Church-Rosser Theorem for sequent lambda calculi

Silvia Ghilezan, Jelena Ivetić, Silvia Likavec

University of Novi Sad
University of Turin

TYPES 2014
Paris, May 2014.

Outline

- **Subject**: untyped intuitionistic sequent lambda calculus - λ^{Gtz}, which is known to be non-confluent;
- **Goal**: to obtain confluence by restrictions on the syntax and operational semantics;
- **Results**:
  - two confluent subcalculi are obtained;
  - their mutual relation and relation with both λ and λ^{Gtz} is discussed;
  - a direct proof of confluence is developed.

Logic and λ

"In the beginning Gentzen created natural deduction, but then He switched to sequent calculus in order to sort out the meta-theory", A.Felty, A. Momigliano, B. Pientka, TYPES 2014.

Curry-Howard

match	ND	λ
	introduction	abstraction
	elimination	application

mismatch	SC	λ
	right introduction	abstraction
	left introduction	application and substitution
	cut	substitution

Paradise of sequent lambda calculi

1994 - present

- H. Herbelin
- R. Dyckhoff and L. Pinto
- J. Espírito Santo and R. Matthes
- and others

$\overline{\lambda}$, λLJ, λ_T, λ_Q, λJ, λ^{Gtz}, among others

1970 - 1994

Pottinger, Zucker, Gallier, Mints, Barendregt and G. and other attempts.

λ^{Gtz}

The syntax:

$$\begin{array}{lrcl} \text{(Terms)} & t & ::= & x \,|\, \lambda x.t \,|\, tk \\ \text{(Contexts)} & k & ::= & \widehat{x}.t \,|\, t :: k \end{array}$$

- proposed by Espírito Santo;
- term: a variable, an abstraction or an application (*cut*);
- context: a selection $\widehat{x}.t$ or a context constructor (*cons*) $t :: k$;
- expression: terms and contexts are together referred to as expressions, denoted by e;
- tk captures the right associativity of the applications - one of the key differences between the sequent-based and natural deduction-based term calculi.

Operational semantics

Reduction rules:

$$\begin{array}{lrcl} (\beta) & (\lambda x.t)(u :: k) & \to & u(\widehat{x}.tk) \\ (\sigma) & t(\widehat{x}.u) & \to & u[t/x] \\ (\pi) & (tk)k' & \to & t(k@k') \\ (\mu) & \widehat{x}.xk & \to & k, \text{ if } x \notin k. \end{array}$$

- meta-operators: substitution $v[t/x]$ and append $k@k'$:

$$(u :: k)@k' = u :: (k@k') \qquad (\widehat{x}.t)@k' = \widehat{x}.tk'.$$

- possibility of delayed substitution:
  (β) creates a substitution, (σ) executes it;
- $(\beta) + (\sigma) + (\pi) =$ cut-elimination

Normal forms:

$$\begin{array}{lrcl} \text{(Terms)} & t_{nf} & = & x_{nf} \mid \lambda x.t_{nf} \mid x(t_{nf} :: k_{nf}) \\ \text{(Contexts)} & k_{nf} & = & \widehat{x}.t_{nf} \mid t_{nf} :: k_{nf}. \end{array}$$

Properties of λ^{Gtz}

- λ^{Gtz} satisfies:
  - subject reduction and strong normalisation of the simply typed version,
  - characterisation of strong normalisation of the system with intersection types,
  - preservation of β-SN, etc...
- it does not enjoy confluence, unlike majority of intuitionistic formal calculi;
- a critical pair exists between reductions (π) and (σ);
- analogous to the CBN / CBV dilemma of Curien-Herbelin's $\bar{\lambda}\mu\tilde{\mu}$-calculus.

An example

Terms of the form $(tk)(\widehat{x}.u)$ are both π-redexes and σ-redexes. For example, consider the term $(z(u :: \widehat{w}.w))(\widehat{x}.y)$.
the call-by-value option:

$$\begin{array}{lcl} (z(u :: \widehat{w}.w))(\widehat{x}.y) & \to_{\pi} & z((u :: \widehat{w}.w)@(\widehat{x}.y)) \\ & \triangleq & z(u :: (\widehat{w}.w@(\widehat{x}.y))) \\ & \triangleq & z(u :: (\widehat{w}.w(\widehat{x}.y))) \\ & \to_{\mu} & z(u :: \widehat{x}.y). \end{array}$$

the call-by-name option:

$$\begin{array}{lcl} (z(u :: \widehat{w}.w))(\widehat{x}.y) & \to_{\sigma} & y[z(u :: \widehat{w}.w)/x] \\ & \triangleq & y. \end{array}$$

Obviously, obtained normal forms differ.

However, if we translate these two nf's to λ-calculus, using the mapping $|\ |:\Lambda^{\mathrm{Gtz}} \rightarrow \Lambda$, which is defined together with the auxiliary mapping $|\ |_{\mathrm{c}}:\Lambda_{C}^{\mathrm{Gtz}} \rightarrow (\Lambda \rightarrow \Lambda)$ in the following way:

$$\begin{array}{rcl} |x| & = & x \\ |\lambda x.t| & = & \lambda x.|t| \\ |tk| & = & |k|_{\mathrm{c}}(|t|) \\ \\ |\widehat{x}.t|_{\mathrm{c}}(M) & = & (\lambda x.|t|)M \\ |t :: k|_{\mathrm{c}}(M) & = & |k|_{\mathrm{c}}(M|t|) \end{array}$$

we get:

$$|z(u :: \widehat{x}.y)| = (\lambda x.y)(zu), \quad |y| = y.$$

It is easy to observe that $(\lambda x.y)(zu) \rightarrow y$.

Regaining confluence

Two possibilities:

- to enrich the operational semantics by adding a new reduction rule that would reduce terms like $z(u :: \widehat{x}.y)$ to y;
- to restrict the syntax and the reduction rules in order to prevent appearance of the critical pair.

We adopt the latter option, and propose two confluent λ^{Gtz}-subcalculi:

- a “call-by-value” subcalculus - λ_V^{Gtz};
- a “call-by-name” subcalculus - λ_N^{Gtz};

The λ_V^{Gtz}-calculus

The syntax:

$$\begin{array}{lrcl} \text{Values} & V & ::= & x \mid \lambda x.t \\ \text{Terms} & t & ::= & V \mid tk \\ \text{Contexts} & k & ::= & \widehat{x}.t \mid t :: k \end{array}$$

The reduction rules:

$$\begin{array}{rrcl} (\beta) & (\lambda x.t)(u :: k) & \to & u(\widehat{x}.tk) \\ (\sigma_V) & V(\widehat{x}.t) & \to & t[V/x] \\ (\pi) & (tk)k' & \to & t(k@k') \\ (\mu) & \widehat{x}.xk & \to & k, \text{ if } x \notin Fv(k). \end{array}$$

- a syntactic category of *values* (a subset of terms) is introduced;
- modified (σ) rule cannot be performed on $(tk)(\widehat{x}.v)$;
- this reduction system is forcing us to reduce the head of the cut to the value before substituting it instead of x in t - the essence of CBV.

The λ_N^{Gtz}-calculus

The syntax:

$$\begin{array}{lccl} \text{Terms} & t & ::= & x \mid \lambda x.t \mid tk \\ \text{Lists} & L & ::= & \widehat{x}.x \mid t :: L \\ \text{Contexts} & k & ::= & L \mid \widehat{x}.t \end{array}$$

The reduction rules:

$$\begin{array}{rrcl} (\beta_N) & (\lambda x.t)(u :: L) & \to & t[u/x]L \\ (\sigma) & t(\widehat{x}.u) & \to & u[t/x] \\ (\pi_N) & (tk)L & \to & t(k@L) \\ (\mu) & \widehat{x}.xk & \to & k, \text{ if } x \notin Fv(k). \end{array}$$

- a syntactic category of lists is introduced: a subset of contexts whose form is $t_1 :: (t_2 :: (... :: (t_n :: \widehat{x}.x)))$;
- modified (π_N) rule cannot be performed on $(tk)(\widehat{x}.u)$;
- modified (β_N) rule provides the implementation of CBN:

$$(\lambda x.t)(u :: L) \to_\beta u\widehat{x}.(tL) \to_\sigma (tL)[u/x] \triangleq t[u/x]L.$$

- there exists an asymmetry between the two introduced syntactic categories: values and lists;
- values simply denote variables and lambda abstractions, and together with applications constitute Λ_V^{Gtz}, the set of λ_V^{Gtz}-terms
- therefore:

$$\Lambda_V^{\mathrm{Gtz}} = \Lambda^{\mathrm{Gtz}}$$

- On the other hand, lists are defined $t :: L$ which is a restriction of $t :: k$;
- the λ^{Gtz}-expressions containing $t :: \widehat{x}.u$ with $u \neq x$ cannot be represent in the λ_N^{Gtz}-calculus;
- therefore:

$$\Lambda_N^{\mathrm{Gtz}} \subset \Lambda^{\mathrm{Gtz}}$$

Mapping from λ to λ_N^{Gtz}

However, the set Λ_N^{Gtz} is still large enough!
All λ-terms can be to embed by the mapping:

$$\lfloor\ \rfloor : \Lambda \to \Lambda_N^{Gtz}, \quad \lceil\ \rceil : \Lambda \to (L \to \Lambda_N^{Gtz})$$

$$\begin{array}{rcl} \lfloor x \rfloor & = & x \\ \lfloor \lambda x.M \rfloor & = & \lambda x.\lfloor M \rfloor \\ \lfloor MN \rfloor & = & \lceil MN \rceil\langle [] \rangle \end{array}$$

$$\begin{array}{rcl} \lceil x \rceil\langle L \rangle & = & xL \\ \lceil \lambda x.M \rceil\langle L \rangle & = & (\lambda x.\lfloor M \rfloor)L \\ \lceil MN \rceil\langle L \rangle & = & \lceil M \rceil\langle \lfloor N \rfloor :: L \rangle \end{array}$$

- the mapping preserves operational semantics and normal forms of the λ-calculus;
- λ_N^{Gtz}-calculus is Turing complete, although it contains less terms than the λ^{Gtz}-calculus.

The proof of confluence

- after eliminating the critical pair, we can prove confluence, i.e., the Church-Rosser property;
- we use a direct, parallel reductions method;
- developed by Takahashi (1995) as a refinement of the standard Martin-Löf proof of confluence;
- based on simultaneous reduction of all existing redexes in a term;
- used by Dougherty et al. (2005) and Likavec and Lescanne (2012) in order to prove the confluence of some classical term calculi;
- we will sketch the proof for the confluence of λ_V^{Gtz}, the proof for λ_N^{Gtz} is analogous.

Parallel reductions for λ_V^{Gtz}

$$\frac{}{x \Rightarrow_V x}\ (g1) \qquad \frac{t \Rightarrow_V t'}{\lambda x.t \Rightarrow_V \lambda x.t'}\ (g2) \qquad \frac{t \Rightarrow_V t',\ k \Rightarrow_V k'}{tk \Rightarrow_V t'k'}\ (g3)$$

$$\frac{t \Rightarrow_V t'}{\widehat{x}.t \Rightarrow_V \widehat{x}.t'}\ (g4) \qquad \frac{t \Rightarrow_V t',\ k \Rightarrow_V k'}{t :: k \Rightarrow_V t' :: k'}\ (g5)$$

$$\frac{t \Rightarrow_V t',\ u \Rightarrow_V u',\ k \Rightarrow_V k'}{(\lambda x.t)(u :: k) \Rightarrow_V u'\widehat{x}.(t'k')}\ (g6) \qquad \frac{V \Rightarrow_V V',\ t \Rightarrow_V t'}{V(\widehat{x}.t) \Rightarrow_V t'[V'/x]}\ (g7)$$

$$\frac{t \Rightarrow_V t',\ k \Rightarrow_V k',\ k_1 \Rightarrow_V k_1'}{(tk)k_1 \Rightarrow_V t'(k'@k_1')}\ (g8) \qquad \frac{k \Rightarrow_V k'}{\widehat{x}.xk \Rightarrow_V k'}\ (g9)$$

Properties of $\Rightarrow$

(i) For every λ_V^{Gtz} expression e, $e \Rightarrow_V e$.

(ii) If $e \rightarrow e'$ then $e \Rightarrow_V e'$.

(iii) If $e \Rightarrow_V e'$ then $e \twoheadrightarrow e'$.

(iv) If $e \Rightarrow_V e'$ and $h \Rightarrow_V h'$, then $e[h/x] \Rightarrow_V e'[h'/x]$.

Confluence

Expression e^* is obtained from e by simultaneously reducing all existing redexes of e.

Properties of $\Rightarrow_V$

Star-property If $e \Rightarrow_V e'$, then $e' \Rightarrow_V e^*$.

Diamond-property If $e_1 \Leftarrow_V e \Rightarrow_V e_2$, then $e_1 \Rightarrow_V e' \Leftarrow_V e_2$ for some e'.

Confluence of λ_V^{Gtz}

If $e_1 \twoheadleftarrow e \twoheadrightarrow e_2$, then $e_1 \twoheadrightarrow e' \twoheadleftarrow e_2$ for some e'.

Summary

- Two subcalculi of λ^{Gtz} are obtained: λ_V^{Gtz} and λ_N^{Gtz} by restricting the operational semantics.
- Both sub-calculi are proven to be confluent using parallel reduction techniques.
- Proof-theoretic meaning of non-confluence in this setting?

Acknowledgement.
Pierre Lescanne, Hugo Herbelin, José Espírito Santo.