The Curry-Howard isomorphism
MAP-i, UP, 2008

Nelma Moreira

Departamento de Ciência de Computadores
Faculdade de Ciências da Universiade do Porto

Program Semantics, Verification, and Construction
3-Part II

NJ_0 for IPC($\longrightarrow$)

IPC: Intuitionistic propositional logic

$$\dfrac{\begin{matrix}[\alpha] \\ \vdots \\ \beta\end{matrix}}{\alpha \longrightarrow \beta}\to\mathbf{I} \qquad \dfrac{\begin{matrix}\vdots \\ \alpha\end{matrix} \quad \begin{matrix}\vdots \\ \alpha\to\beta\end{matrix}}{\beta}\to\mathbf{E}$$

NJ_0 with *sequents* for IPC($\rightarrow$)

Γ set of formulas $\quad\quad$ $\Gamma \vdash \Theta$ *sequent*

$$\frac{}{\Gamma, \alpha \vdash \alpha}$$

$$\frac{\Gamma \vdash \alpha \rightarrow \beta \qquad\qquad \Gamma \vdash \alpha}{\Gamma \vdash \beta} (\rightarrow E)$$

$$\frac{\Gamma, \alpha \vdash \beta}{\Gamma \vdash \alpha \rightarrow \beta} (\rightarrow I)$$

Simple typed λ-calculus, $\mathbf{TA}_\lambda$

Γ set of assignments

$$x : \tau \vdash x : \tau$$

$$\frac{\Gamma_1 \vdash M : \sigma \rightarrow \tau \qquad\qquad \Gamma_2 \vdash N : \sigma}{\Gamma_1 \cup \Gamma_2 \vdash (MN) : \tau} (APP)$$

$\Gamma_1 \cup \Gamma_2$ consistent

$$\frac{\Gamma \vdash M : \tau}{\Gamma - x \vdash (\lambda x.M) : (\sigma \rightarrow \tau)} (ABS)$$

Γ consistent with $x : \sigma$

Γ consistent with $x : \tau$

$(\rightarrow E) = (APP)$, $(\rightarrow I) = (ABS)$

The Curry-Howard isomorphism

Formulas	$\sim$	**Types**	
Proofs	$\sim$	**Terms**	**(Programs)**
Normalizations	$\sim$	**Computations**	
$\vdots$	$\sim$	$\vdots$	

Correspondence $\lambda\rightarrow\ \Rightarrow_L$ IPC($\rightarrow$)

Δ $\mathbf{TA}_\lambda$-deduction $\Gamma \vdash M : \tau$

Δ_L NJ_0-deduction defined by:

- $M \equiv x$ and Δ is $x : \tau \vdash x : \tau$ then Δ_L is $\tau \vdash \tau$
- $M \equiv PQ$, $\Gamma = \Gamma_1 \cup \Gamma_2$ and the last step of Δ is

$$\frac{\overset{\Delta_1}{\Gamma_1 \vdash M : \sigma \rightarrow \tau} \qquad \overset{\Delta_2}{\Gamma_2 \vdash N : \sigma}}{\Gamma_1 \cup \Gamma_2 \vdash (MN) : \tau}\ (\rightarrow E)$$

Δ_L applying $(\rightarrow E)$ to Δ_{1_L} and to Δ_{2_L}

Correspondence $\lambda \rightarrow \Rightarrow_L$ IPC($\rightarrow$)

- $M \equiv \lambda x.P$, $\tau \equiv \rho \rightarrow \sigma$, $\Gamma = \Gamma_1 - x$ and the last step of Δ is Δ_1

$$\frac{\Gamma_1 \ \vdash \ P : \sigma}{\Gamma_1 - x \ \vdash \ (\lambda x.P) : (\rho \rightarrow \sigma)} \ (\rightarrow \ I)$$

Δ_L applying $(\rightarrow \ I)$ to Δ_{1_L} with ρ

If we use NJ_0 without *sequents* we must discharge **all** as occurrences of ρ in Δ_{1_L} whose positions coincide with the free occurrences of x in P

Examples

$\vdash (\lambda xyz.xzy) : (a \rightarrow a \rightarrow c) \rightarrow a \rightarrow a \rightarrow c$

$x{:}a\to a\to c \vdash x{:}a\to a\to c$ $\quad$ $z{:}a \vdash z{:}a$

$x{:}a\to a\to c, z{:}a \vdash (xz){:}a\to c$ $\quad$ $y{:}a \vdash y{:}a$

$x{:}a\to a\to c, z{:}a, y{:}a \vdash (xzy){:}c$

$x{:}a\to a\to c, y{:}a \vdash (\lambda z.xzy){:}a\to c$

$x{:}a\to a\to c \vdash (\lambda yz.xzy){:}a\to a\to c$

$\vdash (\lambda xyz.xzy){:}(a\to a\to c)\to a\to a\to c$

$a\to a\to c \vdash a\to a\to c$

$a\to a\to c, a \vdash a\to c$

$a\to a\to c, a, a \vdash c$

$a\to a\to c, a \vdash a\to c$

$a\to a\to c \vdash a\to a\to c$

$\vdash (a\to a\to c)\to a\to a\to c$

$\vdash (\lambda xyz.xzz) : (a \rightarrow a \rightarrow c) \rightarrow a \rightarrow a \rightarrow c$

$x{:}a\to a\to c \vdash x{:}a\to a\to c$ $\quad$ $z{:}a \vdash z{:}a$

$x{:}a\to a\to c, z{:}a \vdash (xz){:}a\to c$ $\quad$ $z{:}a \vdash z{:}a$

$x{:}a\to a\to c, z{:}a \vdash (xzz){:}c$

$x{:}a\to a\to c \vdash (\lambda z.xzz){:}a\to c$

$x{:}a\to a\to c \vdash (\lambda yz.xzz){:}a\to a\to c$

$\vdash (\lambda xyz.xzz){:}(a\to a\to c)\to a\to a\to c$

$a\to a\to c \vdash a\to a\to c$

$a\to a\to c, a \vdash a\to c$

$a\to a\to c, a \vdash c$

$a\to a\to c \vdash a\to c$

$a\to a\to c \vdash a\to a\to c$

$\vdash (a\to a\to c)\to a\to a\to c$

Examples

NJ_0 without *sequents*

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{x{:}a\to a\to c \vdash x{:}a\to a\to c \qquad z{:}a \vdash z{:}a}{x{:}a\to a\to c, z{:}a \vdash (xz){:}a\to c} \qquad y{:}a \vdash y{:}a}{x{:}a\to a\to c, z{:}a, y{:}a \vdash (xzy){:}c}}{x{:}a\to a\to c, y{:}a \vdash (\lambda z.xzy){:}a\to c}}{x{:}a\to a\to c \vdash (\lambda yz.xzy){:}a\to a\to c}}{\vdash (\lambda xyz.xzy){:}(a\to a\to c)\to a\to a\to c}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{[a\to a\to c]^{(3)} \qquad [a]^{(1)}}{a\to c \qquad [a]^{(2)}}}{c}}{a\to c^{(1)}}}{\dfrac{a\to a\to c^{(2)}}{(a\to a\to c)\to a\to a\to c^{(3)}}}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{x{:}a\to a\to c \vdash x{:}a\to a\to c \qquad z{:}a \vdash z{:}a}{x{:}a\to a\to c, z{:}a \vdash (xz){:}a\to c} \qquad z{:}a \vdash z{:}a}{x{:}a\to a\to c, z{:}a \vdash (xzz){:}c}}{x{:}a\to a\to c \vdash (\lambda z.xzz){:}a\to c}}{x{:}a\to a\to c \vdash (\lambda yz.xzz){:}a\to a\to c}}{\vdash (\lambda xyz.xzz){:}(a\to a\to c)\to a\to a\to c}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{[a\to a\to c]^{(3)} \qquad [a]^{(1)}}{a\to c \qquad [a]^{(1)}}}{c}}{a\to c^{(1)}}}{\dfrac{a\to a\to c^{(2)}}{(a\to a\to c)\to a\to a\to c^{(3)}}}$$

Note: The correspondence $()_L$ is not injective !

IPC($\longrightarrow$) $\Rightarrow_\lambda$ $\lambda\to$

Δ $NJ_0(\longrightarrow)$-deduction of $\Gamma \ \vdash \ \tau$

Δ_λ**TA**$_\lambda$-deduction of $\Gamma' \ \vdash \ M : \tau$, where $\Gamma' = \{x : \tau \mid \tau \in \Gamma\}$, and defined by:

- ifΔ is $\Gamma, \tau \ \vdash \ \tau$ there are two subcases:
  1. $\tau \in \Gamma\dot{T}$hen Δ_λ is $\Gamma' \ \vdash \ x : \tau$
  2. $\tau \notin \Gamma$. Then Δ_λ is $\Gamma', x : \tau \ \vdash \ x : \tau$
- The last step of Δ is ($\to$ E) applied to the conclusion of Δ_1 and of Δ_2 and Δ_{1_λ} and Δ_{2_λ} are deductions of
  $\Gamma'_1 \ \vdash \ M : \sigma \to \tau$ $\qquad\qquad$ $\Gamma'_2 \ \vdash \ N : \sigma$
  apply (APP) to Δ_{1_λ} and Δ_{2_λ} after substituting all variables by new ones, and then

$$\Gamma'_1 \cup \Gamma'_2 \ \vdash \ MN : \tau$$

IPC($\rightarrow$) $\Rightarrow_\lambda$ $\lambda\rightarrow$

- The derivation ends in Δ is $(\rightarrow\ I)$

$$\dfrac{\begin{matrix}\Delta_1\\ \\ \Gamma,\rho\ \vdash\ \sigma\end{matrix}}{\Gamma\ \vdash\ \rho\rightarrow\sigma}$$

We consider two subcases:

1. $\rho\in\Gamma$. Then by the induction hypothesis the conclusion of Δ_{1_λ} is $\Gamma'\ \vdash\ P:\sigma$, with $v_i:\rho\in\Gamma'$ e $v_i\in FV(P)$, $1\leq i\leq k$. We can modify Δ_{1_λ} for a deduction of $\Gamma',x:\rho\ \vdash\ P^*:\sigma$, where x is a new variable and
$$P^*\equiv[x/v_1,\ldots,x/v_k]P$$
Aplying (ABS): $\Gamma'\ \vdash\ (\lambda x.P^*):\rho\rightarrow\sigma$
2. $\rho\notin\Gamma$. Then the conclusion of Δ_{1_λ} is $\Gamma',x:\rho\ \vdash\ P:\sigma$ and applying (ABS) we have
$$\Gamma'\ \vdash\ (\lambda x.P):\rho\rightarrow\sigma$$

Examples

$$\dfrac{\dfrac{a,a\vdash a}{a\vdash a\rightarrow a}}{\vdash a\rightarrow a\rightarrow a}$$

$()_\lambda\Rightarrow$ type inferences for $\lambda xy.x$ and $\lambda yx.x$:

$$\dfrac{\dfrac{x{:}a,y{:}a\vdash x{:}a}{x{:}a\vdash\lambda y.x{:}a\rightarrow a}}{\vdash\lambda xy.x{:}a\rightarrow a\rightarrow a}\qquad\dfrac{\dfrac{x{:}a,y{:}a\vdash y{:}a}{x{:}a\vdash\lambda y.y{:}a\rightarrow a}}{\vdash\lambda xy.y{:}a\rightarrow a\rightarrow a}$$

The two inferences can be distinguished in NJ_0 using the structural rules or if we consider NJ_0 without *sequents*:

$$\dfrac{\dfrac{[a]^{(1)}}{a\rightarrow a^{(2)}}}{a\rightarrow a\rightarrow a^{(1)}}\qquad\dfrac{\dfrac{[a]^{(1)}}{a\rightarrow a^{(1)}}}{a\rightarrow a\rightarrow a^{(2)}}$$

Empty discharges correspond to the weakening rule.

Curry-Howard Isomorphism Theorem

1. The provable formulae of IPC are exactly the types of closed λ-terms.
2. $\sigma_1, \ldots, \sigma_n \vdash \tau$ iff exists M such that $x_1 : \sigma_1, \ldots, x_n : \sigma_n \vdash M : \tau$
3. For all deductions:
   $\Delta_{L_\lambda} \equiv_\alpha \Delta$
   $\Delta_{\lambda_L} = \Delta$

Curry-Howard Isomorphism

TA$_\lambda$	**IPC**$(\rightarrow)$
types	formulas
term variables	assumptions
terms	deduction (construction)
inhabitants	Proofs
typable term	deduction for a formula
type constructor	connective
redex	deduction with redundances
reduction	normalization
normal form	normal form derivation

Inhabitation = Is there a term for this type?

Typability= Is there a type for this term?

Normalization *versus* Reduction

β reduction

$$(\lambda x.t)u \longrightarrow_\beta t[u/x]$$

$$\dfrac{\dfrac{\begin{array}{c}\Delta_1\\ \vdots\\ \Gamma, x{:}\sigma \vdash t{:}\tau\end{array}}{\Gamma \vdash \lambda x.t{:}\sigma\to\tau} \qquad \begin{array}{c}\Delta_2\\ \vdots\\ \Theta \vdash u{:}\sigma\end{array}}{\Gamma,\Theta \vdash (\lambda x.t)u{:}\tau} \quad \Rightarrow \quad \begin{array}{c}\Delta_2 \ldots \Delta_2\\ \vdots\\ \Delta_1\\ \vdots\\ \Gamma,\Theta \vdash t[u/x]{:}\tau\end{array}$$

Extension to $\lambda(\rightarrow, \wedge, \vee)$

Extending the simple types to $\sigma \wedge \tau$ (or $\sigma \times \tau$) and to $\sigma \vee \tau$ (or $\sigma + \tau$)

Extending the simple-typed λ-terms to pairs and disjoint sums:

- If $M : \tau$ and $N : \sigma$ are λ-terms, then $< M, N >: \tau \wedge \sigma$ is a λ-term
- If $M : \tau \wedge \sigma$, then $\pi_1(M) : \tau$, $\pi_2(M) : \sigma$ are λ-terms
- If $M : \tau$, then $in_1^{\tau \vee \sigma}(M) : \tau \vee \sigma$ is a λ-term.
- If $M : \sigma$, then $in_2^{\tau \vee \sigma}(M) : \tau \vee \sigma$ is um λ-term
- If $M : \tau \vee \sigma$, $L : \tau \rightarrow \tau'$ and $K : \sigma \rightarrow \tau'$ are λ-terms, then $case(M, x.L, y.K) : \tau'$ where x and y are variables (of types τ and σ)

Note that here it is not possible to write the above terms only with abstractions and applications, as one can do in the pure λ-calculus (Why?)

Inference rules

The inference rules correspond to $\wedge E$, $\wedge I$, $\vee I$ e $\vee E$,labelled with terms...

$$\frac{\Gamma \vdash M : \sigma \qquad \Gamma \vdash N : \tau}{\Gamma \vdash < M, N >: \sigma \wedge \tau} \wedge \mathbf{I}$$

$$\frac{\Gamma \vdash M : \sigma \wedge \tau}{\Gamma \vdash \pi_1(M) : \sigma} \wedge \mathbf{E}_1 \qquad \frac{\Gamma \vdash M : \sigma \wedge \tau}{\Gamma \vdash \pi_2(M) : \tau} \wedge \mathbf{E}_2$$

$$\frac{\Gamma \vdash M : \tau}{\Gamma \vdash in_1^{\tau \vee \sigma}(M) : \tau \vee \sigma} \vee \mathbf{I}_1 \qquad \frac{\Gamma \vdash M : \sigma}{\Gamma \vdash in_2^{\tau \vee \sigma}(M) : \tau \vee \sigma} \vee \mathbf{I}_2$$

$$\frac{\Gamma \vdash M : \tau \vee \sigma \qquad \Gamma, x : \tau \vdash L : \gamma \qquad \Gamma, y : \sigma \vdash K : \gamma}{\Gamma \vdash case(M; x.L, y.K) : \gamma} \vee \mathbf{E}$$

Reduction rules

The notion of redex extends to the new constructors/destructors:

$$\pi_1(< M, N >) \longrightarrow M$$

$$\pi_2(< M, N >) \longrightarrow N$$

$$case(in_1^{\tau \vee \sigma}(N); x.L, y.K) \longrightarrow L[N/x]$$

$$case(in_2^{\tau \vee \sigma}(N); x.L, y.K) \longrightarrow K[N/y]$$

C-H isomorphism: other variations and extensions

- Hilbert-style axiomatic systems and combinatory logic systems ($\mathbf{IPC}(\rightarrow)$corresponds to $\{\mathbf{B}, \mathbf{C}, \mathbf{K}, \mathbf{W}\}$)
- *sequents* calculi
- Propositional classical logic (1990)
- First-order intuitionistic logic correspond to dependent type systems
- Second order intuitionistic propositional logic corresponds to polymorphic type systems (system **F**)
- ...

Some sub-structural logics

λ**I**-terms: for each subterm $\lambda x.M$, x occurs free in M at least once

BCKλ-terms: for each subterm $\lambda x.M$, x occurs free in M at most once and each free variable occurs only once

BCIλ-terms (linear): **BCK** e λ**I**

The restriction of this classes to TA_λ, corresponds to several logic systems:

Relevance Logic ($R_\rightarrow$): **IPC**($\rightarrow$)where it is forbidden empty discharges, i.e the weakening rule is forbidden.

BCK Logic: **IPC**($\rightarrow$)where multiple discharges are forbidden: or empty or of only an assumption; i.e the contraction rule is forbidden.

BCI Logic: **IPC**($\rightarrow$)where each discharge is of one assumption, i.e the contraction rule is forbidden and left empty *sequents* are also forbidden.

$$\mathbf{BCI} \subseteq \mathbf{BCK} \subseteq \mathbf{IPC}(\rightarrow)(= \mathbf{BCKW})$$

$$\mathbf{BCI} \subseteq R_\rightarrow \subseteq \mathbf{IPC}(\rightarrow)$$

By the **Curry-Howard isomorphism**:

theorems	closed-terms types
$R_\rightarrow$	λ**I**-terms
BCK	**BCK**λ-terms
BCI	**BCI**λ-terms

Bibliography

[GLM97] Cap.4: 1.1-3.2 [PU96]Cap 1,3,4,5,6,7,8 [Hin97] Cap.6

Jean Goubault-Larrecq and Ian Mackie.
Proof Theory and Automated Deduction.
Kluwer Academic Press, 1997.

J. Roger Hindley.
Basic simple type theory.
Number 42 in Cambridge Tracts in Theoretical Computer Science.
CUP, 1997.

Morten B. Sorensen Pawel Urzyczyn.
Lecture on the curry-howard isomorphism.
Technical report, University of Copenhagen, 1996.
http://zls.mimuw.edu.pl/ urzy/ftp.html.