Multi-focusing on extensional rewriting with sums (introduction)

Gabriel Scherer

Gallium – INRIA

March 14, 2014
... but why?

Current research topic: does a given type have a unique inhabitant (modulo program equivalence)?
... but why?

Current research topic: does a given type have a **unique** inhabitant (modulo program equivalence)?

\[
(\lambda(x)\; t)\; u \rightarrow_{\beta} t[u/x] \quad \quad \quad (t : A \rightarrow B) =_{\eta} \lambda(x)\; t \; x
\]

\[
\pi_i\; (t_1, t_2) \rightarrow_{\beta} t_i \quad \quad \quad (t : A \ast B) =_{\eta} (\pi_1 \; t, \pi_2 \; t)
\]
... but why?

Current research topic: does a given type have a **unique** inhabitant (modulo program equivalence)?

\[(\lambda(x) \, t) \, u \rightarrow_{\beta} t[u/x] \quad (t : A \rightarrow B) =_{\eta} \lambda(x) \, t \, x\]

\[\pi_i (t_1, t_2) \rightarrow_{\beta} t_i \quad (t : A \times B) =_{\eta} (\pi_1 \, t, \pi_2 \, t)\]

\[\delta(\sigma_i \, t, x_1.u_1, x_2.u_2) \rightarrow_{\beta} u_i[t/x_i]\]

\[(t : A + B) =_{\eta} \delta(t, x_1.\sigma_1 \, x_1, x_2.\sigma_2 \, x_2)\]
... but why?

Current research topic: does a given type have a unique inhabitant (modulo program equivalence)?

\[(\lambda(x)\ t)\ u \rightarrow_{\beta} t[u/x] \quad (t : A \rightarrow B) =_{\eta} \lambda(x)\ t\ x\]

\[\pi_i (t_1, t_2) \rightarrow_{\beta} t_i \quad (t : A \times B) =_{\eta} (\pi_1\ t, \pi_2\ t)\]

\[\delta(\sigma_i\ t, x_1.u_1, x_2.u_2) \rightarrow_{\beta} u_i[t/x_i]\]

\[(t : A + B) =_{\eta} \delta(t, x_1.\sigma_1\ x_1, x_2.\sigma_2\ x_2)\]

\[(t, u) ?= \delta(t, x_1.(\sigma_1\ x_1, u), x_2.(\sigma_2\ x_2, u))\]
... but why?

Current research topic: does a given type have a **unique** inhabitant (modulo program equivalence)?

\[(\lambda(x) t) \ u \to_{\beta} t[u/x] \quad (t : A \to B) =_{\eta} \lambda(x) t \ x\]

\[\pi_i (t_1, t_2) \to_{\beta} t_i \quad (t : A * B) =_{\eta} (\pi_1 t, \pi_2 t)\]

\[\delta(\sigma_i t, x_1.u_1, x_2.u_2) \to_{\beta} u_i[t/x_i]\]

\[(t : A + B) =_{\eta} \delta(t, x_1.\sigma_1 x_1, x_2.\sigma_2 x_2)\]

\[(t, u) ?= \delta(t, x_1.(\sigma_1 x_1, u), x_2.(\sigma_2 x_2, u)) \quad K = (\Box, u)\]
... but why?

Current research topic: does a given type have a unique inhabitant (modulo program equivalence)?

\[(\lambda(x) \, t) \, u \rightarrow_{\beta} \, t[u/x] \quad (t : A \rightarrow B) =_{\eta} \lambda(x) \, t \, x\]

\[\pi_i \,(t_1, t_2) \rightarrow_{\beta} \, t_i \quad (t : A \times B) =_{\eta} \,(\pi_1 \, t, \pi_2 \, t)\]

\[\delta(\sigma_i \, t, x_1.\, u_1, x_2.\, u_2) \rightarrow_{\beta} \, u_i[t/x_i]\]

\[\forall (K[A_1 + A_2] : B), \quad K[t] =_{\eta} \delta(t, x_1.\, K[\sigma_1 \, x_1], x_2.\, K[\sigma_2 \, x_2])\]
... but why?

Current research topic: does a given type have a **unique** inhabitant (modulo program equivalence)?

\[
(\lambda(x) \ t) \ u \rightarrow_{\beta} t[u/x] \quad (t : A \rightarrow B) =_{\eta} \lambda(x) \ t \ x
\]

\[
\pi_i (t_1, t_2) \rightarrow_{\beta} t_i \quad (t : A \ast B) =_{\eta} (\pi_1 \ t, \pi_2 \ t)
\]

\[
\delta(\sigma_i \ t, x_1.u_1, x_2.u_2) \rightarrow_{\beta} u_i[t/x_i]
\]

\[
\forall(K[A_1 + A_2] : B), \quad K[t] =_{\eta} \delta(t, x_1.K[\sigma_1 x_1], x_2.K[\sigma_2 x_2])
\]

- Sum equivalence looks hard. Can we implement it?
- Are there representations of programs (proofs) that quotient over those equivalences?
My paper in one slide

The equivalence algorithm of

Sam Lindley.  
Extentional rewriting with sums.  

and the normalization of proof representations in

Kaustuv Chaudhuri, Dale Miller, and Alexis Saurin.  
Canonical sequent proofs via multi-focusing.  

are doing (almost) the same thing  
– and we had not noticed.
In this talk

Sam Lindley’s rewriting-based algorithm is the first simple solution (first solution: Neil Ghani, 1995) to deciding sum equivalences.

It’s easy to understand and follow. But to me it felt a bit arbitrary.

On the other hand, (multi-)focusing is beautiful, but requires some background knowledge.

Providing it is the purpose of this talk.
Sequent calculus
(Can be done in natural deduction, but less regular)

\[
\begin{align*}
\Gamma \vdash A & \quad \Gamma, B \vdash C \\
\frac{}{\Gamma, A \rightarrow B \vdash C} & - \\
\Gamma, A \vdash B & \\
\frac{}{\Gamma \vdash A \rightarrow B} & \\
\Gamma, A_i \vdash C & \\
\frac{}{\Gamma, A_1 \ast A_2 \vdash C} & - \\
\Gamma \vdash A_1 & \quad \Gamma \vdash A_2 \\
\frac{}{\Gamma \vdash A_1 \ast A_2} & \\
\Gamma, A_1 \vdash C & \quad \Gamma, A_2 \vdash C \\
\frac{}{\Gamma, A_1 + A_2 \vdash C} & \\
\Gamma \vdash A_i & \\
\frac{}{\Gamma \vdash A_1 + A_2} & +
\end{align*}
\]

Inversible vs. non-inversible rules.
Negatives (interesting on the left): products, arrow, atoms.
Positives (interesting on the right): sum, atoms (or products).
Inversible phase

If applied too early, non-inversible rules can ruin your proof.
Inversible phase

If applied too early, non-inversible rules can ruin your proof.

Focusing restriction 1: inversible phases

Inversible rules must be applied as soon and as long as possible – and their order does not matter.
Inversible phase

\[
\begin{align*}
? & \quad \frac{X + Y \vdash X}{X + Y \vdash X + Y}
\end{align*}
\]

If applied too early, non-inversible rules can ruin your proof.

**Focusing restriction 1: inversible phases**

Inversible rules must be applied as soon and as long as possible – and their order does not matter.

Imposing this restriction gives a single proof of \((X \rightarrow Y) \rightarrow (X \rightarrow Y)\) instead of two \((\lambda(f)f)\) and \((\lambda(f)\lambda(x)f\ x)).\)
Non-inversible phases

After all inversible rules, $\Gamma_n \vdash A_p$

Only step forward: select a formula, apply some non-inversible rules on it.
Non-inversible phases

After all inversible rules, $\Gamma_n \vdash A_p$

Only step forward: select a formula, apply some non-inversible rules on it.

**Focusing restriction 2: non-inversible phase**

When a principal formula is selected for non-inversible rule, they should be applied as long as possible – until its polarity changes.
Non-inversible phases

After all inversible rules, $\Gamma_n \vdash A_p$

Only step forward: select a formula, apply some non-inversible rules on it.

Focusing restriction 2: non-inversible phase

When a principal formula is selected for non-inversible rule, they should be applied as long as possible – until its polarity changes.

Completeness: this restriction preserves provability. Non-trivial!

Example of removed redundancy:

$$
\frac{X_2, \quad Y_1 \vdash A}{X_2 \ast X_3, \quad Y_1 \vdash A}
\frac{X_2 \ast X_3, \quad Y_1 \ast Y_2 \vdash A}{X_1 \ast X_2 \ast X_3, \quad Y_1 \ast Y_2 \vdash A}
$$
This was focusing

Focused proofs are structured in alternating phases, inversible (boring) and non-inversible (focus).

Phases are forced to be as long as possible – to eliminate duplicate proofs.

The idea is independent from the proof system. Applies to sequent calculus or natural deduction; intuitionistic, classical, linear, you-name-it logic.

On proof terms, these restrictions correspond to $\beta\eta$-normal forms (for products and arrows only). But the fun is in the search.
Demo Time

\[ \vdash (1 \rightarrow X \rightarrow (Y + Z)) \rightarrow X \rightarrow (Y \rightarrow W) \rightarrow (Z + W) \]

inversible rules
Demo Time

\[(1 \rightarrow X \rightarrow (Y + Z)) \vdash X \rightarrow (Y \rightarrow W) \rightarrow (Z + W)\]

inversible rules
Demo Time

\[(1 \to X \to (Y + Z)), \quad X \vdash (Y \to W) \to (Z + W)\]

inversible rules
Demo Time

\[
(1 \rightarrow X \rightarrow (Y + Z)), \quad X, \ Y \rightarrow W \vdash Z + W
\]

inversible rules
Demo Time

\[
(1 \rightarrow X \rightarrow (Y + Z)), \quad X, \quad Y \rightarrow W \vdash Z + W
\]

choice of focus
Demo Time

\[
(1 \rightarrow X \rightarrow (Y + Z)), \quad X, \quad Y \rightarrow W \vdash Z + W
\]

choice of focus
(1 \rightarrow X \rightarrow (Y + Z)), \quad X, \quad Y \rightarrow W \quad \vdash \quad Z + W

non-inversible rules
Demo Time

\[
1 \rightarrow X \rightarrow (Y + Z), \quad X, \quad Y \rightarrow W \vdash Z + W
\]

non-inversible rules
Demo Time

\[
(1 \rightarrow X \rightarrow (Y + Z)), \quad X, \quad Y \rightarrow W \vdash Z + W
\]

inversible rules
Demo Time

\[ Y, Y \rightarrow W \vdash Z + W \quad Z \vdash Z + W \]

\[ (1 \rightarrow X \rightarrow (Y + Z)), \quad X, \quad Y \rightarrow W \vdash Z + W \]

inversible rules
Demo Time

\[
\begin{align*}
Y, Y \rightarrow W & \vdash Z + W \\
Z & \vdash Z + W \\
(1 \rightarrow X \rightarrow (Y + Z)), & \quad X, \quad Y \rightarrow W \vdash Z + W
\end{align*}
\]

choice of focus
\[
Y, Y \rightarrow W \vdash Z + W \\
Z \vdash Z + W
\]

\[\frac{(1 \rightarrow X \rightarrow (Y + Z)), \quad X, \quad Y \rightarrow W \vdash Z + W}{\text{conclusion}}\]
Restrictive syntax

So far we’ve defined **focused proofs** as a subset of proofs in our system. We can give them a syntax that enforces their structure.

\[
\begin{align*}
\Gamma, A \vdash C & \quad \Gamma, B \vdash C \\
\hline
\Gamma, A + B \vdash C
\end{align*}
\]

\[
\begin{align*}
\Gamma \vdash A & \quad \Gamma \vdash B \\
\hline
\Gamma \vdash A \times B
\end{align*}
\]

\[
\begin{align*}
\Gamma, A \vdash B \\
\hline
\Gamma \vdash A \to B
\end{align*}
\]
Restrictive syntax

So far we’ve defined focused proofs as a subset of proofs in our system. We can give them a syntax that enforces their structure.

\[
\begin{array}{c}
\Gamma, A \vdash C \quad \Gamma, B \vdash C \\
\hline
\Gamma, A + B \vdash C
\end{array}
\quad
\begin{array}{c}
\Gamma \vdash A \\
\hline
\Gamma \vdash A \times B
\end{array}
\quad
\begin{array}{c}
\Gamma, A \vdash B \\
\hline
\Gamma \vdash A \rightarrow B
\end{array}
\]

\(X\) atomic

\[
\Gamma_n, X \vdash X
\]
Restrictive syntax

So far we’ve defined **focused proofs** as a subset of proofs in our system. We can give them a syntax that enforces their structure.

\[
\begin{align*}
\Gamma, A \vdash C \quad \Gamma, B \vdash C & \quad \Gamma, A + B \vdash C \\
\Gamma \vdash A \quad \Gamma \vdash B & \quad \Gamma \vdash A \times B \\
\Gamma \vdash A \rightarrow B & \quad \Gamma, A \vdash B
\end{align*}
\]

\[
\begin{align*}
X \text{ atomic} & \quad \Gamma_{na}, [A_n] \vdash B_{pa} \\
\Gamma_{na}, X \vdash X & \quad \Gamma_{na}, A_n \vdash B_{pa} \\
& \quad \Gamma_{na} \vdash B_{pa}
\end{align*}
\]
Restrictive syntax

So far we’ve defined **focused proofs** as a subset of proofs in our system. We can give them a syntax that enforces their structure.

\[
\begin{align*}
\Gamma, A \vdash C & \quad \Gamma, B \vdash C \\
\hline
\Gamma, A + B \vdash C
\end{align*}
\]

\[
\begin{align*}
\Gamma \vdash A & \quad \Gamma \vdash B \\
\hline
\Gamma \vdash A \times B
\end{align*}
\]

\[
\begin{align*}
\Gamma, A \vdash B \\
\hline
\Gamma \vdash A \rightarrow B
\end{align*}
\]

\[
\begin{align*}
X \text{ atomic} \\
\hline
\Gamma_n, X \vdash X
\end{align*}
\]

\[
\begin{align*}
\Gamma_{na}, [A_n] \vdash B_{pa} \\
\hline
\Gamma_{na}, A_n \vdash B_{pa}
\end{align*}
\]

\[
\begin{align*}
\Gamma_{na} \vdash [B_{pa}] \\
\hline
\Gamma_{na} \vdash B_{pa}
\end{align*}
\]

\[
\begin{align*}
\Gamma \vdash [A_i] \\
\hline
\Gamma \vdash [A_1 + A_2]
\end{align*}
\]

\[
\begin{align*}
\Gamma, [A_i] \vdash B \\
\hline
\Gamma, [A_1 \times A_2] \vdash B
\end{align*}
\]

\[
\begin{align*}
\Gamma \vdash [A] & \quad \Gamma, [B] \vdash C \\
\hline
\Gamma, [A \rightarrow B] \vdash C
\end{align*}
\]
Restrictive syntax

So far we’ve defined **focused proofs** as a subset of proofs in our system. We can give them a syntax that enforces their structure.

\[
\begin{align*}
\Gamma, A \vdash C & \quad \Gamma, B \vdash C \\
\hline
\Gamma, A + B \vdash C
\end{align*}
\]

\[
\begin{align*}
\Gamma \vdash A & \quad \Gamma \vdash B \\
\hline
\Gamma \vdash A \times B
\end{align*}
\]

\[
\begin{align*}
\Gamma, A \vdash B \\
\hline
\Gamma \vdash A \rightarrow B
\end{align*}
\]

\[
\begin{align*}
X \text{ atomic} & \\
\hline
\Gamma_n, X \vdash X
\end{align*}
\]

\[
\begin{align*}
\Gamma_n, [A_n] \vdash B_{pa} \\
\hline
\Gamma_n, A_n \vdash B_{pa}
\end{align*}
\]

\[
\begin{align*}
\Gamma_n \vdash [B_{pa}] \\
\hline
\Gamma_n \vdash B_{pa}
\end{align*}
\]

\[
\begin{align*}
\Gamma \vdash [A_i] & \\
\hline
\Gamma \vdash [A_1 + A_2]
\end{align*}
\]

\[
\begin{align*}
\Gamma, [A_i] \vdash B \\
\hline
\Gamma, [A_1 \times A_2] \vdash B
\end{align*}
\]

\[
\begin{align*}
\Gamma \vdash [A] & \quad \Gamma, [B] \vdash C \\
\hline
\Gamma, [A \rightarrow B] \vdash C
\end{align*}
\]

\[
\begin{align*}
\Gamma, A_{pa} \vdash B & \\
\hline
\Gamma, [A_{pa}] \vdash B
\end{align*}
\]

\[
\begin{align*}
\Gamma \vdash B_{na} \\
\hline
\Gamma \vdash [B_{na}]
\end{align*}
\]
Success stories

Focusing was introduced by Andreoli in 1992. Revolution in logic programming.

Forward-chaining and backward-chaining expressed in a single system by assigning polarities to atoms.

Synthetic connectives: state-of-the-art automated theorem proving for non-classical logics (+ Jumbo connectives, Paul Blain Levy, 2006)

Lazy vs. strict evaluation (Zeilberger 2008)

A sequent calculus with cut-free search bisimilar to DPLL (Lengrand, 2013).
This is not the end

\[(X + X) \rightarrow X\]

\[(1 \rightarrow (X + X)) \rightarrow X\]

\[\lambda(f) \delta(f 1, x_1.x_1, x_1.x_1)\]

\[\lambda(f) \delta(f 1, x_1.\delta(f 1, x_2.x_2, x_2.x_2), x_1.x_1)\]

\[\lambda(f) \delta(f 1, x_1.x_1, x_1.\delta(f 1, x_2.x_1, x_2.x_2))\]

\[\ldots\]
Multi-focusing

Sometimes several independent foci are possible to make progress in a proof.

Multi-focusing (Miller and Saurin, 2007): do them all at once, in parallel.
Maximal multi-focusing

Given a focused proof, it is possible to put focused sequences in parallel to exhibit some parallelism – without changing the operational meaning of the proof, seen as a pure program.

Does there exists a maximally parallel multi-focused proof?
Maximal multi-focusing

Given a focused proof, it is possible to put focused sequences in parallel to exhibit some parallelism – without changing the operational meaning of the proof, seen as a pure program.

Does there exists a maximally parallel multi-focused proof?

Yes. (In the good logics)
Maximal multi-focusing

Given a focused proof, it is possible to put focused sequences in parallel to exhibit some parallelism – without changing the operational meaning of the proof, seen as a pure program.

Does there exist a maximally parallel multi-focused proof?

Yes. (In the good logics)

Maximally multi-focusing is a powerful notion of canonical structure for proof.

- linear logic: proof nets (Chaudhuri, Miller, Saurin, 2008)
- first-order classical logic: expansion proofs (Chaudhuri, Hetzl, Miller, 2013)

“Evolution rather than revolution” (Dale Miller)
Computing a maximal proof

Preemptive rewriting temporarily breaks the focused structure to move foci as far down as possible.
Computing a maximal proof

**Preemptive** rewriting temporarily breaks the focused structure to move foci as far down as possible.

\[
\begin{align*}
\left\{ \begin{array}{l}
I_3 \\
NI_3 \\
I_2 \\
NI_2 \\
I_1 \\
NI_1
\end{array} \right\} & \rightarrow^* & \left\{ \begin{array}{l}
I_2 \\
NI_2 \\
I_1 \\
NI_1
\end{array} \right\} \\
I_3 & & NI_3; (I_2)
\end{align*}
\]

? \[
\left\{ \begin{array}{l}
I_2 \\
NI_2 \\
I_1 \\
I_3 \\
NI_1 \\
NI_3
\end{array} \right\}
\]
Computing a maximal proof

**Preemptive** rewriting temporarily breaks the focused structure to move foci as far down as possible.

\[
\begin{array}{c}
\{ \begin{array}{c}
I_3 \\
NI_3
\end{array} \} \\
\{ \begin{array}{c}
I_2 \\
NI_2 \\
I_1 \\
NI_1
\end{array} \} \\
\rightarrow^* \\
\{ \begin{array}{c}
I_2 \\
NI_2 \\
I_1 \\
NI_1
\end{array} \} \\
\rightarrow^* \\
\{ \begin{array}{c}
I_2 \\
NI_2 \\
I_1 \\
NI_1
\end{array} \} \\
\rightarrow^* \\
\{ \begin{array}{c}
I_2 \\
NI_2 \\
I_1 \\
NI_1
\end{array} \}
\end{array}
\]
Computing a maximal proof

**Preemptive** rewriting temporarily breaks the focused structure to move foci as far down as possible.

\[
\begin{align*}
&\{ \begin{array}{c} I_3 \\ NI_3 \\ I_2 \\ NI_2 \\ I_1 \\ NI_1 \end{array} \} \\
&\Rightarrow^* \\
&\{ \begin{array}{c} I_2 \\ NI_2 \\ I_1 \\ NI_1 \end{array} \}
\end{align*}
\]

\[
\begin{align*}
&\Rightarrow^* \\
&\{ \begin{array}{c} I_2 \\ NI_2; (I_3) \\ I_1 \\ NI_3; (I_1) \end{array} \}
\end{align*}
\]

This is the heart of the correspondence with Sam Lindley's work.
Computing a maximal proof

Preemptive rewriting temporarily breaks the focused structure to move foci as far down as possible.

\[
\begin{align*}
\left\{ \begin{array}{c}
I_3 \\
NI_3 \\
I_2 \\
NI_2 \\
I_1 \\
NI_1
\end{array} \right\} & \rightarrow^* \left\{ \begin{array}{c}
I_3 \\
NI_3; (I_2)
\end{array} \right\} & \rightarrow^* \left\{ \begin{array}{c}
I_2 \\
NI_2 \\
I_1 \\
NI_1
\end{array} \right\} \\
\rightarrow^* \left\{ \begin{array}{c}
I_2 \\
NI_2; (I_3) \\
I_1 \\
NI_3; (I_1)
\end{array} \right\} & \rightarrow^* \left\{ \begin{array}{c}
I_2 \\
NI_2; (I_3) \\
I_1 \\
NI_1
\end{array} \right\} & \rightarrow^* \left\{ \begin{array}{c}
I_2 \\
NI_2 \\
I_1 \\
NI_1 \\
I_3
\end{array} \right\}
\end{align*}
\]
Computing a maximal proof

Preemptive rewriting temporarily breaks the focused structure to move foci as far down as possible.

\[
\begin{align*}
\{ & \begin{array}{c} I_3 \\ NI_3 \\
 I_2 \\
 NI_2 \\
 I_1 \\
 NI_1 \\
\end{array} \} \rightarrow^* \{ & \begin{array}{c} I_2 \\
 NI_2 \\
 I_1 \\
 NI_1 \\
\end{array} \} \rightarrow^* \{ & \begin{array}{c} I_2 \\
 NI_2 \\
 I_1 \\
 NI_1 \\
\end{array} \} \\
\rightarrow^* \{ & \begin{array}{c} I_2 \\
 NI_2; (I_3) \\
 I_1 \\
 NI_3; (I_1) \\
\end{array} \} \rightarrow^* \{ & \begin{array}{c} I_2 \\
 NI_2; (I_3) \\
 I_1 \\
 NI_1 \\
\end{array} \} \rightarrow^* \{ & \begin{array}{c} I_2 \\
 NI_2 \\
 I_1 \\
 NI_1 \\
\end{array} \} \\
\end{align*}
\]
Computing a maximal proof

**Preemptive** rewriting temporarily breaks the focused structure to move foci as far down as possible.

This is the heart of the correspondence with Sam Lindley’s work
Contribution conclusion


\[
\text{let } \bar{x} = \bar{n} \text{ in } p^? t
\]

? \[\xrightarrow{?} \text{Mf. } \lambda\text{-calculus terms} \]

let-subst \[\xrightarrow{} \lambda\text{-calculus (Lindley)}\]