Verificação de Programas

Nelma Moreira

Departamento de Ciência de Computadores da FCUP

Um Aperitivo para os Demonstradores Interactivos: isomorfismo de Curry-Howard
Aula 22

Demonstradores Interactivos baseado em CoC

Permitem

- a especificao e a obteno de programas que satisfaam essa especificao.
- desenvolvimento de demonstraes matemticas numa lgica de ordem superior
- ambiente de desenvolvimento de lgicas diversas: temporais, modais, de descrio, etc.
- uma linguagem (funcional) de especificao
- baseado num λ-calculus tipificado polimrfico com tipos dependentes e noo primitiva de tipos indutivos: o Clculo de Construes Indutivas (CoC, pCiC).

Sistemas de dedutivos para lgica proposicional

Dado um conjunto de variveis $\mathcal{V}_{prop}$, sejam as frmulas

$$\alpha := \text{true} \mid \text{false} \mid p, q, \ldots \in \mathcal{V}_{prop} \mid \neg\alpha \mid \alpha \vee \alpha \mid \alpha \wedge \alpha \mid \alpha \rightarrow \alpha$$

Um sistema dedutivo um conjunto de regras a partir das quais possvel obter (deduzir) uma frmula (supondo ou no um conjunto inicial Γ): $\vdash \alpha$ ou $\Gamma \vdash \alpha$

Se $\vdash \alpha$, α diz-se um teorema

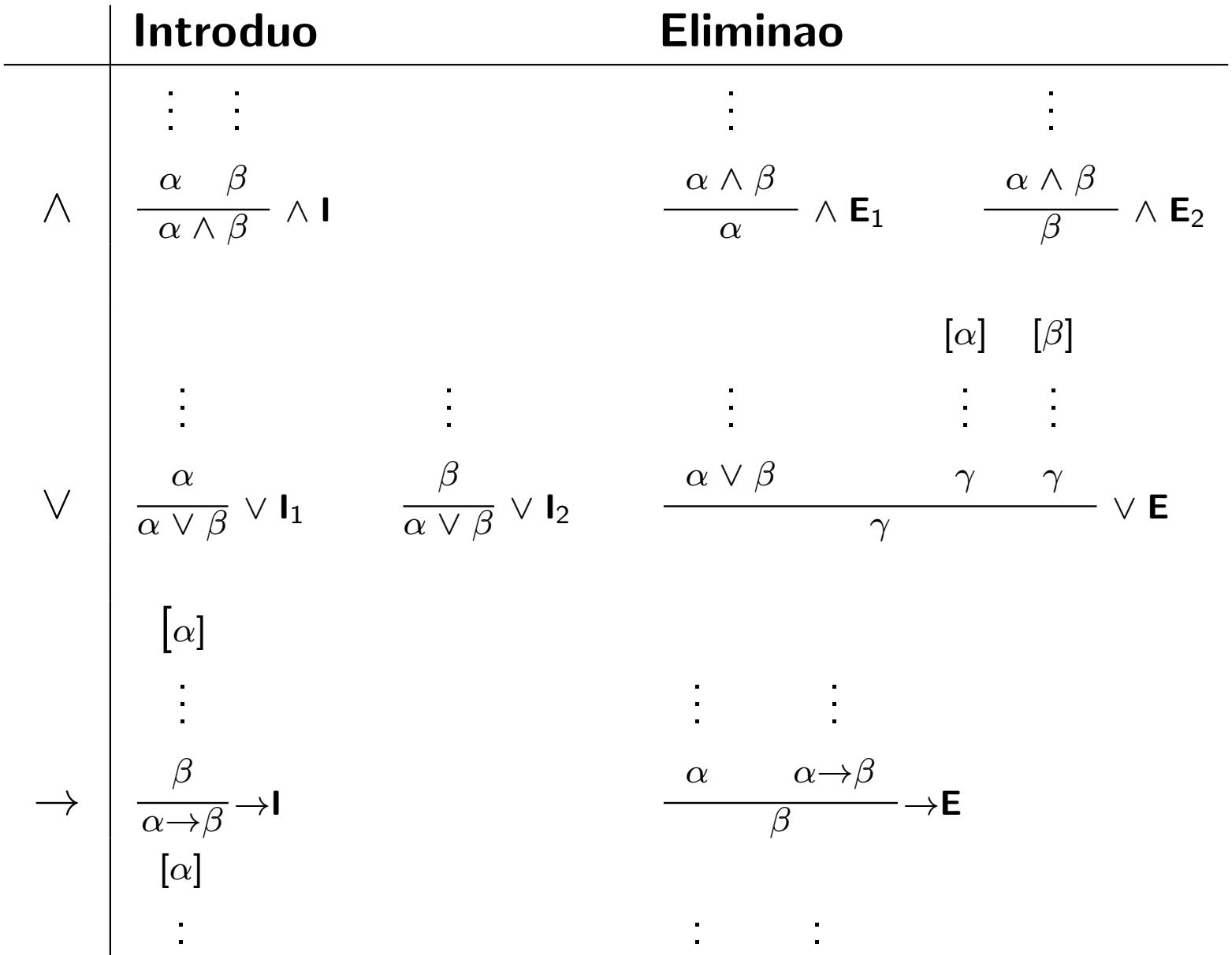
Pretendem-se sistemas ntegros e completos:

$$\vdash \alpha \text{ se e s se } \models \alpha$$

ou mais geralmente:

$$\Gamma \vdash \alpha \text{ se e s se } \Gamma \models \alpha$$

Deduo natural, NK_0 I



No tem axiomas. S regras de inferncia. Para cada conectiva lgica existem dois tipos de regras: de introduo e de eliminao.

As frmulas iniciais podem ser hipteses (premissas) introduzidas para a aplicao duma regra: iniciam um sub-deduo que quando termina cancela as respectivas hipteses

NK_0 em *sequents*

Supondo que Γ (contexto) um conjunto de frmulas:

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

	Introduo	**Eliminao**
$\wedge$	$\dfrac{\Gamma \vdash \alpha \quad \Gamma \vdash \beta}{\Gamma \vdash \alpha \wedge \beta}\,\wedge\mathbf{I}$	$\dfrac{\Gamma \vdash \alpha \wedge \beta}{\Gamma \vdash \alpha}\,\wedge\mathbf{E}_1$ $\quad$ $\dfrac{\Gamma \vdash \alpha \wedge \beta}{\Gamma \vdash \beta}\,\wedge\mathbf{E}_2$
$\vee$	$\dfrac{\Gamma \vdash \alpha}{\Gamma \vdash \alpha \vee \beta}\,\vee\mathbf{I}_1$ $\quad$ $\dfrac{\Gamma \vdash \beta}{\Gamma \vdash \alpha \vee \beta}\,\vee\mathbf{I}_2$	$\dfrac{\Gamma \vdash \alpha \vee \beta \quad \Gamma, \alpha \vdash \gamma \quad \Gamma, \beta \vdash \gamma}{\Gamma \vdash \gamma}\,\vee\mathbf{E}$
$\rightarrow$	$\dfrac{\Gamma, \alpha \vdash \beta}{\Gamma \vdash \alpha \rightarrow \beta}\,\rightarrow\mathbf{I}$	$\dfrac{\Gamma \vdash \alpha \quad \Gamma \vdash \alpha \rightarrow \beta}{\Gamma \vdash \beta}\,\rightarrow\mathbf{E}$
$\neg$	$\dfrac{\Gamma, \alpha \vdash \mathsf{F}}{\Gamma \vdash \neg\alpha}\,\neg\mathbf{I}$	$\dfrac{\Gamma \vdash \alpha \quad \Gamma \vdash \neg\alpha}{\Gamma \vdash \beta}\,\neg\mathbf{E}$
$\neg\neg$	$\dfrac{\Gamma \vdash \alpha}{\Gamma \vdash \neg\neg\alpha}\,\neg\neg\mathbf{I}$	$\dfrac{\Gamma \vdash \neg\neg\alpha}{\Gamma \vdash \alpha}\,\neg\neg\mathbf{E}$

Agora os ns das rvores de deduo so *sequents* e $\vdash \Gamma \ \vdash \ \alpha$ o mesmo que $\Gamma \vdash \alpha$

Exemp.

$\vdash \ \alpha \to (\beta \to \alpha)$

$$\dfrac{\dfrac{\alpha,\beta \vdash \alpha}{\alpha \vdash \beta \to \alpha}(\to \mathbf{I})}{\vdash \alpha \to (\beta \to \alpha)}(\to \mathbf{I})$$

Mtodos de demonstrao

A semntica da lgica clssica baseada na noo de *verdade*. E em particular cada proposio absolutamente verdadeira ou falsa. Isso traduz-se pelo princpio do terceiro excludo: $p \vee \neg p$.

Mas isto no nos d muita informao.

Mostrar que existem irracionais b e c tal que b^c racional

Dem. Demonstrao por casos: Seja $\sqrt{2}^{\sqrt{2}}$. Este nmero racional ou irracional.

- Se $\sqrt{2}^{\sqrt{2}}$ racional ento basta tomar $b = c = \sqrt{2}$
- Se $\sqrt{2}^{\sqrt{2}}$ irracional, ento seja $b = \sqrt{2}^{\sqrt{2}}$ e $c = \sqrt{2}$.
  Vem $b^c = \sqrt{2}^{\sqrt{2}.\sqrt{2}} = \sqrt{2}^2 = 2$, que racional

□

Mas afinal quais so esses valores? A demonstrao no constructiva.

Intuicionismo I

Uma proposio s verdadeira ou falsa, se ns soubermos porqu que isso acontece... ou seja se podermos ter uma demonstrao construtiva dela...(BHK)

A semntica duma proposio deve basear-se na noo de demonstrao: uma frmula verdadeira se tivermos uma construo para uma demonstrao dela e esta noo estende-se para s conectivas:

- Uma construo de $\alpha \wedge \beta$ consiste numa construo de α e numa construo de β
- Uma construo de $\alpha \vee \beta$ consiste numa construo de α ou numa construo de β
- Uma construo de $\alpha \rightarrow \beta$ um mtodo de transformar qualquer construo de α numa construo de β
- Uma construo de $\neg\alpha$ um mtodo de transformar qualquer construo de α num objecto no que existe (ou seja $\neg\alpha \equiv \alpha \rightarrow \mathsf{F}$) (**RA**)

Intuicionismo II

Mostrar que $p \to \neg\neg p$ (ou $p \to ((p \to \mathrm{F}) \to \mathrm{F})$ uma tautologia intuicionista:

> *Dada uma demonstrao de p, podemos obter uma demonstrao para* $((p \to F) \to F)$*: Seja uma demonstrao para* $(p \to F)$*, isto , um mtodo de transformar demonstraes de p em demonstrao de F. Como temos uma demonstrao para p podemos ter uma demonstrao para F*

Mas $\neg\neg p \to p$ no uma tautologia intuicionista: o facto de no termos uma demonstrao para $\neg p$ no nos permite concluir que tenhamos uma demonstrao para p...

E, do mesmo modo $p \vee \neg p$ no uma taulogogia!... em geral no garantido que se tenha uma demonstrao para p ou uma para $\neg p$.

A lgica intuicionista NJ_0 obtm-se da lgica clssica, p.e, retirando a regra $\neg\neg\mathbf{E}$ do sistema NK_0...

NJ_0 com *sequents* para IPC($\rightarrow$)

IPC($\rightarrow$): lgica proposicional intuicionista s com implicao

Γ conjunto de frmulas $\quad\quad$ $\Gamma \vdash \Theta$ *sequent*

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

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

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

λ-calculus (reviso) I

$x \in V$, V conjunto de variveis

λ-termos: variveis, aplicaes, abstraes

$$\Lambda := x \mid (\Lambda\Lambda) \mid (\lambda x.\Lambda)$$

- $xyxx$ (aplicaes associam esquerda)
- $(yz)(\lambda x.x)(yz)$
- $(\lambda x.xy)(\lambda z.z)$
- $(\lambda xy.xy)$
- $(\lambda x.x\lambda x.xy)(yy)$
- $(\lambda x.xx)(\lambda x.xx)$

Redues

- Variveis livres $FV(\Lambda)$:
  $FV(x) = \{x\}$ $FV(MN) = FV(M) \cup FV(N)$ $FV(\lambda x.M) = FV(M) \backslash \{x\}$
- Substituio de N por x em M, $M[N/x]$
- Reduo α: $\lambda x.M \rightarrow_\alpha \lambda y.M[y/x]$, se $y \notin FV(M)$
- Reduo β (um passo): $(\lambda x.M)P \rightarrow_\beta P[M/x]$
  β-Redex: $(\lambda x.M)P$
- Fecho transitivo-reflexivo: $\rightarrow_\beta^\star$
- Converso (simetria) : $=_\beta$

Forma normal β

- Um λ-termo est em forma normal β se no tiver nenhum redex.
- Se um λ-termo tiver forma normal ela nica.
- Existem $\lambda - \textit{termos}$ que no tm forma normal:
  $(\lambda x.xx)(\lambda x.xx)$, $(\lambda x.xxx)(\lambda x.xxx)$

Sistemas de tipos (simples) para o λ-calculus ($\lambda \rightarrow$)

- Sendo $\iota \in U$, U conjunto de variveis de tipo, um tipo simples ($\mathbf{TA}_\lambda$) dado por
$$\tau := \iota \mid \tau \rightarrow \tau$$
- $\tau \rightarrow (\sigma \rightarrow \tau)$ (associam direita)
- Atribuies de tipo: $M : \tau$
- Exemplos
  $x : \tau \qquad \lambda x.x : \sigma \rightarrow \sigma$
  $\lambda x.\lambda y.x : \sigma \rightarrow \tau \rightarrow \sigma$
- Γ conjunto de atribuies $x : \tau$ consistente

Sistema de tipos simples $\mathbf{TA}_\lambda$

Sendo Γ conjunto de atribuies $x : \tau$ consistente, para inferir se $\Gamma \vdash M : \tau$ temos o seguinte sistema de inferncia de tipos (que corresponde a um sistema dedutivo):

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

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

$$\frac{\Gamma \vdash M : \tau}{\Gamma \setminus \{x : \sigma\} \vdash (\lambda x.M) : (\sigma \to \tau)}\ (ABS) \qquad \Gamma \text{ consistente com } x : \sigma$$

Se omitirmos os λ-termostemos s deduo de frmulas em IPC($\rightarrow$):

$$\frac{\Gamma_1 \vdash \sigma \rightarrow \tau \qquad \Gamma_2 \vdash \sigma}{\Gamma_1 \cup \Gamma_2 \vdash \tau}\ (APP) \qquad \Gamma_1 \cup \Gamma_2 \text{ consistente}$$

$$\frac{\Gamma \vdash \tau}{\Gamma \setminus \{\sigma\} \vdash (\sigma \rightarrow \tau)}\ (ABS) \qquad \Gamma \text{ consistente com } x : \sigma$$

Isto

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

Isomorfismo de Curry-Howard

Frmulas	$\sim$	**Tipos**
Demonstraes	$\sim$	**Termos (Programas)**
Normalizaes	$\sim$	**Computaes**
$\vdots$	$\sim$	$\vdots$

Correspondncia $\lambda \rightarrow \Rightarrow_L$ IPC($\rightarrow$) I

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

Δ_L deduo NJ_0 definida por:

- $M \equiv x$ e $\Delta \quad x : \tau \vdash x : \tau$ ento $\Delta_L \quad \tau \vdash \tau$
- $M \equiv PQ$ e $\Gamma = \Gamma_1 \cup \Gamma_2$ e o ltimo passo de Δ

$$\dfrac{\begin{array}{c}\Delta_1 \\ \vdots \\ \Gamma_1 \vdash M : \sigma \rightarrow \tau\end{array} \qquad \begin{array}{c}\Delta_2 \\ \vdots \\ \Gamma_2 \vdash N : \sigma\end{array}}{\Gamma_1 \cup \Gamma_2 \vdash (MN) : \tau} (\rightarrow E) = (APP)$$

Δ_L obtm-se aplicando $(\rightarrow E)$ a Δ_{1_L} e a Δ_{2_L}

Correspondncia $\lambda \rightarrow \Rightarrow_L$ IPC($\rightarrow$) II

- $M \equiv \lambda x.P$, $\tau \equiv \rho \rightarrow \sigma$, $\Gamma = \Gamma_1 - x$ e o ltimo passo em Δ

$$\frac{\begin{array}{c}\Delta_1 \\ \vdots \\ \Gamma \vdash P : \sigma\end{array}}{\Gamma \setminus \{x : \sigma\} \vdash (\lambda x.P) : (\rho \rightarrow \sigma)} (\rightarrow I) = (ABS)$$

Δ_L obtm-se aplicando $(\rightarrow I)$ a Δ_{1_L} a ρ.

Exemplos

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

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

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{a{\to}a{\to}c \vdash a{\to}a{\to}c \qquad a \vdash a}{a{\to}a{\to}c, a \vdash a{\to}c} \qquad a \vdash a}{a{\to}a{\to}c, a, a \vdash c}}{a{\to}a{\to}c, a \vdash a{\to}c}}{a{\to}a{\to}c \vdash a{\to}a{\to}c}}{\vdash (a{\to}a{\to}c){\to}a{\to}a{\to}c}$$

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

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

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{a{\to}a{\to}c \vdash a{\to}a{\to}c \qquad a \vdash a}{a{\to}a{\to}c, a \vdash a{\to}c} \qquad a \vdash a}{a{\to}a{\to}c, a \vdash c}}{a{\to}a{\to}c \vdash a{\to}c}}{a{\to}a{\to}c \vdash a{\to}a{\to}c}}{\vdash (a{\to}a{\to}c){\to}a{\to}a{\to}c}$$

Aplicando a correspondncia Curry-Howard temos em **IPC**($\rightarrow$):

- $\vdash (a \rightarrow b) \rightarrow (c \rightarrow a) \rightarrow (c \rightarrow b)$
- $\vdash (a \rightarrow a)$
- $\vdash (a \rightarrow b \rightarrow a)$
- $\vdash (a \rightarrow b \rightarrow c) \rightarrow b \rightarrow a \rightarrow c$
- $\vdash (a \rightarrow a \rightarrow b) \rightarrow a \rightarrow b$

Porque

- $\vdash \lambda xyz.x(yz) : (a \to b) \to (c \to a) \to (c \to b)$ **(B)**
- $\vdash \lambda x.x : (a \to a)$ **(I)**
- $\vdash \lambda xy.x : (a \to b \to a)$ **(K)**
- $\vdash \lambda xyz.xzy : (a \to b \to c) \to b \to a \to c$ **(C)**
- $\vdash \lambda xy.xyy : (a \to a \to b) \to a \to b$ **(W)**

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

Δ deduo $NJ_0(\rightarrow)$ de $\Gamma \vdash \tau$

$\Delta_\lambda$deduo-**TA**$_\lambda$de $\Gamma' \vdash M : \tau$, onde $\Gamma' = \{x : \tau \mid \tau \in \Gamma\}$, e definida por:

- se $\Delta \quad \Gamma, \tau \vdash \tau$ temos dois subcasos:
  1. $\tau \in \Gamma$. Ento $\Delta_\lambda \quad \Gamma' \vdash x : \tau$
  2. $\tau \notin \Gamma$. Ento $\Delta_\lambda \quad \Gamma', x : \tau \vdash x : \tau$
- ltimo passo de $\Delta \quad (\rightarrow \quad E)$ aplicada a concluses de Δ_1 e Δ_2 e Δ_{1_λ} e Δ_{2_λ} so dedues de
  $\Gamma'_1 \vdash M : \sigma \rightarrow \tau$ $\qquad$ $\Gamma'_2 \vdash N : \sigma$
  aplicar (APP) a Δ_{2_λ} aps substituir **todas** as variveis por novas, e ento

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

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

- ltimo passo de $\Delta \ (\rightarrow \ I)$

$$\frac{\Delta_1}{\Gamma, \rho \ \vdash \ \sigma \quad \Gamma \ \vdash \ \rho \rightarrow \sigma}$$

Consideramos dois sub-casos:

1. $\rho \in \Gamma$. Ento a concluso de $\Delta_{1_\lambda} \ \Gamma' \ \vdash \ P : \sigma$, com $v_i : \rho \in \Gamma'$ e $v_i \in FV(P)$. Podemos modificar Δ_{1_λ} para uma deduo de $\Gamma', x : \rho \ \vdash \ P^* : \sigma$, com x varivel nova e

$$P^* \equiv [x/v_1, \ldots, x/v_k]P$$

Aplicando (ABS) : $\Gamma' \ \vdash \ (\lambda x.P^*) : \rho \rightarrow \sigma$

2. $\rho \notin \Gamma$. Ento a concluso de $\Delta_{1_\lambda} \ \Gamma', x : \rho \ \vdash \ P : \sigma$ e aplicando (ABS) deduz-se

$$\Gamma' \ \vdash \ (\lambda x.P) : \rho \rightarrow \sigma$$

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

Exemp.

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

$()_\lambda \Rightarrow$ *dedues de tipos para* $\lambda xy.x$ *e* $\lambda yx.x$*:*

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

Se Δ uma deduo NJ_0 de $\sigma_1, ..., \sigma_n \vdash \tau$, $i \leq n$, ento Δ_λ uma deduo-TA$_\lambda$cuja concluso

$$x_{1_1} : \sigma_1, \ldots, x_{1_{m_1}} : \sigma_1, \ldots x_{n_1} : \sigma_n, \ldots, x_{n_{m_n}} : \sigma_n \vdash M : \tau$$

x_{i_j} **ocorre uma s vez em** M**.**

$$\Delta_{\lambda_L} = \Delta \qquad \textbf{mas} \qquad \Delta_{L_\lambda} \neq \Delta$$

Em que Δ_{L_λ} difere de Δ

1. Se Δ uma deduo-$\mathbf{TA}_\lambda$ de $\Gamma \vdash P : \tau$, ento Δ_{L_λ} uma deduo-$\mathbf{TA}_\lambda$ de

$$\Gamma_1 \vdash M : \tau$$

tal que

$$P \equiv_\alpha [v_1/x_1] \ldots [v_n/x_n]M$$

$$\Delta \equiv_\alpha [v_1/x_1] \ldots [v_n/x_n]\Delta_{L_\lambda}$$

$x_i \in FV(M)$ e v_i no necessariamente distintas

2. Se Δ uma demonstrao de $\vdash P : \tau$, Δ_{L_λ} uma demonstrao de $\vdash P : \tau$ a menos $\equiv_\alpha$

Teorema de Curry-Howard I

1. A frmulas que so teoremas da IPC so exactamente os tipos $\mathbf{TA}_\lambda$ de λ-termosfechados
2. $\sigma_1, \ldots, \sigma_n \vdash \tau$ sse existe M tal que $x_1 : \sigma_1, \ldots, x_n : \sigma_n \vdash M : \tau$
3. Para todas as demonstraes
   $\Delta_{L_\lambda} \equiv_\alpha \Delta$
   $\Delta_{\lambda_L} = \Delta$

$\mathbf{TA}_\lambda$	$\mathbf{IPC}(\rightarrow)$
tipos	frmulas
variveis	hipteses
termos	deduo (construo)
habitabilidade	derivabilidade
tipificabilidade	deduo para uma frmula
constructor	conectiva
redex	deduo com redundncias
reduo	normalizao
forma normal	derivao em forma normal

Habitabilidade=(Existe um termo deste tipo?)

Tipificabilidade=(Existe um tipo para este termo?)

Assim como temos sistemas de (inferncia) atribuio de tipos a termos, podemos ter sistemas que atribuam termos a frmulas...os mesmos.

Extenso a $\lambda(\rightarrow, \wedge, \vee)$ I

Extenso dos tipos simples a $\sigma \wedge \tau$ (ou $\sigma \times \tau$) e a $\sigma \vee \tau$ (ou $\sigma + \tau$)

Extenso dos λ-termos tipificados a pares e somas disjuntas:

Se $M : \tau$ e $N : \sigma$ so λ-termos, ento $< M, N > : \tau \wedge \sigma$ um λ-termo

Se $M : \tau \wedge \sigma$, ento $fst(M) : \tau$, $snd(M) : \sigma$ um λ-termo

Se $M : \tau$ ento $in_1^{\tau \vee \sigma}(M) : \tau \vee \sigma$ um λ-termo.

Se $M : \sigma$ ento $in_2^{\tau \vee \sigma}(M) : \tau \vee \sigma$ um λ-termo

Se $M : \tau \vee \sigma$, $L : \tau \rightarrow \tau'$ e $K : \sigma \rightarrow \tau'$ so λ-termos, ento $case(M, L, K) : \tau'$

As regras de inferncia correspondem a $\wedge E$, $\wedge I$, $\vee I$ e $\vee E$, anotadas com termos.

Regras de reduo

A noo de redex estende-se a estes construtores/destrutores

Extenso a $\lambda(\rightarrow, \wedge, \vee)$ II

$$fst(< t, u >) \longrightarrow t$$

$$snd(< t, u >) \longrightarrow u$$

$$case(in_1^{\tau \vee \sigma}(N), L, K) \longrightarrow LN$$

$$case(in_1^{\tau \vee \sigma}(N), L, K) \longrightarrow KN$$

Variaes e extenses do isomorfismo C-H

- sistemas axiomticos estilo-Hilbert e sistemas de lgica combinatria (**IPC**($\rightarrow$)corresponde a $\{\mathbf{B}, \mathbf{C}, \mathbf{K}, \mathbf{W}\}$)
- a lgica proposicional clssica (1990): interpretao para o terceiro excludo
- a lgica de primeira ordem intuicionista corresponde a (fragmentos) de sistemas de tipos dependentes
- a lgica proposicional de segunda ordem intuicionista corresponde a sistemas de tipos polimrficos

NJ calculus: regras para os quantificadores (primeira ordem)

$$\frac{\Gamma \vdash \varphi[v/x]}{\Gamma \vdash \forall x\, \varphi}\ \forall\mathbf{I} \quad \text{(a)}$$

$$\frac{\Gamma \vdash \forall x\, \varphi}{\Gamma \vdash \varphi[t/x]}\ \forall\mathbf{E} \quad \text{(b)}$$

$$\frac{\Gamma \vdash \varphi[t/x]}{\Gamma \vdash \exists x\, \varphi}\ \exists\mathbf{I} \quad \text{(b)}$$

$$\frac{\Gamma \vdash \exists x\, \varphi \qquad \Gamma, \varphi[t/x] \vdash \psi}{\Gamma \vdash \psi}\ \exists\mathbf{E} \quad \text{(a)}$$

(a) onde v uma varivel nova que no est em Γ, Δ

(b) onde x livre para t em φ

Lgica Primeira Ordem Intuicionista

A interpretao construtiva de (Brower-Heyting-Komolgorov) estende-se para:

- Uma construo de $\forall x \varphi(x)$ um mtodo de transformar qualquer objecto $\mathbf{a}$ numa construo de $\varphi(\mathbf{a})$.
- Uma construo de $\exists x \varphi(x)$ um par que consiste num objecto $\mathbf{a}$ e uma construo de $\varphi(\mathbf{a})$.

Quantificao universal $\forall$: conjuno generalizada...

Quantificao existncial $\exists$: disjuno generalizada...

Mas: A quantificao universal $\forall$ tambm se assemelha a $\rightarrow$. Em ambos a construo so mtodos.

Tipos dependentes

Generalizam os tipos $\alpha \to \beta$ que correspondem a funes cujo argumento tem tipo α e os objectos tm tipo β.

Suponhamos o tipo *string*(n) das strings de tamanho n. Este tipo depende de n : *int* e pode ser considerado um predicado sobre o tipo *int*. O *constructor string* tem tipo $int \to Type$.

Podemos generalizar a outros predicados n-rios ($\tau_1 \to \cdots \tau_n \to Type$). E quantificar universalmente

No caso anterior, teramos:

$$\forall x : int, string(x)$$

que pode ser o tipo de uma funo que para qualquer inteiro n retorna uma string de tamanho n .

Produto dependente e Isomorfismo Curry-Howard

$\forall x : \tau, \sigma$ o tipo de uma funo que aplicada a objectos de tipo τ e retorna um objecto de tipo $\sigma[x/a]$ para todo $a : \tau$.

Se x no ocorre em σ, $\forall x : \tau, \sigma$ corresponde a $\tau \to \sigma$.

Exemp. (Exemplos de tipos dependentes (Coq))

$\forall n : int, n \leq n$

$\forall n, m : nat, n \leq m \to n \leq m + 1$

$\forall P, Q : \texttt{Prop}, P \vee Q \to Q \vee P$

$nat \to nat \to \texttt{Prop}$

$\forall n, p : nat, bin\, n \to bin\, p \to bin\, (n + p)$

$\forall n : nat, list\, n$

$\forall A : Set, A \to list\, A \to list\, A$

$\forall A, B : Set, A \to B \to A * B$

$\forall A, B : Set, A * B \to A$

Porqu "produto"?BCK outra vez...

No C-H um tipo (frmula) α interpretado como o conjunto de demonstraes de α, $[\![\alpha]\!]$. Temos, em termos de operaes entre conjuntos:

$$\begin{array}{lcl}
[\![\alpha \wedge \beta]\!] & = & [\![\alpha]\!] \times [\![\beta]\!] \\
[\![\alpha \vee \beta]\!] & = & [\![\alpha]\!] \cup [\![\beta]\!] \\
[\![\alpha \to \beta]\!] & = & [\![\alpha]\!] \to [\![\beta]\!] \\
[\![\mathsf{F}]\!] & = & \emptyset \\
[\![\forall x \alpha(x)]\!] & = & \Pi_{a:A}.[\![\alpha(a)]\!] \\
[\![\exists x \alpha(x)]\!] & = & \Sigma_{a:A}.[\![\alpha(a)]\!]
\end{array}$$

onde

$$\begin{array}{lcl}
A \times B & = & \{(a,b) \mid a \in A \text{ e } b \in B\} \\
A \cup B & = & \{(0,a) \mid a \in A\} \cup \{(1,b) \mid b \in B\} \\
A \to B & = & \{f \mid \forall a \in A\, f(a) \in B\} \\
\Pi_{a:A}.Pa & = & \{f : A \to \cup_{a:A} Pa \mid \forall a : A,\, f(a) \in Pa\} \\
\Sigma_{a:A}.Pa & = & \{(a,p) \mid a \in A \text{ e } p \in Pa\}
\end{array}$$

e onde $\{Pa\}_{a:A}$ uma familia indexada de conjuntos.


Yves Bertot and Pierre Castéran.
Interactive Theorem Proving and Program Development Coq'Art: The Calculus of Inductive Constructions.
Texts in Theoretical Computer Science. An EATCS Series. SV, 2004.


Morten B. Sorensen Pawel Urzyczyn.
Lecture on the curry-howard isomorphism.
Technical report, University of Copenhagen, 1996.