s}(x), 0) \to \mathsf{s}(x)$	$\times$	$\checkmark$	$\checkmark$
Cops 146	$+(0, \mathsf{s}(x)) \to \mathsf{s}(x)$	$\times$	$\checkmark$	$\checkmark$
Cops 165	$\mathsf{max}(0, \mathsf{s}(y)) \to \mathsf{s}(y)$	$\times$	$\checkmark$	$\checkmark$
Cops 174	$+(0, \mathsf{s}(x)) \to \mathsf{s}(x)$	$\times$	$\checkmark$	$\checkmark$
Cops 180	$+(\mathsf{s}(x), 0) \to \mathsf{s}(x)$	$\times$	$\checkmark$	$\checkmark$
Cops 186	$+(0, \mathsf{s}(x)) \to \mathsf{s}(x)$	$\times$	$\checkmark$	$\checkmark$
Cops 197	$\mathsf{or}(\mathsf{F}, \mathsf{T}) \to \mathsf{T}$	$\times$	$\checkmark$	$\checkmark$
Cops 210	$+(\mathsf{s}(x), 0) \to \mathsf{s}(x)$	$\times$	$\checkmark$	$\checkmark$
Cops 234	$\mathsf{eq}(0, 0) \to \mathsf{true}$	$\checkmark$	$\checkmark$	$\checkmark$
	total time (seconds)	**32.694**	**32.620**	**33.052**

Improvement: $86/121 \Rightarrow 99/121$

Conclusion

- Rewriting induction for GCR may fail when defining rules are not fully presented.

- Such hidden defining rules may be obtained by (1) computing lack of defining patterns by pattern complementation algorithm and (2) searching an appropriate rhs for the rewrite rule.

- By adding the proposed method to our GCR prover, we can automatically prove 13 new examples from our 121 GCR problem collection.