A Short Mechanized Proof of the Church–Rosser Theorem by the Z-property for the $\lambda\beta$-calculus in Nominal Isabelle[1]

Julian Nagele
Vincent van Oostrom
Christian Sternagel

University of Innsbruck

Friday, September 9th, 2016

[1] Partially supported by FWF projects P27502 and P27528

Overview

- Z
- $\lambda\beta$ nominally
- $\lambda\beta$ has Z
- Z $\Rightarrow$ Church–Rosser

Z idea (Dehornoy)

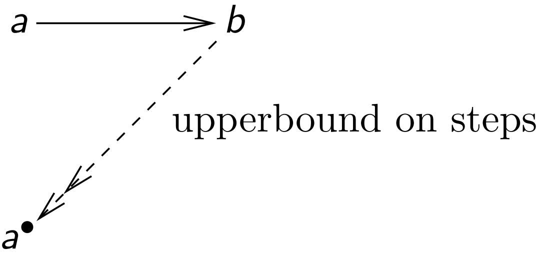
a

Z idea (Dehornoy)

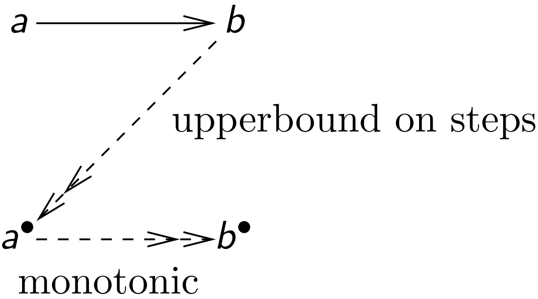
a

$a^{\bullet}$

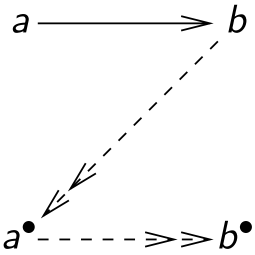
Z idea (Dehornoy)



Z idea (Dehornoy)

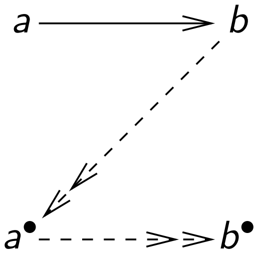


Z formally



$$\exists \bullet : A \to A, \forall a, b \in A : a \to b \;\Rightarrow\; b \twoheadrightarrow a^\bullet, a^\bullet \twoheadrightarrow b^\bullet$$

Z formally

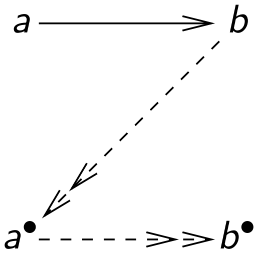


$\exists \bullet : A \to A, \forall a, b \in A : a \to b \Rightarrow b \twoheadrightarrow a^\bullet, a^\bullet \twoheadrightarrow b^\bullet$

Remark

$a \twoheadrightarrow a^\bullet$ may only fail for a isolated

Z formally

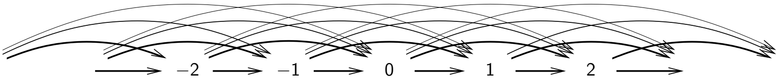


$\exists \bullet : A \to A, \forall a, b \in A : a \to b \Rightarrow b \twoheadrightarrow a^\bullet, a^\bullet \twoheadrightarrow b^\bullet$

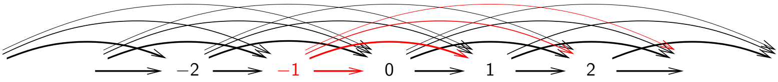
Remark

$a \twoheadrightarrow a^\bullet$ may only fail for a isolated
$a^\bullet = (a^\bullet)^\bullet$ typically fails for non-normal forms; cf. closure operator

$(\mathbb{Z}, <)$?

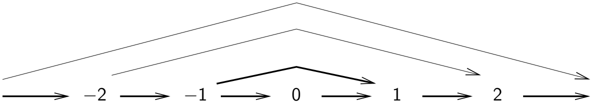


$(\mathbb{Z}, <)$ does not have Z

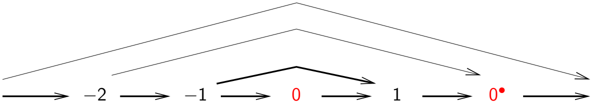


for given integer, no upperbound on steps from it

$\hat{\mathbb{Z}} = (\mathbb{Z}, \{(x, x+1), (-1-n, n+1)\})$?



$\hat{\mathbb{Z}}$ does not have Z



not monotonic (e.g. for -3)

$\mathbb{Z}^\flat = (\mathbb{Z}, \{(x, x+1)\})$?

$$\longrightarrow -2 \longrightarrow -1 \longrightarrow 0 \longrightarrow 1 \longrightarrow 2 \longrightarrow$$

$\mathbb{Z}^\flat$ does have Z

$$\longrightarrow -2 \longrightarrow -1 \longrightarrow 0 \longrightarrow 1 \longrightarrow 2 \longrightarrow$$

Z trivial ($x^\bullet = x + 1$)

λ nominally

Definition (λ-term)

nominal_datatype *term* $=$
  Var name
$|$ *App term term*
$|$ *Abs* x::*name* t::*term* **binds** x **in** t

λ nominally

Definition (λ-term)

nominal_datatype *term* =
  Var name
| *App term term*
| *Abs x::name t::term* **binds** *x* **in** *t*

Definition (substitution)

$$y\,[x := s] = (\textbf{if}\ x = y\ \textbf{then}\ s\ \textbf{else}\ y)$$
$$(t\ u)\,[x := s] = t\,[x := s]\ u\,[x := s]$$
$$y \sharp (x, s) \Longrightarrow (\lambda y.\, t)\,[x := s] = \lambda y.\, t\,[x := s]$$

λ nominally

Definition (λ-term)

nominal_datatype *term* =
  Var name
| *App term term*
| *Abs x::name t::term* **binds** *x* **in** *t*

Definition (substitution)

$$y\,[x := s] = (\textbf{if } x = y \textbf{ then } s \textbf{ else } y)$$
$$(t\ u)\,[x := s] = t\,[x := s]\ u\,[x := s]$$
$$y \sharp (x, s) \Longrightarrow (\lambda y.\, t)\,[x := s] = \lambda y.\, t\,[x := s]$$

Lemma (substitution)

$$x \sharp (y, u) \Longrightarrow t\,[x := s]\,[y := u] = t\,[y := u]\,[x := s\,[y := u]]$$

β nominally

Definition (β-reduction, compatible closure of)

$$x \sharp t \Longrightarrow (\lambda x.\, s)\ t \rightarrow_\beta s[x := t]$$

β nominally

Definition (β-reduction, compatible closure of)

$$x \sharp t \Longrightarrow (\lambda x.\, s)\ t \rightarrow_\beta s[x := t]$$

Lemma (compatibility)

$$s \rightarrow_\beta^* t \Longrightarrow u \rightarrow_\beta^* v \Longrightarrow s\ u \rightarrow_\beta^* t\ v$$
$$s \rightarrow_\beta^* t \Longrightarrow \lambda x.\, s \rightarrow_\beta^* \lambda x.\, t$$
$$s \rightarrow_\beta^* s' \Longrightarrow t \rightarrow_\beta^* t' \Longrightarrow t[x := s] \rightarrow_\beta^* t'[x := s']$$

β nominally

Definition (β-reduction, compatible closure of)

$$x \sharp t \Longrightarrow (\lambda x.\, s)\ t \to_\beta s[x := t]$$

Lemma (compatibility)

$$s \to_\beta^* t \Longrightarrow u \to_\beta^* v \Longrightarrow s\ u \to_\beta^* t\ v$$
$$s \to_\beta^* t \Longrightarrow \lambda x.\, s \to_\beta^* \lambda x.\, t$$
$$s \to_\beta^* s' \Longrightarrow t \to_\beta^* t' \Longrightarrow t[x := s] \to_\beta^* t'[x := s']$$

Lemma (coherence)

$$\lambda x.\, s \to_\beta^* t \Longrightarrow \exists\, u.\ t = \lambda x.\, u \wedge s \to_\beta^* u$$

$\lambda\beta$ has Z

Definition (head-application)

$$x \sharp u \implies (\lambda x.\, s') \cdot_\beta u = s'[x := u]$$
$$x \cdot_\beta u = x\ u$$
$$(s\ t) \cdot_\beta u = s\ t\ u$$

$\lambda\beta$ has Z

Definition (head-application)

$$
\begin{aligned}
&x \sharp u \Longrightarrow (\lambda x.\, s') \cdot_\beta u = s'[x := u] \\
&x \cdot_\beta u = x\ u \\
&(s\ t) \cdot_\beta u = s\ t\ u
\end{aligned}
$$

Definition (full-superdevelopment)

$$
\begin{aligned}
&x^\bullet = x \\
&(\lambda x.\, t)^\bullet = \lambda x.\, t^\bullet \\
&(s\ t)^\bullet = s^\bullet \cdot_\beta t^\bullet
\end{aligned}
$$

$\lambda\beta$ has Z

Definition (head-application)

$$x \sharp u \Longrightarrow (\lambda x.\, s') \cdot_\beta u = s'[x := u]$$
$$x \cdot_\beta u = x\ u$$
$$(s\ t) \cdot_\beta u = s\ t\ u$$

Definition (full-superdevelopment)

$$x^\bullet = x$$
$$(\lambda x.\, t)^\bullet = \lambda x.\, t^\bullet$$
$$(s\ t)^\bullet = s^\bullet \cdot_\beta t^\bullet$$

Example

- $I^\bullet = I$; $(I = \lambda x.x)$
- $(I(II))^\bullet = I$, $(III)^\bullet = I$;
- $((\lambda x.xx)I)^\bullet = II$;

$\lambda\beta$ has Z proof steps

Lemma (Self)

$$t \to_\beta^* t^\bullet$$

$\lambda\beta$ has Z proof steps

Lemma (Self)

$$t \to_\beta^* t^\bullet$$

Lemma (Rhs)

$$t^\bullet[x := s^\bullet] \to_\beta^* t[x := s]^\bullet$$

$\lambda\beta$ has Z proof steps

Lemma (Self)

$$t \to_\beta^* t^\bullet$$

Lemma (Rhs)

$$t^\bullet [x := s^\bullet] \to_\beta^* t[x := s]^\bullet$$

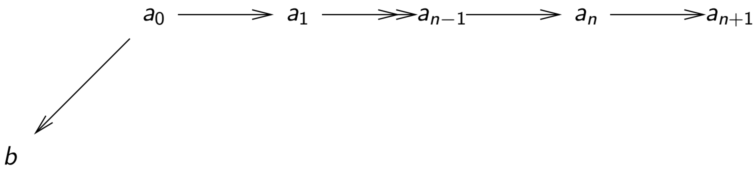
Lemma (Z)

$$s \to_\beta t \Longrightarrow t \to_\beta^* s^\bullet \wedge s^\bullet \to_\beta^* t^\bullet$$

Z ⇒ Church–Rosser

Proof.

using semi-confluence ⇒ confluence

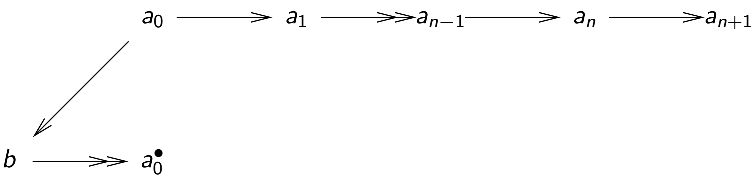


□

Z $\Rightarrow$ Church–Rosser

Proof.

using semi-confluence $\Rightarrow$ confluence

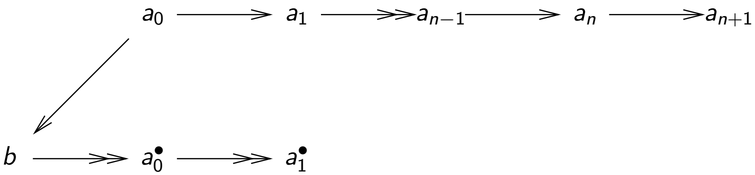


$\square$

Z $\Rightarrow$ Church–Rosser

Proof.

using semi-confluence $\Rightarrow$ confluence

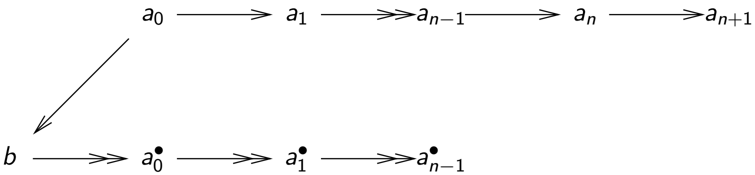


□

Z ⇒ Church–Rosser

Proof.

using semi-confluence ⇒ confluence

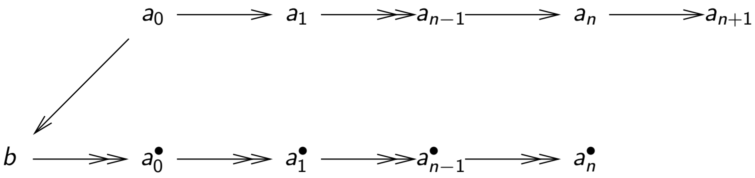


□

Z $\Rightarrow$ Church–Rosser

Proof.

using semi-confluence $\Rightarrow$ confluence

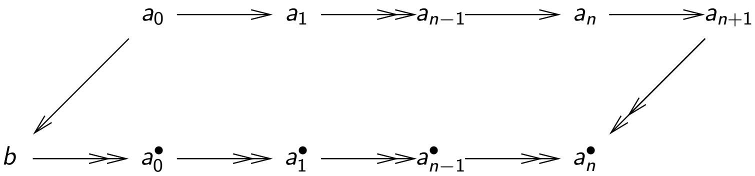


□

Z $\Rightarrow$ Church–Rosser

Proof.

using semi-confluence $\Rightarrow$ confluence



Church–Rosser methods for $\lambda\beta$

- Dehornoy–vO: full-(super)developments $\models$ Z
  compute monotonic upperbound term from term

Church–Rosser methods for $\lambda\beta$

- Dehornoy–vO: full-(super)developments $\models$ Z
  compute monotonic upperbound term from term
- Tait–Martin-Löf: complete developments $\models \diamond$
  compute cofinal complete developments from coinitial ones

Church–Rosser methods for $\lambda\beta$

- Dehornoy–vO: full-(super)developments $\models$ Z
  compute monotonic upperbound term from term
- Tait–Martin-Löf: complete developments $\models \diamond$
  compute cofinal complete developments from coinitial ones
- Takahashi: complete, full-developments $\models \angle$
  compute complete development to monotonic upperbound
  from complete development

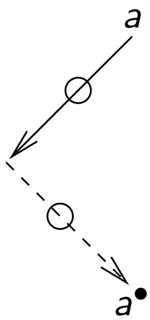
Church–Rosser methods for $\lambda\beta$

- Dehornoy–vO: full-(super)developments $\models$ Z
  compute monotonic upperbound term from term
- Tait–Martin-Löf: complete developments $\models \diamond$
  compute cofinal complete developments from coinitial ones
- Takahashi: complete, full-developments $\models \angle$
  compute complete development to monotonic upperbound from complete development

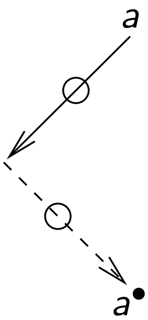
Remark

complete development additional notion of reduction?

Takahashi's ∠

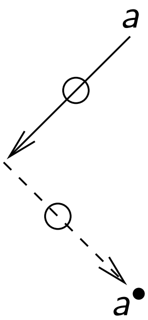


Takahashi's $\angle$



$$\exists \multimap\!\!\to, \bullet : \to \subseteq \multimap\!\!\to \subseteq \twoheadrightarrow \;\&\; \forall a, b \in A : a \multimap\!\!\to b \;\Rightarrow\; b \multimap\!\!\to a^\bullet$$

Takahashi's $\angle$

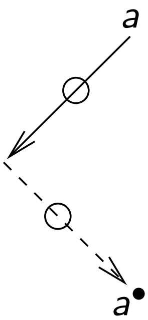


$\exists \multimap\!\to, \bullet : \to \subseteq \multimap\!\to \subseteq \twoheadrightarrow$ & $\forall a, b \in A : a \multimap\!\to b \Rightarrow b \multimap\!\to a^\bullet$

Lemma

$\angle \implies \diamond$

Takahashi's $\angle$



$\exists \mathrel{\circ\!\!\!\rightarrow}, \bullet : \rightarrow \subseteq \mathrel{\circ\!\!\!\rightarrow} \subseteq \twoheadrightarrow \;\&\; \forall a, b \in A : a \mathrel{\circ\!\!\!\rightarrow} b \;\Rightarrow\; b \mathrel{\circ\!\!\!\rightarrow} a^{\bullet}$

Lemma

$\angle \implies \diamond$

Example

$(\mathbb{Z}, <) \models \diamond$ but $\not\models \angle$

Z $\Leftrightarrow$ $\angle$

Theorem

for any map $\bullet$, $Z \Leftrightarrow \angle$

Proof.

$\square$

$Z \Leftrightarrow \angle$

Theorem
for any map $\bullet$, $Z \Leftrightarrow \angle$

Proof.
(if)

$$a \longrightarrow b$$

$\square$

$Z \Leftrightarrow \angle$

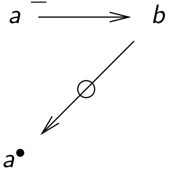
Theorem

for any map $\bullet$, $Z \Leftrightarrow \angle$

Proof.

(if)

$$\rightarrow \subseteq \multimap\!\!\rightarrow \text{ and } \angle$$



$\square$

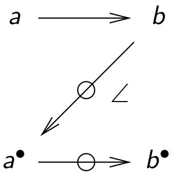
$Z \Leftrightarrow \angle$

Theorem

for any map $\bullet$, $Z \Leftrightarrow \angle$

Proof.

(if)



□

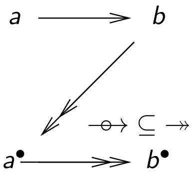
$Z \Leftrightarrow \angle$

Theorem

for any map $\bullet$, $Z \Leftrightarrow \angle$

Proof.

(if)



□

Z $\Leftrightarrow$ $\angle$

Theorem

for any map $\bullet$, $Z \Leftrightarrow \angle$

Proof.

(only if)

Definition

$a \multimap\!\!\rightarrow b$ if b between a and $a^\bullet$ i.e. if $a \twoheadrightarrow b \twoheadrightarrow a^\bullet$

Z $\Leftrightarrow$ $\angle$

Theorem

for any map $\bullet$, $Z \Leftrightarrow \angle$

Proof.

(only if)

Definition

$a \mathrel{\multimap\!\!\!\rightarrow} b$ if b between a and $a^\bullet$ i.e. if $a \twoheadrightarrow b \twoheadrightarrow a^\bullet$

- $a \rightarrow b \overset{upperbound}{\Rightarrow} b \twoheadrightarrow a^\bullet \Rightarrow \rightarrow \subseteq \mathrel{\multimap\!\!\!\rightarrow}$

Z $\Leftrightarrow$ $\angle$

Theorem

for any map $\bullet$, $Z \Leftrightarrow \angle$

Proof.

(only if)

Definition

$a \multimap b$ if b between a and $a^\bullet$ i.e. if $a \twoheadrightarrow b \twoheadrightarrow a^\bullet$

- $a \rightarrow b \overset{\text{upperbound}}{\Rightarrow} b \twoheadrightarrow a^\bullet \Rightarrow \rightarrow \subseteq \multimap$
- $a \multimap b \overset{\text{definition}}{\Rightarrow} a \twoheadrightarrow b \Rightarrow \multimap \subseteq \twoheadrightarrow$

$Z \Leftrightarrow \angle$

Theorem

for any map $\bullet$, $Z \Leftrightarrow \angle$

Proof.

(only if)

Definition

$a \circ\!\!\rightarrow b$ if b between a and $a^\bullet$ i.e. if $a \twoheadrightarrow b \twoheadrightarrow a^\bullet$

- $a \rightarrow b \overset{upperbound}{\Rightarrow} b \twoheadrightarrow a^\bullet \Rightarrow \rightarrow \subseteq \circ\!\!\rightarrow$
- $a \circ\!\!\rightarrow b \overset{definition}{\Rightarrow} a \twoheadrightarrow b \Rightarrow \circ\!\!\rightarrow \subseteq \twoheadrightarrow$
- Suppose $a \circ\!\!\rightarrow b$

$Z \Leftrightarrow \angle$

Theorem
for any map $\bullet$, $Z \Leftrightarrow \angle$

Proof.
(only if)

Definition
$a \twoheadrightarrow\!\!\!\!\!\circ\; b$ if b between a and $a^\bullet$ i.e. if $a \twoheadrightarrow b \twoheadrightarrow a^\bullet$

- $a \rightarrow b \overset{upperbound}{\Rightarrow} b \twoheadrightarrow a^\bullet \Rightarrow \rightarrow \subseteq \twoheadrightarrow\!\!\!\!\!\circ$
- $a \twoheadrightarrow\!\!\!\!\!\circ\; b \overset{definition}{\Rightarrow} a \twoheadrightarrow b \Rightarrow \twoheadrightarrow\!\!\!\!\!\circ \subseteq \twoheadrightarrow$
- Suppose $a \twoheadrightarrow\!\!\!\!\!\circ\; b$
  - $a \twoheadrightarrow\!\!\!\!\!\circ\; b \overset{definition}{\Rightarrow} a \twoheadrightarrow b \twoheadrightarrow a^\bullet \Rightarrow$

$Z \Leftrightarrow \angle$

Theorem

for any map $\bullet$, $Z \Leftrightarrow \angle$

Proof.

(only if)

Definition

$a \multimap b$ if b between a and $a^\bullet$ i.e. if $a \twoheadrightarrow b \twoheadrightarrow a^\bullet$

- $a \to b \overset{upperbound}{\Rightarrow} b \twoheadrightarrow a^\bullet \Rightarrow \to \subseteq \multimap$
- $a \multimap b \overset{definition}{\Rightarrow} a \twoheadrightarrow b \Rightarrow \multimap \subseteq \twoheadrightarrow$
- Suppose $a \multimap b$
    - $a \multimap b \overset{definition}{\Rightarrow} a \twoheadrightarrow b \twoheadrightarrow a^\bullet \Rightarrow$
    - $a \twoheadrightarrow b \overset{monotonic}{\Rightarrow} a^\bullet \twoheadrightarrow b^\bullet \Rightarrow$

$Z \Leftrightarrow \angle$

Theorem

for any map $\bullet$, $Z \Leftrightarrow \angle$

Proof.

(only if)

Definition

$a \multimap b$ if b between a and $a^\bullet$ i.e. if $a \twoheadrightarrow b \twoheadrightarrow a^\bullet$

- $a \rightarrow b \overset{upperbound}{\Rightarrow} b \twoheadrightarrow a^\bullet \Rightarrow \rightarrow \subseteq \multimap$
- $a \multimap b \overset{definition}{\Rightarrow} a \twoheadrightarrow b \Rightarrow \multimap \subseteq \twoheadrightarrow$
- Suppose $a \multimap b$
  - $a \multimap b \overset{definition}{\Rightarrow} a \twoheadrightarrow b \twoheadrightarrow a^\bullet \Rightarrow$
  - $a \twoheadrightarrow b \overset{monotonic}{\Rightarrow} a^\bullet \twoheadrightarrow b^\bullet \Rightarrow$
  - $b \twoheadrightarrow a^\bullet \twoheadrightarrow b^\bullet \overset{definition}{\Rightarrow} b \multimap a^\bullet$

□

Syntax-free developments

Definition

a $\bullet$-develops to b, $a \multimap\!\!\!\rightarrow b$, if $a \twoheadrightarrow b \twoheadrightarrow a^\bullet$
i.e. if b between a and $a^\bullet$

Syntax-free developments

Definition

a $\bullet$-develops to b, $a \multimap\!\!\!\rightarrow b$, if $a \twoheadrightarrow b \twoheadrightarrow a^\bullet$
i.e. if b between a and $a^\bullet$

Theorem

$\bullet$-development coincides with partial development for orthogonal TRSs that are terminating, non-erasing and non-collapsing

Syntax-free developments

Definition

a $\bullet$-develops to b, $a \multimap\!\!\to b$, if $a \twoheadrightarrow b \twoheadrightarrow a^\bullet$
i.e. if b between a and $a^\bullet$

Theorem

$\bullet$-development coincides with partial development for orthogonal TRSs that are terminating, non-erasing and non-collapsing

Example

Let $\bullet$ be full-development map (contract all redexes in term)

Syntax-free developments

Definition

a $\bullet$-develops to b, $a \multimap\!\!\!\rightarrow b$, if $a \twoheadrightarrow b \twoheadrightarrow a^\bullet$
i.e. if b between a and $a^\bullet$

Theorem

$\bullet$-development coincides with partial development for orthogonal TRSs that are terminating, non-erasing and non-collapsing

Example

Let $\bullet$ be full-development map (contract all redexes in term)

- rules $a \to b \to c \to a$; non-terminating
  a $\bullet$-develops to c; $a^\bullet = b$
- rules $a \to b \to c$, $f(x) \to d$; erasing
  $f(a)$ $\bullet$-develops to $f(c)$; $f(a)^\bullet = d$
- rules $g(x) \to h(x) \to i(x) \to x$; collapsing
  $i(h(g(a)))$ $\bullet$-develops to $i(h(i(a)))$; $i(h(g(a)))^\bullet = i(h(a))$

Conclusion

- formalised proof that is short
  (300 lines $\supseteq$ 60 lines of methods (Eisbach));

Conclusion

- formalised proof that is short
  (300 lines $\supseteq$ 60 lines of methods (Eisbach));
- Isabelle proofs follow proof-by-hand closely
  (discharging nominal instead of Variable Convention);

Conclusion

- formalised proof that is short
  (300 lines $\supseteq$ 60 lines of methods (Eisbach));
- Isabelle proofs follow proof-by-hand closely
  (discharging nominal instead of Variable Convention);
- 1 mistake found in proof-by-hand
  (uniformity w.r.t. ordinary developments);

Conclusion

- formalised proof that is short
  (300 lines $\supseteq$ 60 lines of methods (Eisbach));
- Isabelle proofs follow proof-by-hand closely
  (discharging nominal instead of Variable Convention);
- 1 mistake found in proof-by-hand
  (uniformity w.r.t. ordinary developments);
- in AFP; also there: Combinatory Logic has Z (Felgenhauer)
  shared abstract part;

Conclusion

- formalised proof that is short
  (300 lines $\supseteq$ 60 lines of methods (Eisbach));
- Isabelle proofs follow proof-by-hand closely
  (discharging nominal instead of Variable Convention);
- 1 mistake found in proof-by-hand
  (uniformity w.r.t. ordinary developments);
- in AFP; also there: Combinatory Logic has Z (Felgenhauer)
  shared abstract part;
- Z works for many systems:
  (weakly) orthogonal (same proof steps); λ-calculus with
  explicit substitutions self-distributivity (Dehornoy), braids,
  associativity
  terminating systems (normal form)

Conclusion

- formalised proof that is short
  (300 lines $\supseteq$ 60 lines of methods (Eisbach));
- Isabelle proofs follow proof-by-hand closely
  (discharging nominal instead of Variable Convention);
- 1 mistake found in proof-by-hand
  (uniformity w.r.t. ordinary developments);
- in AFP; also there: Combinatory Logic has Z (Felgenhauer)
  shared abstract part;
- Z works for many systems:
  (weakly) orthogonal (same proof steps); λ-calculus with
  explicit substitutions self-distributivity (Dehornoy), braids,
  associativity
  terminating systems (normal form)
- automation (search for monotonic upperbound functions)?

Example: self-distributivity

Definition

Self-distributivity, rewrite relation generated by $xyz \to xz(yz)$

Example: self-distributivity

Definition

Self-distributivity, rewrite relation generated by $xyz \to xz(yz)$

Some models:

- ACI operations
- take middle of points in space
- substitution lemma

Example: self-distributivity

Definition

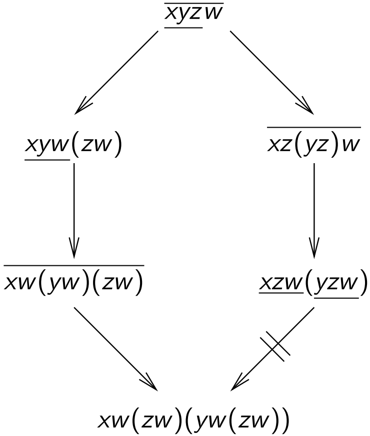
Self-distributivity, rewrite relation generated by $xyz \to xz(yz)$

Some models:

- ACI operations
- take middle of points in space
- substitution lemma

All confluence-proof-tools fail (15-3-2016)

Example: self-distributivity



In depth: Braids and Self-distributivity (Dehornoy 2000)

Example: self-distributivity

Theorem

Self-distributivity has the Z-property, for $\bullet$ full distribution:

$$x^\bullet = x \qquad (ts)^\bullet = t^\bullet[s^\bullet]$$

with $t[s]$ uniform distribution of s over t:

$$t[x_1{:=}x_1 s, x_2{:=}x_2 s, \ldots]$$

Example: self-distributivity

Theorem

Self-distributivity has the Z-property, for $\bullet$ full distribution:

$$x^\bullet = x \qquad (ts)^\bullet = t^\bullet[s^\bullet]$$

with $t[s]$ uniform distribution of s over t:

$$t[x_1{:=}x_1 s, x_2{:=}x_2 s, \ldots]$$

Example

- $(xy)^\bullet = x[y] = x[x{:=}xy] = xy$;
- $(xyz)^\bullet = (xy)[x{:=}xz, y{:=}yz] = xz(yz)$.

Proof.

Example: self-distributivity

Theorem

Self-distributivity has the Z-property, for $\bullet$ *full distribution:*

$$x^\bullet = x \qquad (ts)^\bullet = t^\bullet[s^\bullet]$$

with $t[s]$ *uniform distribution of* s *over* t*:*

$$t[x_1{:=}x_1 s, x_2{:=}x_2 s, \ldots]$$

Proof.

By induction on t:

□

Example: self-distributivity

Theorem

Self-distributivity has the Z-property, for $\bullet$ *full distribution:*

$$x^\bullet = x \qquad (ts)^\bullet = t^\bullet[s^\bullet]$$

with $t[s]$ *uniform distribution of* s *over* t*:*

$$t[x_1{:=}x_1 s, x_2{:=}x_2 s, \ldots]$$

Proof.

By induction on t:

- (Sequentialisation) $\quad ts \twoheadrightarrow t[s]$;

□

Example: self-distributivity

Theorem

Self-distributivity has the Z-property, for $\bullet$ full distribution:

$$x^\bullet = x \qquad (ts)^\bullet = t^\bullet[s^\bullet]$$

with $t[s]$ uniform distribution of s over t:

$$t[x_1{:=}x_1 s, x_2{:=}x_2 s, \ldots]$$

Proof.

By induction on t:

- (Sequentialisation) $\quad ts \twoheadrightarrow t[s]$;
- (Substitution) $\quad t[s][r] \twoheadrightarrow t[r][s[r]]$

□

Example: self-distributivity

Theorem

Self-distributivity has the Z-property, for $\bullet$ full distribution:

$$x^\bullet = x \qquad (ts)^\bullet = t^\bullet[s^\bullet]$$

with $t[s]$ uniform distribution of s over t:

$$t[x_1{:=}x_1 s, x_2{:=}x_2 s, \ldots]$$

Proof.

By induction on t:

- (Sequentialisation) $ts \twoheadrightarrow t[s]$;
- (Substitution) $t[s][r] \twoheadrightarrow t[r][s[r]]$
- (Self) $t \twoheadrightarrow t^\bullet$;

□

Example: self-distributivity

Theorem

Self-distributivity has the Z-property, for $\bullet$ full distribution:

$$x^\bullet = x \qquad (ts)^\bullet = t^\bullet[s^\bullet]$$

with $t[s]$ uniform distribution of s over t:

$$t[x_1{:=}x_1 s, x_2{:=}x_2 s, \ldots]$$

Proof.

By induction on t:

- (Sequentialisation) $ts \twoheadrightarrow t[s]$;
- (Substitution) $t[s][r] \twoheadrightarrow t[r][s[r]]$
- (Self) $t \twoheadrightarrow t^\bullet$;
- (Z) $s \twoheadrightarrow t^\bullet \twoheadrightarrow s^\bullet$, if $t \to s$.

□