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 especificação e a obtenção de programas que satisfaçam essa especificação.
- desenvolvimento de demonstrações matemáticas numa lógica de ordem superior
- ambiente de desenvolvimento de lógicas diversas: temporais, modais, de descrição, etc.
- uma linguagem (funcional) de especificação
- baseado num λ-calculus tipificado polimórfico com tipos dependentes e noção primitiva de tipos indutivos: o Cálculo de Construções Indutivas (CoC, pCiC).

Sistemas de dedutivos para lógica proposicional

Dado um conjunto de variáveis $\mathcal{V}_{prop}$, sejam as fórmulas

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

Um sistema dedutivo é um conjunto de regras a partir das quais é possível obter (deduzir) uma fórmula (supondo ou não um conjunto inicial Γ): $\vdash \alpha$ ou $\Gamma \vdash \alpha$

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

Pretendem-se sistemas íntegros e completos:

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

ou mais geralmente:

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

Não tem axiomas. Só regras de inferência. Para cada conectiva lógica existem dois tipos de regras: de introdução e de eliminação.

As fórmulas iniciais podem ser hipóteses (premissas) introduzidas para a aplicação duma regra: iniciam um sub-dedução que quando termina cancela as respectivas hipóteses

Dedução natural, NK_0

	Introdução	**Eliminação**
$\wedge$	$\dfrac{\alpha \quad \beta}{\alpha \wedge \beta} \wedge \mathbf{I}$	$\dfrac{\alpha \wedge \beta}{\alpha} \wedge \mathbf{E}_1 \qquad \dfrac{\alpha \wedge \beta}{\beta} \wedge \mathbf{E}_2$
$\vee$	$\dfrac{\alpha}{\alpha \vee \beta} \vee \mathbf{I}_1 \qquad \dfrac{\beta}{\alpha \vee \beta} \vee \mathbf{I}_2$	$\dfrac{\alpha \vee \beta \qquad \begin{matrix}[\alpha] \\ \gamma\end{matrix} \qquad \begin{matrix}[\beta] \\ \gamma\end{matrix}}{\gamma} \vee \mathbf{E}$
$\rightarrow$	$\dfrac{\begin{matrix}[\alpha] \\ \beta\end{matrix}}{\alpha \rightarrow \beta} \rightarrow \mathbf{I}$	$\dfrac{\alpha \qquad \alpha \rightarrow \beta}{\beta} \rightarrow \mathbf{E}$

Dedução natural, NK_0 (cont.)

	Introdução	**Eliminação**
$\neg$	$\dfrac{\begin{array}{c}[\alpha]\\ \vdots \\ \mathsf{F}\end{array}}{\neg\alpha}\,\neg\mathbf{I}$	$\dfrac{\alpha \quad \neg\alpha}{\beta}\,\neg\mathbf{E}$
$\neg\neg$	$\dfrac{\begin{array}{c}\vdots \\ \alpha\end{array}}{\neg\neg\alpha}\,\neg\neg\mathbf{I}$	$\dfrac{\begin{array}{c}\vdots \\ \neg\neg\alpha\end{array}}{\alpha}\,\neg\neg\mathbf{E}$

NK_0 em *sequents*

Supondo que Γ (contexto) é um conjunto de fórmulas:

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

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

Deduções com *sequents* I

Agora os nós das árvores de dedução são *sequents* e $\vdash \Gamma \vdash \alpha$ é o mesmo que $\Gamma \vdash \alpha$

Exemplo

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

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

Métodos de demonstração

A semântica da lógica clássica é baseada na noção de *verdade*. E em particular cada proposição é absolutamente verdadeira ou falsa. Isso traduz-se pelo princípio do terceiro excluído: $p \vee \neg p$.

Mas isto não nos dá muita informação.

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

Dem. Demonstração por casos: Seja $\sqrt{2}^{\sqrt{2}}$. Este número é racional ou irracional.

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

□

Mas afinal quais são esses valores? A demonstração não é constructiva.

Intuicionismo I

Uma proposição só é verdadeira ou falsa, se nós soubermos porquê que isso acontece... ou seja se podermos ter uma demonstração construtiva dela...(BHK)

A semântica duma proposição deve basear-se na noção de demonstração: uma fórmula é verdadeira se tivermos uma construção para uma demonstração dela e esta noção estende-se para às conectivas:

- Uma construção de $\alpha \wedge \beta$ consiste numa construção de α e numa construção de β
- Uma construção de $\alpha \vee \beta$ consiste numa construção de α ou numa construção de β
- Uma construção de $\alpha \rightarrow \beta$ é um método de transformar qualquer construção de α numa construção de β

Intuicionismo II

- Uma construção de $\neg\alpha$ é um método de transformar qualquer construção de α num objecto não que existe (ou seja $\neg\alpha \equiv \alpha \rightarrow \mathsf{F}$) (**RA**)

Mostrar que $p \rightarrow \neg\neg p$ (ou $p \rightarrow ((p \rightarrow \mathsf{F}) \rightarrow \mathsf{F})$ é uma tautologia intuicionista:

> *Dada uma demonstração de p, podemos obter uma demonstração para* $((p \rightarrow F) \rightarrow F)$*: Seja uma demonstração para* $(p \rightarrow F)$*, isto é, um método de transformar demonstrações de p em demonstração de F. Como temos uma demonstração para p podemos ter uma demonstração para F*

Mas $\neg\neg p \rightarrow p$ não é uma tautologia intuicionista: o facto de não termos uma demonstração para $\neg p$ não nos permite concluir que tenhamos uma demonstração para p...

E, do mesmo modo $p \vee \neg p$ não é uma taulogogia!... em geral não é garantido que se tenha uma demonstração para p ou uma para $\neg p$.

Intuicionismo III

A lógica intuicionista NJ_0 obtêm-se da lógica clássica, p.e, retirando a regra $\neg\neg\mathbf{E}$ do sistema NK_0...

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

IPC($\rightarrow$): lógica proposicional intuicionista só com implicação

Γ conjunto de fórmulas $\qquad$ $\Gamma \vdash \Theta$ *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 I

$x \in V$, V conjunto de variáveis

λ-termos: variáveis, aplicações, abstrações

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

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

Reduções

- Variáveis livres $FV(\Lambda)$:
  $FV(x) = \{x\}$ $FV(MN) = FV(M) \cup FV(N)$ $FV(\lambda x.M) = FV(M) \setminus \{x\}$
- Substituição de N por x em M, $M[N/x]$
- Redução α: $\lambda x.M \to_\alpha \lambda y.M[y/x]$, se $y \notin FV(M)$
- Redução β (um passo): $(\lambda x.M)P \to_\beta P[M/x]$
  β-Redex: $(\lambda x.M)P$
- Fecho transitivo-reflexivo: $\to_\beta^\star$
- Conversão (simetria) : $=_\beta$

Forma normal β

- Um λ-termo está em forma normal β se não tiver nenhum redex.
- Se um λ-termo tiver forma normal ela é única.
- Existem $\lambda - \textit{termos}$ que não têm 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 variáveis de tipo, um tipo simples (**TA**$_\lambda$) é dado por
$$\tau := \iota \mid \tau \rightarrow \tau$$
- $\tau \rightarrow (\sigma \rightarrow \tau)$ (associam à direita)
- Atribuições 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 atribuições $x : \tau$ consistente

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

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

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

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

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

Se omitirmos os λ-termos temos só dedução de fórmulas em IPC($\rightarrow$):

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

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

Isto é

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

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

IPC($\rightarrow$): lógica proposicional intuicionista só com implicação

Γ conjunto de fórmulas $\qquad$ $\Gamma \vdash \Theta$ *sequent*

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

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

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

Isomorfismo de Curry-Howard

Fórmulas	$\sim$	**Tipos**
Demonstrações	$\sim$	**Termos (Programas)**
Normalizações	$\sim$	**Computações**
$\vdots$	$\sim$	$\vdots$

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

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

Δ_L dedução NJ_0 definida por:

- $M \equiv x$ e Δ é $x : \tau \vdash x : \tau$ então Δ_L é $\tau \vdash \tau$
- $M \equiv PQ$ e $\Gamma = \Gamma_1 \cup \Gamma_2$ e o último passo de Δ é

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

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

Correspondência $\lambda \to \Rightarrow_L$ IPC($\to$) II

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

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

  Δ_L obtém-se aplicando $(\to \ I)$ 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 correspondência 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)**

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

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

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

- se Δ é $\Gamma, \tau \vdash \tau$ temos dois subcasos:
  1. $\tau \in \Gamma$. Então Δ_λ é $\Gamma' \vdash x : \tau$
  2. $\tau \notin \Gamma$. Então Δ_λ é $\Gamma', x : \tau \vdash x : \tau$
- último passo de Δ é $(\rightarrow E)$ aplicada a conclusões de Δ_1 e Δ_2 e Δ_{1_λ} e Δ_{2_λ} são deduções de
  $\Gamma'_1 \vdash M : \sigma \rightarrow \tau$ $\qquad$ $\Gamma'_2 \vdash N : \sigma$
  aplicar (APP) a Δ_{2_λ} após substituir **todas** as variáveis por novas, e então

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

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

- último passo de Δ é ($\rightarrow$ I)

$$\frac{\begin{array}{c}\Delta_1 \\ \Gamma, \rho \vdash \sigma\end{array}}{\Gamma \vdash \rho \rightarrow \sigma}$$

Consideramos dois sub-casos:

1. $\rho \in \Gamma$. Então a conclusão de Δ_{1_λ} é $\Gamma' \vdash P : \sigma$, com $v_i : \rho \in \Gamma'$ e $v_i \in FV(P)$. Podemos modificar Δ_{1_λ} para uma dedução de $\Gamma', x : \rho \vdash P^* : \sigma$, com x variável nova e

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

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

2. $\rho \notin \Gamma$. Então a conclusão de Δ_{1_λ} é $\Gamma', x : \rho \vdash P : \sigma$ e aplicando (ABS) deduz-se

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

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

Exemplo

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

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

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

Se Δ é uma dedução NJ_0 de $\sigma_1, ..., \sigma_n \vdash \tau$, $i \leq n$, então Δ_λ é uma dedução-TA_λcuja conclusão é

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

x_{i_j} **ocorre uma só 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 é uma dedução-$\mathbf{TA}_\lambda$ de $\Gamma \vdash P : \tau$, então Δ_{L_λ} é uma dedução-$\mathbf{TA}_\lambda$ 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 não necessariamente distintas

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

Teorema de Curry-Howard I

1. A fórmulas que são teoremas da IPC são exactamente os tipos $\mathbf{TA}_\lambda$ de λ-termos fechados
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 demonstrações
   $\Delta_{L_\lambda} \equiv_\alpha \Delta$
   $\Delta_{\lambda_L} = \Delta$

$\mathbf{TA}_\lambda$	$\mathbf{IPC}(\rightarrow)$
tipos	fórmulas
variáveis	hipóteses
termos	dedução (construção)
habitabilidade	derivabilidade
tipificabilidade	dedução para uma fórmula
constructor	conectiva
redex	dedução com redundâncias
redução	normalização
forma normal	derivação em forma normal

Habitabilidade=(Existe um termo deste tipo?)

Tipificabilidade=(Existe um tipo para este termo?)

Assim como temos sistemas de (inferência) atribuição de tipos a termos, podemos ter sistemas que atribuam termos a fórmulas...os mesmos.

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

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

Extensão dos λ-termo s tipificados a pares e somas disjuntas:

Se $M : \tau$ e $N : \sigma$ são λ-termo s, então $< M, N >: \tau \wedge \sigma$ é um λ-termo

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

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

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

Se $M : \tau \vee \sigma$, $L : \tau \rightarrow \tau'$ e $K : \sigma \rightarrow \tau'$ são λ-termo s, então $case(M, L, K) : \tau'$

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

Regras de redução

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

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

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

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

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

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

Variações e extensões do isomorfismo C-H

- sistemas axiomáticos estilo-Hilbert e sistemas de lógica combinatória (**IPC**($\rightarrow$)corresponde a $\{\mathbf{B}, \mathbf{C}, \mathbf{K}, \mathbf{W}\}$)
- a lógica proposicional clássica (1990): interpretação para o terceiro excluído
- a lógica de primeira ordem intuicionista corresponde a (fragmentos) de sistemas de tipos dependentes
- a lógica proposicional de segunda ordem intuicionista corresponde a sistemas de tipos polimórficos

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 é uma variável nova que não está em Γ, Δ

(b) onde x é livre para t em φ

Lógica Primeira Ordem Intuicionista

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

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

Quantificação universal $\forall$: conjunção generalizada...

Quantificação existêncial $\exists$: disjunção generalizada...

Mas: A quantificação universal $\forall$ também se assemelha a $\rightarrow$. Em ambos a construção são métodos.

Tipos dependentes

Generalizam os tipos $\alpha \to \beta$ que correspondem a funções cujo argumento tem tipo α e os objectos têm 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-ários ($\tau_1 \to \cdots \tau_n \to Type$). E quantificar universalmente

No caso anterior, teríamos:

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

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

Produto dependente e Isomorfismo Curry-Howard

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

Se x não ocorre em σ, $\forall x : \tau, \sigma$ corresponde a $\tau \to \sigma$.

Exemplo (Exemplos de tipos dependentes (Coq))

$\forall n : int, n \leq n$
$\forall n, m : nat, n \leq m \to n \leq m + 1$
$\forall P, Q : \texttt{Prop}, P \vee Q \to Q \vee P$
$nat \to nat \to \texttt{Prop}$
$\forall n, p : nat, bin\, n \to bin\, p \to bin\, (n + p)$
$\forall n : nat, list\, n$
$\forall A : Set, A \to list\, A \to list\, A$
$\forall A, B : Set, A \to B \to A * B$
$\forall A, B : Set, A * B \to A$

Porquê "produto"?BCK outra vez...

No C-H um tipo (fórmula) α é interpretado como o conjunto de demonstrações de α, $[\![\alpha]\!]$. Temos, em termos de operações 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 $\{Pa\}_{a:A}$ é uma familia indexada de conjuntos.