Second-order Church-Rosser Modulo, Without Normalization

Thiago Felicissimo

IWC 2024

July 9

A motivating example from dependent type theory

In dependent type theory, we can consider type of lists of length n:

$$l : \mathrm{List}(n)$$

A motivating example from dependent type theory

In dependent type theory, we can consider type of lists of length n:

$$l : \mathsf{List}(n)$$

If we add an operation for append $+\!+$, we might want to prove the proposition

$$\mathsf{isPermutation}(l_1 +\!+ l_2, l_2 +\!+ l_1)$$

for all $l_1 : \mathsf{List}(n_1)$ and $l_2 : \mathsf{List}(n_2)$

A motivating example from dependent type theory

In dependent type theory, we can consider type of lists of length n:

$$l : \mathsf{List}(n)$$

If we add an operation for append $+\!+$, we might want to prove the proposition

$$\mathsf{isPermutation}(l_1 +\!+ l_2, l_2 +\!+ l_1)$$

for all $l_1 : \mathsf{List}(n_1)$ and $l_2 : \mathsf{List}(n_2)$

Problem We have

$$l_1 +\!+ l_2 : \mathsf{List}(n_1 + n_2) \qquad \text{and} \qquad l_2 +\!+ l_1 : \mathsf{List}(n_2 + n_1)$$

but the types $\mathsf{List}(n_2 + n_1)$ and $\mathsf{List}(n_1 + n_2)$ are *not* convertible

A motivating example from dependent type theory

In dependent type theory, we can consider type of lists of length n:

$$l : \mathsf{List}(n)$$

If we add an operation for append $++$, we might want to prove the proposition

$$\mathsf{isPermutation}(l_1 ++ l_2, l_2 ++ l_1)$$

for all $l_1 : \mathsf{List}(n_1)$ and $l_2 : \mathsf{List}(n_2)$

Problem We have

$$l_1 ++ l_2 : \mathsf{List}(n_1 + n_2) \qquad \text{and} \qquad l_2 ++ l_1 : \mathsf{List}(n_2 + n_1)$$

but the types $\mathsf{List}(n_2 + n_1)$ and $\mathsf{List}(n_1 + n_2)$ are *not* convertible

Consequence The proposition $\mathsf{isPermutation}(l_1 ++ l_2, l_2 ++ l_1)$ is ill-typed

In search of a solution

The standard solution $\mathrm{List}(n_2 + n_1)$ and $\mathrm{List}(n_1 + n_2)$ are not convertible

In search of a solution

The standard solution $\mathrm{List}(n_2 + n_1)$ and $\mathrm{List}(n_1 + n_2)$ are not convertible

But we have a *proof* p that they are *equal*

In search of a solution

The standard solution $\mathrm{List}(n_2 + n_1)$ and $\mathrm{List}(n_1 + n_2)$ are not convertible

But we have a *proof* p that they are *equal*

In type theory, we can cast $l_2 \mathbin{++} l_1 : \mathrm{List}(n_2 + n_1)$ using the proof p to obtain

$$\mathrm{cast}(p, l_2 \mathbin{++} l_1) : \mathrm{List}(n_1 + n_2)$$

In search of a solution

The standard solution $\mathrm{List}(n_2 + n_1)$ and $\mathrm{List}(n_1 + n_2)$ are not convertible

But we have a *proof* p that they are *equal*

In type theory, we can cast $l_2 \mathbin{+\!\!+} l_1 : \mathrm{List}(n_2 + n_1)$ using the proof p to obtain

$$\mathrm{cast}(p, l_2 \mathbin{+\!\!+} l_1) : \mathrm{List}(n_1 + n_2)$$

Now the proposition

$$\mathrm{isPermutation}(l_1 \mathbin{+\!\!+} l_2, \mathrm{cast}(p, l_2 \mathbin{+\!\!+} l_1))$$

is well-typed, and has a proof

In search of a solution

The standard solution $\text{List}(n_2 + n_1)$ and $\text{List}(n_1 + n_2)$ are not convertible

But we have a *proof* p that they are *equal*

In type theory, we can cast $l_2 \mathbin{++} l_1 : \text{List}(n_2 + n_1)$ using the proof p to obtain

$$\text{cast}(p, l_2 \mathbin{++} l_1) : \text{List}(n_1 + n_2)$$

Now the proposition

$$\text{isPermutation}(l_1 \mathbin{++} l_2, \text{cast}(p, l_2 \mathbin{++} l_1))$$

is well-typed, and has a proof

Problem Putting cast everywhere becomes unfeasable

Known in the type theory community as *transport hell* (transport = cast)

In search of a solution

The standard solution $\mathsf{List}(n_2 + n_1)$ and $\mathsf{List}(n_1 + n_2)$ are not convertible

But we have a *proof* p that they are *equal*

In type theory, we can cast $l_2 +\!\!+\ l_1 : \mathsf{List}(n_2 + n_1)$ using the proof p to obtain

$$\mathsf{cast}(p, l_2 +\!\!+\ l_1) : \mathsf{List}(n_1 + n_2)$$

Now the proposition

$$\mathsf{isPermutation}(l_1 +\!\!+\ l_2, \mathsf{cast}(p, l_2 +\!\!+\ l_1))$$

is well-typed, and has a proof

Problem Putting cast everywhere becomes unfeasable

Known in the type theory community as *transport hell* (transport = cast)

A better solution Make $n_2 + n_1$ and $n_1 + n_2$ convertible

So that $\mathsf{isPermutation}(l_1 +\!\!+\ l_2, l_2 +\!\!+\ l_1)$ is well-typed

Equational theory of a type theory with AC addition

The equational theory of our dependent type theory should have:

Equational theory of a type theory with AC addition

The equational theory of our dependent type theory should have:

- Associative-commutative (AC) addition

$$\mathtt{t} + 0 \approx \mathtt{t} \qquad \mathtt{t} + S(\mathtt{u}) \approx S(\mathtt{t} + \mathtt{u})$$

$$\mathtt{t} + \mathtt{u} \approx \mathtt{u} + \mathtt{t} \qquad (\mathtt{t} + \mathtt{u}) + \mathtt{v} \approx \mathtt{t} + (\mathtt{u} + \mathtt{v})$$

Equational theory of a type theory with AC addition

The equational theory of our dependent type theory should have:

- Associative-commutative (AC) addition

$$\mathtt{t} + 0 \approx \mathtt{t} \qquad \mathtt{t} + S(\mathtt{u}) \approx S(\mathtt{t} + \mathtt{u})$$

$$\mathtt{t} + \mathtt{u} \approx \mathtt{u} + \mathtt{t} \qquad (\mathtt{t} + \mathtt{u}) + \mathtt{v} \approx \mathtt{t} + (\mathtt{u} + \mathtt{v})$$

- β-conversion

$$@(\lambda(x.\mathtt{t}\{x\}), \mathtt{u}) \approx \mathtt{t}\{\mathtt{u}\}$$

Equational theory of a type theory with AC addition

The equational theory of our dependent type theory should have:

- Associative-commutative (AC) addition

$$\mathsf{t} + 0 \approx \mathsf{t} \qquad \mathsf{t} + S(\mathsf{u}) \approx S(\mathsf{t} + \mathsf{u})$$

$$\mathsf{t} + \mathsf{u} \approx \mathsf{u} + \mathsf{t} \qquad (\mathsf{t} + \mathsf{u}) + \mathsf{v} \approx \mathsf{t} + (\mathsf{u} + \mathsf{v})$$

- β-conversion

$$@(\lambda(x.\mathsf{t}\{x\}), \mathsf{u}) \approx \mathsf{t}\{\mathsf{u}\}$$

- Induction/recursion over natural numbers (think of Gödel's System T)

$$\mathbb{N}_{\mathsf{rec}}(0, \mathsf{p}, xy.\mathsf{q}\{x, y\}) \approx \mathsf{p}$$

$$\mathbb{N}_{\mathsf{rec}}(S(\mathsf{n}), \mathsf{p}, xy.\mathsf{q}\{x, y\}) \approx \mathsf{q}\{\mathsf{n}, \mathbb{N}_{\mathsf{rec}}(\mathsf{n}, \mathsf{p}, xy.\mathsf{q}\{x, y\})\}$$

Equational theory of a type theory with AC addition

The equational theory of our dependent type theory should have:

- Associative-commutative (AC) addition

$$\mathsf{t} + 0 \approx \mathsf{t} \qquad \mathsf{t} + S(\mathsf{u}) \approx S(\mathsf{t} + \mathsf{u})$$

$$\mathsf{t} + \mathsf{u} \approx \mathsf{u} + \mathsf{t} \qquad (\mathsf{t} + \mathsf{u}) + \mathsf{v} \approx \mathsf{t} + (\mathsf{u} + \mathsf{v})$$

- β-conversion

$$@(\lambda(x.\mathsf{t}\{x\}), \mathsf{u}) \approx \mathsf{t}\{\mathsf{u}\}$$

- Induction/recursion over natural numbers (think of Gödel's System T)

$$\mathbb{N}_{\mathsf{rec}}(0, \mathsf{p}, xy.\mathsf{q}\{x, y\}) \approx \mathsf{p}$$

$$\mathbb{N}_{\mathsf{rec}}(S(\mathsf{n}), \mathsf{p}, xy.\mathsf{q}\{x, y\}) \approx \mathsf{q}\{\mathsf{n}, \mathbb{N}_{\mathsf{rec}}(\mathsf{n}, \mathsf{p}, xy.\mathsf{q}\{x, y\})\}$$

Goal Church-Rosser rewrite system for the above (second-order) equational theory which can be shown terminating over typed terms

Rewriting modulo

Cannot orient $t + u \approx u + t$ in a terminating way

1

Rewriting modulo

Cannot orient $t + u \approx u + t$ in a terminating way

We must instead consider *rewriting modulo*, where we have:

1

Rewriting modulo

Cannot orient $\mathtt{t} + \mathtt{u} \approx \mathtt{u} + \mathtt{t}$ in a terminating way

We must instead consider *rewriting modulo*, where we have:

- Rewrite rules $l \longmapsto r \in \mathcal{R}$, defining rewrite relation $\longrightarrow$

1

Rewriting modulo

Cannot orient $\mathtt{t} + \mathtt{u} \approx \mathtt{u} + \mathtt{t}$ in a terminating way

We must instead consider *rewriting modulo*, where we have:

- Rewrite rules $l \longmapsto r \in \mathcal{R}$, defining rewrite relation $\longrightarrow$
- Undirected equations $t \approx u \in \mathcal{E}$, defining congruence $\simeq$

1

Rewriting modulo

Cannot orient $\mathtt{t} + \mathtt{u} \approx \mathtt{u} + \mathtt{t}$ in a terminating way

We must instead consider *rewriting modulo*, where we have:

- Rewrite rules $l \longmapsto r \in \mathcal{R}$, defining rewrite relation $\longrightarrow$
- Undirected equations $t \approx u \in \mathcal{E}$, defining congruence $\simeq$

In this setting, we now want to show *Church-Rosser modulo* (or CR modulo):

$$t \equiv u \qquad \text{implies} \qquad t \overset{\sim}{\longrightarrow}{}^{*} \circ \simeq \circ {}^{*}\overset{\sim}{\longleftarrow} u$$

where $\equiv$ is $(\longrightarrow \cup \longleftarrow \cup \simeq)^{*}$ and

1

Rewriting modulo

Cannot orient $\mathtt{t} + \mathtt{u} \approx \mathtt{u} + \mathtt{t}$ in a terminating way

We must instead consider *rewriting modulo*, where we have:

- Rewrite rules $l \longmapsto r \in \mathcal{R}$, defining rewrite relation $\longrightarrow$
- Undirected equations $t \approx u \in \mathcal{E}$, defining congruence $\simeq$

In this setting, we now want to show *Church-Rosser modulo* (or CR modulo):

$$t \equiv u \qquad \text{implies} \qquad t \overset{\sim}{\longrightarrow}{}^{*} \circ \simeq \circ {}^{*}\overset{\sim}{\longleftarrow} u$$

where $\equiv$ is $(\longrightarrow \cup \longleftarrow \cup \simeq)^{*}$ and

- Strong[1] CR modulo: $\overset{\sim}{\longrightarrow}$ is $\longrightarrow$ (Huet)

[1]This terminology is non-standard, but I don't know if there is a standard one.

Rewriting modulo

Cannot orient $\mathtt{t} + \mathtt{u} \approx \mathtt{u} + \mathtt{t}$ in a terminating way

We must instead consider *rewriting modulo*, where we have:

- Rewrite rules $l \longmapsto r \in \mathcal{R}$, defining rewrite relation $\longrightarrow$
- Undirected equations $t \approx u \in \mathcal{E}$, defining congruence $\simeq$

In this setting, we now want to show *Church-Rosser modulo* (or CR modulo):

$$t \equiv u \qquad \text{implies} \qquad t \overset{\sim}{\longrightarrow}{}^* \circ \simeq \circ {}^*\overset{\sim}{\longleftarrow} u$$

where $\equiv$ is $(\longrightarrow \cup \longleftarrow \cup \simeq)^*$ and

- Strong[1] CR modulo: $\overset{\sim}{\longrightarrow}$ is $\longrightarrow$ (Huet)
- Weak CR modulo: $\overset{\sim}{\longrightarrow}$ between $\longrightarrow$ and $\simeq \circ \longrightarrow$ (Stickel, Jouannaud)
  Needed when $\simeq$ can block $\longrightarrow$, implementation usually requires *matching modulo* $\mathcal{E}$

[1]This terminology is non-standard, but I don't know if there is a standard one.

This work

Problem Most criteria in the literature for CR modulo rely on termination

This work

Problem Most criteria in the literature for CR modulo rely on termination

But in type theory, we often show CR over untyped terms, β non-terminating

And we can use rewrite rules without proving termination (eg like in Agda or Coq)

But CR modulo needed for subject reduction, which is needed for soundness of type-checking

This work

Problem Most criteria in the literature for CR modulo rely on termination

But in type theory, we often show CR over untyped terms, β non-terminating

And we can use rewrite rules without proving termination (eg like in AGDA or COQ)

But CR modulo needed for subject reduction, which is needed for soundness of type-checking

Worse, second- and higher-order criteria for CR modulo are even rarer

This work

Problem Most criteria in the literature for CR modulo rely on termination

But in type theory, we often show CR over untyped terms, β non-terminating
And we can use rewrite rules without proving termination (eg like in Agda or Coq)
But CR modulo needed for subject reduction, which is needed for soundness of type-checking

Worse, second- and higher-order criteria for CR modulo are even rarer

This work We investigate criteria for 2nd order CR modulo that *do not* rely on termination:

This work

Problem Most criteria in the literature for CR modulo rely on termination

But in type theory, we often show CR over untyped terms, β non-terminating

And we can use rewrite rules without proving termination (eg like in Agda or Coq)

But CR modulo needed for subject reduction, which is needed for soundness of type-checking

Worse, second- and higher-order criteria for CR modulo are even rarer

This work We investigate criteria for 2nd order CR modulo that *do not* rely on termination:

- **Criterion 1** Proves weak CR modulo, but avoids the use of matching modulo

This work

Problem Most criteria in the literature for CR modulo rely on termination

But in type theory, we often show CR over untyped terms, β non-terminating

And we can use rewrite rules without proving termination (eg like in Agda or Coq)

But CR modulo needed for subject reduction, which is needed for soundness of type-checking

Worse, second- and higher-order criteria for CR modulo are even rarer

This work We investigate criteria for 2nd order CR modulo that *do not* rely on termination:

- **Criterion 1** Proves weak CR modulo, but avoids the use of matching modulo
- **Criterion 2** Proves strong CR modulo, easy consequence of known results

This work

Problem Most criteria in the literature for CR modulo rely on termination

But in type theory, we often show CR over untyped terms, β non-terminating

And we can use rewrite rules without proving termination (eg like in Agda or Coq)

But CR modulo needed for subject reduction, which is needed for soundness of type-checking

Worse, second- and higher-order criteria for CR modulo are even rarer

This work We investigate criteria for 2nd order CR modulo that *do not* rely on termination:

- **Criterion 1** Proves weak CR modulo, but avoids the use of matching modulo
- **Criterion 2** Proves strong CR modulo, easy consequence of known results

Each criterion proves CR modulo for a variant of our example

Second-order rewriting

Second-order rewriting

We consider a framework of *Second-Order Rewriting*. This means

Second-order rewriting

We consider a framework of *Second-Order Rewriting*. This means

- Hamana's Second-Order Computation Systems

Second-order rewriting

We consider a framework of *Second-Order Rewriting*. This means

- Hamana's Second-Order Computation Systems
- Nipkow's Higher-order Rewriting Systems (HRSs), over a single base type with variables of order ≤ 1 and symbols of order ≤ 2

Second-order rewriting

We consider a framework of *Second-Order Rewriting*. This means

- Hamana's Second-Order Computation Systems
- Nipkow's Higher-order Rewriting Systems (HRSs), over a single base type with variables of order ≤ 1 and symbols of order ≤ 2

Terms defined as

$$\mathcal{T}(\mathcal{F}) \ni t, u, v ::=$$

Second-order rewriting

We consider a framework of *Second-Order Rewriting*. This means

- Hamana's Second-Order Computation Systems
- Nipkow's Higher-order Rewriting Systems (HRSs), over a single base type with variables of order ≤ 1 and symbols of order ≤ 2

Terms defined as

$$\mathcal{T}(\mathcal{F}) \ni t, u, v ::= \mid x \qquad\qquad x \in \mathcal{V}$$

Second-order rewriting

We consider a framework of *Second-Order Rewriting*. This means

- Hamana's Second-Order Computation Systems
- Nipkow's Higher-order Rewriting Systems (HRSs), over a single base type with variables of order ≤ 1 and symbols of order ≤ 2

Terms defined as

$$\mathcal{T}(\mathcal{F}) \ni t, u, v ::= \mid x \qquad x \in \mathcal{V}$$
$$\mid \mathsf{x}\{t_1, \ldots, t_k\} \qquad \mathsf{x} \in \mathcal{M} \quad \text{with } \mathrm{arity}(\mathsf{x}) = k$$

Second-order rewriting

We consider a framework of *Second-Order Rewriting*. This means

- Hamana's Second-Order Computation Systems
- Nipkow's Higher-order Rewriting Systems (HRSs), over a single base type with variables of order ≤ 1 and symbols of order ≤ 2

Terms defined as

$$
\begin{aligned}
\mathcal{T}(\mathcal{F}) \ni t, u, v ::= \;& \mid x && x \in \mathcal{V} \\
& \mid \mathsf{x}\{t_1, \ldots, t_k\} && \mathsf{x} \in \mathcal{M} \quad \text{with } \mathrm{arity}(\mathsf{x}) = k \\
& \mid f(\vec{x}_1.t_1, \ldots, \vec{x}_k.t_k) && f \in \mathcal{F} \quad \text{with } \mathrm{arity}(f) = (n_1, \ldots, n_k) \text{ and } |\vec{x}_i| = n_i
\end{aligned}
$$

Second-order rewriting

We consider a framework of *Second-Order Rewriting*. This means

- Hamana's Second-Order Computation Systems
- Nipkow's Higher-order Rewriting Systems (HRSs), over a single base type with variables of order ≤ 1 and symbols of order ≤ 2

Terms defined as

$$\begin{array}{rlll} \mathcal{T}(\mathcal{F}) \ni t, u, v ::= & \mid x & x \in \mathcal{V} & \\ & \mid \mathsf{x}\{t_1, \ldots, t_k\} & \mathsf{x} \in \mathcal{M} & \text{with } \mathrm{arity}(\mathsf{x}) = k \\ & \mid f(\vec{x}_1.t_1, \ldots, \vec{x}_k.t_k) & f \in \mathcal{F} & \text{with } \mathrm{arity}(f) = (n_1, \ldots, n_k) \text{ and } |\vec{x}_i| = n_i \end{array}$$

Example If arity($@$) = $(0, 0)$ and arity(λ) = (1) then $@(\lambda(x.x), y) \in \mathcal{T}(\mathcal{F})$

Second-order rewriting

Second-order rewriting

Rewrite system Set of rewrite rules $l \longmapsto r$

with l a (fully applied) *pattern* headed by symbol, and $\mathrm{mv}(r) \subseteq \mathrm{mv}(l)$ and $\mathrm{fv}(l) = \mathrm{fv}(r) = \emptyset$

Second-order rewriting

Rewrite system Set of rewrite rules $l \longmapsto r$
with l a (fully applied) *pattern* headed by symbol, and $\mathsf{mv}(r) \subseteq \mathsf{mv}(l)$ and $\mathsf{fv}(l) = \mathsf{fv}(r) = \emptyset$

Example: $@(\lambda(x.\mathtt{t}\{x\}), \mathtt{u}) \longmapsto \mathtt{t}\{\mathtt{u}\}$

Second-order rewriting

Rewrite system Set of rewrite rules $l \longmapsto r$
with l a (fully applied) *pattern* headed by symbol, and $\mathsf{mv}(r) \subseteq \mathsf{mv}(l)$ and $\mathsf{fv}(l) = \mathsf{fv}(r) = \emptyset$

Example: $@(\lambda(x.\mathtt{t}\{x\}), \mathsf{u}) \longmapsto \mathtt{t}\{\mathsf{u}\}$

Equational system Set $\mathcal{E}$ of equations $t \approx u$
with t, u (fully applied) patterns and $\mathsf{fv}(t) = \mathsf{fv}(u) = \emptyset$ (and $\mathsf{mv}(t)$ and $\mathsf{mv}(u)$ are arbitrary)

Second-order rewriting

Rewrite system Set of rewrite rules $l \longmapsto r$
with l a (fully applied) *pattern* headed by symbol, and $\mathrm{mv}(r) \subseteq \mathrm{mv}(l)$ and $\mathrm{fv}(l) = \mathrm{fv}(r) = \emptyset$

Example: $@(\lambda(x.\mathtt{t}\{x\}), \mathtt{u}) \longmapsto \mathtt{t}\{\mathtt{u}\}$

Equational system Set $\mathcal{E}$ of equations $t \approx u$
with t, u (fully applied) patterns and $\mathrm{fv}(t) = \mathrm{fv}(u) = \emptyset$ (and $\mathrm{mv}(t)$ and $\mathrm{mv}(u)$ are arbitrary)

Example: $\mathtt{t} + \mathtt{u} \approx \mathtt{u} + \mathtt{t}$ and $\mathtt{t} \approx \mathtt{t} + 0$ (or, more formally, $+(\mathtt{t}, \mathtt{u}) \approx +(\mathtt{u}, \mathtt{t})$ and $\mathtt{t} \approx +(\mathtt{t}, 0)$)

Second-order rewriting

Rewrite system Set of rewrite rules $l \longmapsto r$
with l a (fully applied) *pattern* headed by symbol, and $\mathrm{mv}(r) \subseteq \mathrm{mv}(l)$ and $\mathrm{fv}(l) = \mathrm{fv}(r) = \emptyset$

Example: $@(\lambda(x.\mathtt{t}\{x\}), \mathtt{u}) \longmapsto \mathtt{t}\{\mathtt{u}\}$

Equational system Set $\mathcal{E}$ of equations $t \approx u$
with t, u (fully applied) patterns and $\mathrm{fv}(t) = \mathrm{fv}(u) = \emptyset$ (and $\mathrm{mv}(t)$ and $\mathrm{mv}(u)$ are arbitrary)

Example: $\mathtt{t} + \mathtt{u} \approx \mathtt{u} + \mathtt{t}$ and $\mathtt{t} \approx \mathtt{t} + 0$ (or, more formally, $+(\mathtt{t}, \mathtt{u}) \approx +(\mathtt{u}, \mathtt{t})$ and $\mathtt{t} \approx +(\mathtt{t}, 0)$)

Rewrite system modulo Pair $(\mathcal{R}, \mathcal{E})$ with $\mathcal{R}$ rewrite system and $\mathcal{E}$ equational system

The 1st Criterion

Back to (a variant of) the example

$$@(\lambda(x.\mathsf{t}\{x\}), \mathsf{u}) \longmapsto \mathsf{t}\{\mathsf{u}\} \qquad \mathbb{N}_{\mathsf{rec}}(0, \mathsf{p}, xy.\mathsf{q}\{x, y\}) \longmapsto \mathsf{p}$$

$$\mathbb{N}_{\mathsf{rec}}(\mathsf{S}(\mathsf{n}), \mathsf{p}, xy.\mathsf{q}\{x, y\}) \longmapsto \mathsf{q}\{\mathsf{n}, \mathbb{N}_{\mathsf{rec}}(\mathsf{n}, \mathsf{p}, xy.\mathsf{q}\{x, y\})\}$$

$$\mathsf{t} + 0 \approx \mathsf{t} \qquad \mathsf{t} + \mathsf{S}(\mathsf{u}) \approx \mathsf{S}(\mathsf{t} + \mathsf{u})$$

$$\mathsf{t} + \mathsf{u} \approx \mathsf{u} + \mathsf{t} \qquad (\mathsf{t} + \mathsf{u}) + \mathsf{v} \approx \mathsf{t} + (\mathsf{u} + \mathsf{v})$$

Back to (a variant of) the example

$$@(\lambda(x.\mathsf{t}\{x\}), \mathsf{u}) \longmapsto \mathsf{t}\{\mathsf{u}\} \qquad \mathbb{N}_{\mathsf{rec}}(0, \mathsf{p}, xy.\mathsf{q}\{x, y\}) \longmapsto \mathsf{p}$$

$$\mathbb{N}_{\mathsf{rec}}(\mathsf{S}(\mathsf{n}), \mathsf{p}, xy.\mathsf{q}\{x, y\}) \longmapsto \mathsf{q}\{\mathsf{n}, \mathbb{N}_{\mathsf{rec}}(\mathsf{n}, \mathsf{p}, xy.\mathsf{q}\{x, y\})\}$$

$$\mathsf{t} + 0 \approx \mathsf{t} \qquad \mathsf{t} + \mathsf{S}(\mathsf{u}) \approx \mathsf{S}(\mathsf{t} + \mathsf{u})$$

$$\mathsf{t} + \mathsf{u} \approx \mathsf{u} + \mathsf{t} \qquad (\mathsf{t} + \mathsf{u}) + \mathsf{v} \approx \mathsf{t} + (\mathsf{u} + \mathsf{v})$$

Strong CR modulo does not hold, redexes can get blocked:

Back to (a variant of) the example

$$@(\lambda(x.\mathsf{t}\{x\}),\mathsf{u}) \longmapsto \mathsf{t}\{\mathsf{u}\} \qquad \mathbb{N}_{\mathsf{rec}}(0,\mathsf{p},xy.\mathsf{q}\{x,y\}) \longmapsto \mathsf{p}$$

$$\mathbb{N}_{\mathsf{rec}}(S(\mathsf{n}),\mathsf{p},xy.\mathsf{q}\{x,y\}) \longmapsto \mathsf{q}\{\mathsf{n},\mathbb{N}_{\mathsf{rec}}(\mathsf{n},\mathsf{p},xy.\mathsf{q}\{x,y\})\}$$

$$\mathsf{t}+0 \approx \mathsf{t} \qquad \mathsf{t}+S(\mathsf{u}) \approx S(\mathsf{t}+\mathsf{u})$$

$$\mathsf{t}+\mathsf{u} \approx \mathsf{u}+\mathsf{t} \qquad (\mathsf{t}+\mathsf{u})+\mathsf{v} \approx \mathsf{t}+(\mathsf{u}+\mathsf{v})$$

Strong CR modulo does not hold, redexes can get blocked:

- Collapsible term inserted in the middle of redex

$$@(\lambda(x.t)+0,u) \qquad \text{where } (\square+0)[\lambda(x.t)] \simeq \square[\lambda(x.t)]$$

Back to (a variant of) the example

$$@(\lambda(x.\mathsf{t}\{x\}), \mathsf{u}) \longmapsto \mathsf{t}\{\mathsf{u}\} \qquad \mathbb{N}_{\mathsf{rec}}(0, \mathsf{p}, xy.\mathsf{q}\{x, y\}) \longmapsto \mathsf{p}$$

$$\mathbb{N}_{\mathsf{rec}}(\mathsf{S}(\mathsf{n}), \mathsf{p}, xy.\mathsf{q}\{x, y\}) \longmapsto \mathsf{q}\{\mathsf{n}, \mathbb{N}_{\mathsf{rec}}(\mathsf{n}, \mathsf{p}, xy.\mathsf{q}\{x, y\})\}$$

$$\mathsf{t} + 0 \approx \mathsf{t} \qquad \mathsf{t} + \mathsf{S}(\mathsf{u}) \approx \mathsf{S}(\mathsf{t} + \mathsf{u})$$

$$\mathsf{t} + \mathsf{u} \approx \mathsf{u} + \mathsf{t} \qquad (\mathsf{t} + \mathsf{u}) + \mathsf{v} \approx \mathsf{t} + (\mathsf{u} + \mathsf{v})$$

Strong CR modulo does not hold, redexes can get blocked:

- Collapsible term inserted in the middle of redex

$$@(\lambda(x.t) + 0, u) \qquad \text{where } (\square + 0)[\lambda(x.t)] \simeq \square[\lambda(x.t)]$$

- Symbol in $\mathcal{E}$ matched by rule not maximally exposed

$$\mathbb{N}_{\mathsf{rec}}(x + \mathsf{S}(y), p, xy.q) \qquad \text{where } x + \mathsf{S}(y) \simeq \mathsf{S}(x + y)$$

Back to (a variant of) the example

$$@(\lambda(x.\mathsf{t}\{x\}), \mathsf{u}) \longmapsto \mathsf{t}\{\mathsf{u}\} \qquad \mathbb{N}_{\mathsf{rec}}(0, \mathsf{p}, xy.\mathsf{q}\{x, y\}) \longmapsto \mathsf{p}$$

$$\mathbb{N}_{\mathsf{rec}}(\mathsf{S}(\mathsf{n}), \mathsf{p}, xy.\mathsf{q}\{x, y\}) \longmapsto \mathsf{q}\{\mathsf{n}, \mathbb{N}_{\mathsf{rec}}(\mathsf{n}, \mathsf{p}, xy.\mathsf{q}\{x, y\})\}$$

$$\mathsf{t} + 0 \approx \mathsf{t} \qquad \mathsf{t} + \mathsf{S}(\mathsf{u}) \approx \mathsf{S}(\mathsf{t} + \mathsf{u})$$

$$\mathsf{t} + \mathsf{u} \approx \mathsf{u} + \mathsf{t} \qquad (\mathsf{t} + \mathsf{u}) + \mathsf{v} \approx \mathsf{t} + (\mathsf{u} + \mathsf{v})$$

Strong CR modulo does not hold, redexes can get blocked:

- Collapsible term inserted in the middle of redex

$$@(\lambda(x.t) + 0, u) \qquad \text{where } (\square + 0)[\lambda(x.t)] \simeq \square[\lambda(x.t)]$$

- Symbol in $\mathcal{E}$ matched by rule not maximally exposed

$$\mathbb{N}_{\mathsf{rec}}(x + \mathsf{S}(y), p, xy.q) \qquad \text{where } x + \mathsf{S}(y) \simeq \mathsf{S}(x + y)$$

But do we need matching modulo?

A criterion for abstract rewriting

Abstract rewrite systems modulo Set $\mathcal{A}$ with binary relation $\succ$ and equiv. relation $\sim$

[2]

A criterion for abstract rewriting

Abstract rewrite systems modulo Set $\mathcal{A}$ with binary relation $\succ$ and equiv. relation $\sim$

Unblocking subset is a subset $\mathcal{U} \subseteq \mathcal{A}$ such that

2

A criterion for abstract rewriting

Abstract rewrite systems modulo Set $\mathcal{A}$ with binary relation $\succ$ and equiv. relation $\sim$

Unblocking subset is a subset $\mathcal{U} \subseteq \mathcal{A}$ such that

1. For all a there is $b \in \mathcal{U}$ with $a \sim b$.
   Intuition: all elements can be unblocked

2

A criterion for abstract rewriting

Abstract rewrite systems modulo Set $\mathcal{A}$ with binary relation $\succ$ and equiv. relation $\sim$

Unblocking subset is a subset $\mathcal{U} \subseteq \mathcal{A}$ such that

1. For all a there is $b \in \mathcal{U}$ with $a \sim b$.
   Intuition: all elements can be unblocked
2. If $a \succ a'$ and $a \sim b$ with $b \in \mathcal{U}$ then $b \succ b' \sim a'$ for some b'
   Intuition: in an unblocked term, all redexes are available

---

2

A criterion for abstract rewriting

Abstract rewrite systems modulo Set $\mathcal{A}$ with binary relation $\succ$ and equiv. relation $\sim$

Unblocking subset is a subset $\mathcal{U} \subseteq \mathcal{A}$ such that

1. For all a there is $b \in \mathcal{U}$ with $a \sim b$.
   Intuition: all elements can be unblocked
2. If $a \succ a'$ and $a \sim b$ with $b \in \mathcal{U}$ then $b \succ b' \sim a'$ for some b'
   Intuition: in an unblocked term, all redexes are available

Define $\triangleright_{\mathcal{U}}$ by $a \triangleright_{\mathcal{U}} b$ iff $a \sim c \succ b$ for some $c \in \mathcal{U}$

Unblocking replaces matching modulo

2

A criterion for abstract rewriting

Abstract rewrite systems modulo Set $\mathcal{A}$ with binary relation $\succ$ and equiv. relation $\sim$

Unblocking subset is a subset $\mathcal{U} \subseteq \mathcal{A}$ such that

1. For all a there is $b \in \mathcal{U}$ with $a \sim b$.
   Intuition: all elements can be unblocked
2. If $a \succ a'$ and $a \sim b$ with $b \in \mathcal{U}$ then $b \succ b' \sim a'$ for some b'
   Intuition: in an unblocked term, all redexes are available

Define $\triangleright_{\mathcal{U}}$ by $a \triangleright_{\mathcal{U}} b$ iff $a \sim c \succ b$ for some $c \in \mathcal{U}$
Unblocking replaces matching modulo

Proposition Suppose that $\succ$ satisfies the diamond property[2] and that we have an unblocking subset $\mathcal{U} \subseteq \mathcal{A}$. Then $a \ (\succ \cup \prec \cup \sim)^* \ b$ implies $a \triangleright_{\mathcal{U}}^* \circ \sim \circ {}_{\mathcal{U}}^*\!\triangleleft \ b$

---

[2]Think of $\succ$ as simultaneous/orthogonal/multi-step rewriting

Unblocked terms

Two ways a redex can get blocked in our example:

- Collapsible term inserted in the middle of redex

$$@(\lambda(x.t) + 0, u) \qquad \text{where } (\square + 0)[\lambda(x.t)] \simeq \square[\lambda(x.t)]$$

- Symbol in $\mathcal{E}$ matched by rule not maximally exposed

$$\mathbb{N}_{\mathsf{rec}}(x + \mathsf{S}(y), p, xy.q) \qquad \text{where } x + \mathsf{S}(y) \simeq \mathsf{S}(x + y)$$

Unblocked terms

Two ways a redex can get blocked in our example:

- Collapsible term inserted in the middle of redex

$$@(\lambda(x.t) + 0, u) \qquad \text{where } (\square + 0)[\lambda(x.t)] \simeq \square[\lambda(x.t)]$$

- Symbol in $\mathcal{E}$ matched by rule not maximally exposed

$$\mathbb{N}_{\mathsf{rec}}(x + \mathsf{S}(y), p, xy.q) \qquad \text{where } x + \mathsf{S}(y) \simeq \mathsf{S}(x + y)$$

Write $\mathcal{F}_{\mathcal{E}}$ for symbols of $\mathcal{E}$ and $\mathcal{F}_{\mathcal{R}}$ for symbols of left-hand sides of $\mathcal{R}$

Unblocked terms

Two ways a redex can get blocked in our example:

- Collapsible term inserted in the middle of redex

$$@(\lambda(x.t) + 0, u) \qquad \text{where } (\square + 0)[\lambda(x.t)] \simeq \square[\lambda(x.t)]$$

- Symbol in $\mathcal{E}$ matched by rule not maximally exposed

$$\mathbb{N}_{\mathsf{rec}}(x + \mathsf{S}(y), p, xy.q) \qquad \text{where } x + \mathsf{S}(y) \simeq \mathsf{S}(x + y)$$

Write $\mathcal{F}_{\mathcal{E}}$ for symbols of $\mathcal{E}$ and $\mathcal{F}_{\mathcal{R}}$ for symbols of left-hand sides of $\mathcal{R}$

A context E is an $\mathcal{E}$-*fragment* of t if $E \in \mathcal{T}(\mathcal{F}_{\mathcal{E}})$ and $E[\vec{u}]$ is a subterm of t

Unblocked terms

Two ways a redex can get blocked in our example:

- Collapsible term inserted in the middle of redex

$$@(\lambda(x.t) + 0, u) \qquad\qquad \text{where } (\square + 0)[\lambda(x.t)] \simeq \square[\lambda(x.t)]$$

- Symbol in $\mathcal{E}$ matched by rule not maximally exposed

$$\mathbb{N}_{\mathsf{rec}}(x + \mathsf{S}(y), p, xy.q) \qquad\qquad \text{where } x + \mathsf{S}(y) \simeq \mathsf{S}(x + y)$$

Write $\mathcal{F}_{\mathcal{E}}$ for symbols of $\mathcal{E}$ and $\mathcal{F}_{\mathcal{R}}$ for symbols of left-hand sides of $\mathcal{R}$

A context E is an $\mathcal{E}$-*fragment* of t if $E \in \mathcal{T}(\mathcal{F}_{\mathcal{E}})$ and $E[\vec{u}]$ is a subterm of t

A term is said to be *unblocked* if, for all $\mathcal{E}$-fragments of t,

Unblocked terms

Two ways a redex can get blocked in our example:

- Collapsible term inserted in the middle of redex

$$@(\lambda(x.t) + 0, u) \qquad \text{where } (\square + 0)[\lambda(x.t)] \simeq \square[\lambda(x.t)]$$

- Symbol in $\mathcal{E}$ matched by rule not maximally exposed

$$\mathbb{N}_{\mathsf{rec}}(x + \mathsf{S}(y), p, xy.q) \qquad \text{where } x + \mathsf{S}(y) \simeq \mathsf{S}(x + y)$$

Write $\mathcal{F}_{\mathcal{E}}$ for symbols of $\mathcal{E}$ and $\mathcal{F}_{\mathcal{R}}$ for symbols of left-hand sides of $\mathcal{R}$

A context E is an $\mathcal{E}$-*fragment* of t if $E \in \mathcal{T}(\mathcal{F}_{\mathcal{E}})$ and $E[\vec{u}]$ is a subterm of t

A term is said to be *unblocked* if, for all $\mathcal{E}$-fragments of t,

- $E \simeq \square$ implies $E = \square$

Unblocked terms

Two ways a redex can get blocked in our example:

- Collapsible term inserted in the middle of redex

$$@(\lambda(x.t) + 0, u) \qquad \text{where } (\Box + 0)[\lambda(x.t)] \simeq \Box[\lambda(x.t)]$$

- Symbol in $\mathcal{E}$ matched by rule not maximally exposed

$$\mathbb{N}_{\mathsf{rec}}(x + \mathsf{S}(y), p, xy.q) \qquad \text{where } x + \mathsf{S}(y) \simeq \mathsf{S}(x + y)$$

Write $\mathcal{F}_{\mathcal{E}}$ for symbols of $\mathcal{E}$ and $\mathcal{F}_{\mathcal{R}}$ for symbols of left-hand sides of $\mathcal{R}$

A context E is an $\mathcal{E}$-*fragment* of t if $E \in \mathcal{T}(\mathcal{F}_{\mathcal{E}})$ and $E[\vec{u}]$ is a subterm of t

A term is said to be *unblocked* if, for all $\mathcal{E}$-fragments of t,

- $E \simeq \Box$ implies $E = \Box$
- $E \simeq f(\vec{x}_1.t_1 \ldots \vec{x}_k.t_k)$ and $f \in \mathcal{F}_{\mathcal{E}} \cap \mathcal{F}_{\mathcal{R}}$ implies $E = f(\vec{x}_1.u_1 \ldots \vec{x}_k.u_k)$ and $t_i \simeq u_i$

The 1st Criterion

Criterion 1 Let $(\mathcal{R}, \mathcal{E})$ be a second-order rewrite system modulo st

1. Equations $t_1 \approx t_2 \in \mathcal{E}$ are linear, and we have $\mathsf{mv}(t_1) = \mathsf{mv}(t_2)$
2. Symbols in $\mathcal{F}_\mathcal{E}$ have a binding arity of the form $(0, \ldots, 0)$
3. For every context $E \in \mathcal{T}(\mathcal{F}_\mathcal{E})$, there is unblocked $E' \in \mathcal{T}(\mathcal{F}_\mathcal{E})$ with $E \simeq E'$
4. $\mathcal{R}$ is left-linear and no left-hand side is headed by a symbol in $\mathcal{F}_\mathcal{E}$
5. Orthogonal/simultaneous/multi-step rewriting $\Longrightarrow$ with $\mathcal{R}$ satisfies diamond prop.

The 1st Criterion

$$@(\lambda(x.\mathsf{t}\{x\}),\mathsf{u}) \longmapsto \mathsf{t}\{\mathsf{u}\} \qquad \mathbb{N}_{\mathsf{rec}}(0,\mathsf{p},xy.\mathsf{q}\{x,y\}) \longmapsto \mathsf{p}$$

$$\mathbb{N}_{\mathsf{rec}}(\mathsf{S}(\mathsf{n}),\mathsf{p},xy.\mathsf{q}\{x,y\}) \longmapsto \mathsf{q}\{\mathsf{n},\mathbb{N}_{\mathsf{rec}}(\mathsf{n},\mathsf{p},xy.\mathsf{q}\{x,y\})\}$$

$$\mathsf{t} + 0 \approx \mathsf{t} \qquad \mathsf{t} + \mathsf{S}(\mathsf{u}) \approx \mathsf{S}(\mathsf{t} + \mathsf{u})$$

$$\mathsf{t} + \mathsf{u} \approx \mathsf{u} + \mathsf{t} \qquad (\mathsf{t} + \mathsf{u}) + \mathsf{v} \approx \mathsf{t} + (\mathsf{u} + \mathsf{v})$$

The 1st Criterion

$$@(\lambda(x.\mathsf{t}\{x\}),\mathsf{u}) \longmapsto \mathsf{t}\{\mathsf{u}\} \qquad \mathbb{N}_{\mathsf{rec}}(0,\mathsf{p},xy.\mathsf{q}\{x,y\}) \longmapsto \mathsf{p}$$

$$\mathbb{N}_{\mathsf{rec}}(\mathsf{S}(\mathsf{n}),\mathsf{p},xy.\mathsf{q}\{x,y\}) \longmapsto \mathsf{q}\{\mathsf{n},\mathbb{N}_{\mathsf{rec}}(\mathsf{n},\mathsf{p},xy.\mathsf{q}\{x,y\})\}$$

$$\mathsf{t} + 0 \approx \mathsf{t} \qquad \mathsf{t} + \mathsf{S}(\mathsf{u}) \approx \mathsf{S}(\mathsf{t} + \mathsf{u})$$

$$\mathsf{t} + \mathsf{u} \approx \mathsf{u} + \mathsf{t} \qquad (\mathsf{t} + \mathsf{u}) + \mathsf{v} \approx \mathsf{t} + (\mathsf{u} + \mathsf{v})$$

1. Equations $t_1 \approx t_2 \in \mathcal{E}$ are linear, and we have $\mathrm{mv}(t_1) = \mathrm{mv}(t_2)$

The 1st Criterion

$$@(\lambda(x.\mathsf{t}\{x\}), \mathsf{u}) \longmapsto \mathsf{t}\{\mathsf{u}\} \qquad \mathbb{N}_{\mathsf{rec}}(0, \mathsf{p}, xy.\mathsf{q}\{x, y\}) \longmapsto \mathsf{p}$$

$$\mathbb{N}_{\mathsf{rec}}(\mathsf{S}(\mathsf{n}), \mathsf{p}, xy.\mathsf{q}\{x, y\}) \longmapsto \mathsf{q}\{\mathsf{n}, \mathbb{N}_{\mathsf{rec}}(\mathsf{n}, \mathsf{p}, xy.\mathsf{q}\{x, y\})\}$$

$$\mathsf{t} + 0 \approx \mathsf{t} \qquad \mathsf{t} + \mathsf{S}(\mathsf{u}) \approx \mathsf{S}(\mathsf{t} + \mathsf{u})$$

$$\mathsf{t} + \mathsf{u} \approx \mathsf{u} + \mathsf{t} \qquad (\mathsf{t} + \mathsf{u}) + \mathsf{v} \approx \mathsf{t} + (\mathsf{u} + \mathsf{v})$$

1. Equations $t_1 \approx t_2 \in \mathcal{E}$ are linear, and we have $\mathrm{mv}(t_1) = \mathrm{mv}(t_2)$ ✓

The 1st Criterion

$$@(\lambda(x.\mathsf{t}\{x\}), \mathsf{u}) \longmapsto \mathsf{t}\{\mathsf{u}\} \qquad \mathbb{N}_{\mathsf{rec}}(0, \mathsf{p}, xy.\mathsf{q}\{x, y\}) \longmapsto \mathsf{p}$$

$$\mathbb{N}_{\mathsf{rec}}(\mathsf{S}(\mathsf{n}), \mathsf{p}, xy.\mathsf{q}\{x, y\}) \longmapsto \mathsf{q}\{\mathsf{n}, \mathbb{N}_{\mathsf{rec}}(\mathsf{n}, \mathsf{p}, xy.\mathsf{q}\{x, y\})\}$$

$$\mathsf{t} + 0 \approx \mathsf{t} \qquad \mathsf{t} + \mathsf{S}(\mathsf{u}) \approx \mathsf{S}(\mathsf{t} + \mathsf{u})$$

$$\mathsf{t} + \mathsf{u} \approx \mathsf{u} + \mathsf{t} \qquad (\mathsf{t} + \mathsf{u}) + \mathsf{v} \approx \mathsf{t} + (\mathsf{u} + \mathsf{v})$$

1. Equations $t_1 \approx t_2 \in \mathcal{E}$ are linear, and we have $\mathrm{mv}(t_1) = \mathrm{mv}(t_2)$ ✓
2. Symbols in $\mathcal{F}_{\mathcal{E}}$ have a binding arity of the form $(0, \ldots, 0)$

The 1st Criterion

$$@(\lambda(x.\mathsf{t}\{x\}), \mathsf{u}) \longmapsto \mathsf{t}\{\mathsf{u}\} \qquad \mathbb{N}_{\mathsf{rec}}(0, \mathsf{p}, xy.\mathsf{q}\{x, y\}) \longmapsto \mathsf{p}$$

$$\mathbb{N}_{\mathsf{rec}}(\mathsf{S}(\mathsf{n}), \mathsf{p}, xy.\mathsf{q}\{x, y\}) \longmapsto \mathsf{q}\{\mathsf{n}, \mathbb{N}_{\mathsf{rec}}(\mathsf{n}, \mathsf{p}, xy.\mathsf{q}\{x, y\})\}$$

$$\mathsf{t} + 0 \approx \mathsf{t} \qquad \mathsf{t} + \mathsf{S}(\mathsf{u}) \approx \mathsf{S}(\mathsf{t} + \mathsf{u})$$

$$\mathsf{t} + \mathsf{u} \approx \mathsf{u} + \mathsf{t} \qquad (\mathsf{t} + \mathsf{u}) + \mathsf{v} \approx \mathsf{t} + (\mathsf{u} + \mathsf{v})$$

1. Equations $t_1 \approx t_2 \in \mathcal{E}$ are linear, and we have $\mathrm{mv}(t_1) = \mathrm{mv}(t_2)$ ✓
2. Symbols in $\mathcal{F}_\mathcal{E}$ have a binding arity of the form $(0, \ldots, 0)$ ✓
   We have $\mathrm{arity}(+) = (0, 0)$ and $\mathrm{arity}(\mathsf{S}) = (0)$ and $\mathrm{arity}(0) = ()$

The 1st Criterion

$$@(\lambda(x.\mathsf{t}\{x\}), \mathsf{u}) \longmapsto \mathsf{t}\{\mathsf{u}\} \qquad \mathbb{N}_{\mathsf{rec}}(0, \mathsf{p}, xy.\mathsf{q}\{x, y\}) \longmapsto \mathsf{p}$$

$$\mathbb{N}_{\mathsf{rec}}(\mathsf{S}(\mathsf{n}), \mathsf{p}, xy.\mathsf{q}\{x, y\}) \longmapsto \mathsf{q}\{\mathsf{n}, \mathbb{N}_{\mathsf{rec}}(\mathsf{n}, \mathsf{p}, xy.\mathsf{q}\{x, y\})\}$$

$$\mathsf{t} + 0 \approx \mathsf{t} \qquad \mathsf{t} + \mathsf{S}(\mathsf{u}) \approx \mathsf{S}(\mathsf{t} + \mathsf{u})$$

$$\mathsf{t} + \mathsf{u} \approx \mathsf{u} + \mathsf{t} \qquad (\mathsf{t} + \mathsf{u}) + \mathsf{v} \approx \mathsf{t} + (\mathsf{u} + \mathsf{v})$$

1. Equations $t_1 \approx t_2 \in \mathcal{E}$ are linear, and we have $\mathrm{mv}(t_1) = \mathrm{mv}(t_2)$ ✓
2. Symbols in $\mathcal{F}_{\mathcal{E}}$ have a binding arity of the form $(0, \ldots, 0)$ ✓
   We have $\mathrm{arity}(+) = (0, 0)$ and $\mathrm{arity}(\mathsf{S}) = (0)$ and $\mathrm{arity}(0) = ()$
3. For every context $E \in \mathcal{T}(\mathcal{F}_{\mathcal{E}})$, there is unblocked $E' \in \mathcal{T}(\mathcal{F}_{\mathcal{E}})$ with $E \simeq E'$

The 1st Criterion

$$@(\lambda(x.\mathsf{t}\{x\}), \mathsf{u}) \longmapsto \mathsf{t}\{\mathsf{u}\} \qquad \mathbb{N}_{\mathsf{rec}}(0, \mathsf{p}, xy.\mathsf{q}\{x, y\}) \longmapsto \mathsf{p}$$

$$\mathbb{N}_{\mathsf{rec}}(\mathsf{S}(\mathsf{n}), \mathsf{p}, xy.\mathsf{q}\{x, y\}) \longmapsto \mathsf{q}\{\mathsf{n}, \mathbb{N}_{\mathsf{rec}}(\mathsf{n}, \mathsf{p}, xy.\mathsf{q}\{x, y\})\}$$

$$\mathsf{t} + 0 \approx \mathsf{t} \qquad \mathsf{t} + \mathsf{S}(\mathsf{u}) \approx \mathsf{S}(\mathsf{t} + \mathsf{u})$$

$$\mathsf{t} + \mathsf{u} \approx \mathsf{u} + \mathsf{t} \qquad (\mathsf{t} + \mathsf{u}) + \mathsf{v} \approx \mathsf{t} + (\mathsf{u} + \mathsf{v})$$

1. Equations $t_1 \approx t_2 \in \mathcal{E}$ are linear, and we have $\mathsf{mv}(t_1) = \mathsf{mv}(t_2)$ ✓
2. Symbols in $\mathcal{F}_{\mathcal{E}}$ have a binding arity of the form $(0, \ldots, 0)$ ✓
   We have $\mathsf{arity}(+) = (0, 0)$ and $\mathsf{arity}(\mathsf{S}) = (0)$ and $\mathsf{arity}(0) = ()$
3. For every context $E \in \mathcal{T}(\mathcal{F}_{\mathcal{E}})$, there is unblocked $E' \in \mathcal{T}(\mathcal{F}_{\mathcal{E}})$ with $E \simeq E'$ ✓
   Every context $E \in \mathcal{T}(\mathcal{F}_{\mathcal{E}})$ is $\simeq$ to $\mathsf{S}^n(\square_1 + \cdots + \square_k)$, which is unblocked

The 1st Criterion

$$@(\lambda(x.\mathsf{t}\{x\}),\mathsf{u}) \longmapsto \mathsf{t}\{\mathsf{u}\} \qquad \mathbb{N}_{\mathsf{rec}}(0,\mathsf{p},xy.\mathsf{q}\{x,y\}) \longmapsto \mathsf{p}$$

$$\mathbb{N}_{\mathsf{rec}}(\mathsf{S}(\mathsf{n}),\mathsf{p},xy.\mathsf{q}\{x,y\}) \longmapsto \mathsf{q}\{\mathsf{n},\mathbb{N}_{\mathsf{rec}}(\mathsf{n},\mathsf{p},xy.\mathsf{q}\{x,y\})\}$$

$$\mathsf{t}+0 \approx \mathsf{t} \qquad \mathsf{t}+\mathsf{S}(\mathsf{u}) \approx \mathsf{S}(\mathsf{t}+\mathsf{u})$$

$$\mathsf{t}+\mathsf{u} \approx \mathsf{u}+\mathsf{t} \qquad (\mathsf{t}+\mathsf{u})+\mathsf{v} \approx \mathsf{t}+(\mathsf{u}+\mathsf{v})$$

1. Equations $t_1 \approx t_2 \in \mathcal{E}$ are linear, and we have $\mathrm{mv}(t_1) = \mathrm{mv}(t_2)$ ✓
2. Symbols in $\mathcal{F}_{\mathcal{E}}$ have a binding arity of the form $(0,\dots,0)$ ✓
   We have $\mathrm{arity}(+) = (0,0)$ and $\mathrm{arity}(\mathsf{S}) = (0)$ and $\mathrm{arity}(0) = ()$
3. For every context $E \in \mathcal{T}(\mathcal{F}_{\mathcal{E}})$, there is unblocked $E' \in \mathcal{T}(\mathcal{F}_{\mathcal{E}})$ with $E \simeq E'$ ✓
   Every context $E \in \mathcal{T}(\mathcal{F}_{\mathcal{E}})$ is $\simeq$ to $\mathsf{S}^n(\square_1 + \cdots + \square_k)$, which is unblocked
4. $\mathcal{R}$ is left-linear and no left-hand side is headed by a symbol in $\mathcal{F}_{\mathcal{E}}$

The 1st Criterion

$$@(\lambda(x.\mathsf{t}\{x\}), \mathsf{u}) \longmapsto \mathsf{t}\{\mathsf{u}\} \qquad \mathbb{N}_{\mathsf{rec}}(0, \mathsf{p}, xy.\mathsf{q}\{x, y\}) \longmapsto \mathsf{p}$$

$$\mathbb{N}_{\mathsf{rec}}(\mathsf{S}(\mathsf{n}), \mathsf{p}, xy.\mathsf{q}\{x, y\}) \longmapsto \mathsf{q}\{\mathsf{n}, \mathbb{N}_{\mathsf{rec}}(\mathsf{n}, \mathsf{p}, xy.\mathsf{q}\{x, y\})\}$$

$$\mathsf{t} + 0 \approx \mathsf{t} \qquad \mathsf{t} + \mathsf{S}(\mathsf{u}) \approx \mathsf{S}(\mathsf{t} + \mathsf{u})$$

$$\mathsf{t} + \mathsf{u} \approx \mathsf{u} + \mathsf{t} \qquad (\mathsf{t} + \mathsf{u}) + \mathsf{v} \approx \mathsf{t} + (\mathsf{u} + \mathsf{v})$$

1. Equations $t_1 \approx t_2 \in \mathcal{E}$ are linear, and we have $\mathsf{mv}(t_1) = \mathsf{mv}(t_2)$ ✓
2. Symbols in $\mathcal{F}_{\mathcal{E}}$ have a binding arity of the form $(0, \ldots, 0)$ ✓
   We have $\mathsf{arity}(+) = (0, 0)$ and $\mathsf{arity}(\mathsf{S}) = (0)$ and $\mathsf{arity}(0) = ()$
3. For every context $E \in \mathcal{T}(\mathcal{F}_{\mathcal{E}})$, there is unblocked $E' \in \mathcal{T}(\mathcal{F}_{\mathcal{E}})$ with $E \simeq E'$ ✓
   Every context $E \in \mathcal{T}(\mathcal{F}_{\mathcal{E}})$ is $\simeq$ to $\mathsf{S}^n(\Box_1 + \cdots + \Box_k)$, which is unblocked
4. $\mathcal{R}$ is left-linear and no left-hand side is headed by a symbol in $\mathcal{F}_{\mathcal{E}}$ ✓

The 1st Criterion

$$@(\lambda(x.\mathsf{t}\{x\}),\mathsf{u}) \longmapsto \mathsf{t}\{\mathsf{u}\} \qquad \mathbb{N}_{\mathsf{rec}}(0,\mathsf{p},xy.\mathsf{q}\{x,y\}) \longmapsto \mathsf{p}$$

$$\mathbb{N}_{\mathsf{rec}}(\mathsf{S}(\mathsf{n}),\mathsf{p},xy.\mathsf{q}\{x,y\}) \longmapsto \mathsf{q}\{\mathsf{n},\mathbb{N}_{\mathsf{rec}}(\mathsf{n},\mathsf{p},xy.\mathsf{q}\{x,y\})\}$$

$$\mathsf{t} + 0 \approx \mathsf{t} \qquad \mathsf{t} + \mathsf{S}(\mathsf{u}) \approx \mathsf{S}(\mathsf{t}+\mathsf{u})$$

$$\mathsf{t} + \mathsf{u} \approx \mathsf{u} + \mathsf{t} \qquad (\mathsf{t}+\mathsf{u}) + \mathsf{v} \approx \mathsf{t} + (\mathsf{u}+\mathsf{v})$$

1. Equations $t_1 \approx t_2 \in \mathcal{E}$ are linear, and we have $\mathrm{mv}(t_1) = \mathrm{mv}(t_2)$ ✓
2. Symbols in $\mathcal{F}_{\mathcal{E}}$ have a binding arity of the form $(0,\ldots,0)$ ✓
   We have $\mathrm{arity}(+) = (0,0)$ and $\mathrm{arity}(\mathsf{S}) = (0)$ and $\mathrm{arity}(0) = ()$
3. For every context $E \in \mathcal{T}(\mathcal{F}_{\mathcal{E}})$, there is unblocked $E' \in \mathcal{T}(\mathcal{F}_{\mathcal{E}})$ with $E \simeq E'$ ✓
   Every context $E \in \mathcal{T}(\mathcal{F}_{\mathcal{E}})$ is $\simeq$ to $\mathsf{S}^n(\square_1 + \cdots + \square_k)$, which is unblocked
4. $\mathcal{R}$ is left-linear and no left-hand side is headed by a symbol in $\mathcal{F}_{\mathcal{E}}$ ✓
5. Orthogonal/Simultaneous rewriting $\Longrightarrow$ with $\mathcal{R}$ satisfies diamond prop.

The 1st Criterion

$$@(\lambda(x.\mathsf{t}\{x\}), \mathsf{u}) \longmapsto \mathsf{t}\{\mathsf{u}\} \qquad \mathbb{N}_{\mathsf{rec}}(0, \mathsf{p}, xy.\mathsf{q}\{x, y\}) \longmapsto \mathsf{p}$$

$$\mathbb{N}_{\mathsf{rec}}(\mathsf{S}(\mathsf{n}), \mathsf{p}, xy.\mathsf{q}\{x, y\}) \longmapsto \mathsf{q}\{\mathsf{n}, \mathbb{N}_{\mathsf{rec}}(\mathsf{n}, \mathsf{p}, xy.\mathsf{q}\{x, y\})\}$$

$$\mathsf{t} + 0 \approx \mathsf{t} \qquad \mathsf{t} + \mathsf{S}(\mathsf{u}) \approx \mathsf{S}(\mathsf{t} + \mathsf{u})$$

$$\mathsf{t} + \mathsf{u} \approx \mathsf{u} + \mathsf{t} \qquad (\mathsf{t} + \mathsf{u}) + \mathsf{v} \approx \mathsf{t} + (\mathsf{u} + \mathsf{v})$$

1. Equations $t_1 \approx t_2 \in \mathcal{E}$ are linear, and we have $\mathrm{mv}(t_1) = \mathrm{mv}(t_2)$ ✓
2. Symbols in $\mathcal{F}_{\mathcal{E}}$ have a binding arity of the form $(0, \ldots, 0)$ ✓
   We have $\mathrm{arity}(+) = (0, 0)$ and $\mathrm{arity}(\mathsf{S}) = (0)$ and $\mathrm{arity}(0) = ()$
3. For every context $E \in \mathcal{T}(\mathcal{F}_{\mathcal{E}})$, there is unblocked $E' \in \mathcal{T}(\mathcal{F}_{\mathcal{E}})$ with $E \simeq E'$ ✓
   Every context $E \in \mathcal{T}(\mathcal{F}_{\mathcal{E}})$ is $\simeq$ to $\mathsf{S}^n(\square_1 + \cdots + \square_k)$, which is unblocked
4. $\mathcal{R}$ is left-linear and no left-hand side is headed by a symbol in $\mathcal{F}_{\mathcal{E}}$ ✓
5. Orthogonal/Simultaneous rewriting $\Longrightarrow$ with $\mathcal{R}$ satisfies diamond prop. ✓
   By orthogonality of the rewrite rules

The 1st Criterion

Criterion 1 Let $(\mathcal{R}, \mathcal{E})$ be a second-order rewrite system modulo st

1. Equations $t_1 \approx t_2 \in \mathcal{E}$ are linear, and we have $\mathsf{mv}(t_1) = \mathsf{mv}(t_2)$
2. Symbols in $\mathcal{F}_\mathcal{E}$ have a binding arity of the form $(0, \ldots, 0)$
3. For every context $E \in \mathcal{T}(\mathcal{F}_\mathcal{E})$, there is unblocked $E' \in \mathcal{T}(\mathcal{F}_\mathcal{E})$ with $E \simeq E'$
4. $\mathcal{R}$ is left-linear and no left-hand side is headed by a symbol in $\mathcal{F}_\mathcal{E}$
5. Orthogonal/simultaneous/multi-step rewriting $\Longrightarrow$ with $\mathcal{R}$ satisfies diamond prop.

The 1st Criterion

Criterion 1 Let $(\mathcal{R}, \mathcal{E})$ be a second-order rewrite system modulo st

1. Equations $t_1 \approx t_2 \in \mathcal{E}$ are linear, and we have $\mathsf{mv}(t_1) = \mathsf{mv}(t_2)$
2. Symbols in $\mathcal{F}_\mathcal{E}$ have a binding arity of the form $(0, \ldots, 0)$
3. For every context $E \in \mathcal{T}(\mathcal{F}_\mathcal{E})$, there is unblocked $E' \in \mathcal{T}(\mathcal{F}_\mathcal{E})$ with $E \simeq E'$
4. $\mathcal{R}$ is left-linear and no left-hand side is headed by a symbol in $\mathcal{F}_\mathcal{E}$
5. Orthogonal/simultaneous/multi-step rewriting $\Longrightarrow$ with $\mathcal{R}$ satisfies diamond prop.

Then $t \equiv u$ implies $t \overset{\sim}{\longrightarrow}{}^* \circ \simeq \circ {}^*\overset{\sim}{\longleftarrow} u$

where $\overset{\sim}{\longrightarrow}$ defined by: $t \overset{\sim}{\longrightarrow} u$ iff $t \simeq t' \longrightarrow u$ for some unblocked t'

The 1st Criterion

Criterion 1 Let $(\mathcal{R}, \mathcal{E})$ be a second-order rewrite system modulo st

1. Equations $t_1 \approx t_2 \in \mathcal{E}$ are linear, and we have $\mathsf{mv}(t_1) = \mathsf{mv}(t_2)$
2. Symbols in $\mathcal{F}_\mathcal{E}$ have a binding arity of the form $(0, \ldots, 0)$
3. For every context $E \in \mathcal{T}(\mathcal{F}_\mathcal{E})$, there is unblocked $E' \in \mathcal{T}(\mathcal{F}_\mathcal{E})$ with $E \simeq E'$
4. $\mathcal{R}$ is left-linear and no left-hand side is headed by a symbol in $\mathcal{F}_\mathcal{E}$
5. Orthogonal/simultaneous/multi-step rewriting $\Longrightarrow$ with $\mathcal{R}$ satisfies diamond prop.

Then $t \equiv u$ implies $t \xrightarrow{\sim}{}^{*} \circ \simeq \circ {}^{*}\xleftarrow{\sim} u$
where $\xrightarrow{\sim}$ defined by: $t \xrightarrow{\sim} u$ iff $t \simeq t' \longrightarrow u$ for some unblocked t'

Proof We show that the set of unblocked terms is an unblocking subset for $(\Longrightarrow, \simeq)$
We do some small adjustments and we obtain the result

The 2nd Criterion

The 2nd Criterion

Criterion 2 Let $(\mathcal{R} \cup \mathcal{S}, \mathcal{E})$ be a second-order rewrite system modulo st

1. $\mathcal{R} \cup \mathcal{S}$ is left-linear
2. For all $t \approx u \in \mathcal{E}$, we have t, u linear, headed by symbols, and $\mathsf{mv}(t) = \mathsf{mv}(u)$
3. $\mathcal{R}$ is confluent
4. $(\mathcal{S}, \mathcal{E})$ is strong CR modulo
5. No critical pairs between $\mathcal{R}$ and $\mathcal{S} \cup \mathcal{E}^{\pm}$

   Where $\mathcal{E}^{\pm} := \mathcal{E} \cup \mathcal{E}^{-1}$

The 2nd Criterion

$$\mathcal{R} = \qquad @(\lambda(x.\mathsf{t}\{x\}), \mathsf{u}) \longmapsto \mathsf{t}\{\mathsf{u}\} \qquad \mathbb{N}_{\mathsf{rec}}(0, \mathsf{p}, xy.\mathsf{q}\{x, y\}) \longmapsto \mathsf{p}$$

$$\mathbb{N}_{\mathsf{rec}}(\mathsf{S}(\mathsf{n}), \mathsf{p}, xy.\mathsf{q}\{x, y\}) \longmapsto \mathsf{q}\{\mathsf{n}, \mathbb{N}_{\mathsf{rec}}(\mathsf{n}, \mathsf{p}, xy.\mathsf{q}\{x, y\})\}$$

$$\mathcal{S} = \qquad \mathsf{t} + 0 \longmapsto \mathsf{t} \qquad \mathsf{t} + \mathsf{S}(\mathsf{u}) \longmapsto \mathsf{S}(\mathsf{t} + \mathsf{u}) \qquad 0 + \mathsf{t} \longmapsto \mathsf{t} \qquad \mathsf{S}(\mathsf{u}) + \mathsf{t} \longmapsto \mathsf{S}(\mathsf{t} + \mathsf{u})$$

$$\mathcal{E} = \qquad \mathsf{t} + \mathsf{u} \approx \mathsf{u} + \mathsf{t} \qquad (\mathsf{t} + \mathsf{u}) + \mathsf{v} \approx \mathsf{t} + (\mathsf{u} + \mathsf{v})$$

3

The 2nd Criterion

$$\mathcal{R} = \qquad @(\lambda(x.\mathsf{t}\{x\}), \mathsf{u}) \longmapsto \mathsf{t}\{\mathsf{u}\} \qquad \mathbb{N}_{\mathsf{rec}}(0, \mathsf{p}, xy.\mathsf{q}\{x, y\}) \longmapsto \mathsf{p}$$

$$\mathbb{N}_{\mathsf{rec}}(\mathsf{S}(\mathsf{n}), \mathsf{p}, xy.\mathsf{q}\{x, y\}) \longmapsto \mathsf{q}\{\mathsf{n}, \mathbb{N}_{\mathsf{rec}}(\mathsf{n}, \mathsf{p}, xy.\mathsf{q}\{x, y\})\}$$

$$\mathcal{S} = \qquad \mathsf{t} + 0 \longmapsto \mathsf{t} \qquad \mathsf{t} + \mathsf{S}(\mathsf{u}) \longmapsto \mathsf{S}(\mathsf{t} + \mathsf{u}) \qquad 0 + \mathsf{t} \longmapsto \mathsf{t} \qquad \mathsf{S}(\mathsf{u}) + \mathsf{t} \longmapsto \mathsf{S}(\mathsf{t} + \mathsf{u})$$

$$\mathcal{E} = \qquad \mathsf{t} + \mathsf{u} \approx \mathsf{u} + \mathsf{t} \qquad (\mathsf{t} + \mathsf{u}) + \mathsf{v} \approx \mathsf{t} + (\mathsf{u} + \mathsf{v})$$

1. $\mathcal{R} \cup \mathcal{S}$ is left-linear

3

The 2nd Criterion

$$\mathcal{R} = \qquad @(\lambda(x.\mathsf{t}\{x\}), \mathsf{u}) \longmapsto \mathsf{t}\{\mathsf{u}\} \qquad \mathbb{N}_{\mathsf{rec}}(0, \mathsf{p}, xy.\mathsf{q}\{x, y\}) \longmapsto \mathsf{p}$$

$$\mathbb{N}_{\mathsf{rec}}(\mathsf{S}(\mathsf{n}), \mathsf{p}, xy.\mathsf{q}\{x, y\}) \longmapsto \mathsf{q}\{\mathsf{n}, \mathbb{N}_{\mathsf{rec}}(\mathsf{n}, \mathsf{p}, xy.\mathsf{q}\{x, y\})\}$$

$$\mathcal{S} = \qquad \mathsf{t} + 0 \longmapsto \mathsf{t} \qquad \mathsf{t} + \mathsf{S}(\mathsf{u}) \longmapsto \mathsf{S}(\mathsf{t} + \mathsf{u}) \qquad 0 + \mathsf{t} \longmapsto \mathsf{t} \qquad \mathsf{S}(\mathsf{u}) + \mathsf{t} \longmapsto \mathsf{S}(\mathsf{t} + \mathsf{u})$$

$$\mathcal{E} = \qquad \mathsf{t} + \mathsf{u} \approx \mathsf{u} + \mathsf{t} \qquad (\mathsf{t} + \mathsf{u}) + \mathsf{v} \approx \mathsf{t} + (\mathsf{u} + \mathsf{v})$$

1. $\mathcal{R} \cup \mathcal{S}$ is left-linear ✓

3

The 2nd Criterion

$$\mathcal{R} = \quad @(\lambda(x.\mathsf{t}\{x\}), \mathsf{u}) \longmapsto \mathsf{t}\{\mathsf{u}\} \qquad \mathbb{N}_{\mathsf{rec}}(0, \mathsf{p}, xy.\mathsf{q}\{x, y\}) \longmapsto \mathsf{p}$$

$$\mathbb{N}_{\mathsf{rec}}(\mathsf{S}(\mathsf{n}), \mathsf{p}, xy.\mathsf{q}\{x, y\}) \longmapsto \mathsf{q}\{\mathsf{n}, \mathbb{N}_{\mathsf{rec}}(\mathsf{n}, \mathsf{p}, xy.\mathsf{q}\{x, y\})\}$$

$$\mathcal{S} = \quad \mathsf{t} + 0 \longmapsto \mathsf{t} \qquad \mathsf{t} + \mathsf{S}(\mathsf{u}) \longmapsto \mathsf{S}(\mathsf{t} + \mathsf{u}) \qquad 0 + \mathsf{t} \longmapsto \mathsf{t} \qquad \mathsf{S}(\mathsf{u}) + \mathsf{t} \longmapsto \mathsf{S}(\mathsf{t} + \mathsf{u})$$

$$\mathcal{E} = \quad \mathsf{t} + \mathsf{u} \approx \mathsf{u} + \mathsf{t} \qquad (\mathsf{t} + \mathsf{u}) + \mathsf{v} \approx \mathsf{t} + (\mathsf{u} + \mathsf{v})$$

1. $\mathcal{R} \cup \mathcal{S}$ is left-linear ✓
2. For all $t \approx u \in \mathcal{E}$, we have t, u linear, headed by symbols, and $\mathrm{mv}(t) = \mathrm{mv}(u)$[3]

[3]Therefore, $\mathcal{E}^{\pm} := \mathcal{E} \cup \mathcal{E}^{-1}$ is a left-linear rewrite system

The 2nd Criterion

$$\mathcal{R} = \quad @(\lambda(x.\mathsf{t}\{x\}), \mathsf{u}) \longmapsto \mathsf{t}\{\mathsf{u}\} \qquad \mathbb{N}_{\mathsf{rec}}(0, \mathsf{p}, xy.\mathsf{q}\{x, y\}) \longmapsto \mathsf{p}$$

$$\mathbb{N}_{\mathsf{rec}}(\mathsf{S}(\mathsf{n}), \mathsf{p}, xy.\mathsf{q}\{x, y\}) \longmapsto \mathsf{q}\{\mathsf{n}, \mathbb{N}_{\mathsf{rec}}(\mathsf{n}, \mathsf{p}, xy.\mathsf{q}\{x, y\})\}$$

$$\mathcal{S} = \quad \mathsf{t} + 0 \longmapsto \mathsf{t} \qquad \mathsf{t} + \mathsf{S}(\mathsf{u}) \longmapsto \mathsf{S}(\mathsf{t} + \mathsf{u}) \qquad 0 + \mathsf{t} \longmapsto \mathsf{t} \qquad \mathsf{S}(\mathsf{u}) + \mathsf{t} \longmapsto \mathsf{S}(\mathsf{t} + \mathsf{u})$$

$$\mathcal{E} = \quad \mathsf{t} + \mathsf{u} \approx \mathsf{u} + \mathsf{t} \qquad (\mathsf{t} + \mathsf{u}) + \mathsf{v} \approx \mathsf{t} + (\mathsf{u} + \mathsf{v})$$

1. $\mathcal{R} \cup \mathcal{S}$ is left-linear ✓
2. For all $t \approx u \in \mathcal{E}$, we have t, u linear, headed by symbols, and $\mathrm{mv}(t) = \mathrm{mv}(u)$[3] ✓

[3] Therefore, $\mathcal{E}^{\pm} := \mathcal{E} \cup \mathcal{E}^{-1}$ is a left-linear rewrite system

The 2nd Criterion

$$\mathcal{R} = \quad @(\lambda(x.\mathsf{t}\{x\}), \mathsf{u}) \longmapsto \mathsf{t}\{\mathsf{u}\} \qquad \mathbb{N}_{\mathsf{rec}}(0, \mathsf{p}, xy.\mathsf{q}\{x, y\}) \longmapsto \mathsf{p}$$

$$\mathbb{N}_{\mathsf{rec}}(\mathsf{S}(\mathsf{n}), \mathsf{p}, xy.\mathsf{q}\{x, y\}) \longmapsto \mathsf{q}\{\mathsf{n}, \mathbb{N}_{\mathsf{rec}}(\mathsf{n}, \mathsf{p}, xy.\mathsf{q}\{x, y\})\}$$

$$\mathcal{S} = \quad \mathsf{t} + 0 \longmapsto \mathsf{t} \qquad \mathsf{t} + \mathsf{S}(\mathsf{u}) \longmapsto \mathsf{S}(\mathsf{t} + \mathsf{u}) \qquad 0 + \mathsf{t} \longmapsto \mathsf{t} \qquad \mathsf{S}(\mathsf{u}) + \mathsf{t} \longmapsto \mathsf{S}(\mathsf{t} + \mathsf{u})$$

$$\mathcal{E} = \quad \mathsf{t} + \mathsf{u} \approx \mathsf{u} + \mathsf{t} \qquad (\mathsf{t} + \mathsf{u}) + \mathsf{v} \approx \mathsf{t} + (\mathsf{u} + \mathsf{v})$$

1. $\mathcal{R} \cup \mathcal{S}$ is left-linear ✓
2. For all $t \approx u \in \mathcal{E}$, we have t, u linear, headed by symbols, and $\mathrm{mv}(t) = \mathrm{mv}(u)$[3] ✓
3. $\mathcal{R}$ is confluent

[3] Therefore, $\mathcal{E}^{\pm} := \mathcal{E} \cup \mathcal{E}^{-1}$ is a left-linear rewrite system

The 2nd Criterion

$$\mathcal{R} = \quad @(\lambda(x.\mathsf{t}\{x\}),\mathsf{u}) \longmapsto \mathsf{t}\{\mathsf{u}\} \qquad \mathbb{N}_{\mathsf{rec}}(0,\mathsf{p},xy.\mathsf{q}\{x,y\}) \longmapsto \mathsf{p}$$

$$\mathbb{N}_{\mathsf{rec}}(\mathsf{S}(\mathsf{n}),\mathsf{p},xy.\mathsf{q}\{x,y\}) \longmapsto \mathsf{q}\{\mathsf{n},\mathbb{N}_{\mathsf{rec}}(\mathsf{n},\mathsf{p},xy.\mathsf{q}\{x,y\})\}$$

$$\mathcal{S} = \quad \mathsf{t}+0 \longmapsto \mathsf{t} \qquad \mathsf{t}+\mathsf{S}(\mathsf{u}) \longmapsto \mathsf{S}(\mathsf{t}+\mathsf{u}) \qquad 0+\mathsf{t} \longmapsto \mathsf{t} \qquad \mathsf{S}(\mathsf{u})+\mathsf{t} \longmapsto \mathsf{S}(\mathsf{t}+\mathsf{u})$$

$$\mathcal{E} = \quad \mathsf{t}+\mathsf{u} \approx \mathsf{u}+\mathsf{t} \qquad (\mathsf{t}+\mathsf{u})+\mathsf{v} \approx \mathsf{t}+(\mathsf{u}+\mathsf{v})$$

1. $\mathcal{R} \cup \mathcal{S}$ is left-linear ✓
2. For all $t \approx u \in \mathcal{E}$, we have t, u linear, headed by symbols, and $\mathrm{mv}(t) = \mathrm{mv}(u)$[3] ✓
3. $\mathcal{R}$ is confluent ✓

   Because $\mathcal{R}$ is orthogonal

[3] Therefore, $\mathcal{E}^{\pm} := \mathcal{E} \cup \mathcal{E}^{-1}$ is a left-linear rewrite system

The 2nd Criterion

$$\mathcal{R} = \qquad @(\lambda(x.\mathsf{t}\{x\}),\mathsf{u}) \longmapsto \mathsf{t}\{\mathsf{u}\} \qquad \mathbb{N}_{\mathsf{rec}}(0,\mathsf{p},xy.\mathsf{q}\{x,y\}) \longmapsto \mathsf{p}$$

$$\mathbb{N}_{\mathsf{rec}}(\mathsf{S}(\mathsf{n}),\mathsf{p},xy.\mathsf{q}\{x,y\}) \longmapsto \mathsf{q}\{\mathsf{n},\mathbb{N}_{\mathsf{rec}}(\mathsf{n},\mathsf{p},xy.\mathsf{q}\{x,y\})\}$$

$$\mathcal{S} = \qquad \mathsf{t}+0 \longmapsto \mathsf{t} \qquad \mathsf{t}+\mathsf{S}(\mathsf{u}) \longmapsto \mathsf{S}(\mathsf{t}+\mathsf{u}) \qquad 0+\mathsf{t} \longmapsto \mathsf{t} \qquad \mathsf{S}(\mathsf{u})+\mathsf{t} \longmapsto \mathsf{S}(\mathsf{t}+\mathsf{u})$$

$$\mathcal{E} = \qquad \mathsf{t}+\mathsf{u} \approx \mathsf{u}+\mathsf{t} \qquad (\mathsf{t}+\mathsf{u})+\mathsf{v} \approx \mathsf{t}+(\mathsf{u}+\mathsf{v})$$

1. $\mathcal{R} \cup \mathcal{S}$ is left-linear ✓
2. For all $t \approx u \in \mathcal{E}$, we have t, u linear, headed by symbols, and $\mathrm{mv}(t) = \mathrm{mv}(u)$[3] ✓
3. $\mathcal{R}$ is confluent ✓

   Because $\mathcal{R}$ is orthogonal
4. $(\mathcal{S}, \mathcal{E})$ is strong CR modulo

[3]Therefore, $\mathcal{E}^{\pm} := \mathcal{E} \cup \mathcal{E}^{-1}$ is a left-linear rewrite system

The 2nd Criterion

$$\mathcal{R} = \quad @(\lambda(x.\mathsf{t}\{x\}), \mathsf{u}) \longmapsto \mathsf{t}\{\mathsf{u}\} \qquad \mathbb{N}_{\mathsf{rec}}(0, \mathsf{p}, xy.\mathsf{q}\{x, y\}) \longmapsto \mathsf{p}$$

$$\mathbb{N}_{\mathsf{rec}}(\mathsf{S}(\mathsf{n}), \mathsf{p}, xy.\mathsf{q}\{x, y\}) \longmapsto \mathsf{q}\{\mathsf{n}, \mathbb{N}_{\mathsf{rec}}(\mathsf{n}, \mathsf{p}, xy.\mathsf{q}\{x, y\})\}$$

$$\mathcal{S} = \quad \mathsf{t} + 0 \longmapsto \mathsf{t} \qquad \mathsf{t} + \mathsf{S}(\mathsf{u}) \longmapsto \mathsf{S}(\mathsf{t} + \mathsf{u}) \qquad 0 + \mathsf{t} \longmapsto \mathsf{t} \qquad \mathsf{S}(\mathsf{u}) + \mathsf{t} \longmapsto \mathsf{S}(\mathsf{t} + \mathsf{u})$$

$$\mathcal{E} = \quad \mathsf{t} + \mathsf{u} \approx \mathsf{u} + \mathsf{t} \qquad (\mathsf{t} + \mathsf{u}) + \mathsf{v} \approx \mathsf{t} + (\mathsf{u} + \mathsf{v})$$

1. $\mathcal{R} \cup \mathcal{S}$ is left-linear ✓
2. For all $t \approx u \in \mathcal{E}$, we have t, u linear, headed by symbols, and $\mathrm{mv}(t) = \mathrm{mv}(u)$[3] ✓
3. $\mathcal{R}$ is confluent ✓

   Because $\mathcal{R}$ is orthogonal
4. $(\mathcal{S}, \mathcal{E})$ is strong CR modulo ✓

   Follows by a criterion by Nipkow, because $\simeq \circ \longrightarrow_{\mathcal{S}}$ is SN and all critical pairs close modulo $\simeq$

[3] Therefore, $\mathcal{E}^{\pm} := \mathcal{E} \cup \mathcal{E}^{-1}$ is a left-linear rewrite system

The 2nd Criterion

$$\mathcal{R} = \quad @(\lambda(x.\mathsf{t}\{x\}), \mathsf{u}) \longmapsto \mathsf{t}\{\mathsf{u}\} \qquad \mathbb{N}_{\mathsf{rec}}(0, \mathsf{p}, xy.\mathsf{q}\{x, y\}) \longmapsto \mathsf{p}$$

$$\mathbb{N}_{\mathsf{rec}}(\mathsf{S}(\mathsf{n}), \mathsf{p}, xy.\mathsf{q}\{x, y\}) \longmapsto \mathsf{q}\{\mathsf{n}, \mathbb{N}_{\mathsf{rec}}(\mathsf{n}, \mathsf{p}, xy.\mathsf{q}\{x, y\})\}$$

$$\mathcal{S} = \quad \mathsf{t} + 0 \longmapsto \mathsf{t} \qquad \mathsf{t} + \mathsf{S}(\mathsf{u}) \longmapsto \mathsf{S}(\mathsf{t} + \mathsf{u}) \qquad 0 + \mathsf{t} \longmapsto \mathsf{t} \qquad \mathsf{S}(\mathsf{u}) + \mathsf{t} \longmapsto \mathsf{S}(\mathsf{t} + \mathsf{u})$$

$$\mathcal{E} = \quad \mathsf{t} + \mathsf{u} \approx \mathsf{u} + \mathsf{t} \qquad (\mathsf{t} + \mathsf{u}) + \mathsf{v} \approx \mathsf{t} + (\mathsf{u} + \mathsf{v})$$

1. $\mathcal{R} \cup \mathcal{S}$ is left-linear ✓
2. For all $t \approx u \in \mathcal{E}$, we have t, u linear, headed by symbols, and $\mathrm{mv}(t) = \mathrm{mv}(u)$[3] ✓
3. $\mathcal{R}$ is confluent ✓

   Because $\mathcal{R}$ is orthogonal
4. $(\mathcal{S}, \mathcal{E})$ is strong CR modulo ✓

   Follows by a criterion by Nipkow, because $\simeq \circ \longrightarrow_{\mathcal{S}}$ is SN and all critical pairs close modulo $\simeq$
5. No critical pairs between $\mathcal{R}$ and $\mathcal{S} \cup \mathcal{E}^{\pm}$

[3] Therefore, $\mathcal{E}^{\pm} := \mathcal{E} \cup \mathcal{E}^{-1}$ is a left-linear rewrite system

The 2nd Criterion

$$\mathcal{R} = \qquad @(\lambda(x.\mathsf{t}\{x\}),\mathsf{u}) \longmapsto \mathsf{t}\{\mathsf{u}\} \qquad \mathbb{N}_{\mathsf{rec}}(0,\mathsf{p},xy.\mathsf{q}\{x,y\}) \longmapsto \mathsf{p}$$

$$\mathbb{N}_{\mathsf{rec}}(\mathsf{S}(\mathsf{n}),\mathsf{p},xy.\mathsf{q}\{x,y\}) \longmapsto \mathsf{q}\{\mathsf{n},\mathbb{N}_{\mathsf{rec}}(\mathsf{n},\mathsf{p},xy.\mathsf{q}\{x,y\})\}$$

$$\mathcal{S} = \qquad \mathsf{t}+0 \longmapsto \mathsf{t} \qquad \mathsf{t}+\mathsf{S}(\mathsf{u}) \longmapsto \mathsf{S}(\mathsf{t}+\mathsf{u}) \qquad 0+\mathsf{t} \longmapsto \mathsf{t} \qquad \mathsf{S}(\mathsf{u})+\mathsf{t} \longmapsto \mathsf{S}(\mathsf{t}+\mathsf{u})$$

$$\mathcal{E} = \qquad \mathsf{t}+\mathsf{u} \approx \mathsf{u}+\mathsf{t} \qquad (\mathsf{t}+\mathsf{u})+\mathsf{v} \approx \mathsf{t}+(\mathsf{u}+\mathsf{v})$$

1. $\mathcal{R} \cup \mathcal{S}$ is left-linear ✓
2. For all $t \approx u \in \mathcal{E}$, we have t, u linear, headed by symbols, and $\mathrm{mv}(t) = \mathrm{mv}(u)$[3] ✓
3. $\mathcal{R}$ is confluent ✓

   Because $\mathcal{R}$ is orthogonal
4. $(\mathcal{S},\mathcal{E})$ is strong CR modulo ✓

   Follows by a criterion by Nipkow, because $\simeq \circ \longrightarrow_{\mathcal{S}}$ is SN and all critical pairs close modulo $\simeq$
5. No critical pairs between $\mathcal{R}$ and $\mathcal{S} \cup \mathcal{E}^{\pm}$ ✓

---

[3]Therefore, $\mathcal{E}^{\pm} := \mathcal{E} \cup \mathcal{E}^{-1}$ is a left-linear rewrite system

The 2nd Criterion

Criterion 2 Let $(\mathcal{R} \cup \mathcal{S}, \mathcal{E})$ be a second-order rewrite system modulo st

1. $\mathcal{R} \cup \mathcal{S}$ is left-linear
2. For all $t \approx u \in \mathcal{E}$, we have t, u linear, headed by symbols, and $\mathrm{mv}(t) = \mathrm{mv}(u)$
3. $\mathcal{R}$ is confluent
4. $(\mathcal{S}, \mathcal{E})$ is strong CR modulo
5. No critical pairs between $\mathcal{R}$ and $\mathcal{S} \cup \mathcal{E}^{\pm}$

   Where $\mathcal{E}^{\pm} := \mathcal{E} \cup \mathcal{E}^{-1}$

The 2nd Criterion

Criterion 2 Let $(\mathcal{R} \cup \mathcal{S}, \mathcal{E})$ be a second-order rewrite system modulo st

1. $\mathcal{R} \cup \mathcal{S}$ is left-linear
2. For all $t \approx u \in \mathcal{E}$, we have t, u linear, headed by symbols, and $\mathrm{mv}(t) = \mathrm{mv}(u)$
3. $\mathcal{R}$ is confluent
4. $(\mathcal{S}, \mathcal{E})$ is strong CR modulo
5. No critical pairs between $\mathcal{R}$ and $\mathcal{S} \cup \mathcal{E}^{\pm}$

   Where $\mathcal{E}^{\pm} := \mathcal{E} \cup \mathcal{E}^{-1}$

Then $(\mathcal{R} \cup \mathcal{S}, \mathcal{E})$ is strong CR modulo

The 2nd Criterion

Criterion 2 Let $(\mathcal{R} \cup \mathcal{S}, \mathcal{E})$ be a second-order rewrite system modulo st

1. $\mathcal{R} \cup \mathcal{S}$ is left-linear
2. For all $t \approx u \in \mathcal{E}$, we have t, u linear, headed by symbols, and $\mathrm{mv}(t) = \mathrm{mv}(u)$
3. $\mathcal{R}$ is confluent
4. $(\mathcal{S}, \mathcal{E})$ is strong CR modulo
5. No critical pairs between $\mathcal{R}$ and $\mathcal{S} \cup \mathcal{E}^{\pm}$

   Where $\mathcal{E}^{\pm} := \mathcal{E} \cup \mathcal{E}^{-1}$

Then $(\mathcal{R} \cup \mathcal{S}, \mathcal{E})$ is strong CR modulo

Therefore, we still need to show the subsystem $(\mathcal{S}, \mathcal{E})$ to be strong CR modulo
The point is that $(\mathcal{S}, \mathcal{E})$ might be terminating, allowing application of other criteria

The proof idea

The main tool for proving the criterion is the following well-known result:

Proposition If $\mathcal{R}$ and $\mathcal{S}$ are left-linear Pattern Rewrite Systems (PRSs) with no critical pairs between them, then they commute

The proof idea

The main tool for proving the criterion is the following well-known result:

Proposition If $\mathcal{R}$ and $\mathcal{S}$ are left-linear Pattern Rewrite Systems (PRSs) with no critical pairs between them, then they commute

Locally proven in the proof of a theorem by Van Oostrom and Van Raamsdonk
Can also be easily shown by adapting proof of confluence by orthogonality

The proof idea

The main tool for proving the criterion is the following well-known result:

Proposition If $\mathcal{R}$ and $\mathcal{S}$ are left-linear Pattern Rewrite Systems (PRSs) with no critical pairs between them, then they commute

Locally proven in the proof of a theorem by Van Oostrom and Van Raamsdonk
Can also be easily shown by adapting proof of confluence by orthogonality

Proof idea for Criterion 2 We know that that $(\mathcal{S}, \mathcal{E})$ is strong CR modulo

$\mathcal{R}$ commutes with $\mathcal{E}^{\pm}$ and $\mathcal{S}$ by the above result, and with itself by confluence

We conclude with some easy diagram manipulations

Conclusion

Conclusion

We have seen two criteria for CR modulo:

Conclusion

We have seen two criteria for CR modulo:

- **Criterion 1** Weak CR modulo but replaces matching modulo by unblocking

Conclusion

We have seen two criteria for CR modulo:

- **Criterion 1** Weak CR modulo but replaces matching modulo by unblocking
- **Criterion 2** Strong CR modulo

  Easy consequence of a known result, maybe not original?

Conclusion

We have seen two criteria for CR modulo:

- **Criterion 1** Weak CR modulo but replaces matching modulo by unblocking
- **Criterion 2** Strong CR modulo

  Easy consequence of a known result, maybe not original?

Both address our initial motivation: How to show CR modulo for dependent type theories?

Conclusion

We have seen two criteria for CR modulo:

- **Criterion 1** Weak CR modulo but replaces matching modulo by unblocking
- **Criterion 2** Strong CR modulo

  Easy consequence of a known result, maybe not original?

Both address our initial motivation: How to show CR modulo for dependent type theories?

Main limitations Linearity and left-linearity, cannot have $\mathtt{t} \sqcup \mathtt{t} \approx \mathtt{t}$

Unclear how to do without in second-order rewriting, because of Klop's countexample

Conclusion

We have seen two criteria for CR modulo:

- **Criterion 1** Weak CR modulo but replaces matching modulo by unblocking
- **Criterion 2** Strong CR modulo

  Easy consequence of a known result, maybe not original?

Both address our initial motivation: How to show CR modulo for dependent type theories?

Main limitations Linearity and left-linearity, cannot have $\mathtt{t} \sqcup \mathtt{t} \approx \mathtt{t}$

Unclear how to do without in second-order rewriting, because of Klop's countexample

Future work

- Dedukti with rewriting modulo

Conclusion

We have seen two criteria for CR modulo:

- **Criterion 1** Weak CR modulo but replaces matching modulo by unblocking
- **Criterion 2** Strong CR modulo

  Easy consequence of a known result, maybe not original?

Both address our initial motivation: How to show CR modulo for dependent type theories?

Main limitations Linearity and left-linearity, cannot have $\mathtt{t} \sqcup \mathtt{t} \approx \mathtt{t}$

Unclear how to do without in second-order rewriting, because of Klop's countexample

Future work

- Dedukti with rewriting modulo
- And why not Agda and Coq with rewriting modulo? We have the tools do to it!

Conclusion

We have seen two criteria for CR modulo:

- **Criterion 1** Weak CR modulo but replaces matching modulo by unblocking
- **Criterion 2** Strong CR modulo

  Easy consequence of a known result, maybe not original?

Both address our initial motivation: How to show CR modulo for dependent type theories?

Main limitations Linearity and left-linearity, cannot have $\mathtt{t} \sqcup \mathtt{t} \approx \mathtt{t}$

Unclear how to do without in second-order rewriting, because of Klop's countexample

Future work

- Dedukti with rewriting modulo
- And why not Agda and Coq with rewriting modulo? We have the tools do to it!

Thank you for your attention!