



Representação de Provas em Teoria de Tipos

*Encontro Nacional da Sociedade Portuguesa de Matemática
6 de Maio de 2004*

Luís Cruz-Filipe

Universidade de Nijmegen, Holanda
Centro de Lógica e Computação, Portugal

Plano



1. Introdução

1. Introdução

2. O Isomorfismo de Curry–Howard

1. Introdução
2. O Isomorfismo de Curry–Howard
3. A Biblioteca CoRN

1. Introdução
2. O Isomorfismo de Curry–Howard
3. A Biblioteca CoRN
4. Aplicações & Exemplos

1. Introdução
2. O Isomorfismo de Curry–Howard
3. A Biblioteca CoRN
4. Aplicações & Exemplos
5. Conclusões

O Isomorfismo de Curry–Howard



O Isomorfismo de Curry–Howard

Proposições \leftrightarrow Tipos

O Isomorfismo de Curry–Howard

Proposições \leftrightarrow Tipos

Provas \leftrightarrow Termos

O Isomorfismo de Curry–Howard

Proposições \leftrightarrow Tipos

Provas \leftrightarrow Termos

prova correcta? \leftrightarrow verificação de tipo

O Isomorfismo de Curry–Howard

Proposições \leftrightarrow Tipos

Provas \leftrightarrow Termos

prova correcta? \leftrightarrow verificação de tipo
 \rightsquigarrow decidível

O Isomorfismo de Curry–Howard

Proposições \leftrightarrow Tipos

Provas \leftrightarrow Termos

prova correcta? \leftrightarrow verificação de tipo
 \rightsquigarrow decidível
 \rightsquigarrow algoritmo simples

Exemplos



Exemplos

$$\frac{\begin{array}{c} [A] \\ \vdots \\ B \end{array}}{A \rightarrow B}$$

Exemplos

$$\frac{[A] \quad \vdots \quad B}{A \rightarrow B} \leftrightarrow \frac{x : A \vdash M : B}{\lambda x : A. M : A \rightarrow B}$$

Exemplos

$$\frac{[A] \quad \vdots \quad B}{A \rightarrow B} \leftrightarrow \frac{x : A \vdash M : B}{\lambda x : A. M : A \rightarrow B}$$

Cálculo- λ \leftrightarrow “Minimal Logic”

Exemplos

$$\frac{[A] \quad \vdots \quad B}{A \rightarrow B} \leftrightarrow \frac{x : A \vdash M : B}{\lambda x : A. M : A \rightarrow B}$$

Cálculo- λ \leftrightarrow “Minimal Logic”

λP \leftrightarrow FOL intuicionista

Exemplos

$$\frac{[A] \quad \vdots \quad B}{A \rightarrow B} \leftrightarrow \frac{x : A \vdash M : B}{\lambda x : A. M : A \rightarrow B}$$

Cálculo- λ \leftrightarrow “Minimal Logic”

λP \leftrightarrow FOL intuicionista

λP_{ω} \leftrightarrow HOL

Exemplos

$$\frac{[A] \quad \vdots \quad B}{A \rightarrow B} \leftrightarrow \frac{x : A \vdash M : B}{\lambda x : A. M : A \rightarrow B}$$

Cálculo- λ \leftrightarrow “Minimal Logic”

λP \leftrightarrow FOL intuicionista

λP_ω \leftrightarrow HOL

CiC \leftrightarrow HOL com tipos indutivos

Formalização de Matemática



Formalização de Matemática

- ⑥ Representação fidedigna de *provas* num computador

Formalização de Matemática

- ⑥ Representação fidedigna de *provas* num computador
- ⑥ Garantia elevada de correcção

Formalização de Matemática

- ⑥ Representação fidedigna de *provas* num computador
- ⑥ Garantia elevada de correcção
- ⑥ Apresentação e visualização de resultados

Formalização de Matemática

- ⑥ Representação fidedigna de *provas* num computador
- ⑥ Garantia elevada de correcção
- ⑥ Apresentação e visualização de resultados
- ⑥ Troca de informação

Formalização de Matemática

- ⑥ Representação fidedigna de *provas* num computador
- ⑥ Garantia elevada de correcção
- ⑥ Apresentação e visualização de resultados
- ⑥ Troca de informação
- ⑥ Aplicações

O Projecto CoRN



O Projecto CoRN

- ⑥ Biblioteca de matemática formalizada em Coq

O Projecto CoRN

- ⑥ Biblioteca de matemática formalizada em Coq
- ⑥ Formalização sistemática

O Projecto CoRN

- ⑥ Biblioteca de matemática formalizada em Coq
- ⑥ Formalização sistemática
 - ~→ analisar também o *processo* de formalização

O Projecto CoRN

- ⑥ Biblioteca de matemática formalizada em Coq
- ⑥ Formalização sistemática
 - ↔ analisar também o *processo* de formalização
- ⑥ Apresentação e partilha

O Projecto CoRN

- ⑥ Biblioteca de matemática formalizada em Coq
- ⑥ Formalização sistemática
 - ↪ analisar também o *processo* de formalização
- ⑥ Apresentação e partilha
- ⑥ Aplicações

CoRN: Conteúdo



CoRN: Conteúdo

- ⑥ Estruturas algébricas, polinómios
- ⑥ Números reais e complexos
- ⑥ Teorema Fundamental da Álgebra (Barendregt, Geuvers, Niqui, Pollack, Wiedijk, Zwanenburg)

CoRN: Conteúdo

- ⑥ Estruturas algébricas, polinómios
- ⑥ Números reais e complexos
- ⑥ Teorema Fundamental da Álgebra (Barendregt, Geuvers, Niqui, Pollack, Wiedijk, Zwanenburg)
- ⑥ Análise Real (Cálculo Diferencial e Integral)
- ⑥ Séries de funções, funções transcendentas (Cruz-Filipe)

CoRN: Conteúdo

- ⑥ Estruturas algébricas, polinómios
- ⑥ Números reais e complexos
- ⑥ Teorema Fundamental da Álgebra (Barendregt, Geuvers, Niqui, Pollack, Wiedijk, Zwanenburg)
- ⑥ Análise Real (Cálculo Diferencial e Integral)
- ⑥ Séries de funções, funções transcendentas (Cruz-Filipe)
- ⑥ Teoria de Grupos (Barendregt, Synek)

CoRN: Conteúdo

- ⑥ Estruturas algébricas, polinómios
- ⑥ Números reais e complexos
- ⑥ Teorema Fundamental da Álgebra (Barendregt, Geuvers, Niqui, Pollack, Wiedijk, Zwanenburg)
- ⑥ Análise Real (Cálculo Diferencial e Integral)
- ⑥ Séries de funções, funções transcendentas (Cruz-Filipe)
- ⑥ Teoria de Grupos (Barendregt, Synek)
- ⑥ Modelos e contra-exemplos (Loeb)

CoRN: Conteúdo

- ⑥ Estruturas algébricas, polinómios
- ⑥ Números reais e complexos
- ⑥ Teorema Fundamental da Álgebra (Barendregt, Geuvers, Niqui, Pollack, Wiedijk, Zwanenburg)
- ⑥ Análise Real (Cálculo Diferencial e Integral)
- ⑥ Séries de funções, funções transcendententes (Cruz-Filipe)
- ⑥ Teoria de Grupos (Barendregt, Synek)
- ⑥ Modelos e contra-exemplos (Loeb)
- ⑥ ... (Hendriks, Hinderer, Mamane, Spitters)

CoRN: Exemplos



CoRN: Exemplos

- ⑥ Da biblioteca:

CoRN: Exemplos

- 6 Da biblioteca:

Álgebra: $\forall f:R[\mathbb{C}].(\text{nc } f) \Rightarrow \exists z:\mathbb{C}.f(z) = 0$

CoRN: Exemplos

6 Da biblioteca:

Álgebra: $\forall f:R[\mathbb{C}].(\text{nc } f) \Rightarrow \exists z:\mathbb{C}.f(z) = 0$

Trigonometria: $\forall x:\mathbb{R}.\cos^2(x) + \sin^2(x) = 1$

CoRN: Exemplos

6 Da biblioteca:

Álgebra: $\forall f:R[\mathbb{C}].(\text{nc } f) \Rightarrow \exists z:\mathbb{C}.f(z) = 0$

Trigonometria: $\forall x:\mathbb{R}.\cos^2(x) + \sin^2(x) = 1$

Números Complexos: $e^{i\pi} + 1 = 0$

CoRN: Exemplos

6 Programas extraídos:

aproximação	valor de e	valor de $\sqrt{2}$
0	$\frac{0}{1} = 0$	$\frac{0}{1} = 0$
1	$\frac{1}{1} = 1$	$\frac{3}{3} = 1$
2	$\frac{2}{1} = 2$	$\frac{3}{3} = 1$
5	$\frac{65}{24} \approx 2.70833$	$\frac{35}{27} \approx 1.2963$
10	$\frac{98641}{36288} \approx 2.71828$	$\frac{27755}{19683} \approx 1.4101$

Conclusões



Conclusões

- ⑥ Isomorfismo de Curry–Howard permite representar conceitos matemáticos (definição, teorema, demonstração) num computador

Conclusões

- ⑥ Isomorfismo de Curry–Howard permite representar conceitos matemáticos (definição, teorema, demonstração) num computador
- ⑥ Utilidade e possibilidade de desenvolver bibliotecas extensas

Conclusões

- ⑥ Isomorfismo de Curry–Howard permite representar conceitos matemáticos (definição, teorema, demonstração) num computador
- ⑥ Utilidade e possibilidade de desenvolver bibliotecas extensas
- ⑥ Aplicações