Modular Church-Rosser Modulo

Jean-Pierre Jouannaud
École Polytechnique
91400 Palaiseau, France

Project LogiCal, Pôle Commun de Recherche en Informatique du Plateau de Saclay, CNRS, École Polytechnique, INRIA, Université Paris-Sud

Joint work with Yoshihito Toyama
Tohoku University, Sendai, Japan

NII, Tokyo, december 8, 2006

Outline

Confluent rewrite systems

- Rewrite system:

$$R = \{x + 0 \rightarrow x, \quad x + S(y) \rightarrow S(x + y)\}$$

- Derivation:

$$S(0) + S(0 + 0) \longrightarrow_R S(0) + S(0) \longrightarrow_R S(S(0) + 0) \longrightarrow_R S(S(0))$$

- Confluence:

$$\forall s, t, u. \quad u \longrightarrow^* s \text{ and } u \longrightarrow^* t$$
$$\exists v. \ s \longrightarrow^* v \text{ and } t \longrightarrow^* v$$

- Modularity: does $R \cup S$ inherit the confluence property of R, S ?

Confluent rewrite systems

- Rewrite system:

$$R = \{x + 0 \to x, \quad x + S(y) \to S(x + y)\}$$

- Derivation:

$$S(0) + S(0 + 0) \longrightarrow_R S(0) + S(0)$$
$$\longrightarrow_R S(S(0) + 0) \longrightarrow_R S(S(0))$$

- Confluence:

$$\forall s, t, u. \quad u \longrightarrow^* s \text{ and } u \longrightarrow^* t$$
$$\exists v. \, s \longrightarrow^* v \text{ and } t \longrightarrow^* v$$

- Modularity: does $R \cup S$ inherit the confluence property of R, S ?

Confluent rewrite systems

- Rewrite system:

$$R = \{x + 0 \to x, \quad x + S(y) \to S(x + y)\}$$

- Derivation:

$$S(0) + S(0 + 0) \longrightarrow_R S(0) + S(0)$$
$$\longrightarrow_R S(S(0) + 0) \longrightarrow_R S(S(0))$$

- Confluence:

$$\forall s, t, u. \quad u \longrightarrow^* s \text{ and } u \longrightarrow^* t$$
$$\exists v. \, s \longrightarrow^* v \text{ and } t \longrightarrow^* v$$

- Modularity: does $R \cup S$ inherit the confluence property of R, S ?

Confluent rewrite systems

- Rewrite system:

$$R = \{x + 0 \to x, \quad x + S(y) \to S(x + y)\}$$

- Derivation:

$$S(0) + S(0 + 0) \longrightarrow_R S(0) + S(0)$$
$$\longrightarrow_R S(S(0) + 0) \longrightarrow_R S(S(0))$$

- Confluence:

$$\forall s, t, u. \quad u \longrightarrow^* s \text{ and } u \longrightarrow^* t$$
$$\exists v.\ s \longrightarrow^* v \text{ and } t \longrightarrow^* v$$

- Modularity: does $R \cup S$ inherit the confluence property of R, S ?

Toyama's modularity theorem

- Let R, S be two confluent rewrite systems
- Assumptions:
  (i) R and S share no function symbol
  (ii) Rules have no extra variables on the right
  (iii) No lefthand side of rule is a variable
- Conclusion: $R \cup S$ is confluent

Bibliography

1. Initial proof: [Toyama, JACM 1987]
2. Improved proof: [Klop, Middledorp, Toyama, de Vrijer, IPL 1994]
3. Shared constructor: [Ohlebusch, JSC 1995]
4. Assumption (ii) superflous: [Ghani, Luth, Abbott, RTA 2005]
5. Modulo case: [Jouannaud, RTA 2006]
6. Modularity is constructive: [Van Oostrom, 2006]
7. Assumption (iii) is necessary (here)
8. More general modulo case (here)

Need for assumption (iii)

- Assumption (iii) is necessary:

$$R = \{g(a) \to b\} \qquad S = \{x \to f(x)\}$$

- Diverging computation:

$$g(a) \xrightarrow[S]{} b \text{ and } g(a) \xrightarrow[R]{} g(f(a))$$

- $b \longrightarrow^* u \in \{f^n(b) \mid n \geq 0\}$
- $g(f(a)) \longrightarrow^* v \in \{f^m(g(f^{n+1}(a))) \mid m, n \geq 0\}$
- $\{f^n(b) \mid n \geq 0\} \cap$
  $\{f^m(g(f^{n+1}(a))) \mid m, n \geq 0\} = \emptyset$

Need for assumption (iii)

- Assumption (iii) is necessary:

$$R = \{g(a) \to b\} \qquad S = \{x \to f(x)\}$$

- Diverging computation:

$$g(a) \xrightarrow[S]{} b \text{ and } g(a) \xrightarrow[R]{} g(f(a))$$

- $b \longrightarrow^* u \in \{f^n(b) \mid n \geq 0\}$
- $g(f(a)) \longrightarrow^* v \in \{f^m(g(f^{n+1}(a))) \mid m, n \geq 0\}$
- $\{f^n(b) \mid n \geq 0\} \cap \{f^m(g(f^{n+1}(a))) \mid m, n \geq 0\} = \emptyset$

Need for assumption (iii)

- Assumption (iii) is necessary:

$$R = \{g(a) \to b\} \qquad S = \{x \to f(x)\}$$

- Diverging computation:

$$g(a) \underset{S}{\longrightarrow} b \text{ and } g(a) \underset{R}{\longrightarrow} g(f(a))$$

- $b \longrightarrow^* u \in \{f^n(b) \mid n \geq 0\}$
- $g(f(a)) \longrightarrow^* v \in \{f^m(g(f^{n+1}(a))) \mid m, n \geq 0\}$
- $\{f^n(b) \mid n \geq 0\} \cap$
  $\{f^m(g(f^{n+1}(a))) \mid m, n \geq 0\} = \emptyset$

Need for assumption (iii)

- Assumption (iii) is necessary:

$$R = \{g(a) \to b\} \qquad S = \{x \to f(x)\}$$

- Diverging computation:

$$g(a) \xrightarrow[S]{} b \text{ and } g(a) \xrightarrow[R]{} g(f(a))$$

- $b \longrightarrow^* u \in \{f^n(b) \mid n \geq 0\}$
- $g(f(a)) \longrightarrow^* v \in \{f^m(g(f^{n+1}(a))) \mid m, n \geq 0\}$
- $\{f^n(b) \mid n \geq 0\} \cap$
  $\{f^m(g(f^{n+1}(a))) \mid m, n \geq 0\} = \emptyset$

Need for assumption (iii)

- Assumption (iii) is necessary:

$$R = \{g(a) \to b\} \qquad S = \{x \to f(x)\}$$

- Diverging computation:

$$g(a) \underset{S}{\longrightarrow} b \text{ and } g(a) \underset{R}{\longrightarrow} g(f(a))$$

- $b \longrightarrow^* u \in \{f^n(b) \mid n \geq 0\}$
- $g(f(a)) \longrightarrow^* v \in \{f^m(g(f^{n+1}(a))) \mid m, n \geq 0\}$
- $\{f^n(b) \mid n \geq 0\} \cap$
  $\{f^m(g(f^{n+1}(a))) \mid m, n \geq 0\} = \emptyset$

A term s can be decomposed into

- a topmost maximal homogeneous cap $\widehat{s}$
- An *alien substitution* γ_s

such that $s = \widehat{s}\gamma_s$

Example:

$\mathcal{F} = \{f, c, a\} \quad \mathcal{G} = \{g\} \quad \mathcal{X} = \{x\}$

$s = c(g(c(a, a)), f(g(c(a, a))))$

$\widehat{s} = c(x, f(x))$

$\gamma_s = \{x \mapsto g(c(a, a))\}$

A term s can be decomposed into

- a topmost maximal homogeneous cap $\widehat{s}$
- An *alien substitution* γ_s

such that $s = \widehat{s}\gamma_s$

Example:

$\mathcal{F} = \{f, c, a\} \quad \mathcal{G} = \{g\} \quad \mathcal{X} = \{x\}$

$s = c(g(c(a, a)), f(g(c(a, a))))$

$\widehat{s} = c(x, f(x))$

$\gamma_s = \{x \mapsto g(c(a, a))\}$

A term s can be decomposed into

- a topmost maximal homogeneous cap $\widehat{s}$
- An *alien substitution* γ_s

such that $s = \widehat{s}\gamma_s$

Example:

$\mathcal{F} = \{f, c, a\} \quad \mathcal{G} = \{g\} \quad \mathcal{X} = \{x\}$

$s = c(g(c(a, a)), f(g(c(a, a))))$

$\widehat{s} = c(x, f(x))$

$\gamma_s = \{x \mapsto g(c(a, a))\}$

A term s can be decomposed into

- a topmost maximal homogeneous cap $\widehat{s}$
- An *alien substitution* γ_s

such that $s = \widehat{s}\gamma_s$

Example:

$\mathcal{F} = \{f, c, a\} \quad \mathcal{G} = \{g\} \quad \mathcal{X} = \{x\}$

$s = c(g(c(a, a)), f(g(c(a, a))))$

$\widehat{s} = c(x, f(x))$

$\gamma_s = \{x \mapsto g(c(a, a))\}$

A term s can be decomposed into

- a topmost maximal homogeneous cap $\widehat{s}$
- An *alien substitution* γ_s

such that $s = \widehat{s}\gamma_s$

Example:

$\mathcal{F} = \{f, c, a\} \quad \mathcal{G} = \{g\} \quad \mathcal{X} = \{x\}$

$s = c(g(c(a, a)), f(g(c(a, a))))$

$\widehat{s} = c(x, f(x))$

$\gamma_s = \{x \mapsto g(c(a, a))\}$

Difficulties

- Collapsing rules such as $x + 0 \to x$ may decrease the rank of terms along derivations
- Rules with new variables in their righthand side such as $0 \to 0 \times y$ may increase the rank of terms along derivations
- The confluence property is not general enough for inductive proofs to go through

We use the Church-Rosser property instead of confluence:

$$\forall u, v. \quad u \stackrel{*}{\longleftrightarrow} v \quad \exists s, t. \quad u \stackrel{*}{\longrightarrow} s = t \stackrel{*}{\longleftarrow} v$$

Difficulties

- Collapsing rules such as $x + 0 \to x$ may decrease the rank of terms along derivations
- Rules with new variables in their righthand side such as $0 \to 0 \times y$ may increase the rank of terms along derivations
- The confluence property is not general enough for inductive proofs to go through

We use the Church-Rosser property instead of confluence:

$$\forall u, v. \quad u \overset{*}{\longleftrightarrow} v \quad \exists s, t. \quad u \overset{*}{\longrightarrow} s = t \overset{*}{\longleftarrow} v$$

Difficulties

- Collapsing rules such as $x + 0 \to x$ may decrease the rank of terms along derivations
- Rules with new variables in their righthand side such as $0 \to 0 \times y$ may increase the rank of terms along derivations
- The confluence property is not general enough for inductive proofs to go through

We use the Church-Rosser property instead of confluence:

$$\forall u, v. \quad u \xleftrightarrow{*} v \quad \exists s, t. \quad u \xrightarrow{*} s = t \xleftarrow{*} v$$

A naive “proof” of the CR property

- **Start:** $v \leftrightarrow^*_{R \cup S} w$
- **Reasonnable Intuition:**

  $\widehat{v} \leftrightarrow^*_{R \uplus S} \widehat{w}$ and $\gamma_v \leftrightarrow^*_{R \cup S} \gamma_w$
- **Assumption:**

  $\widehat{v} \longrightarrow^*_{R \uplus S} s = t \longleftarrow^*_{R \uplus S} \widehat{w}$
- **Induction:**

  $\gamma_v \longrightarrow^*_{R \cup S} \sigma = \tau \longleftarrow^*_{R \cup S} \gamma_w$
- **Conclusion:**

$$
\begin{array}{l}
v = \widehat{v}\gamma_v \xrightarrow[Ass]{*} s\gamma_v \xrightarrow[Ind]{*} s\sigma \\
\qquad\qquad\qquad\qquad\qquad\quad = \\
w = \widehat{w}\gamma_w \xrightarrow[Ass]{*} t\gamma_w \xrightarrow[Ind]{*} t\tau
\end{array}
$$

A naive "proof" of the CR property

- Start: $v \leftrightarrow^*_{R \cup S} w$
- Reasonnable Intuition:

$$\widehat{v} \leftrightarrow^*_{R \uplus S} \widehat{w} \quad \text{and} \quad \gamma_v \leftrightarrow^*_{R \cup S} \gamma_w$$

- Assumption:

$$\widehat{v} \longrightarrow^*_{R \uplus S} s = t \longleftarrow^*_{R \uplus S} \widehat{w}$$

- Induction:

$$\gamma_v \longrightarrow^*_{R \cup S} \sigma = \tau \longleftarrow^*_{R \cup S} \gamma_w$$

- Conclusion:

$$v = \widehat{v}\gamma_v \xrightarrow[Ass]{*} s\gamma_v \xrightarrow[Ind]{*} s\sigma$$

$$=$$

$$w = \widehat{w}\gamma_w \xrightarrow[Ass]{*} t\gamma_w \xrightarrow[Ind]{*} t\tau$$

A naive “proof” of the CR property

- Start: $v \leftrightarrow^*_{R\cup S} w$
- Reasonnable Intuition:

  $\widehat{v} \leftrightarrow^*_{R\uplus S} \widehat{w}$ and $\gamma_v \leftrightarrow^*_{R\cup S} \gamma_w$
- Assumption:

  $\widehat{v} \longrightarrow^*_{R\uplus S} s = t \longleftarrow^*_{R\uplus S} \widehat{w}$
- Induction:

  $\gamma_v \longrightarrow^*_{R\cup S} \sigma = \tau \longleftarrow^*_{R\cup S} \gamma_w$
- Conclusion:

$$\begin{array}{c}
v = \widehat{v}\gamma_v \xrightarrow[Ass]{*} s\gamma_v \xrightarrow[Ind]{*} s\sigma \\
\qquad\qquad\qquad\qquad\qquad\quad\; = \\
w = \widehat{w}\gamma_w \xrightarrow[Ass]{*} t\gamma_w \xrightarrow[Ind]{*} t\tau
\end{array}$$

A naive "proof" of the CR property

- Start: $v \leftrightarrow^*_{R \cup S} w$
- Reasonnable Intuition:

  $\widehat{v} \leftrightarrow^*_{R \uplus S} \widehat{w}$ and $\gamma_v \leftrightarrow^*_{R \cup S} \gamma_w$
- Assumption:

  $\widehat{v} \longrightarrow^*_{R \uplus S} s = t \longleftarrow^*_{R \uplus S} \widehat{w}$
- Induction:

  $\gamma_v \longrightarrow^*_{R \cup S} \sigma = \tau \longleftarrow^*_{R \cup S} \gamma_w$
- Conclusion:

$$v = \widehat{v}\gamma_v \xrightarrow[Ass]{*} s\gamma_v \xrightarrow[Ind]{*} s\sigma$$

$$=$$

$$w = \widehat{w}\gamma_w \xrightarrow[Ass]{*} t\gamma_w \xrightarrow[Ind]{*} t\tau$$

A naive "proof" of the CR property

- Start: $v \leftrightarrow^*_{R \cup S} w$
- Reasonnable Intuition:

  $\widehat{v} \leftrightarrow^*_{R \uplus S} \widehat{w}$ and $\gamma_v \leftrightarrow^*_{R \cup S} \gamma_w$
- Assumption:

  $\widehat{v} \longrightarrow^*_{R \uplus S} s = t \longleftarrow^*_{R \uplus S} \widehat{w}$
- Induction:

  $\gamma_v \longrightarrow^*_{R \cup S} \sigma = \tau \longleftarrow^*_{R \cup S} \gamma_w$
- Conclusion:

$$
\begin{array}{ccccc}
v = \widehat{v}\gamma_v & \xrightarrow[Ass]{*} & s\gamma_v & \xrightarrow[Ind]{*} & s\sigma \\
 & & & & = \\
w = \widehat{w}\gamma_w & \xrightarrow[Ass]{*} & t\gamma_w & \xrightarrow[Ind]{*} & t\tau
\end{array}
$$

Stable Equalizers

Definition

- A term is an equalizer iff it is homogeneous, or else any two equivalent aliens are identical equalizers.
- A substitution is an equalizer if if $\forall x.\quad x\gamma$ is an equalizer, and $\forall x, y.\quad x\gamma \leftrightarrow^* y\gamma$ iff $x = y$.
- An equalizer is cap-stable if the cap is not equivalent to one of its variables.
- An equalizer t is stable if it is cap-stable and its aliens are stable.

Note: Assuming variables are in normal form,

$$s \overset{*}{\longleftrightarrow} x \quad \text{iff} \quad s \overset{*}{\longrightarrow} x$$

Stable Equalizers

Definition

- A term is an equalizer iff it is homogeneous, or else any two equivalent aliens are identical equalizers.
- A substitution is an equalizer if if $\forall x. \quad x\gamma$ is an equalizer, and $\forall x, y. \quad x\gamma \leftrightarrow^* y\gamma$ iff $x = y$.
- An equalizer is cap-stable if the cap is not equivalent to one of its variables.
- An equalizer t is stable if it is cap-stable and its aliens are stable.

Note: Assuming variables are in normal form,

$$s \overset{*}{\longleftrightarrow} x \quad \text{iff} \quad s \overset{*}{\longrightarrow} x$$

Definition

- A term is an equalizer iff it is homogeneous, or else any two equivalent aliens are identical equalizers.
- A substitution is an equalizer if if $\forall x. \quad x\gamma$ is an equalizer, and $\forall x, y. \quad x\gamma \leftrightarrow^* y\gamma$ iff $x = y$.
- An equalizer is cap-stable if the cap is not equivalent to one of its variables.
- An equalizer t is stable if it is cap-stable and its aliens are stable.

Note: Assuming variables are in normal form,

$$s \overset{*}{\leftrightarrow} x \quad \text{iff} \quad s \overset{*}{\longrightarrow} x$$

Definition

- A term is an equalizer iff it is homogeneous, or else any two equivalent aliens are identical equalizers.
- A substitution is an equalizer if if $\forall x.\quad x\gamma$ is an equalizer, and $\forall x, y.\quad x\gamma \leftrightarrow^* y\gamma$ iff $x = y$.
- An equalizer is cap-stable if the cap is not equivalent to one of its variables.
- An equalizer t is stable if it is cap-stable and its aliens are stable.

Note: Assuming variables are in normal form,

$$s \xleftrightarrow{*} x \quad \text{iff} \quad s \xrightarrow{*} x$$

Stable Equalizers

Definition

- A term is an equalizer iff it is homogeneous, or else any two equivalent aliens are identical equalizers.
- A substitution is an equalizer if if $\forall x. \quad x\gamma$ is an equalizer, and $\forall x, y. \quad x\gamma \leftrightarrow^* y\gamma$ iff $x = y$.
- An equalizer is cap-stable if the cap is not equivalent to one of its variables.
- An equalizer t is stable if it is cap-stable and its aliens are stable.

Note: Assuming variables are in normal form,

$$s \overset{*}{\leftrightarrow} x \quad \text{iff} \quad s \overset{*}{\longrightarrow} x$$

Stable Equalizers

Definition

- A term is an equalizer iff it is homogeneous, or else any two equivalent aliens are identical equalizers.
- A substitution is an equalizer if if $\forall x. \quad x\gamma$ is an equalizer, and $\forall x, y. \quad x\gamma \leftrightarrow^* y\gamma$ iff $x = y$.
- An equalizer is cap-stable if the cap is not equivalent to one of its variables.
- An equalizer t is stable if it is cap-stable and its aliens are stable.

Note: Assuming variables are in normal form,

$$s \overset{*}{\leftrightarrow} x \quad \text{iff} \quad s \overset{*}{\longrightarrow} x$$

Example

$$\mathcal{F} = \{f, c, +, a, b\} \quad \mathcal{G} = \{g, h\} \quad \text{X=\{x\}}$$

$$\begin{aligned} R &= \{c(x,x) \rightarrow x \\ &\quad +(a,b) \rightarrow +(b,a)\} \\ S &= \{g(x) \rightarrow h(x)\} \end{aligned}$$

$c(g(+(b,a)), f(g(+(b,a))))$
is a stable $R \cup S$-equalizer while

$c(g(+(a,b)), h(+(b,a))) \longrightarrow^{*}_{R \cup S} h(+(b,a))$
is a cap-collapsing non-equalizer.

Lemma (Cleaning)

Let u be a term such that the set of all its non-trivial aliens has the Church-Rosser property with respect to $R \cup S$. Then, there exists a stable equalizer s such that $u \longrightarrow^*_{R \cup S} s$.

Proof: By CR assumption, we assume that u is an equalizer and proceed by induction on rank.
If u is stable, done.
Otherwise, by induction hypothesis, we stabilize its aliens yielding v. If v is stable, done.
Otherwise, $\widehat{v}$ projects on one of its variables, hence v rewrites to one of its aliens. Done.

Reachability of stable equalizers

Lemma (Cleaning)

Let u be a term such that the set of all its non-trivial aliens has the Church-Rosser property with respect to $R \cup S$. Then, there exists a stable equalizer s such that $u \longrightarrow^*_{R \cup S} s$.

Proof: By CR assumption, we assume that u is an equalizer and proceed by induction on rank.

If u is stable, done.

Otherwise, by induction hypothesis, we stabilize its aliens yielding v. If v is stable, done.

Otherwise, $\widehat{v}$ projects on one of its variables, hence v rewrites to one of its aliens. Done.

Example

$\mathcal{F} = \{f, c, +, a, b\} \quad \mathcal{G} = \{g, h\} \quad$ X={x}

$$R = \begin{array}{rcl} \{c(x, x) & \rightarrow & x \\ +(a, b) & \rightarrow & +(b, a)\} \end{array}$$

$$S = \{g(x) \rightarrow h(x)\}$$

$$c(g(+(a, b)), h(+(b, a))) \stackrel{*}{\longrightarrow}_{R \cup S} h(+(b, a))$$

Structure Lemma

- Input:
  E, an arbitrary set of equations
  $\succ$, a rewrite ordering total on ground terms
- Ordered rewriting with E is defined as:
  $s \longrightarrow_E^{\succ} t$ iff $s \leftrightarrow_E t$ and $s \succ t$
- Output:
  E^{∞}, an (infinite) terminating set of equations which is CR:

$$\forall s \overset{*}{\underset{E}{\leftrightarrow}} t \quad \exists u \text{ s.t. } s \xrightarrow[E^{\infty}]{*,\succ} u \text{ and } t \xrightarrow[E^{\infty}]{*,\succ} u$$

- Note: equations $s = x$ become rules $s \rightarrow x$

- Input:
  E, an arbitrary set of equations
  $\succ$, a rewrite ordering total on ground terms
- Ordered rewriting with E is defined as:
  $s \longrightarrow^{\succ}_{E} t$ iff $s \leftrightarrow_E t$ and $s \succ t$
- Output:
  E^∞, an (infinite) terminating set of equations which is CR:

$$\forall s \overset{*}{\underset{E}{\leftrightarrow}} t \quad \exists u \text{ s.t. } s \xrightarrow[E^\infty]{*,\succ} u \text{ and } t \xrightarrow[E^\infty]{*,\succ} u$$

- Note: equations $s = x$ become rules $s \to x$

- Input:
  E, an arbitrary set of equations
  $\succ$, a rewrite ordering total on ground terms
- Ordered rewriting with E is defined as:
  $s \longrightarrow_E^{\succ} t$ iff $s \leftrightarrow_E t$ and $s \succ t$
- Output:
  E^∞, an (infinite) terminating set of equations which is CR:

$$\forall s \overset{*}{\underset{E}{\leftrightarrow}} t \quad \exists u \text{ s.t. } s \xrightarrow[E^\infty]{*,\succ} u \text{ and } t \xrightarrow[E^\infty]{*,\succ} u$$

- Note: equations $s = x$ become rules $s \rightarrow x$

Ordered Completion

- Input:
  E, an arbitrary set of equations
  $\succ$, a rewrite ordering total on ground terms
- Ordered rewriting with E is defined as:
  $s \longrightarrow^{\succ}_{E} t$ iff $s \leftrightarrow_E t$ and $s \succ t$
- Output:
  E^{∞}, an (infinite) terminating set of equations which is CR:

$$\forall s \overset{*}{\underset{E}{\leftrightarrow}} t \quad \exists u \text{ s.t. } s \xrightarrow[E^{\infty}]{*,\succ} u \text{ and } t \xrightarrow[E^{\infty}]{*,\succ} u$$

- Note: equations $s = x$ become rules $s \to x$

Lemma (Structure)

Let $R \cup S$ be a disjoint union, and v and w be stable equalizers such that $v \leftrightarrow^*_{R\cup S} w$. Then, there exists a variable renaming η such that

$$\eta\widehat{v} \overset{*}{\underset{R\cup S}{\longleftrightarrow}} \widehat{w} \quad \text{and} \quad \gamma_v \overset{*}{\underset{R\cup S}{\longleftrightarrow}} \eta\gamma_w$$

The proof relies on three simple properties of ordered completion:

1. modularity: $(R \cup S)^\infty = R^\infty \cup S^\infty$;
2. Variables are in normal form for $R^\infty \cup S^\infty$.
3. $\forall u. \quad u \downarrow_{R^\infty}$ is a stable equalizer;

Lemma (Structure)

Let $R \cup S$ be a disjoint union, and v and w be stable equalizers such that $v \leftrightarrow^*_{R\cup S} w$. Then, there exists a variable renaming η such that

$$\eta\widehat{v} \overset{*}{\underset{R\cup S}{\longleftrightarrow}} \widehat{w} \quad \textit{and} \quad \gamma_v \overset{*}{\underset{R\cup S}{\longleftrightarrow}} \eta\gamma_w$$

The proof relies on three simple properties of ordered completion:

1. modularity: $(R \cup S)^\infty = R^\infty \cup S^\infty$;
2. Variables are in normal form for $R^\infty \cup S^\infty$.
3. $\forall u. \quad u \downarrow_{R^\infty}$ is a stable equalizer;

Generalization to Rewriting Modulo

- Let R (resp. S) be a set of rewrite rules built over $\mathcal{F}$ (resp. $\mathcal{G}$) with $\mathcal{F} \cap \mathcal{G} = \emptyset$;
- Let E (resp. D) be a set of *regular* equations built over $\mathcal{F}$ (resp. $\mathcal{G}$);
- Let $E^{\rightarrow}$ and $E^{\leftarrow}$ (resp. $D^{\rightarrow}$ and $D^{\leftarrow}$) be the rewrite systems obtained from E (resp. D).

Definition

$\Longrightarrow_{R,E}$ is CR modulo E iff

$$\forall u, v. \quad u \longleftrightarrow^*_{R \cup E} v$$

$$\exists s, t. \quad u \Longrightarrow^*_{R,E} s \longleftrightarrow^*_E t \Longleftarrow^*_{R,E} v$$

- Let R (resp. S) be a set of rewrite rules built over $\mathcal{F}$ (resp. $\mathcal{G}$) with $\mathcal{F} \cap \mathcal{G} = \emptyset$;
- Let E (resp. D) be a set of *regular* equations built over $\mathcal{F}$ (resp. $\mathcal{G}$);
- Let $E^{\rightarrow}$ and $E^{\leftarrow}$ (resp. $D^{\rightarrow}$ and $D^{\leftarrow}$) be the rewrite systems obtained from E (resp. D).

Definition

$\Longrightarrow_{R,E}$ is CR modulo E iff

$$\forall u, v. \quad u \leftrightarrow^{*}_{R \cup E} v$$

$$\exists s, t. \quad u \Longrightarrow^{*}_{R,E} s \leftrightarrow^{*}_{E} t \Longleftarrow^{*}_{R,E} v$$

Zoo of rewriting relations

- Class rewriting [Lankford]
- Plain rewriting modulo [Huet]
- Rewriting modulo [Stickel]
- Normalized rewriting [Marché]
- Normal rewriting [Jouannaud, van Raamsdonk, Rubio]

Zoo of rewriting relations

- Class rewriting [Lankford]
- Plain rewriting modulo [Huet]
- Rewriting modulo [Stickel]
- Normalized rewriting [Marché]
- Normal rewriting [Jouannaud, van Raamsdonk, Rubio]

Zoo of rewriting relations

- Class rewriting [Lankford]
- Plain rewriting modulo [Huet]
- Rewriting modulo [Stickel]
- Normalized rewriting [Marché]
- Normal rewriting
  [Jouannaud, van Raamsdonk, Rubio]

Zoo of rewriting relations

- Class rewriting [Lankford]
- Plain rewriting modulo [Huet]
- Rewriting modulo [Stickel]
- Normalized rewriting [Marché]
- Normal rewriting [Jouannaud, van Raamsdonk, Rubio]

Zoo of rewriting relations

- Class rewriting [Lankford]
- Plain rewriting modulo [Huet]
- Rewriting modulo [Stickel]
- Normalized rewriting [Marché]
- Normal rewriting
  [Jouannaud, van Raamsdonk, Rubio]

Modularity of CR modulo

Theorem

Any rewrite relation $\Longrightarrow_{R,E}$ satisfying

$$
\begin{array}{rl}
(i) & \Longrightarrow_{R,E} \subseteq (\leftrightarrow_E^* \longrightarrow_R \leftrightarrow_E^*)^* \\
(ii) & \longrightarrow_R \subseteq (\leftrightarrow_E^* \Longrightarrow_{R,E} \leftrightarrow_E^*)^* \\
(iii) & \textit{Variables are in normal form for } \Longrightarrow_{R,E} \\
(iv) & E \textit{ is non-collapsing}
\end{array}
$$

enjoys a modular Church-Rosser property.

A simple case: Class Rewriting

Since arbitrary E-equational steps are allowed with class-rewriting

1. Plain rewriting with $R \cup E^{\rightarrow} \cup E^{\leftarrow}$ is CR if class-rewriting with (R, E) is CR;
2. Toyama's theorem applies to $(R \cup E^{\rightarrow} \cup E^{\leftarrow}) \cup (S \cup D^{\rightarrow} \cup D^{\leftarrow})$;
3. Class-rewriting with $(R \cup S, E \cup D)$ is CR if plain rewriting with $(R \cup E^{\rightarrow} \cup E^{\leftarrow}) \cup (S \cup D^{\rightarrow} \cup D^{\leftarrow})$ is CR.

The last step of this proof does not scale up for other forms of *rewriting modulo*.

Lemma (Cleaning)

Let u be a term such that the set of its non-trivial aliens has the Church-Rosser property for $\Longrightarrow$. Then, there exists a stable equalizer s such that $u \Longrightarrow^* s$.

Simple induction using the cleaning Lemma for the (confluent on aliens) rewrite relation $R \cup E^{\rightarrow} \cup E^{\leftarrow} \cup S \cup D^{\rightarrow} \cup D^{\leftarrow}$.

Modularity proof

- Cleaning Lemma: $v \Longrightarrow^*_{R \cup S, E \cup D} v'$, $w \Longrightarrow^*_{R \cup S. E \cup D} w'$, for stable equalizers v', w'.
- Assumption (ii): $v'\eta \leftrightarrow^*_{R \cup E \cup S \cup D} w'$.
- Structure Lemma: $\widehat{v'}\eta \leftrightarrow^*_{R \cup E \cup S \cup D} \widehat{w'}$ and $\gamma_{v'} \leftrightarrow^*_{R \cup E \cup S \cup D} \eta\gamma_{w'}$.
- Church-Rosser assumption: $\widehat{v'}\eta \Longrightarrow^* \; s = t \; \Longleftarrow^* \widehat{w'}$.
- Induction hypothesis: $\gamma_{v'} \Longrightarrow^* \; \sigma = \tau \; \Longleftarrow^* \eta\gamma_{w'}$.
- Conclusion:

$$v \Longrightarrow^* v' = \widehat{v'}\gamma_{v'} = \widehat{v'}\eta\eta^{-1}\gamma_{v'} \Longrightarrow^* s\gamma_{v'} \Longrightarrow^* s\eta^{-1}\sigma$$

$$=_{E \cup D}$$

$$w \Longrightarrow^* w' = \widehat{w'}\eta^{-1}\eta\gamma_{w'} = t\eta^{-1}\gamma_{w'} \Longleftarrow^* t\eta^{-1}\tau$$

Conclusion

- Comprehensive proof of Toyama's theorem
- Easy generalization to rewriting modulo
- easy extension to constructor-sharing case
- Open problem: modulo collapsing equations
- Use the proof method for similar problems:
  higher-order case
  unique normal form property