Računske interpretacije intuicionističke i klasične logike

Silvia Ghilezan
Univerzitet u Novom Sadu
Srbija

Sustavi dokazivanja 2012
Dubrovnik, Hrvatska, 28.06.2012

1. Computational interpretations of intuitionistic logic
   - Axiomatic and Natural Deduction

2. Computational interpretations of intuitionistic logic
   - Sequent Calculus

3. Computational interpretations of classical logic

4. Curry-Howard paradigm extended to processes calculi

Working group at University of Novi Sad

University of Novi Sad, Serbia
Computation, Concurrency, Logic and Reasoning - Co^{2}LoR

- Silvia Ghilezan, Professor,
- Jovanka Pantović, Professor
- Jelena Ivetić, Teaching Assistant, PhD student
- Svetlana Jakšić, Teaching Assistant, PhD student
- Dragiša Zunić, Assistant Professor, (PhD, ENS-Lyon)
- Jelena Čolić, Teaching Assistant, PhD student
- Andrijana Stamenković, PhD student

Group members abroad (Italy, Switzerland, France, USA)

- Silvia Likavec, U. Torino, (PhD, U. Torino, ENS-Lyon)
- Viktor Kunčak, EPFL Lausanne, (PhD MIT)

Computational interpretations of intuitionistic logic

- 1950s Curry
- 1968 (1980) Howard formulae-as-types
- 1970s Lambek - CCC Cartesian Closed Categories
- 1970s de Bruijn AUTOMATH

logic vs term calculus

$$\vdash A \;\; \Leftrightarrow \vdash t : A$$

Curry - Howard - Lambek - de Bruijn correspondence

Curry-Howard paradigm:

formulae – as – types
proofs – as – terms
proofs – as – programs

Computational interpretations of intuitionistic logic

Logic vs *term calculi*

- Axiomatic (Hilbert) system (axioms/Modus Ponens)
  Combinatory Logic (combinators/application)
  1930s Schönfinkel, Curry
- Natural Deduction (introduction/elimination)
  λ *calculus(abstraction/ application)*
  1940s Church
- Sequent Calculus (right/left introduction/cut)
  various attempts λ *calculus (abstraction/application/substitution)*
  1970s

Axiomatic (Hilbert style) system - Combinatory Logic

(AxI) $\qquad \vdash \quad A \to A$

(AxK) $\qquad \vdash \quad A \to (B \to A)$

(AxS)

$$\vdash \quad (A \to (B \to C)) \to ((A \to B) \to (A \to C))$$

(MP)

$$\frac{\vdash \quad A \to B \qquad \vdash \quad A}{\vdash B}$$

Axiomatic (Hilbert style) system - Combinatory Logic

(*AxI*) $\vdash I : A \rightarrow A$

(*AxK*) $\vdash K : A \rightarrow (B \rightarrow A)$

(*AxS*)

$$\vdash S : (A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C))$$

(*MP*)

$$\frac{\vdash t : A \rightarrow B \quad \vdash s : A}{ts : \vdash B}$$

$$\vdash A \ \Leftrightarrow \vdash t : A$$

Natural Deduction - λ-calculus

$$(axiom) \quad \frac{}{\Gamma, \quad A \vdash \quad A}$$

$$(\to_{elim}) \quad \frac{\Gamma \vdash \quad A \to B \qquad \Gamma \vdash \quad A}{\Gamma \vdash \quad B}$$

$$(\to_{intr}) \quad \frac{\Gamma, \quad A \vdash \quad B}{\Gamma \vdash \quad A \to B}$$

Natural Deduction - λ-calculus

$(axiom)$
$$\frac{}{\Gamma, x:A \vdash x:A}$$

$(\rightarrow_{elim})$ (app)
$$\frac{\Gamma \vdash t:A \rightarrow B \qquad \Gamma \vdash s:A}{\Gamma \vdash ts:B}$$

$(\rightarrow_{intr})$ (abs)
$$\frac{\Gamma, x:A \vdash t:B}{\Gamma \vdash \lambda x.t:A \rightarrow B}$$

$$\vdash A \Leftrightarrow \vdash t : A$$

Sequent calculus - ?

$(axiom)$ $$\frac{}{\Gamma, A \vdash A}$$

$(\rightarrow_{left})$ $$\frac{\Gamma \vdash A \quad \Gamma, B \vdash C}{\Gamma, A \rightarrow B \vdash C}$$

$(\rightarrow_{right})$ $$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \rightarrow B}$$

(cut) $$\frac{\Gamma \vdash A \quad \Gamma, A \vdash B}{\Gamma \vdash B}$$

Sequent calculus intuitionistic logic

- Pottinger, Zucker 1970s comparing cut-elimination to proof normalization
- Gallier [1991]
- Mints [1996]
- Barendregt, Ghilezan [2000]: λLJ-calculus

But in these, terms do not encode derivations.

- Herbelin [1995]: $\bar{\lambda}$-calculus - developed the idea of making terms explicitly represent sequent calculus derivations.
- Computation over terms reflects cut-elimination
- Espírito Santo [2006]: λ^{Gtz}-calculus

λ^{Gtz}-calculus

Syntax

$$
\begin{array}{lrcl}
\text{(terms)} & t, u, v & ::= & x \mid \lambda x.t \mid tk \\
\text{(contexts)} & k & ::= & \widehat{x}.t \mid u :: k
\end{array}
$$

Reductions

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

- $t[x := v]$ is a meta-substitution;
- $k@k'$ is defined by:

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

λ^{Gtz} - simple types

Types:

$$A, B \ ::= \ p \mid A \to B$$

Type assignments:

- $\Gamma \vdash t : A$ - for terms;
- $\Gamma; B \vdash k : A$ - for contexts

$$\frac{}{\Gamma, x : A \vdash x : A}\,(Ax) \qquad \frac{\Gamma, x : A \vdash t : B}{\Gamma \vdash \lambda x.t : A \to B}\,(\to_R)$$

$$\frac{\Gamma \vdash t : A \qquad \Gamma; B \vdash k : C}{\Gamma; A \to B \vdash t :: k : C}\,(\to_L) \qquad \frac{\Gamma, x : A \vdash t : B}{\Gamma; A \vdash \widehat{x}.t : B}\,(Sel)$$

$$\frac{\Gamma \vdash t : A \qquad \Gamma; A \vdash k : B}{\Gamma \vdash tk : B}\,(Cut)$$

Our contributions

Properties:

- Subject reduction.
- Strong normalisation property (Typeability implies SN)
  the inverse does not hold.

Our contributions

Properties:

- Subject reduction.
- Strong normalisation property (Typeability implies SN) the inverse does not hold.

Our contributions:

- Intersection types (syntax directed).
- Characterisation of strong normalisation with intersection types (SN implies typeability)

$$\text{Typeability} \Leftrightarrow \text{SN}$$

Our contributions

Properties:

- Subject reduction.
- Strong normalisation property (Typeability implies SN) the inverse does not hold.

Our contributions:

- Intersection types (syntax directed).
- Characterisation of strong normalisation with intersection types (SN implies typeability)

$$\text{Typeability} \Leftrightarrow \text{SN}$$

- Relation to λx - explicit substitutions, ΛJ - generalised application

Our contributions

Properties:

- Subject reduction.
- Strong normalisation property (Typeability implies SN) the inverse does not hold.

Our contributions:

- Intersection types (syntax directed).
- Characterisation of strong normalisation with intersection types (SN implies typeability)

$$\text{Typeability} \Leftrightarrow \text{SN}$$

- Relation to λx - explicit substitutions, ΛJ - generalised application
- Intuitionistic logic with explicit structural rules - Jelena Ivetić.

Publications

H. P. Barendregt, S. Ghilezan.
Lambda terms for natural deduction, sequent calculus and cut-elimination.
Journal of Functional Programming 10(1): 121-134 (2000)

J. Espírito Santo, S. Ghilezan, J. Ivetić.
Characterizing strongly normalising intuitionistic sequent terms.
TYPES 2007, Lecture Notes in Computer Science 4941: 85-99 (2007).

S. Ghilezan, J. Ivetić, P. Lescanne and D. Žunić.
Intuitionistic sequent-style calculus with explicit structural rules.
TBiLLC 2009, LNAI 6618: 101–124, (2010).

S. Ghilezan, J. Ivetić, P. Lescanne, and S. Likavec.
Intersection types for the resource control lambda calculi.
ICTAC 2011, LNCS 6916: 116-134 (2011).

Computational interpretations of classical logic

- Griffin 1990
  formulae-as-types notion of control (axiomatic)
- Parigot 1992
  algorithmic interpretation of classical logic (natural deduction)
- Barbanera, Berardi 1996
  symmetric lambda calculus - classical program extraction
- Curien, Herbelin 2000
  symmetric lambda calculus - duality of computation
- Wadler 2003
  dual calculus (all connectives) - duality of computation
- Urban 2000
  symmetric lambda calculus - cut elimination in classical logic
- Lescanne, van Bakel 2005
  symmetric lambda calculus - diagramatic calculus functional calculus

$\overline{\lambda}\mu\widetilde{\mu}$ calculus

Curien, Hereblin [2000]

Syntax

$$\begin{array}{llll} \text{Terms:} & r & ::= & x \mid \lambda x.r \mid \mu\alpha.c \\ \text{Envir:} & e & ::= & \alpha \mid r \bullet e \mid \widetilde{\mu}x.c \\ \text{Comm:} & c & ::= & \langle r \parallel e \rangle \end{array}$$

Reduction rules

$$\begin{array}{llll} (\lambda) & \langle \lambda x.r' \parallel r \bullet e \rangle & \rightarrow & \langle r' \parallel \widetilde{\mu}x.\langle r \parallel e \rangle \rangle \\ (\mu - red) & \langle \mu\alpha.c \parallel e \rangle & \rightarrow & c\{e/\alpha\} \\ (\widetilde{\mu} - red) & \langle r \parallel \widetilde{\mu}x.c \rangle & \rightarrow & c\{r/x\} \end{array}$$

Failure of confluence (non reparable): critical pair between μ and $\widetilde{\mu}$.

$$\langle\ \mu\alpha.\langle y \parallel \beta \rangle \parallel \widetilde{\mu}x.\langle z \parallel \gamma \rangle\ \rangle \rightarrow \langle y \parallel \beta \rangle$$

$$\langle\ \mu\alpha.\langle y \parallel \beta \rangle \parallel \widetilde{\mu}x.\langle z \parallel \gamma \rangle\ \rangle \rightarrow \langle z \parallel \gamma \rangle$$

Duality of computation: Call-by-value, Call-by-name

$$
\begin{array}{llcll}
(\mu - red) & \langle \mu\alpha.c \parallel \widetilde{\mu}x.d \rangle & \rightarrow & c\{\widetilde{\mu}x.c/\alpha\} & CBV \\
(\widetilde{\mu} - red) & \langle \mu\alpha.c \parallel \widetilde{\mu}x.d \rangle & \rightarrow & d\{\mu\alpha.c/x\} & CBN
\end{array}
$$

Two confluent subsystems of $\overline{\lambda}\mu\widetilde{\mu}_{CBV}$ and $\overline{\lambda}\mu\widetilde{\mu}_{CBN}$

- Strong normalization of CBV and CBN: CPS translations of $\overline{\lambda}\mu\widetilde{\mu}_{CBV}$ and $\overline{\lambda}\mu\widetilde{\mu}_{CBN}$ into simply-typed λ-calculus
- SN of free reduction?
- Characterization of SN?

Typeability implies SN

- The difficulty in proving SN in $\overline{\lambda}\mu\widetilde{\mu}$ using a traditional reducibility (or "candidates") argument arises from the critical pairs $\langle \mu\alpha.c \parallel \widetilde{\mu}x.d \rangle$
- Neither of the expressions here can be identified as the preferred redex one cannot define candidates by induction on the structure of types
- This difficulty arises already in the simply-(arrow)-typed case
- The "symmetric candidates" technique of Barbanera and Berardi uses a fixed-point technique to define the candidates and suffices to prove strong normalization for simply-typed $\overline{\lambda}\mu\widetilde{\mu}$
- The interaction between intersection types and symmetric candidates is technically problematic (David and Nour)

Delimited continuation

- Call-by-name in Parigot, de Groote classical natural deduction
- Böhm separability
- Shift and reset
- Classical sequent calculus - uniform framework for CBN and CBV delimited continuation

Publications

- D. Dougherty, S. Ghilezan and P. Lescanne.
  Characterizing strong normalization in the Curien-Herbelin symmetric lambda calculus: extending the Coppo-Dezani heritage.
  Theoretical Computer Science 398: 114-128 (2008).

- D. Dougherty, S. Ghilezan, P. Lescanne, S. Likavec.
  Strong normalization of the Dual classical calculus.
  LPAR 2005, Lecture Notes in Computer Science 3835: 169-183 (2005).

- D. Dougherty, S. Ghilezan and P. Lescanne.
  Characterizing strong normalization in a language with control operators.
  PPDP 2004 155-166.

- H. Herbelin and S. Ghilezan.
  An approach to call-by-name delimited continuations.
  POPL 2008 383-394.

Curry-Howard paradigm extended

COMPUTATION	COMMUNICATION
determinism	non-determinism
term	process
sequential composition	concurrency
computational behaviour	interactional behaviour
λ calculus	π calculus

Curry-Howard paradigm:

formulae – as – types
proofs – as – terms
proofs – as – programs

Curry-Howard paradigm extended

COMPUTATION	COMMUNICATION
determinism	non-determinism
term	process
sequential composition	concurrency
computational behaviour	interactional behaviour
λ calculus	π calculus

Curry-Howard paradigm:

formulae – as – types
proofs – as – terms
proofs – as – programs
proofs – as – processes

Publications

M. Dezani-Ciancaglini, S. Ghilezan, S. Jaksić, J. Pantovic.
Types for Role-based Access Control of Dynamic Web Data.
WFLP'10 - Functional and Constraint Logic Programming, LNCS 6559: 1-29 (2011).

M. Dezani-Ciancaglini, S. Ghilezan, J. Pantovic, and D. Varacca.
Security types for dynamic web data.
Theor. Comput. Sci., 402(2-3):156–171 (2008).

M. Dezani-Ciancaglini, S. Ghilezan, J. Pantovic
Security types for dynamic web data.
TGC'06- Thrustworthy Global Computing, LNCS 4661: 263-280 (2006).

Joint work with

- Henk Barendregt, *Radboud University, Nijmegen, The Netherlands*
- Mariangiola Dezani-Ciancaglini, *University of Torino, Italy*
- Daniel Dougherty, *Worcester Polytechnic Institute, USA*
- Jose Espírito Santo, *University of Minho, Braga, Portugal*
- Hugo Herbelin, *INRIA, Paris, France*
- Jelena Ivetić
- Svetlana Jaksić
- Viktor Kunčak, *EPFL Lausanne, Switzerland*
- Silvia Likavec, *University of Torino, Italy*
- Pierre Lescanne, *École Normale Supérieure de Lyon, France*
- Jovanka Pantović
- Daniel Varacca, *Université Paris 7, France*
- Betty Vennery, *University of Florence, Italy*
- Dragiša Žunić
- Joviša Žunić, *University of Exeter, UK*