



UNIVERSIDADE ABERTA  
DEPARTAMENTO de CIÊNCIAS e TECNOLOGIAS  
MESTRADO em ESTATÍSTICA, MATEMÁTICA e COMPUTAÇÃO

# **Polimorfismo Atómico e o Teorema da Normalização Forte**

Maria do Rosário Dinis Inácio

Dissertação de Mestrado

2014

MESTRADO em ESTATÍSTICA, MATEMÁTICA e COMPUTAÇÃO

# Polimorfismo Atômico e o Teorema da Normalização Forte

Maria do Rosário Dinis Inácio

Orientador: Professor Doutor Mário Jorge Edmundo

Co-orientador: Professora Doutora Gilda Maria Saraiva Dias Ferreira

Dissertação apresentada ao programa de **Mestrado em Estatística, Matemática e Computação** do **Departamento de Matemática e Tecnologia da Universidade Aberta** como requisito parcial para obtenção do grau de Mestre em **Estatística, Matemática e Computação**.

2014

*Ao meu filho - José Pedro*

# Agradecimentos

Esta dissertação é resultado de muito esforço e dedicação, e não poderia deixar de agradecer a todos os que estiveram do meu lado durante o seu desenvolvimento.

Ao Professor Doutor Mário Jorge Edmundo, por ter atendido ao meu pedido para ser orientador de um trabalho em Lógica Matemática, pela sugestão do tema e pela sua constante disponibilidade para me ajudar.

À Professora Doutora Gilda Maria Ferreira, pelas sugestões, críticas, orientações e apoio para o desenvolvimento da pesquisa e escrita do trabalho sem as quais não teria conseguido concretizar este projeto. Agradeço também a sua constante disponibilidade para me ajudar. Aos meus amigos pelo incentivo. À Glória pela ajuda com o Inglês. À Isabel pela ajuda com a escrita.

Por fim, à minha família, por me transmitir a coragem necessária para levar a cabo um trabalho desta natureza. Este trabalho não seria possível sem o apoio e generosidade dos meus pais.

## Resumo

Nesta dissertação provamos, através do sistema  $\mathbf{F}_{\text{at}}$  (restrição predicativa do sistema polimórfico  $\mathbf{F}$  de Jean-Yves Girard), que o cálculo proposicional intuicionista é fortemente normalizável considerando  $\beta$ -conversões.

Embora o resultado em si seja bem conhecido, a estratégia (via  $\mathbf{F}_{\text{at}}$ ) seguida nesta dissertação é muito recente, tendo sido apresentada em 2013 no artigo Atomic Polymorphism [7]. Esta dissertação pretende ser um estudo autocontido e detalhado dos resultados desse artigo.

O sistema  $\mathbf{F}_{\text{at}}$  começa por ser apresentado em  $\lambda$ -cálculo e através do Isomorfismo de Curry-Howard apresentamos também a sua formulação no cálculo de dedução natural. O sistema contém apenas dois geradores de tipos (fórmulas): implicação e quantificação universal de segunda-ordem restrita a instanciações atómicas, daí a designação de polimorfismo atómico ( $\mathbf{F}_{\text{at}}$ ).

Dois resultados centrais em  $\mathbf{F}_{\text{at}}$  são demonstrados:

- i. o cálculo proposicional intuicionista pode ser imerso em  $\mathbf{F}_{\text{at}}$  (via definição de conectivos de Prawitz e transbordo de instanciação);
- ii. o sistema  $\mathbf{F}_{\text{at}}$  é fortemente normalizável considerando  $\beta\eta$ -conversões (adaptação simples da técnica de redutibilidade de Tait).

Por último, e com o objectivo de mostrar que a normalização forte de  $\mathbf{F}_{\text{at}}$  implica a normalização forte do cálculo proposicional intuicionista, provamos que as  $\beta$ -conversões deste último cálculo se traduzem num número finito de  $\beta\eta$ -conversões em  $\mathbf{F}_{\text{at}}$ .

Tal como nos resultados anteriores também nesta demonstração apresentamos todos os casos, incluindo aqueles que no artigo, por uma questão de limitação de espaço estavam omissos. Um limite ao número máximo de  $\beta\eta$ -conversões que surgem aquando da tradução das  $\beta$ -conversões é também apresentado.

**Palavras-chave:** Polimorfismo atómico, cálculo proposicional intuicionista, normalização forte,  $\lambda$ -cálculo, dedução natural, isomorfismo de Curry-Howard, transbordo de instanciação.

## Abstract

In this dissertation we prove through the system  $\mathbf{F}_{\text{at}}$  (predicative restriction of Jean-Yves Girard's system  $\mathbf{F}$ ) that the intuitionistic propositional calculus is strongly normalizable, considering  $\beta$ -conversions.

Although the result is well-known, the strategy (via  $\mathbf{F}_{\text{at}}$ ) followed in this dissertation is quite recent. It was presented in 2013 in the paper Atomic Polymorphism [7]. The present dissertation intends to be a self-contained and detailed study of the results in the paper.

System  $\mathbf{F}_{\text{at}}$  is firstly presented in  $\lambda$ -calculus, and via Curry-Howard's isomorphism we also present its formulation in the natural deduction calculus. The system contains only two generators of types (formulas): implication and second-order universal quantification, restricted to atomic instantiations - which explains the designation of atomic polymorphism  $\mathbf{F}_{\text{at}}$ .

Two central results in  $\mathbf{F}_{\text{at}}$  are proved:

- i. the intuitionistic propositional calculus can be embedded into  $\mathbf{F}_{\text{at}}$  (via Prawitz's definition of connectives and instantiation overflow);
- ii. the system  $\mathbf{F}_{\text{at}}$  is strongly normalizable, considering  $\beta\eta$ -conversions (simple adaptation of the Tait's reducibility technique).

Finally, aiming at demonstrating that the strong normalization of  $\mathbf{F}_{\text{at}}$  implies the strong normalization of intuitionistic propositional calculus, we prove that the  $\beta$ -conversions of this latter calculus can be translated into a finite number of  $\beta\eta$ -conversions of  $\mathbf{F}_{\text{at}}$ .

As in the previous results, we present all the cases, including those which were left aside in the article, due to space limitations. An upper-bound on the number of  $\beta\eta$ -conversions that appear during the translation of the  $\beta$ -conversions is also presented.

**Keywords:** Atomic polyphormism, intuitionistic propositional calculus, strong normalization,  $\lambda$ -calculus, natural deduction, Curry-Howard isomorphism, instantiation overflow.

# Conteúdo

<b>1</b>	<b>Introdução</b>	<b>2</b>
<b>2</b>	<b>Lógica Proposicional Intuicionista</b>	<b>4</b>
2.1	Intuicionismo . . . . .	4
2.2	Sistema de Hilbert . . . . .	5
2.3	Sistema de Dedução Natural . . . . .	7
2.3.1	Normalização em Dedução Natural . . . . .	12
<b>3</b>	<b>Cálculo Lambda e o Isomorfismo de Curry-Howard</b>	<b>15</b>
3.1	Cálculo lambda simplesmente tipado . . . . .	16
3.1.1	Tipos . . . . .	16
3.1.2	Termos . . . . .	16
3.1.3	Conversões, reduções, forma normal . . . . .	17
3.2	Isomorfismo de Curry-Howard . . . . .	18
3.3	O Sistema $\mathbf{F}$ . . . . .	20
3.4	O Sistema $\mathbf{F}_{\text{at}}$ . . . . .	22
<b>4</b>	<b>Teorema da Normalização Forte para <math>\mathbf{F}_{\text{at}}</math></b>	<b>27</b>
<b>5</b>	<b>Imersão do Cálculo Proposicional Intuicionista em <math>\mathbf{F}_{\text{at}}</math></b>	<b>33</b>
<b>6</b>	<b>Normalização Forte para o Cálculo Prop. Intuicionista</b>	<b>52</b>

# Capítulo 1

## Introdução

Normalização é um conceito fundamental em Teoria da Demonstração. O teorema da normalização (na sua versão fraca) afirma que sendo possível derivar uma asserção a partir de um conjunto de hipóteses, será possível conseguir uma derivação dessa mesma asserção, partindo das mesmas hipóteses, evitando certas formas de raciocínio redundante. Estas últimas derivações, optimizadas no sentido acima, são chamadas *normais*. Mais, existe uma forma de chegar à derivação normal, partindo da inicial, aplicando um número finito de transformações elementares concretas conhecidas como conversões. Nesta dissertação estamos contudo interessados num resultado mais forte que implica o anterior: *o teorema da normalização forte*. O teorema da normalização forte, mais do que garantir que existe uma sequência de reduções que conduz a uma forma normal, afirma que *qualquer* sequência de reduções conduz a uma derivação normal, i.e. a ordem em que as reduções são aplicadas não põe em causa a obtenção da forma normal.

Nesta dissertação fazemos um estudo sobre o sistema dedutivo formal  $\mathbf{F}_{\text{at}}$  ou polimorfismo atómico que consiste na restrição do tão conhecido sistema formal  $\mathbf{F}$  de Jean-Yves Girard [11] a instanciações universais atómicas. O sistema  $\mathbf{F}_{\text{at}}$  foi introduzido em 2006 por Fernando Ferreira na altura sob o nome de *atomic PSOL*<sup>i</sup>.

O nosso estudo tem por base o artigo “Atomic Polymorphism” de Fernando Ferreira e Gilda Ferreira [7]. Fez-se uma análise detalhada e rigorosa dos conceitos e propriedades considerados no artigo com o objetivo de compreender e apresentar de forma detalhada a demonstração do teorema da normalização forte para  $\mathbf{F}_{\text{at}}$  e daí concluir que o cálculo proposicional intuicionista é fortemente normalizável recorrendo à imersão do mesmo no sistema  $\mathbf{F}_{\text{at}}$ .

Embora o sistema  $\mathbf{F}_{\text{at}}$  tenha apenas dois geradores de tipos, implicação e quantificação universal de segunda ordem (com instanciações atómicas) ainda é suficientemente expressivo para interpretar o cálculo proposicional intuicionista.

Certos resultados, no contexto  $\mathbf{F}_{\text{at}}$ , admitem estratégias de demonstração mais simples do que no contexto impredicativo de  $\mathbf{F}$ . Ficará patente que a prova da normalização forte para  $\mathbf{F}_{\text{at}}$ , se apresenta de uma forma muito mais simples quando comparada com a engenhosa prova da normalização forte para o sistema  $\mathbf{F}$  que pode encontrar-se em “Proofs and Types” de Jean-Yves Girard [11].

A dissertação encontra-se dividida em seis capítulos sendo o capítulo 1 esta introdução. No capítulo 2 motiva-se e introduz-se o cálculo proposicional intuicionista, apresentando dois métodos que servem de procedimentos de dedução para o cálculo proposicional intuicionista, o formalismo axiomático à Hilbert e a dedução natural.

No capítulo 3 estuda-se um terceiro sistema formal, o *cálculo lambda*, muito usado em ciência da computação. Ainda neste capítulo se torna evidente a relação que existe entre o cálculo de dedução natural e o cálculo lambda através do Isomorfismo de Curry-Howard. A dicoto-

mia dedutivo/funcional que existe entre a dedução natural e o cálculo lambda será usada no estudo dos dois sistemas formais já referidos,  $\mathbf{F}$  e  $\mathbf{F}_{\text{at}}$ .

No capítulo 4 será apresentada a demonstração do teorema da normalização forte para  $\mathbf{F}_{\text{at}}$  considerando  $\beta\eta$ -conversões.

No capítulo 5 mostraremos que o cálculo proposicional intuicionista se imerge em  $\mathbf{F}_{\text{at}}$ , recorrendo ao transbordo de instanciação.

Por último, no capítulo 6, concluiremos que o cálculo proposicional intuicionista é fortemente normalizável considerando  $\beta$ -conversões. Ainda que este resultado não seja novo (é bem conhecido que o cálculo proposicional intuicionista e clássico, até mesmo o cálculo de predicados, tem a propriedade da normalização fraca e forte [14, 15, 18, 20]), a estratégia usada nesta dissertação, que segue o artigo [7], tem a vantagem de assentar sobre uma demonstração bastante simples no contexto de  $\mathbf{F}_{\text{at}}$  e de evitar conversões permutativas.

# Capítulo 2

## Lógica Proposicional Intuicionista

### 2.1 Intuicionismo

A lógica clássica é baseada na noção de verdade e assenta em três princípios fundamentais, formulados a partir das necessidades práticas de filósofos e matemáticos:

- 1) **Identidade**: toda a proposição deriva de si mesma.
- 2) **Terceiro excluído**: toda a proposição é verdadeira ou falsa.
- 3) **Não-contradição**: não é possível que uma proposição seja simultaneamente verdadeira e falsa.

Ao longo dos tempos foram surgindo algumas situações que colocaram em causa algumas das ideias clássicas nomeadamente o princípio do terceiro excluído estas situações foram motivação para a fundação da Lógica Intuicionista.

Considere-se, por exemplo, a seguinte afirmação:

*Existem sete 7s consecutivos na expansão decimal do número  $\pi$*

Se se conseguir uma representação do número  $\pi$  com um número de casas decimais suficientemente grande e na qual a sequência de sete 7s consecutivos ocorra, poder-se-á garantir a veracidade da afirmação acima. Não se sendo capaz de provar a veracidade ou falsidade de uma asserção, o intuicionista não assume que ela ou a sua negação têm de ser verdadeiras, i.e. não aceita o princípio do terceiro excluído, não se compromete a afirmar que toda a asserção tem de ser verdadeira ou falsa.

Foram situações como esta onde não se podem testar todas as (infinitas) hipóteses que levaram o matemático holandês Luitzen Brouwer a fundar o intuicionismo matemático.

No intuicionismo, um objeto matemático é considerado um produto da construção da mente. As provas intuicionistas são provas construtivas, nestas a demonstração da existência de um determinado objeto deve criar esse objeto ou fornecer um caminho para a sua criação.

A Lógica Intuicionista, foi desenvolvida por volta do ano de 1930. O seu surgimento e desenvolvimento deve-se a matemáticos como Brouwer, Arend Heyting e Andrei Kolmogorov, daí que a interpretação informal dos operadores da lógica intuicionista no que respeita às noções primitivas de “construção” e “provas construtivas” é conhecida por interpretação de “Brouwer-Heyting-Kolmogorov” (BHK). [17]

Do ponto de vista intuicionista uma fórmula lógica só é válida se existir uma prova da mesma.

O sistema BHK oferece uma interpretação informal da lógica intuicionista assente na propagação de provas ao longo dos conectivos lógicos. Mais tarde apresentaremos uma formalização rigorosa do cálculo proposicional intuicionista.

A ideia de começarmos por apresentar a interpretação de BHK antes mesmo de apresentar rigorosamente a sintaxe é para fornecer intuição sobre a dinâmica da lógica intuicionista e a razão da rejeição do princípio do terceiro excluído.

1- **Conjunção:** Uma demonstração de  $A \wedge B$  consiste numa demonstração de  $A$  e uma demonstração de  $B$ .

2- **Disjunção:** Uma demonstração de  $A \vee B$  consiste numa demonstração de  $A$  ou uma demonstração de  $B$ .

3- **Implicação:** Uma demonstração de  $A \rightarrow B$  é um método que converte uma demonstração de  $A$  numa demonstração de  $B$ .

4- **Negação:** Uma demonstração de  $\neg A$  é um método de transformar qualquer demonstração de  $A$ , numa contradição, num objeto que não existe ( $\perp$ ).

Temos então que não se aceita  $A \vee \neg A$  a não ser que se apresente uma prova concreta de  $A$  ou uma prova concreta de  $\neg A$ , ou seja rejeita-se o princípio do terceiro excluído.

Com o desaparecimento do princípio do terceiro excluído desaparecem algumas propriedades da lógica clássica como por exemplo:

- $A \leftrightarrow \neg\neg A$  (em lógica intuicionista apenas se verifica  $A \rightarrow \neg\neg A$ ).
- $(A \rightarrow B) \leftrightarrow \neg A \vee B$  (em lógica intuicionista  $\rightarrow$  não se transforma em  $\vee$  ou seja  $A \rightarrow B$  não se transforma em  $\neg A \vee B$ ).
- Leis de De Morgan  $\neg(A \wedge B) \leftrightarrow \neg A \vee \neg B$ .

## 2.2 Sistema de Hilbert

A lógica proposicional intuicionista, ou lógica construtivista, foi criada por Heyting para dotar de uma base formal o intuicionismo de Brouwer.

Existem muitos métodos que servem de procedimentos de dedução (formalismos axiomática à Hilbert, dedução natural, tableaux, cálculo de sequentes, etc.). A escolha de um método específico deve ter em conta características como por exemplo a simplicidade de execução para os fins a que se destinam. Um dos métodos pioneiros foi o método axiomático. Os primórdios do método axiomático remontam à Grécia antiga onde encontramos por exemplo

por parte de Euclides de Alexandria [330 - 295 ac] esforços com vista à sistematização da geometria. Contudo, apenas no final do séc. XIX o método axiomático adquiriu um aspeto formal rigoroso devido a trabalhos como o do matemático alemão David Hilbert. Muitos dos lógicos e matemáticos até 1931 trabalhavam no projeto proposto por David Hilbert, que pretendia provar que a matemática podia reduzir-se a um conjunto finito, completo e consistente, de axiomas.

Contudo, algumas descobertas mostraram que o projeto de Hilbert era impossível de ser concretizado em toda a sua magnitude. Por detrás dessas descobertas encontra-se Kurt Gödel, com os seus teoremas de incompletude provando que uma teoria axiomática recursivamente enumerável e capaz de expressar algumas propriedades básicas de aritmética não pode ser completa e consistente ao mesmo tempo. Porém realizações parciais do programa foram conseguidas e à luz do desafio importantes ferramentas e técnicas, no que é hoje a Teoria da Demonstração foram desenvolvidas.

Nesta secção iremos apresentar o método axiomático para o Cálculo Proposicional Intuicionista. Começamos por recordar os aspetos sintáticos da linguagem do cálculo proposicional [4].

**DEFINIÇÃO 2.2.1** *A linguagem do cálculo proposicional consiste em:*

- *letras esquemáticas (variáveis proposicionais):*  $P, Q, R, \dots$
- *conetivos lógicos:*  $\vee, \wedge, \neg$  e  $\rightarrow$ ;
- *parênteses curvos:*  $(, )$

**DEFINIÇÃO 2.2.2** *As fórmulas proposicionais são definidas indutivamente por:*

- 1) *Uma variável proposicional é uma fórmula proposicional (ou fórmula atómica).*
- 2) *Se  $A$  é uma fórmula proposicional, então  $\neg A$  também o é.*
- 3) *Se  $A$  e  $B$  são fórmulas proposicionais, então  $A \vee B$ ,  $A \wedge B$  e  $A \rightarrow B$  também o são.*

O Cálculo de Hilbert consiste num conjunto de axiomas (que são as pedras basilares do cálculo, não requerendo demonstração) e regras de inferências que permitem derivar novas asserções a partir dos axiomas ou de asserções já derivadas anteriormente. Apresentamos, de seguida, uma lista dos axiomas do Cálculo Proposicional Intuicionista, a listagem de axiomas não é única, existem outras listas equivalentes.

1.  $A \rightarrow (B \rightarrow A)$
2.  $(A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C))$
3.  $(A \rightarrow B) \rightarrow ((A \rightarrow \neg B) \rightarrow \neg A)$
4.  $A \wedge B \rightarrow A$
5.  $A \wedge B \rightarrow B$
6.  $A \rightarrow A \vee B$
7.  $B \rightarrow A \vee B$
8.  $(A \rightarrow C) \rightarrow ((B \rightarrow C) \rightarrow (A \vee B \rightarrow C))$
9.  $(A \rightarrow B) \rightarrow ((A \rightarrow C) \rightarrow (A \rightarrow B \wedge C))$
10.  $(A \wedge \neg A) \rightarrow B$

Regra do cálculo proposicional -*Modus Ponens* (*MP*): de  $A$  e de  $A \rightarrow B$  pode deduzir-se  $B$ .

**Nota:** A lista de axiomas para o Cálculo Proposicional Clássico apenas difere da apresentada em dois axiomas, mas mantém-se a regra de inferência *MP*.

No Cálculo Proposicional Clássico os axiomas 3. e 10. são substituídos por:

$$(\neg A \rightarrow B) \rightarrow ((\neg A \rightarrow \neg B) \rightarrow A) \text{ e } \neg(A \wedge B) \rightarrow (\neg A \vee \neg B) \text{ respetivamente.}$$

**DEFINIÇÃO 2.2.3** *Seja  $\Gamma$  um conjunto (finito) de fórmulas proposicionais e  $A$  uma fórmula proposicional. Diz-se que  $A$  é dedutível em  $\Gamma$  ( $\Gamma \vdash A$ ), se existir uma sequência de fórmulas proposicionais  $A_1, \dots, A_n$ , tal que  $A_n$  é  $A$  e para cada  $i \leq n$ ,  $A_i$  é axioma ou elemento de  $\Gamma$ , ou obtida de  $A_j$  e  $A_k$  com  $j, k < i$ , por *MP* (ou seja,  $A_j$  é uma fórmula  $C$ ,  $A_k$  é uma fórmula  $C \rightarrow D$  e  $A_i$  é a fórmula  $D$ ).*

**EXEMPLO 2.2.4** *A título de exemplo, ilustramos o aspecto das derivações no sistema axiomático para o cálculo proposicional intuicionista acima apresentado, provando que  $A \rightarrow A$ .*

*Pelo axioma 2., tem-se:*

$$A \rightarrow ((B \rightarrow A) \rightarrow A) \rightarrow ((A \rightarrow (B \rightarrow A)) \rightarrow (A \rightarrow A)) \quad (1)$$

*Pelo axioma 1., tem-se:*

$$A \rightarrow ((B \rightarrow A) \rightarrow A) \quad (2)$$

*de (1) e (2) e por MP, tem-se:*

$$(A \rightarrow (B \rightarrow A)) \rightarrow (A \rightarrow A) \quad (3)$$

*Pelo axioma 1., tem-se:*

$$A \rightarrow (B \rightarrow A) \quad (4)$$

*de (3) e (4) e por MP, tem-se:*

$$A \rightarrow A$$

Os métodos ou sistemas axiomáticos (sistemas à la Hilbert) que usam axiomas e regras de inferências, no caso do Cálculo Proposicional apenas a regra *MP*, são muito utilizados por filósofos para formalizar a argumentação lógica. Como podemos ver no exemplo anterior tais sistemas são, em geral, fáceis de compreender mas difíceis de usar nas deduções. Apresentamos de seguida o Sistema de Dedução Natural onde apenas se usam regras de inferência e que permite uma forma mais fácil e intuitiva de fazer deduções.

## 2.3 Sistema de Dedução Natural

Em 1934, novos métodos de dedução começaram a ser usados pelos lógicos. Podemos referir o sistema de Dedução Natural que foi introduzido por Gerhard Gentzen (1935) [10] na mesma tese em que introduziu o cálculo de seqüentes de primeira ordem, uma das ferramentas lógicas mais usadas em trabalhos técnicos avançados. Em Basic Proof Theory [19], podemos ler que a motivação de Gentzen, segundo o próprio, para definir a dedução natural foi “a criação de um raciocínio tão semelhante quanto possível do raciocínio real”. *“to set up a formula system which comes as close as possible to actual reasoning”*

Para além do sistema de dedução natural, como acima mencionado, o matemático Gentzen ainda desenvolveu um outro sistema conhecido por cálculo de sequentes conseguindo demonstrar o importante Teorema da Eliminação do Corte. Este teorema diz que qualquer prova que utiliza a regra do corte pode ser transformada numa prova sem a regra do corte. [5]

A importância da dedução natural foi estabelecida pelos resultados clássicos de Dag Prawitz (1965) ficando patente que a eliminação do corte também é válida em dedução natural, propriedade conhecida neste contexto como *normalização*.

Será justo dizer que o processo de construção das provas em dedução natural é de facto “natural” na medida em que corresponde de perto ao raciocínio humano.

O sistema de Dedução Natural aparece nos manuais de Lógica com diferentes estilos. Nesta tese será adotado o estilo Gentzen-Prawitz (em que as derivações são árvores de fórmulas) [20], em detrimento do também bastante popular estilo Fitch (em que as derivações são sequências de fórmulas) [2].

O sistema de dedução natural permite recorrendo a regras de inferência, demonstrar a validade de fórmulas ou argumentos baseando-se na forma lógica (estrutura) das asserções. O sistema de dedução natural é constituído por regras que unem ou prolongam árvores (finitas) que são geradas a partir de um conjunto finito de premissas até derivar uma certa conclusão. A raiz da árvore é a conclusão, os ramos são as derivações que geram a conclusão. As folhas da árvore representam premissas ou hipóteses. Para cada conectivo lógico existem regras de introdução e regras de eliminação (à exceção do absurdo só com regra de eliminação). Cada passo, ou seja, cada derivação realizada na árvore deve ser baseado numa das regras do sistema. À representação da derivação através de árvores chamamos árvore de prova. As provas de dedução natural são particularmente elegantes para a lógica intuicionista. Para apresentar as demonstrações em dedução natural usaremos a abordagem feita em [11].

Usa-se

$$\begin{array}{c} \vdots \\ A \end{array}$$

para designar uma dedução de  $A$ , ou seja que termina em  $A$ .

Por exemplo

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

é uma dedução de  $A \rightarrow B$ . Note-se que tal dedução é possível pois temos uma dedução de  $B$  a partir de  $A$ . Os parêntesis retos em torno de  $A$  significam que ao concluir que  $A \rightarrow B$  a hipótese  $A$  foi cancelada. Desta forma, uma prova de  $B$  depende de uma prova de  $A$ , enquanto que a prova de  $A \rightarrow B$  não. Na derivação acima, em vez de uma fórmula (hipótese) única podemos ter um conjunto finito (possivelmente vazio) de ocorrências da fórmula  $A$ . Para controlar as hipóteses canceladas, alguns autores usam marcadores, ver [19].

Por exemplo, a dedução acima com marcadores ficaria:

$$\frac{[A]^u \quad \vdots \quad B}{A \rightarrow B} \mathcal{I}_u \rightarrow$$

O uso do marcador  $u$ , identifica exatamente a regra que foi responsável pelo cancelamento da hipótese  $A$  (neste caso a introdução da implicação).

Tem-se então que as hipóteses inicialmente abertas ao longo da construção da demonstração i.e., à medida que se vão aplicando regras podem ir sendo fechadas (canceladas) (o cancelamento de uma hipótese é marcado com  $[ ]$ ). As hipóteses podem ser utilizadas mais do que uma vez, desde que não estejam fechadas. Isto é, depois de estarem fechadas, as hipóteses não podem ser utilizadas, salvo se forem introduzidas como novas hipóteses (abertas). A regra base do cálculo de dedução natural consiste na possibilidade de se formar uma árvore com um único nodo:

$$A$$

A fórmula  $A$  é folha e raiz, ou seja assumindo  $A$  como hipótese podemos (trivialmente) concluir  $A$ . Todas as outras regras de inferência do sistema dedução natural são de dois tipos: de introdução de conectivos e de eliminação de conectivos.

Serão agora apresentadas as regras de *Introdução* (designada por  $\mathcal{I}$ ) / *Eliminação* (designada por  $\mathcal{E}$ ) para a conjunção ( $\wedge$ ); implicação ( $\rightarrow$ ) e disjunção ( $\vee$ ). Serão também apresentadas algumas definições relativas às regras de inferência.

### conjunção

$$\frac{\begin{array}{c} \vdots \\ A \end{array} \quad \begin{array}{c} \vdots \\ B \end{array}}{A \wedge B} \mathcal{I} \wedge; \quad \frac{\begin{array}{c} \vdots \\ A \wedge B \end{array}}{A} \mathcal{E} \wedge; \quad \frac{\begin{array}{c} \vdots \\ A \wedge B \end{array}}{B} \mathcal{E} \wedge$$

### implicação

$$\frac{\begin{array}{c} [A] \\ \vdots \\ B \end{array}}{A \rightarrow B} \mathcal{I} \rightarrow; \quad \frac{\begin{array}{c} \vdots \\ A \rightarrow B \end{array} \quad \begin{array}{c} \vdots \\ A \end{array}}{B} \mathcal{E} \rightarrow$$

disjunção

$$\frac{\vdots}{A} \mathcal{I} \vee; \quad \frac{\vdots}{B} \mathcal{I} \vee; \quad \frac{\vdots \quad \begin{array}{c} [A] \\ \vdots \\ C \end{array} \quad \begin{array}{c} [B] \\ \vdots \\ C \end{array}}{A \vee B \quad C} \mathcal{E} \vee$$

**DEFINIÇÃO 2.3.1** *Numa regra de inferência:*

**Premissa** são as fórmulas imediatamente acima do traço de inferência.

**Consequência** ou **resultado** é a fórmula imediatamente abaixo do traço de inferência.

**Premissa principal** é a premissa que se encontra representada mais à esquerda (segundo a configuração acima) numa regra de eliminação.

**Premissas menores** são as premissas de uma regra de eliminação que não são premissas principais, caso existam.

Contrariamente ao que aconteceu quando da apresentação do cálculo de Hilbert na secção 2.2 em que introduzimos  $\neg$  como um conectivo primitivo, é usual em dedução natural considerar  $\perp$  como símbolo primitivo e denotar por  $\neg A$  a abreviação de  $A \rightarrow \perp$ .

Em dedução natural, a distinção entre lógica clássica, lógica intuicionista e lógica minimal faz-se através da regra de eliminação que o sistema dispõe para  $\perp$

para a lógica clássica temos a seguinte regra que se designa por “Reduction ad Absurdum”

$$\frac{[\neg A] \quad \vdots \quad \frac{\perp}{A} \mathcal{E} \perp}{\perp} \mathcal{E} \perp$$

para a lógica intuicionista temos a seguinte regra que se designa por “Ex Falsum Quod Libet”

$$\frac{\perp}{A} \mathcal{E} \perp$$

a regra acima indica que toda a fórmula se deduz a partir de  $\perp$ .

A lógica minimal **M** é uma variante da lógica intuicionista obtida pela rejeição do princípio “from a falsehood follows whatever you like” (a partir de uma falsidade segue o que quiser), temos então que em **M** o símbolo de falsidade  $\perp$  não é assistido por nenhuma regra. [19].

Apresentam-se agora alguns exemplos de derivações em Dedução Natural.

**EXEMPLOS 2.3.2**  $i) \vdash A \rightarrow A$ 

$$\frac{[A]^u}{A \rightarrow A} \mathcal{I}_u \rightarrow$$

Note-se que a derivação de  $A \rightarrow A$  fica muito mais simples no sistema de Dedução Natural do que no sistema de Hilbert.

 ii)  $A \wedge B \rightarrow C \vdash A \rightarrow (B \rightarrow C)$ 

$$\frac{\frac{\frac{A \wedge B \rightarrow C}{C} \mathcal{I}_v \rightarrow}{B \rightarrow C} \mathcal{I}_u \rightarrow}{A \rightarrow (B \rightarrow C)} \mathcal{I}_u \rightarrow$$

$$\frac{\frac{[A]^u}{A \wedge B} \mathcal{I} \wedge}{A \wedge B \rightarrow C} \mathcal{E} \rightarrow$$

 iii)  $A \vdash \neg\neg A$ 

$$\frac{\frac{[A \rightarrow \perp]^u}{\perp} \mathcal{E} \rightarrow}{(A \rightarrow \perp) \rightarrow \perp} \mathcal{I}_u \rightarrow$$

 iv)  $A \rightarrow (B \rightarrow A)$ 

$$\frac{\frac{[A]^u}{B \rightarrow A} \mathcal{I} \rightarrow}{A \rightarrow (B \rightarrow A)} \mathcal{I}_u \rightarrow$$

 v)  $A \rightarrow A \vee B$ 

$$\frac{\frac{[A]^u}{A \vee B} \mathcal{I}_R \vee}{A \rightarrow (A \vee B)} \mathcal{I}_u \rightarrow$$

 vi)  $B \rightarrow A \vee B$ 

$$\frac{\frac{[B]^u}{A \vee B} \mathcal{I}_L \vee}{B \rightarrow (A \vee B)} \mathcal{I}_u \rightarrow$$

 vii)  $(A \rightarrow C) \rightarrow [(B \rightarrow C) \rightarrow (A \vee B) \rightarrow C]$ 

$$\frac{\frac{\frac{[A \vee B]^v}{C} \mathcal{E} \rightarrow}{\frac{[A]^u}{C} \mathcal{E} \rightarrow} \mathcal{E}_{u,t} \vee}{\frac{\frac{[B \rightarrow C]^w}{C} \mathcal{E} \rightarrow}{\frac{[B]^t}{C} \mathcal{E} \rightarrow} \mathcal{E}_{u,t} \vee} \mathcal{E}_{u,t} \vee}$$

$$\frac{\frac{\frac{C}{A \vee B \rightarrow C} \mathcal{I}_v \rightarrow}{(B \rightarrow C) \rightarrow (A \vee B \rightarrow C)} \mathcal{I}_w \rightarrow}{(A \rightarrow C) \rightarrow [(B \rightarrow C) \rightarrow (A \vee B) \rightarrow C]} \mathcal{I}_r \rightarrow$$

viii)  $\perp \rightarrow A$

$$\frac{\frac{[\perp]^u}{A} \mathcal{E} \perp}{\perp \rightarrow A} \mathcal{I}_u \rightarrow$$

ix)  $(\neg\neg A \rightarrow \neg\neg B) \rightarrow \neg\neg(A \rightarrow B)$

$$\frac{\frac{\frac{[A \rightarrow \perp]^v}{\perp} \mathcal{E} \perp}{A \rightarrow B} \mathcal{I}_u \rightarrow}{\frac{[\neg(A \rightarrow B)]^x}{\neg\neg A} \mathcal{I}_v \rightarrow} \mathcal{E} \rightarrow \quad \frac{\frac{[A]^u}{\neg\neg B} \mathcal{E} \rightarrow}{[\neg\neg A \rightarrow \neg\neg B]^z} \mathcal{E} \rightarrow}{\frac{\frac{[\perp] \mathcal{E} \perp}{\neg\neg(A \rightarrow B)} \mathcal{I}_x \rightarrow}{(\neg\neg A \rightarrow \neg\neg B) \rightarrow \neg\neg(A \rightarrow B)} \mathcal{I}_z \rightarrow} \quad \frac{\frac{[\neg(A \rightarrow B)]^x}{\perp} \mathcal{I}_t \rightarrow}{\neg B} \mathcal{E} \rightarrow}{\frac{[B]^t}{A \rightarrow B} \mathcal{I} \rightarrow}{\neg B} \mathcal{E} \rightarrow} \mathcal{E} \rightarrow$$

### 2.3.1 Normalização em Dedução Natural

Em Dedução Natural podem existir várias deduções para uma mesma fórmula. Existem também deduções nas quais são aplicadas regras de inferência desnecessárias, embora corretas. Esta situação foi descrita por Prawitz que observou uma espécie de princípio da inversão que reflete as simetrias existentes entre as regras de introdução e a correspondente regra de eliminação no sistema de Dedução Natural. As regras de eliminação, em certo sentido, são o inverso da correspondente regra de introdução. O princípio da inversão define essa simetria. Apesar de esse princípio já estar contido nos trabalhos de Gentzen [10] quando diz que uma regra de introdução dá a definição da constante lógica e a regra de eliminação é somente uma consequência da correspondente regra de introdução, foi Prawitz quem observou um conjunto de regras de redução que formam o procedimento de normalização conhecido por teorema de normalização, utilizado para obter a forma normal das derivações. No processo de normalização estamos atentos a certas estruturas:

- 1) *conversões de tipo  $\beta$*  ou abreviadamente  *$\beta$ -conversões*: uma regra de eliminação é aplicada imediatamente a seguir a uma regra de introdução para o mesmo conetivo, podendo evitar-se este duplo passo.
- 2) *conversões de tipo  $\eta$*  ou abreviadamente  *$\eta$ -conversões*: uma regra de introdução é aplicada imediatamente a seguir a uma regra de eliminação para o mesmo conetivo, podendo evitar-se este duplo passo.

Vamos agora exemplificar as conversões referidas.

**Nota:** No que se segue, e porque um maior grau de detalhe é, para o efeito, necessário, a porção de derivação que anteriormente era representada por reticências na vertical, é agora representada por  $\Sigma_n$ .

Conversões de tipo  $\beta$ :

$$\frac{\frac{\Sigma_1 \quad \Sigma_2}{A \quad B}}{A \wedge B} \quad \text{converte-se em} \quad \frac{\Sigma_1}{A}$$

No exemplo acima, temos que a partir das árvores  $\Sigma_1$  e  $\Sigma_2$  deduzimos  $A$  e  $B$ , respectivamente. A seguir, usamos a introdução do conetivo  $\wedge$ , e logo a seguir a eliminação do mesmo conetivo para chegarmos novamente a  $A$ . Para simplificar a dedução, usou-se a conversão de tipo  $\beta$ , que consiste em retirar da árvore a introdução e a eliminação da conjunção com vista a aproximarmo-nos da forma normal da mesma, conceito que definiremos em seguida.

Situações semelhantes às apresentadas anteriormente podem ocorrer para a disjunção ( $\vee$ ) e para a implicação ( $\rightarrow$ ), como se mostra nos exemplos seguintes:

$$\frac{\frac{\Sigma_1 \quad [A] \quad [B]}{A \quad \Sigma_2 \quad \Sigma_3}}{A \vee B} \quad \frac{C \quad C}{C} \quad \text{converte-se em} \quad \frac{\Sigma_1}{A} \quad \Sigma_2 \quad C$$

$$\frac{\frac{[A] \quad \Sigma_1}{B} \quad \Sigma_2}{A \rightarrow B} \quad \frac{A}{A} \quad \text{converte-se em} \quad \frac{\Sigma_2}{A} \quad \Sigma_1 \quad B$$

Vejamos agora as conversões de tipo  $\eta$

$$\frac{\frac{\Sigma_1 \quad \Sigma_1}{A \wedge B} \quad \frac{A \wedge B}{B}}{A \wedge B} \quad \text{converte-se em} \quad \frac{\Sigma_1}{A \wedge B}$$

No exemplo podemos ver que para concluir  $A \wedge B$ ,  $A$  e  $B$  foram extraídos de  $A \wedge B$  por eliminação mas tal não era necessário uma vez que se voltou a considerar  $A \wedge B$  por introdução do mesmo conetivo ( $\wedge$ ). Para simplificar a derivação aplicou-se uma conversão de tipo  $\eta$ .

Tal como aconteceu com as conversões de tipo  $\beta$ , vamos apresentar as  $\eta$ -conversões para a disjunção e a implicação

$$\frac{\Sigma_1 \quad \frac{[A]}{A \vee B} \quad \frac{[B]}{A \vee B}}{A \vee B} \quad \text{converte-se} \quad \frac{\Sigma_1}{A \vee B}$$

$$\frac{\frac{\Sigma_1}{A \rightarrow B} \quad [A]}{B} \quad \text{converte-se em} \quad \frac{\Sigma_1}{A \rightarrow B}$$

**DEFINIÇÃO 2.3.3** *Uma dedução diz-se na forma normal, considerando  $\beta$ -conversão (respetivamente,  $\eta$ -conversão ou  $\beta\eta$ -conversão), se não for possível efetuar nenhuma  $\beta$ -conversão (respetivamente,  $\eta$ -conversão ou  $\beta\eta$ -conversão).*

As conversões permutativas saem fora do âmbito desta dissertação, razão pela qual não as apresentamos juntamente com as  $\beta$  e  $\eta$ -conversões. Nos sistemas em que iremos trabalhar mais tarde, desprovidos dos conectivos  $\perp$ ,  $\vee$  e  $\exists$ , não faz sentido falar de conversões permutativas. Elas são contudo essenciais no cálculo proposicional (ou de predicados) para garantir que derivações normais possuem a propriedade da subfórmula, i.e. toda a fórmula na dedução é uma subfórmula da conclusão ou de uma hipótese não cancelada.

Para um estudo sobre normalização (existência ou obtenção de formas normais) para o cálculo proposicional ou de predicados (considerando também conversões permutativas) aconselhamos a consulta de [19, 20].

## Capítulo 3

# Cálculo Lambda e o Isomorfismo de Curry-Howard

O cálculo lambda (também designado por  $\lambda$ -cálculo) é um sistema formal introduzido na década de 1930 pelo matemático norte-americano Alonzo Church (1903 - 1995), como parte de um sistema para a fundamentação da Matemática.

No entanto, em 1935, Stephen Kleene e J. B. Rosser, alunos de Church, provaram que o sistema original era inconsistente (*Paradoxo de Kleene-Rosser*).

Posteriormente, em 1936, Church isolou a parte do sistema relevante para a computação atualmente conhecida como cálculo lambda não tipado. Na versão não tipada do cálculo lambda, toda a função recursiva pode ser representada, i.e. toda a função computável pode ser escrita como um  $\lambda$ -termo (*Tese de Church*). Dessa forma, o  $\lambda$ -cálculo constitui a base das linguagens de programação funcional.

O  $\lambda$ -cálculo é uma teoria de funções que representa funções como regras, procurando o aspecto computacional das mesmas. Ou seja, para definir uma função de A para B, é preciso dar uma regra que dirá como produzir um elemento de B a partir de um elemento de A. As funções são definidas como  $\lambda$ -expressões que ditam o comportamento das mesmas. Por exemplo, a função  $f(x) = x^2$  é representada no cálculo lambda por  $\lambda x.x^2$ .

Para calcular o valor de  $f$  num determinado argumento, temos que introduzir o conceito de  $\beta$ -conversão, que basicamente diz que calcular uma função num argumento significa substituir todas as ocorrências da variável da função pelo argumento.

No exemplo acima  $f(3)$  é dado por  $(\lambda x.x^2)3 \rightsquigarrow_{\beta} x^2[3/x] = 3^2 = 9$ . As reduções no contexto do  $\lambda$ -cálculo serão analisadas adiante com mais detalhe.

No cálculo lambda não tipado, um  $\lambda$ -termo pode ser aplicado a qualquer outro  $\lambda$ -termo, inclusive a ele próprio, podendo a computação não terminar. Para evitar esse problema, pode usar-se um sistema de tipos. Como veremos adiante, na sua forma mais simples, os tipos são construídos, a partir de tipos atômicos através da implicação.

No *cálculo lambda simplesmente tipado* apenas são permitidas aplicações em que o tipo do argumento é igual ao tipo do domínio da função, i.e. se a função tem tipo  $A \rightarrow B$  ela pode apenas ser aplicada a argumentos do tipo  $A$ . Esta limitação irá garantir que todos os termos são fortemente normalizáveis, i.e. a computação termina sempre.

### 3.1 Cálculo lambda simplesmente tipado

O  $\lambda$ -cálculo tipado é um formalismo interessante do ponto de vista computacional. Neste formalismo, além dos termos, é necessário introduzir uma classe de tipos, que é definida usando certos tipos básicos e operações que geram novos tipos a partir de tipos já gerados. Nesta secção apresentaremos o cálculo lambda simplesmente tipado, denotado usualmente por  $\lambda^{\rightarrow}$ , que apenas tem um construtor de tipos:  $\rightarrow$ .

O cálculo lambda simplesmente tipado é o exemplo mais simples de um  $\lambda$ -cálculo tipado e foi originalmente introduzido em 1940 por Church.

Todas as versões de cálculo lambda consideradas ao longo desta dissertação serão tipadas e com tipagem rígida, i.e. todos os termos e todos os subtermos de um termo têm um tipo fixo.

Vamos, agora apresentar a sintaxe e as regras de redução do cálculo lambda simplesmente tipado. Adotaremos o formalismo de [19].

#### 3.1.1 Tipos

Os tipos são construídos a partir de um conjunto contável de variáveis de tipo  $X, Y, Z, \dots$  através de uma operação de formação de tipos (construtor de tipos)  $\rightarrow$ . Mais formalmente, os tipos definem-se da seguinte forma:

1. as variáveis de tipo são tipos;
2. se  $A$  e  $B$  são tipos, então  $A \rightarrow B$  (implicação) é um tipo;
3. os únicos tipos são os construídos em 1. e 2.

Quando se fala em tipos, não é necessário referir os seus elementos. Intuitivamente podemos pensar em tipos como nomes de conjuntos: as variáveis de tipo denotariam conjuntos arbitrários e dados tipos  $A$  e  $B$ , o tipo  $A \rightarrow B$  denotaria o conjunto de funções de  $A$  para  $B$ .

Para simplificar a notação é usual convencionar-se que  $A_1 \rightarrow A_2 \rightarrow \dots \rightarrow A_{n-1} \rightarrow A_n$  denota o tipo  $A_1 \rightarrow (A_2 \rightarrow \dots \rightarrow (A_{n-1} \rightarrow A_n) \dots)$ .

#### 3.1.2 Termos

Todos os termos têm um tipo. Os termos de tipo  $A$  são geralmente representados por  $t^A, s^A, r^A, \dots$

Os termos são gerados pelas seguintes condições:

1. Para cada tipo  $A$ , existe um número infinito, contável, de variáveis,  $x^A, y^A, z^A, \dots$  Estas variáveis são termos de tipo  $A$ .
2. Se  $t^{A \rightarrow B}$  é um termo de tipo  $A \rightarrow B$  e  $q^A$  é um termo de tipo  $A$ , então  $(t^{A \rightarrow B} q^A)^B$  é um termo de tipo  $B$ .
3. Se  $t^B$  é um termo de tipo  $B$  e  $x^A$  é uma variável de tipo  $A$ , então  $(\lambda x^A. t^B)^{A \rightarrow B}$  é um termo de tipo  $A \rightarrow B$ .

Quando o tipo de um termo se percebe facilmente pelo contexto é usual omiti-lo, i.e. escrevemos  $t$  em vez de  $t^A$ .

Nos termos em que o tipo é omitido, geralmente simplifica-se retirando os parêntesis, por exemplo  $(ts)$  escreve-se  $ts$ . Os termos da forma  $tq$  são conhecidos como *aplicações* e os da forma  $\lambda x.t$  como *abstrações*.

$t_1 t_2 \dots t_n$  abrevia a expressão que é definida por recorrência em  $n$  como  $(t_1 t_2 \dots t_{n-1}) t_n$ , i.e.  $t_1 t_2 \dots t_n$  é  $(\dots((t_1 t_2) t_3 \dots) t_n$  ou seja, contrariamente aos tipos que se associam à direita os termos associam-se à esquerda.

No que respeita às abstrações,  $\lambda x_1.(\lambda x_2.(\dots(\lambda x_n.t)\dots))$  escreve-se simplesmente  $\lambda x_1 \lambda x_2 \dots \lambda x_n.t$  ou até  $\lambda x_1 x_2 \dots x_n.t$ . As aplicações têm prioridade relativamente às abstrações, assim  $\lambda x.t_1 t_2$ , representa  $\lambda x.(t_1 t_2)$  e não  $(\lambda x.t_1) t_2$ .

O conjunto  $FV(t)$  das *variáveis livres* em  $t$  define-se da seguinte forma:

$$\begin{aligned} FV(x^A) &:= \{x^A\}; \\ FV(ts) &:= FV(t) \cup FV(s); \\ FV(\lambda x.t) &:= FV(t) \setminus \{x\}. \end{aligned}$$

A substituição de uma variável  $x$  por um termo  $s$  num termo  $t$ , denota-se por  $t([s/x])$  e define-se da seguinte forma:

$$\begin{aligned} x[s/x] &:= s; \\ y[s/x] &:= y \text{ para } y \neq x; \\ (t_1 t_2)[s/x] &:= t_1[s/x] t_2[s/x]; \\ (\lambda x.t)[s/x] &:= \lambda x.t; \\ (\lambda y.t)[s/x] &:= \lambda y.t[s/x] \text{ para } y \neq x; \text{ sem perda de generalidade } y \notin FV(s). \end{aligned}$$

**Nota:** Estamos a assumir  $\alpha$ -equivalência dos termos do cálculo lambda, i.e. podemos livremente renomear variáveis mudas. Por exemplo, os termos  $\lambda x.x$  e  $\lambda y.y$  são vistos como o mesmo termo ( $\alpha$ -equivalentes), eles representam a mesma função, a função identidade.

### 3.1.3 Conversões, reduções, forma normal

Diz-se que um termo  $t$  se *converte* num termo  $t'$  quando acontece uma das duas seguintes situações:

- $t \equiv (\lambda x.q)s$  e  $t' \equiv q[s/x]$ ;
- $t \equiv \lambda x.(qx)$  e  $t' \equiv q$  com  $x \notin FV(q)$ .

O termo  $t$  designa-se por *redex* e o termo  $t'$  por *contractum*.

A substituição de um redex pelo seu contractum é conhecida por *conversão*.

No primeiro caso temos uma  $\beta$ -conversão:

$$(\lambda x.q)s \rightsquigarrow q[s/x]$$

No segundo caso uma  $\eta$ -conversão:

$\lambda x.(qx) \rightsquigarrow q$  com  $x \notin FV(q)$ .

Prosseguimos com alguma notação standard:

Escrevemos  $r \succ_1 s$  ( $r$  reduz-se a  $s$  num passo) se  $s$  se obtém de  $r$  substituindo um redex  $r'$  de  $r$  por um contractum  $r''$  i.e. aplica-se uma única conversão.

A relação  $\succ$  é o fecho transitivo de  $\succ_1$  e a relação  $\succeq$  é o fecho reflexivo e transitivo de  $\succ_1$ .

A relação  $\succeq$  é conhecida como a relação de *redução* gerada pelas conversões.

Um termo  $t$  está em *forma normal* ou é *normal* se não contém redexes. Um termo  $t$  tem uma forma normal se se reduz a um termo  $s$  normal, i.e.  $t \succeq s$  com  $s$  termo normal.

Uma *sequência de redução* é uma sequência (finita ou infinita) de termos  $t_0, t_1, t_2, \dots$  tais que  $t_i \succ_1 t_{i+1}$ . Geralmente denota-se por  $t_0 \succ_1 t_1 \succ_1 t_2 \dots$ .

A coleção de todas as sequências de redução a partir de  $t$  chama-se *árvore de redução* de  $t$ .

Um termo é *fracamente normalizável* se a sua árvore de redução tem um ramo finito.

Um termo é *fortemente normalizável* se a sua árvore de redução é finita, i.e. qualquer sequência de redução termina.

**TEOREMA 3.1.1** *Os termos de  $\lambda^\rightarrow$  são fortemente normalizáveis (considerando  $\beta\eta$ -conversões).*

Iremos no Capítulo 4 provar normalização forte de um sistema que estende o cálculo  $\lambda^\rightarrow$ , saindo o resultado do teorema 3.1.1 como caso particular.

## 3.2 Isomorfismo de Curry-Howard

O isomorfismo de Curry-Howard essencialmente transforma cada etapa de uma dedução em Dedução Natural num termo do cálculo  $\lambda$ , que é a codificação da construção até esse momento. Este isomorfismo faz corresponder fórmulas lógicas da Dedução Natural com tipos de um  $\lambda$ -cálculo tipado e demonstrações em Dedução Natural com termos; mais precisamente, cada demonstração da fórmula  $A$  que depende de hipóteses  $A_1, \dots, A_n$  transforma-se num termo  $t$  de tipo  $A$  que tem variáveis livres  $x_1, \dots, x_n$  de tipo  $A_1, \dots, A_n$  respetivamente. Este conceito é conhecido por paradigma *'proofs-as-programs'*, ou pela correspondência *'formulas-as-types'*

Também as noções de conversão e de normalização que se introduziram quer em Dedução Natural quer em cálculo lambda se correspondem com o isomorfismo de Curry-Howard. Por exemplo um termo  $t^A$  diz-se normal (não tem nenhum redex pelo que não se pode reduzir mais) se e só se a demonstração em Dedução Natural de  $A$  (via isomorfismo de Curry-Howard) é normal.

Mais geralmente, a correspondência de Curry-Howard é a observação de que duas famílias de formalismos (sistemas formais de provas, no nosso caso materializados em Dedução Natural e modelos de computação, no nosso caso materializados em  $\lambda$ -cálculo) são formas diferentes de representar as mesmas entidades. A Teoria da Demonstração e a Teoria da Computação são dois lados da mesma moeda. A correspondência, inicialmente descoberta por Haskell Brookes Curry nos anos 30 e encarada como princípio fundamental desde os trabalhos de William Howard no final dos anos 60 generalizou-se a outros sistemas lógicos.

Os conceitos de Teoria da Demonstração podem ser interpretados em termo de computações e a sintaxe dos diversos cálculos lambda e sistemas similares pode ser formulada na linguagem da Teoria da Demonstração.

Nesta secção descrevemos o Isomorfismo de Curry-Howard apenas para o fragmento implicacional do Cálculo Proposicional Intuicionista, já que o cálculo lambda foi apresentado neste contexto. Generalizações do isomorfismo para os outros conectivos encontram-se bem descritas na literatura [17]. Adiante na tese consideramos generalizações do isomorfismo à segunda ordem.

Descrever o isomorfismo não é mais do que a indicação precisa da correspondência entre termos e provas.

1. A variável  $x^A$  corresponde à derivação  $A$  <sup>1</sup>
2.  $\lambda x^A.v$  corresponde à derivação

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

se  $v$  corresponde à derivação de  $B$ . <sup>2</sup>

3. O termo  $tu$  corresponde à derivação

$$\frac{\begin{array}{c} \vdots \\ A \end{array} \quad \begin{array}{c} \vdots \\ A \rightarrow B \end{array}}{B} \mathcal{E} \rightarrow$$

onde  $t$  e  $u$  correspondem às derivações de  $A \rightarrow B$  e  $A$  respetivamente.

Os exemplos que se seguem mostram a correspondência entre a escrita de derivações no sistema de dedução natural e termos do cálculo lambda.

**EXEMPLOS 3.2.1** *Os termos do Cálculo Lambda que correspondem às derivações*

$$\frac{\frac{[A]^u}{A \rightarrow A} \mathcal{I}_u \rightarrow}{A \rightarrow A \rightarrow A} \mathcal{I} \rightarrow$$

e

$$\frac{\frac{[A]^u}{A \rightarrow A} \mathcal{I} \rightarrow}{A \rightarrow A \rightarrow A} \mathcal{I}_u \rightarrow$$

são respetivamente  $\lambda y^A \lambda u^A.u$  e  $\lambda u^A \lambda y^A.u$

<sup>1</sup>Note que numa derivação a mesma fórmula  $A$  pode aparecer várias vezes entre as hipóteses. A fórmulas  $A$  com o mesmo marcador fazemos corresponder a mesma variável  $x^A$ .

<sup>2</sup>As hipóteses  $A$  canceladas são todas as que correspondem a  $x^A$ , ie, têm o mesmo marcador.

Embora para simplificar seja usual trabalharmos com derivações em Dedução Natural sem marcadores, este exemplo extraído de [17] mostra que, para termos um “verdadeiro” isomorfismo entre termos fechados e derivações sem hipóteses não canceladas, é necessário o uso de marcadores.

**EXEMPLO 3.2.2** *Apresentaremos a derivação em dedução natural que corresponde ao termo*

$$\lambda x(((A \rightarrow B) \rightarrow A) \rightarrow A) \rightarrow B . x(\lambda y^{(A \rightarrow B) \rightarrow A} . y(\lambda z^A . x(\lambda u^{(A \rightarrow B) \rightarrow A} . z)))$$

$$\frac{\frac{\frac{[A]^z}{((A \rightarrow B) \rightarrow A) \rightarrow A}}{\frac{B}{A \rightarrow B} \mathcal{I}_z \rightarrow} \quad \frac{[[((A \rightarrow B) \rightarrow A) \rightarrow A] \rightarrow B]^x \quad \mathcal{E} \rightarrow}{\frac{A}{((A \rightarrow B) \rightarrow A) \rightarrow A} \mathcal{I}_y \rightarrow} \quad \frac{[(A \rightarrow B) \rightarrow A]^y \quad \mathcal{E} \rightarrow}{\frac{B}{(((A \rightarrow B) \rightarrow A) \rightarrow A) \rightarrow B} \mathcal{I}_x \rightarrow} \quad \frac{[[((A \rightarrow B) \rightarrow A) \rightarrow A] \rightarrow B]^x \quad \mathcal{E} \rightarrow}{\mathcal{E} \rightarrow}}$$

### 3.3 O Sistema F

O sistema **F** surge como uma extensão do cálculo lambda simplesmente tipado, ao qual se adiciona quantificação sobre tipos.

Este sistema foi introduzido, independentemente por John Reynolds [16], no âmbito da teoria da computação e Jean-Yves Girard [12] no âmbito da teoria da demonstração. Iremos apresentar o sistema **F** na sua forma mais primitiva que se baseia na implicação e na quantificação universal de segunda ordem.

**DEFINIÇÃO 3.3.1** *Os tipos são definidos por variáveis de tipo  $X, Y, Z, \dots$  e duas operações ( $\rightarrow$  e  $\forall$ ) da seguinte forma:*

- 1) *Variáveis de tipo são tipos.*
- 2) *Se  $A$  e  $B$  são tipos então  $A \rightarrow B$  é um tipo.*
- 3) *Se  $A$  é um tipo e  $X$  é uma variável de tipo então  $\forall X.A$  é um tipo.*

**DEFINIÇÃO 3.3.2** *Os termos são gerados pelos seguinte esquemas:*

- i) *Para cada tipo  $A$  existe um número infinito contável de variáveis:  $x^A, y^A, z^A, \dots$ . Estas variáveis são termos de tipo  $A$ .*
- ii) *tu é um termo de tipo  $B$ , se  $t$  é um termo de tipo  $A \rightarrow B$  e  $u$  é um termo de tipo  $A$  (aplicação).*

iii)  $\lambda x^A.v$  é um termo de tipo  $A \rightarrow B$ , se  $x^A$  é variável de tipo  $A$  e  $v$  é um termo de tipo  $B$  ( $\lambda$ -abstração).

iv)  $tF$  é um termo de tipo  $A[F/X]$ , se  $t$  for um termo de tipo  $\forall X.A$  e  $F$  for um tipo (aplicação universal).

v)  $\Lambda X.v$  é um termo de tipo  $\forall X.A$ , e  $v$  for um termo de tipo  $A$ , desde que a variável  $X$  não ocorra livre no tipo de nenhuma variável livre de  $v$  (abstração universal).

No sistema  $\mathbf{F}$ , além das usuais  $\beta$ -conversões associadas às aplicações/ $\lambda$ -abstrações, temos também  $\beta$ -conversões associadas às aplicações universais/abstrações universais:

$$(\Lambda X.v)U \rightsquigarrow v[U/X]$$

O isomorfismo de Curry-Howard, apresentado na secção 3.2 a propósito do Cálculo Lambda simplesmente tipado, estende-se ao sistema  $F$  [11]. Os tipos em  $\mathbf{F}$  podem ser vistos como fórmulas, em que, além de implicações se têm quantificadores universais de segunda ordem, e o isomorfismo que foi estabelecido para a implicação estende-se a estes quantificadores.

A abstração universal e a aplicação universal correspondem exatamente às seguintes regras:

$$\frac{\vdots}{\forall X.A} \forall \mathcal{I} \qquad \frac{\vdots}{A[F/X]} \forall \mathcal{E}$$

Na primeira regra  $X$  não ocorre livre em nenhuma hipótese não cancelada e na segunda regra  $F$  é uma fórmula (tipo) qualquer.

Se  $t$  de tipo  $A$  representa a dedução acima de  $\forall \mathcal{I}$ , então  $\Lambda X.t$  representa a dedução na sua totalidade. As restrições habituais de variáveis em dedução natural ( $X$  não ocorre livre nas hipóteses não canceladas) corresponde às restrições na abstração universal. Por outro lado,  $\forall \mathcal{E}$  corresponde a uma aplicação universal ao tipo  $F$ .

Se  $t$  de tipo  $\forall X.A$  representa a dedução acima de  $\forall \mathcal{E}$ , então  $tF$  representa a dedução na sua totalidade.

A  $\beta$ -conversão  $(\Lambda X.t)F \rightsquigarrow t[F/X]$  corresponde em dedução natural, à  $\beta$ -conversão

$$\frac{\frac{\vdots}{A}}{\forall X.A}}{A[F/X]} \rightsquigarrow A[F/X]$$

onde a configuração à direita acima da fórmula  $A[F/X]$  se obtém da derivação à esquerda acima de  $A$ , substituindo as ocorrências livres de  $X$  por  $F$ .

### 3.4 O Sistema $\mathbf{F}_{\text{at}}$

O Sistema  $\mathbf{F}_{\text{at}}$ , também conhecido como polimorfismo atômico [9, 7], consiste numa restrição do sistema  $\mathbf{F}$  em que as instanciações universais estão restritas a fórmulas atômicas. Vamos apresentar o sistema  $\mathbf{F}_{\text{at}}$  em  $\lambda$ -cálculo e mais tarde a sua correspondência em dedução natural.

**DEFINIÇÃO 3.4.1** *Os tipos são construídos a partir de tipos atômicos (constantes posicionais  $P, Q, R, \dots$  e variáveis de tipo  $X, Y, Z, \dots$ ) usando duas operações ( $\rightarrow$  e  $\forall$ ) da seguinte forma:*

- 1) tipos atômicos são tipos.
- 2) Se  $A$  e  $B$  são tipos então  $A \rightarrow B$  é um tipo.
- 3) Se  $A$  é um tipo e  $X$  é uma variável de tipo então  $\forall X.A$  é um tipo.

Embora os sistemas  $\mathbf{F}$  e  $\mathbf{F}_{\text{at}}$  partilhem os mesmos tipos, já no que diz respeito aos termos, há uma diferença fundamental. Para que fique clara essa diferença, apresentamos a definição de termo de  $\mathbf{F}_{\text{at}}$  seguindo o esquema da definição 3.3.2

**DEFINIÇÃO 3.4.2** *Os termos são gerados pelas seguintes cláusulas*

- i) Para cada tipo  $A$  existe um número infinito contável de variáveis:  $x^A, y^A, z^A, \dots$ . Estas variáveis são termos de tipo  $A$ .
- ii)  $tq$  é um termo de tipo  $B$ , se  $t$  é um termo de tipo  $A \rightarrow B$  e  $q$  é um termo de tipo  $A$  (implicação).
- iii)  $\lambda x^A.t$  é um termo de tipo  $A \rightarrow B$ , se  $x^A$  é variável de tipo  $A$  e  $t$  é um termo de tipo  $B$  ( $\lambda$ -abstração).
- iv)  $tC$  é um termo de tipo  $A[C/X]$ , se  $t$  for um termo de tipo  $\forall X.A$  e  $C$  for um tipo atômico. (aplicação universal).
- v)  $\Lambda X.t$  é um termo de tipo  $\forall X.A$ , e  $t$  for um termo de tipo  $A$ , desde que a variável  $X$  não ocorra livre no tipo de nenhuma variável livre de  $t$  (abstração universal).

A diferença entre os sistemas  $\mathbf{F}$  e  $\mathbf{F}_{\text{at}}$  reside apenas na cláusula iv): o sistema  $\mathbf{F}$  permite a construção de termos  $tF$  de tipo  $A[F/X]$ , com  $F$  um qualquer tipo, enquanto que no sistema  $\mathbf{F}_{\text{at}}$   $F$  apenas pode ser um tipo atômico.

A noção de subfórmula, que desempenha, como veremos no capítulo 4, um papel crucial na prova do Teorema da normalização forte em  $\mathbf{F}_{\text{at}}$ , não existe no sistema  $\mathbf{F}$  porque os tipos universais  $\forall X.A$  permitem instanciações da forma  $A[D/X]$  com  $D$  qualquer tipo, por mais complexo que seja. No sistema  $\mathbf{F}_{\text{at}}$  a restrição da aplicação universal a tipos atômicos permite uma definição natural de subfórmula que apresentaremos de seguida.

**DEFINIÇÃO 3.4.3** *As subfórmulas da fórmula  $A$  são definidas por:*

- i)  $A$  é subfórmula de  $A$ .*
- ii) Se  $B \rightarrow C$  é subfórmula de  $A$  então  $B$  é subfórmula de  $A$  e  $C$  é subfórmula de  $A$ .*
- iii) Se  $\forall X.B$  é subfórmula de  $A$  então  $B[C/X]$  é subfórmula de  $A$  para toda a fórmula atômica  $C$  livre para  $X$  em  $B$ .<sup>3</sup>*

Temos que subfórmulas imediatas de  $A \rightarrow B$  são as fórmulas  $A$  e  $B$ . Subfórmulas imediatas de  $\forall X.A$  são as fórmulas  $A[C/X]$ , com  $C$  tipo atômico (livre para  $X$  em  $A$ ).

Na definição seguinte, por  $FV(A)$  com  $A$  um tipo referimo-nos ao usual conceito de conjunto de variáveis que ocorrem livres na fórmula  $A$ , i.e., não estão quantificadas.

**DEFINIÇÃO 3.4.4** *O conjunto das variáveis livres num termo  $t$ , representado por  $FV(t)$ , define-se por:*

$$FV(x^A) := \{x^A\} \cup FV(A)$$

$$FV(tq) := FV(t) \cup FV(q)$$

$$FV(\lambda x^A.t) := (FV(t) \setminus \{x^A\}) \cup FV(A)$$

$$FV(tC) := FV(t) \cup FV(C)$$

$$FV(\Lambda X.t) := FV(t) \setminus \{X\}.$$

Variáveis que não ocorrem livres num termo  $t$  chamam-se variáveis mudas em  $t$ . Sempre que necessário, assume-se que os conjuntos de variáveis livres e mudas num termo são disjuntos. A substituição de uma variável livre  $x^A$  num termo  $t$  por um termo  $s^A$ , faz-se da forma usual e representa-se por  $t[s/x]$ .

**DEFINIÇÃO 3.4.5** *Dado um termo  $t$  de tipo  $A$  e  $C$  um tipo atômico, define-se um novo termo  $t[C/X]$  de tipo  $A[C/X]$  da seguinte forma:*

$$x^A[C/X] := x^{A[C/X]}$$

$$(qr)[C/X] := q[C/X]r[C/X]$$

$$(\lambda x^A.q)[C/X] := \lambda x^{A[C/X]}.q[C/X]$$

$$(\Lambda X.q)[C/X] := \Lambda X.q$$

$$(\Lambda Y.q)[C/X] := \Lambda Y.(q[C/X]), \text{ para } Y \neq X; \text{ supondo, sem perda de generalidade que } C \neq Y$$

$$(qD)[C/X] := q[C/X]D[C/X], \text{ com } D \text{ tipo atômico.}$$

<sup>3</sup> $C$  ser livre para  $X$  em  $B$  significa que no caso de  $C$  ser uma variável ela não fica muda em  $B$  como resultado da substituição. Convencionamos que nas substituições tal é sempre salvaguardado.

No que respeita à substituição simultânea usaremos a seguinte notação:  $t[s_1/x_1, \dots, s_n/x_n]$  e  $t[C_1/X_1, \dots, C_n/X_n]$ .

Tal como no sistema  $\mathbf{F}$ , tem-se em  $\mathbf{F}_{\text{at}}$  duas  $\beta$ -conversões, uma para a implicação, a  $\beta$ -conversão implicacional, e outra para a quantificação universal, a  $\beta$ -conversão universal. As mesmas são respetivamente:

$$(\lambda x.t)s \rightsquigarrow t[s/x]$$

$$(\Lambda X.t)C \rightsquigarrow t[C/X], \text{ com } C \text{ tipo atómico.}$$

O lado esquerdo destas conversões designa-se por *redex* e o lado direito por *contractum*. As conversões anteriores são bem definidas, originando contractums em  $\mathbf{F}_{\text{at}}$  do mesmo tipo dos redexes. Necessitaremos também das chamadas  $\eta$ -conversões:

$$\lambda x.(tx) \rightsquigarrow t, \text{ em que } x \notin FV(t)$$

$$\Lambda X.(tX) \rightsquigarrow t, \text{ em que } X \notin FV(t)$$

A primeira é a  $\eta$ -conversão implicacional, a segunda a  $\eta$ -conversão universal. À semelhança das anteriores, o lado esquerdo das conversões designa-se por *redex* e o lado direito por *contractum*.

**DEFINIÇÃO 3.4.6** *Um termo  $t$  reduz-se a um termo  $q$  ( $t \succeq q$ ) se existir uma sequência de  $\beta\eta$ -conversões de  $t$  para  $q$ , ie, uma sequência  $t \equiv u_0, u_1, \dots, u_n \equiv q$ , tal que para  $i = 0, 1, \dots, n-1$ ,  $u_{i+1}$  obtém-se de  $u_i$  substituindo um redex pelo seu contractum.*

Um termo diz-se *normal* se não tiver redexes não lhe podendo assim ser aplicada mais nenhuma conversão.

Um termo  $t$  é *fortemente normalizável* se todas as sequências de reduções que começam com  $t$  têm um número finito de passos.

Pela correspondência de Curry-Howard, podemos apresentar o sistema  $\mathbf{F}_{\text{at}}$  como um cálculo de dedução natural.

As fórmulas são geradas por apenas dois conectivos lógicos primitivos, a saber a implicação e quantificador universal de segunda ordem e correspondem aos tipos no cálculo lambda. As derivações em dedução natural correspondem aos termos no cálculo lambda e são construídos através das seguintes regras:

### Regras de introdução

$$\frac{[A] \quad \vdots \quad B}{A \rightarrow B} \rightarrow \mathcal{I} \qquad \frac{\vdots \quad A}{\forall X.A} \forall \mathcal{I}$$

Na segunda regra,  $X$  não ocorre livre em nenhuma das hipóteses não canceladas.

**Regras de eliminação:**

$$\frac{\frac{\vdots}{A \rightarrow B} \quad \frac{\vdots}{A}}{B} \rightarrow \mathcal{E} \qquad \frac{\frac{\vdots}{\forall X.A}}{A[C/X]} \forall \mathcal{E}$$

Na segunda regra  $C$  é uma fórmula atômica, livre para  $X$  em  $A$ . Mais uma vez é esta restrição de  $C$  que distingue  $\mathbf{F}_{\text{at}}$  de  $\mathbf{F}$ .

Considerando a formulação em dedução natural temos que:

1) a  $\beta$ -conversão implicacional e a  $\beta$ -conversão universal têm respetivamente as seguintes formas:

$$\frac{\frac{[A]}{\vdots} \quad \frac{B}{A \rightarrow B} \quad \frac{\vdots}{A}}{B} \rightsquigarrow \frac{\vdots}{A} \quad \frac{\vdots}{B}$$

$$\frac{\frac{\vdots}{A}}{\forall X.A} \rightsquigarrow \frac{\vdots}{A[C/X]}$$

Onde  $C$  é uma fórmula atômica, livre para  $X$  em  $A$  e a derivação acima de  $A[C/X]$  resulta da derivação acima de  $A$ , substituindo as ocorrências livres de  $X$  por  $C$ .

2) a  $\eta$ -conversão implicacional e a  $\eta$ -conversão universal têm respetivamente as seguintes formas:

$$\frac{\frac{\vdots}{A \rightarrow B} \quad [A]}{B} \rightsquigarrow \frac{\vdots}{A \rightarrow B}$$

$$\frac{\frac{\vdots}{\forall X.A} \quad A}{\forall X.A} \rightsquigarrow \frac{\vdots}{\forall X.A}$$

**EXEMPLO 3.4.7** Para ilustrarmos a diferença entre trabalharmos no sistema  $\mathbf{F}$  ou no sistema  $\mathbf{F}_{\text{at}}$ , apresentamos uma derivação de  $A \rightarrow \forall Y(Y \rightarrow B)$ , com  $B$  fórmula atômica no sistema  $\mathbf{F}_{\text{at}}$  a partir de  $\forall X.X$ .

$$\frac{\frac{\frac{\frac{\forall X.X}{B} \forall \mathcal{E}}{Y \rightarrow B} \rightarrow \mathcal{I}}{\forall Y(Y \rightarrow B)} \forall \mathcal{I}}{A \rightarrow \forall Y(Y \rightarrow B)} \rightarrow \mathcal{I}}$$

Note que idêntica derivação é válida no sistema  $\mathbf{F}$ , contudo nesse sistema seria possível uma derivação mais simples

$$\frac{\forall X.X}{A \rightarrow \forall Y(Y \rightarrow B)} \forall \mathcal{E}$$

Note-se que em  $\mathbf{F}$  a regra  $\forall \mathcal{E}$  permite substituir  $X$  por uma fórmula qualquer, em particular por  $A \rightarrow \forall Y(Y \rightarrow B)$ , enquanto que em  $\mathbf{F}_{\text{at}}$  só permite substituir  $X$  por uma fórmula atômica.

# Capítulo 4

## Teorema da Normalização Forte para $\mathbf{F}_{\text{at}}$

É bem conhecido que o sistema de Girard  $\mathbf{F}$  é fortemente normalizável [11]. A sua demonstração é contudo nada trivial. Ela assenta na técnica de “reduzibilidade” de Tait sendo necessário recorrer a uma estratégia muito intrincada desenvolvida pelo próprio Girard e conhecida como “candidatos de reduzibilidade”. Tendo o sistema  $\mathbf{F}$  a propriedade da normalização forte, por maioria de razão,  $\mathbf{F}_{\text{at}}$  (um seu subsistema) também será fortemente normalizável. O que se mostra neste Capítulo é que em  $\mathbf{F}_{\text{at}}$  é possível apresentar uma prova de normalização forte muito mais simples do que no contexto de  $\mathbf{F}$ , baseada simplesmente na técnica de Tait, sem necessidade de candidatos de reduzibilidade. Tal demonstração encontra-se no artigo [7] sendo aqui apresentada com grande detalhe.

Neste Capítulo iremos demonstrar portanto que a árvore de reduções de qualquer derivação em  $\mathbf{F}_{\text{at}}$ , considerando  $\beta\eta$ -conversões, é finita, i.e. provaremos o teorema que se segue:

**TEOREMA 4.0.8 (Teorema da normalização forte)** *O sistema  $\mathbf{F}_{\text{at}}$  é fortemente normalizável considerando  $\beta\eta$ -conversões.*

A demonstração irá requerer alguns resultados auxiliares, adiante organizados em 3 lemas e 1 proposição. Antes porém apresentamos algumas definições.

**DEFINIÇÃO 4.0.9** *Seja  $t$  um termo fortemente normalizável, denota-se por  $v(t)$  o comprimento da maior sequência de reduções a começar em  $t$ .*

Para cada tipo  $T$  definimos um conjunto  $RED_T$  (chamado de conjunto de termos redutíveis de tipo  $T$ ) que se constrói por indução na complexidade dos tipos segundo a definição que se segue:

**DEFINIÇÃO 4.0.10** 1) *Se  $t$  é um termo de tipo atômico  $C$ ,  $t \in RED_C$  se e só se for fortemente normalizável.*

2) *Se  $t$  é um termo de tipo  $A \rightarrow B$ ,  $t \in RED_{A \rightarrow B}$  se e só se  $\forall u \in RED_A, tu \in RED_B$ .*

3) *Se  $t$  é um termo de tipo  $\forall X.A$ ,  $t \in RED_{\forall X.A}$  se e só se para todo o tipo atômico  $C$ ,  $tC \in RED_{A[C/X]}$ .*

Por vezes em vez de  $t \in RED_A$ , escreveremos com o mesmo significado “ $t$  é redutível de tipo  $A$ ” ou simplesmente “ $t$  é redutível” quando não há ambiguidade quanto ao tipo do termo.

**DEFINIÇÃO 4.0.11** *Um termo diz-se neutro se não for uma abstração i.e., não for da forma  $\lambda x.u$  nem da forma  $\Lambda X.t$  por outras palavras são neutros os termos da forma  $x$ ;  $tu$  e  $tC$ .*

**LEMA 4.0.12 Propriedades da redutibilidade**

$RED_T$  satisfaz as seguintes condições:

(CR1) Se  $t \in RED_T$  então  $t$  é fortemente normalizável.

(CR2) Se  $t \in RED_T$  e  $t \succeq t'$ , então  $t' \in RED_T$ .

(CR3) Se  $t$  é neutro e sempre que  $t \succ_1 t'$  se tem  $t' \in RED_T$  então  $t \in RED_T$ .

Um caso particular de (CR3) será:

(CR4) Se  $t$  é neutro e normal então  $t \in RED_T$ .

**DEMONSTRAÇÃO:** A demonstração de que  $RED$  satisfaz as propriedades acima será feita por indução na complexidade dos tipos.

**1 - Tipo atómico**

Sendo  $T$  um tipo atómico sabemos, por definição de  $RED_T$ , que os termos redutíveis desse tipo, isto é os termos em  $RED_T$ , são exactamente os que são fortemente normalizáveis.

(CR1) Verifica-se por definição de  $RED_T$ .

(CR2) Se  $t \in RED_T$  então  $t$  é fortemente normalizável. Assim se  $t \succeq t'$  então  $t'$  é fortemente normalizável, provando-se (CR2).

(CR3) Se todas as reduções num passo a partir de um termo  $t$  dão origem a termos em  $RED_T$ , i.e. fortemente normalizáveis, então  $t$  é fortemente normalizável (a sua árvore de redução terá de ser finita, pois há um número finito de reduções num passo a partir de  $t$  e todas as árvores de redução a partir dessas derivações em um passo são finitas). Sendo  $t$  fortemente normalizável,  $t \in RED_T$ , provando-se (CR3).

**2 - Tipo implicação ( $A \rightarrow B$ )**

Um termo de tipo implicação é redutível se e só se todas as suas aplicações a termos redutíveis são redutíveis.

(CR1) Seja  $x$  uma variável de tipo  $A$ , a hipótese de indução (CR4) em  $A$  diz-nos que  $x$ , sendo neutro e normal é redutível.

Sendo  $t$  de tipo  $A \rightarrow B$  e redutível ( $t \in RED_{A \rightarrow B}$ ) tem-se que  $tx$  é redutível de tipo  $B$  ( $tx \in RED_B$ ), e pela hipótese de indução, (CR1), em  $B$   $tx$  é fortemente normalizável. Se existisse uma sequência  $t \succeq_1 t_1 \succeq_1 t_2 \dots$  infinita, então  $tx \succeq_1 t_1x \succeq_1 t_2x \dots$  seria infinita o que

é um absurdo. Temos então, dado que  $tx$  é fortemente normalizável também  $t$  é fortemente normalizável o que prova (CR1).

(CR2) Se  $t$  é redutível e  $t \succeq t'$  queremos mostrar que se considerarmos  $s \in RED_A$  então  $t's \in RED_B$ . Seja então  $s$  redutível de tipo  $A$ ,  $ts$  é redutível de tipo  $B$  ( $ts \in RED_B$ ) e  $ts \succeq t's$ . Por hipótese de indução (CR2) em  $B$  tem-se que  $t's$  é redutível de tipo  $B$ . Tem-se então, por definição, que  $t'$  é redutível ( $t' \in RED_{A \rightarrow B}$ ) o que prova (CR2).

(CR3) Seja  $t$  um termo neutro de tipo  $A \rightarrow B$ , tal que sempre que  $t \succ_1 t'$ ,  $t' \in RED_{A \rightarrow B}$ . Seja  $p \in RED_A$ , por hipótese de indução (CR1) em  $A$ ,  $p$  é fortemente normalizável. Vamos usar indução sobre o comprimento da maior sequência de reduções a começar em  $p$  ( $v(p)$ ) para mostrar que  $tp$  é redutível de tipo  $B$ .  
Num passo,  $tp$  reduz-se em:

i)  $t'p$ , onde  $t \succeq_1 t'$ . Mas  $t' \in RED_{A \rightarrow B}$  logo, por definição,  $t'p \in RED_B$

ii)  $tp'$ , onde  $p \succeq_1 p'$ . Por hipótese de indução (CR2) em  $A$ , dado que  $p \in RED_A$  temos que  $p' \in RED_A$ . Como  $v(p') < v(p)$  ou seja a maior sequência de reduções a começar em  $p'$  é mais curta do que a que começa em  $p$ , por hipótese de indução em  $v(p')$  tem-se que  $tp' \in RED_B$ .

Como  $t$  é neutro,  $t$  não é da forma  $\lambda x.u$  nem da forma  $\Lambda X.u$  não pode acontecer que  $tp$  seja da forma  $(\lambda x.u)p$  nem da forma  $(\Lambda X.u)p$ , não existindo outras hipóteses de redução num passo além das acima apresentadas.

Sendo  $tp$  uma aplicação é obviamente um termo neutro, é de tipo  $B$  e, num passo, só se reduz a termos redutíveis. Assim, pela hipótese de indução (CR3) em  $B$ ,  $tp \in RED_B$  e por definição,  $t \in RED_{A \rightarrow B}$  e fica provado (CR3).

### 3 - Tipo $\forall X.B$

Um termo de tipo  $\forall X.B$  é redutível se e só se todas as aplicações a tipos atômicos também o forem.

(CR1) Vamos considerar  $t \in RED_{\forall X.B}$  e mostrar que  $t$  é fortemente normalizável. Por definição de  $RED_{\forall X.B}$ ,  $tX \in RED_B$  pois  $B[X/X] \equiv B$ . Por hipótese de indução (CR1)  $tX$  é fortemente normalizável (pois  $RED_B$  satisfaz (CR1)). Como cada sequência de reduções de  $t$ , dá origem a uma sequência de reduções de  $tX$ , aplicando cada termo da sequência a  $X$ , concluímos que  $t$  é fortemente normalizável e fica provado (CR1).

(CR2) Vamos considerar  $t \in RED_{\forall X.B}$  e  $t \succeq t'$ . Queremos mostrar que  $t' \in RED_{\forall X.B}$ . Seja  $C$  um tipo atômico, por definição, sabe-se que  $tC \in RED_{B[C/X]}$ . Como  $tC \succeq t'C$ , por hipótese de indução (CR2) em  $B[C/X]$  tem-se que  $t'C \in RED_{B[C/X]}$ . Por definição  $t' \in RED_{\forall X.B}$  e fica provado (CR2).

(CR3) Vamos considerar  $t$  de tipo  $\forall X.B$ , neutro e tal que todo o termo que resulte de  $t$  num passo seja redutível, queremos provar que  $t \in RED_{\forall X.B}$ . Seja  $C$  um tipo atômico, vamos mostrar que  $tC \in RED_{B[C/X]}$ . Note-se que  $tC$  é neutro e que os redexes em  $tC$  apenas podem ocorrer em  $t$  visto que  $t$  é neutro e por conseguinte não é abstração universal. Assim qualquer redução em um passo de  $tC$  tem a forma de  $t'C$  com  $t \succeq_1 t'$ . Como por

hipótese  $t' \in RED_{\forall X.B}$  e por definição  $t'C \in RED_{B[C/X]}$ , a hipótese de indução (CR3) em  $RED_{B[C/X]}$  garante que  $tC \in RED_{B[C/X]}$ . Por definição tem-se que  $t \in RED_{\forall X.B}$  e fica provado (CR3).  $\square$

Com vista a mostrar que todos os termos são redutíveis começamos por apresentar dois lemas auxiliares envolvendo abstrações.

**LEMA 4.0.13 (abstração implicacional)** *Se  $\forall q \in RED_A, p[q/x^A] \in RED_B$  então  $\lambda x.p \in RED_{A \rightarrow B}$ .*

DEMONSTRAÇÃO: Por definição de  $RED$ , para provarmos que  $\lambda x.p \in RED_{A \rightarrow B}$  basta tomar  $q \in RED_A$  arbitrário e mostrarmos que  $(\lambda x.p)q \in RED_B$ . Note que pelo lema 4.0.12  $q$  é fortemente normalizável e também sabemos que  $x \in RED_A$ .

Queremos mostrar que  $(\lambda x.p)q$  é redutível de tipo  $B$  ( $(\lambda x.p)q \in RED_B$ ) para todo o  $q \in RED_A$ . Vamos usar indução na soma dos comprimentos das maiores reduções que começam em  $q$  e em  $p$  ( $v(q) + v(p)$ ). O termo  $(\lambda x.p)q$  pode reduzir-se em um passo a:

i)  $p[q/x]$  que é redutível por hipótese.

ii)  $(\lambda x.p')q$  com  $p \succeq_1 p'$ . Note que, como  $x \in RED_A$ , por hipótese  $p[x/x] \equiv p$  é redutível e portanto fortemente normalizável pelo que  $p'$  também é fortemente normalizável. Mais tem-se que  $v(p') < v(p)$  e logo, por hipótese de indução  $(\lambda x.p')q$  é redutível.

iii)  $(\lambda x.p)q'$  com  $q \succeq_1 q'$  com  $v(q') < v(q)$  logo  $q'$  é redutível e por hipótese de indução  $(\lambda x.p)q'$  é redutível.

iv)  $sq$  com  $p = sx$  e  $x$  não ocorre livre em  $s$  ( $x \notin FV(s)$ ), mas neste caso  $sq \equiv (sx)[q/x] \equiv p[q/x]$  que é redutível por hipótese.

Em qualquer dos casos o termo neutro  $(\lambda x.p)q$  reduz-se em um passo a termos redutíveis, logo por (CR3),  $(\lambda x.p)q \in RED_B$  e por definição  $\lambda x.p \in RED_{A \rightarrow B}$ .  $\square$

**LEMA 4.0.14 (Abstração universal)** *Se para todo o tipo atômico  $C$ ,  $t[C/X]$  é redutível e  $X$  não ocorre livre no tipo de nenhuma variável livre de  $t$ , então  $\Lambda X.t$  é redutível.*

DEMONSTRAÇÃO: Seja  $t$ , tal que para todo o tipo atômico  $C$ ,  $t[C/X]$  é redutível e  $X$  não ocorre livre no tipo de nenhuma variável livre de  $t$ . Temos que  $t$  é fortemente normalizável pois  $t \equiv t[X/X]$  que por hipótese é redutível e por (CR1) é fortemente normalizável. Vamos então mostrar que para todo o tipo atômico  $C$ ,  $(\Lambda X.t)C$  é redutível.

A prova será feita usando indução sobre  $v(t)$ . Sendo  $(\Lambda X.t)C$  neutro, apenas será necessário mostrar que as reduções em um passo deste termo são redutíveis.

Uma redução em um passo de  $(\Lambda X.t)C$  pode ter uma das seguintes formas:

i)  $t[C/X]$  que é redutível por hipótese.

ii)  $(\Lambda X.t')C$  com  $t \succ_1 t'$ , sendo  $v(t') < v(t)$  e para qualquer tipo atômico  $D$ , por (CR2) tem-se que  $t'[D/X]$  é redutível. Logo, por hipótese de indução  $(\Lambda X.t')C$  é redutível.

iii)  $sC$ , sendo  $t \equiv sX$  e  $X$  não ocorre livre em  $s$ . Neste caso tem-se  $sC \equiv sX[C/X] \equiv t[C/X]$  que é redutível por hipótese.

Em qualquer dos casos o termo neutro  $(\Lambda X.t)C$  reduz-se em um passo num termo redutível sendo por (CR3) redutível. Logo, por definição  $\Lambda X.t$  é redutível.  $\square$

Para provarmos que todo o termo é redutível necessitamos de apresentar uma propriedade mais forte.

**PROPOSIÇÃO 4.0.15** *Seja  $t$  um termo (não necessariamente redutível) de variáveis livres  $x_1, x_2, \dots, x_n$  de tipo  $A_1, A_2, \dots, A_n$  respectivamente. Se  $X_1, X_2, \dots, X_m$  são todas as variáveis de tipo livres do termo  $t$ ;  $C_1, C_2, \dots, C_m$  são tipos atômicos e  $q_1, q_2, \dots, q_n$  são termos redutíveis de tipo  $A_1[C_1/X_1, \dots, C_m/X_m], \dots, A_n[C_1/X_1, \dots, C_m/X_m]$  então o termo  $t[C_1/X_1, \dots, C_m/X_m][q_1/x_1, \dots, q_n/x_n]$  é redutível.*

**DEMONSTRAÇÃO:** A demonstração faz-se por indução na complexidade do termo  $t$ . Vamos escrever  $t[\underline{C}/\underline{X}][\underline{q}/\underline{x}]$  para representar  $t[C_1/X_1, \dots, C_m/X_m][q_1/x_1, \dots, q_n/x_n]$ .

i) Se  $t$  é uma variável  $x_i$  de tipo  $A_i$  então  $t[\underline{C}/\underline{X}][\underline{q}/\underline{x}] \equiv q_i$  que é redutível por hipótese.

ii) Se  $t \equiv wv$ . Tem-se que  $t[\underline{C}/\underline{X}][\underline{q}/\underline{x}]$  é redutível pois por hipótese de indução  $v[\underline{C}/\underline{X}][\underline{q}/\underline{x}]$  e  $w[\underline{C}/\underline{X}][\underline{q}/\underline{x}]$  são ambos redutíveis e por definição de redutibilidade  $w[\underline{C}/\underline{X}][\underline{q}/\underline{x}]v[\underline{C}/\underline{X}][\underline{q}/\underline{x}]$  é redutível mas este termo é  $t[\underline{C}/\underline{X}][\underline{q}/\underline{x}]$ .

iii) Se  $t \equiv \lambda y.w$  de tipo  $B \rightarrow E$ . Vamos provar que  $(\lambda y.w)[\underline{C}/\underline{X}][\underline{q}/\underline{x}]$  é redutível. Por definição de substituição o termo considerado é igual a  $\lambda y.(w[\underline{C}/\underline{X}][\underline{q}/\underline{x}])$ . Pelo lema 4.0.13 basta mostrarmos que  $(w[\underline{C}/\underline{X}][\underline{q}/\underline{x}])[v/y]$  é redutível para todo o  $v$  redutível. O termo é igual a  $(\lambda y.w)[\underline{C}/\underline{X}][\underline{q}/\underline{x}, v/y]$  que é redutível por hipótese de indução. Assim, pelo lema 4.0.13,  $\lambda y.w$  é redutível.

iv) Seja  $t \equiv pD$ , de tipo  $B[D/Y]$  com  $D$  um tipo atômico. Seja  $Z$  uma variável de tipo tal que  $FV(D) \subseteq \{Z\}$  ou seja se  $D$  é variável de tipo então é a variável  $Z$ .

Queremos mostrar que o termo  $(pD)[\underline{C}/\underline{X}, P/Z][\underline{q}/\underline{x}]$  é redutível com  $\underline{C}$  e  $P$  tipos atômicos e  $\underline{q}$  uma sequência de termos redutíveis. Por hipótese de indução tem-se que  $p[\underline{C}/\underline{X}, P/Z][\underline{q}/\underline{x}]$  é redutível de tipo  $\forall Y.B[\underline{C}/\underline{X}, P/Z]$ . Por definição de redutibilidade tem-se que o termo  $(p[\underline{C}/\underline{X}, P/Z][\underline{q}/\underline{x}])D[P/Z]$  é redutível mas este termo é igual a  $(pD)[\underline{C}/\underline{X}, P/Z][\underline{q}/\underline{x}]$  e fica provado o pretendido.

v) Seja  $t \equiv \Lambda Y.p$ . Queremos mostrar que  $(\Lambda Y.p)[\underline{C}/\underline{X}][\underline{q}/\underline{x}]$  é redutível. Por definição de substituição este termo é  $\Lambda Y.(p[\underline{C}/\underline{X}][\underline{q}/\underline{x}])$ . Basta então provar que para todo o tipo atômico  $D$ ,  $(p[\underline{C}/\underline{X}][\underline{q}/\underline{x}])[D/Y]$  é redutível, mas este termo é  $(p[\underline{C}/\underline{X}, D/Y][\underline{q}/\underline{x}])$  que é redutível por hipótese de indução. e pelo lema 4.0.14 fica provado o pretendido.  $\square$

Podemos agora concluir a seguinte propriedade.

**TEOREMA 4.0.16** *Todos os termos de  $\mathbf{F}_{\text{at}}$  são redutíveis.*

DEMONSTRAÇÃO:

Seja  $t[X_1, \dots, X_m][x_1, \dots, x_n]$  um termo qualquer no qual todas as variáveis livres estão entre as apresentadas. Cada  $x_i, i = 1, \dots, n$  é neutro e normal. Sabe-se por (CR4) que cada  $x_i$  é redutível.  $X_j$  para  $j = 1, \dots, m$  são variáveis de tipo, logo são tipos atômicos. Pela proposição 4.0.15, tem-se que  $t[X_1, \dots, X_m][x_1, \dots, x_n]$  é redutível.  $\square$

O Teorema 4.0.8 sai como corolário imediato do Teorema 4.0.16 tendo em conta o Lema 4.0.12 (CR1).

Se tentássemos, com a estratégia anterior, provar normalização forte para o sistema  $\mathbf{F}$ , deparar-nos-íamos imediatamente com um problema: a correspondente definição de *RED* no contexto de  $\mathbf{F}$  não faria sentido pois o sistema não tem o conceito de subfórmula.

Em  $\mathbf{F}$  as instanciações universais podendo ser de qualquer tipo. De facto, sendo  $u$  um termo de tipo  $\forall X.T$  e  $G$  um tipo qualquer,  $uG$  terá tipo  $T[G/X]$ , o que pode ser uma fórmula muito mais complexa do que  $\forall X.T$ . Não se podendo aplicar diretamente a estratégia por indução na complexidade do tipo.

Para contornar esta dificuldade na prova da normalização forte em  $\mathbf{F}$  recorre-se a “candidatos de redutibilidade” que são conjuntos arbitrários de termos de um certo tipo que verificam as condições de redutibilidade.

# Capítulo 5

## Imersão do Cálculo Proposicional Intuicionista em $\mathbf{F}_{\text{at}}$

Neste capítulo iremos demonstrar um conjunto de resultados que permitirão no Capítulo 6 chegar a uma prova da Normalização Forte para o Cálculo Proposicional Intuicionista, considerando  $\beta$ -conversões, através da Normalização Forte em  $\mathbf{F}_{\text{at}}$ .

Começaremos por mostrar que apesar da forte restrição da regra  $\forall\mathcal{E}$  em  $\mathbf{F}_{\text{at}}$ , quando comparada com a regra  $\forall\mathcal{E}$  em  $\mathbf{F}$ , essa restrição não é tão severa quando à partida possa parecer. Para três tipos de fórmulas universais, como veremos de seguida, a restrição acaba por não ser de todo limitativa.

**PROPOSIÇÃO 5.0.17** *Em  $\mathbf{F}_{\text{at}}$ , existe transbordo de instanciação para fórmulas da forma:*

$$\begin{aligned} &\forall X.X \\ &\forall X((A \rightarrow (B \rightarrow X)) \rightarrow X) \\ &\forall X((A \rightarrow X) \rightarrow ((B \rightarrow X) \rightarrow X)) \end{aligned}$$

onde  $X$  é uma variável de segunda-ordem que não ocorre em  $A$  ou  $B$ , i.e. das fórmulas acima é possível deduzir em  $\mathbf{F}_{\text{at}}$ , respetivamente

$$\begin{aligned} &C \\ &(A \rightarrow (B \rightarrow C)) \rightarrow C \\ &(A \rightarrow C) \rightarrow ((B \rightarrow C) \rightarrow C) \end{aligned}$$

para qualquer fórmula  $C$  (não necessariamente atômica).

Note que a proposição acima, além de apresentar um resultado, define o que entendemos por “transbordo de instanciação”.

**DEMONSTRAÇÃO:**

**Caso 1**

Vejamos, por indução na complexidade da fórmula  $C$ , que de  $\forall X.X$  se deduz  $C$  em  $\mathbf{F}_{\text{at}}$ .

i)  $C$  fórmula atômica (imediatamente, basta aplicar a regra de eliminação do  $\forall$ )

$$\frac{\forall X.X}{C} \forall \mathcal{E}$$

ii) Suponhamos que  $C$  é da forma  $C_1 \rightarrow C_2$ . Por hipótese de indução assumimos que o resultado é válido para  $C_1$  e  $C_2$ , i.e.,

$$\frac{\forall X.X}{C_1} \quad \text{e} \quad \frac{\forall X.X}{C_2}$$

Em geral o traço duplo numa derivação indica que pode existir mais que uma regra (podemos estar a omitir parte da demonstração). Neste caso concreto o duplo traço representa a parte da demonstração que se obtém por transbordo de instanciação.

Tem-se então

$$\frac{\frac{\forall X.X}{C_2} H.I.}{C_1 \rightarrow C_2} \rightarrow \mathcal{I}$$

iii) Suponhamos que  $C$  é da forma  $\forall X.C_1$ . Por hipótese de indução assumimos que o resultado é válido para  $C_1$ , i.e.,

$$\frac{\forall X.X}{C_1}$$

tem-se então

$$\frac{\frac{\forall X.X}{C_1} H.I.}{\forall X.C_1} \forall \mathcal{I}$$

## Caso 2

Vejamos, por indução na complexidade da fórmula  $C$ , que de  $\forall X((A \rightarrow (B \rightarrow X)) \rightarrow X)$  se deduz  $(A \rightarrow (B \rightarrow C)) \rightarrow C$  em  $\mathbf{F}_{\text{at}}$ .

i)  $C$  atômica (imediatamente)

ii)  $C \equiv C_1 \rightarrow C_2$

$$\frac{\frac{\forall X((A \rightarrow (B \rightarrow X)) \rightarrow X)}{(A \rightarrow (B \rightarrow C_2)) \rightarrow C_2} H.I. \quad \frac{\frac{\frac{[A \rightarrow (B \rightarrow (C_1 \rightarrow C_2))]}{[B \rightarrow (C_1 \rightarrow C_2)]} \quad [A]}{C_1 \rightarrow C_2} \quad [B]}{C_2} \quad [C_1]}{A \rightarrow (B \rightarrow C_2)}}{\frac{C_2}{C_1 \rightarrow C_2}} \rightarrow \mathcal{I}$$

iii)  $C \equiv \forall X C_1$

$$\frac{\frac{\frac{\forall X((A \rightarrow (B \rightarrow X)) \rightarrow X)}{(A \rightarrow (B \rightarrow C_1)) \rightarrow C_1} H.I.}{\frac{C_1}{\forall X.C_1}}}{(A \rightarrow (B \rightarrow \forall X.C_1)) \rightarrow \forall X C_1} \quad \frac{\frac{\frac{[A \rightarrow (B \rightarrow \forall X.C_1)] \quad [A]}{B \rightarrow \forall X.C_1} \quad [B]}{\frac{\forall X.C_1}{C_1}}}{\frac{B \rightarrow C_1}{A \rightarrow (B \rightarrow C_1)}}$$

### Caso 3

Veamos, por indução na complexidade da fórmula  $C$ , que de  $\forall X((A \rightarrow X) \rightarrow ((B \rightarrow X) \rightarrow X))$  se deduz  $(A \rightarrow C) \rightarrow ((B \rightarrow C) \rightarrow C)$  em  $\mathbf{F}_{\text{at}}$ .

i)  $C$  atômica (imediato)

ii)  $C \equiv C_1 \rightarrow C_2$

$$\frac{\frac{\frac{\forall X((A \rightarrow X) \rightarrow ((B \rightarrow X) \rightarrow X))}{(A \rightarrow C_2) \rightarrow ((B \rightarrow C_2) \rightarrow C_2)} H.I.}{(B \rightarrow C_2) \rightarrow C_2} \quad \frac{\frac{\frac{[A \rightarrow (C_1 \rightarrow C_2)] \quad [A]}{C_1 \rightarrow C_2} \quad [C_1]}{C_2}}{A \rightarrow C_2} \quad \frac{\frac{[B \rightarrow (C_1 \rightarrow C_2)] \quad [B]}{C_1 \rightarrow C_2} \quad [C_1]}{C_2}}{B \rightarrow C_2}}{\frac{C_2}{C_1 \rightarrow C_2}}}{(A \rightarrow (C_1 \rightarrow C_2)) \rightarrow ((B \rightarrow (C_1 \rightarrow C_2)) \rightarrow (C_1 \rightarrow C_2))}$$

iii)  $C \equiv \forall X.C_1$

$$\frac{\frac{\frac{\forall X((A \rightarrow X) \rightarrow ((B \rightarrow X) \rightarrow X))}{(A \rightarrow C_1) \rightarrow ((B \rightarrow C_1) \rightarrow C_1)} H.I.}{(B \rightarrow C_1) \rightarrow C_1} \quad \frac{\frac{[A \rightarrow \forall X.C_1] \quad [A]}{\forall X.C_1} \quad [A]}{\frac{C_1}{A \rightarrow C_1}} \quad \frac{\frac{[B \rightarrow \forall X.C_1] \quad [B]}{\forall X.C_1} \quad [B]}{\frac{C_1}{B \rightarrow C_1}}}{\frac{C_1}{\forall X.C_1}}}{(B \rightarrow \forall X.C_1) \rightarrow \forall X.C_1} \quad \frac{\frac{C_1}{\forall X.C_1}}{(A \rightarrow \forall X.C_1) \rightarrow ((B \rightarrow \forall X.C_1) \rightarrow \forall X.C_1)}$$

□

**Observação:** A proposição anterior também é válida em  $\mathbf{F}$ , pois qualquer dedução em  $\mathbf{F}_{\text{at}}$  é válida em  $\mathbf{F}$ . Note-se, contudo, que em  $\mathbf{F}$  a demonstração da proposição seria imediata: Para uma fórmula  $C$  qualquer, em  $\mathbf{F}$  teríamos:

$$\frac{\forall X.X}{C} \forall \mathcal{E} \quad \frac{\forall X((A \rightarrow (B \rightarrow X)) \rightarrow X)}{(A \rightarrow (B \rightarrow C)) \rightarrow C} \forall \mathcal{E} \quad \frac{\forall X((A \rightarrow X) \rightarrow ((B \rightarrow X) \rightarrow X))}{(A \rightarrow C) \rightarrow ((B \rightarrow C) \rightarrow C)} \forall \mathcal{E}$$

O transbordo de instanciação será necessário para demonstrar que o cálculo proposicional intuicionista pode ser imerso em  $\mathbf{F}_{\text{at}}$ . A tradução de provas que se seguirá à tradução de fórmulas irá usar transbordo de instanciação e dará origem ao que chamaremos *tradução canônica*. Começaremos por apresentar uma definição, que resulta da conhecida definição de Prawitz [15], onde a tradução de fórmulas do cálculo proposicional intuicionista será denotada por  $(.)^*$

**DEFINIÇÃO 5.0.18** *As fórmulas do cálculo proposicional intuicionista serão traduzidas em  $\mathbf{F}_{\text{at}}$  indutivamente da seguinte forma:*

$$\begin{aligned} (P)^* &: \equiv P, P \text{ proposição atômica, } P \neq \perp \\ (\perp)^* &: \equiv \forall X.X \\ (A \rightarrow B)^* &: \equiv A^* \rightarrow B^* \\ (A \vee B)^* &: \equiv \forall X ((A^* \rightarrow X) \rightarrow ((B^* \rightarrow X) \rightarrow X)) \\ (A \wedge B)^* &: \equiv \forall X ((A^* \rightarrow (B^* \rightarrow X)) \rightarrow X). \end{aligned}$$

Vamos então provar que o cálculo proposicional intuicionista se imerge em  $\mathbf{F}_{\text{at}}$ .

**TEOREMA 5.0.19** *O cálculo proposicional intuicionista (com os conetivos  $\perp, \vee, \wedge, \rightarrow$ ) pode ser imerso em  $\mathbf{F}_{\text{at}}$ , usando a tradução  $(.)^*$ . I.e. traduzindo as fórmulas através de  $(.)^*$ , as regras de introdução e de eliminação em Dedução Natural para os conetivos do cálculo Proposicional Intuicionista são válidas em  $\mathbf{F}_{\text{at}}$ .*

**DEMONSTRAÇÃO:**

i) As regras para  $\rightarrow$

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

são primitivas em  $\mathbf{F}_{\text{at}}$ .

ii) Analisemos as regras para  $\perp$ :

$$\frac{\perp}{C} \quad \text{com } C \text{ fórmula qualquer.}$$

Usando a tradução  $(.)^*$ , queremos provar que

$$\frac{\forall X.X}{C^*}$$

é válido em  $\mathbf{F}_{\text{at}}$ . Tal é imediato pois pela proposição 5.0.17 sabemos que  $\forall X.X$  admite transbordo de instanciação, i.e., existe uma dedução em  $\mathbf{F}_{\text{at}}$

$$\frac{\forall X.X}{C^*} \quad \text{com } C^* \text{ fórmula qualquer.}$$

iii) Analisemos as regras para  $\wedge$ <sup>1</sup>:

$$\frac{\vdots}{A \wedge B} \quad A \quad \text{e} \quad \frac{\vdots \quad \vdots}{A \wedge B} \quad A \quad B$$

Para a 1<sup>a</sup> regra, queremos provar que em  $\mathbf{F}_{\text{at}}$  há uma derivação

$$\frac{\vdots}{\forall X((A^* \rightarrow (B^* \rightarrow X)) \rightarrow X)} \quad A^*$$

Ora

$${}_2 \frac{\frac{\vdots}{\forall X((A^* \rightarrow (B^* \rightarrow X)) \rightarrow X)} \quad \frac{[A^*]}{B^* \rightarrow A^*}}{(A^* \rightarrow (B^* \rightarrow A^*)) \rightarrow A^*} \quad A^* \rightarrow (B^* \rightarrow A^*)}{A^*}$$

Para a 2<sup>a</sup> regra, queremos provar que em  $\mathbf{F}_{\text{at}}$  há uma derivação

$$\frac{\frac{\vdots \quad \vdots}{A^* \quad B^*}}{\forall X((A^* \rightarrow (B^* \rightarrow X)) \rightarrow X)}$$

Ora,

$$\frac{\frac{\frac{\vdots}{A^*} \quad [A^* \rightarrow (B^* \rightarrow X)]}{B^* \rightarrow X} \quad \frac{\vdots}{B^*}}{X} \quad \frac{(A^* \rightarrow (B^* \rightarrow X)) \rightarrow X}{\forall X((A^* \rightarrow (B^* \rightarrow X)) \rightarrow X)}$$

<sup>1</sup>Relativamente às regras de eliminação da conjunção ilustramos com a eliminação da conjunção à direita dado que a regra de eliminação à esquerda se analisa de forma completamente análoga.

<sup>2</sup>A derivação omitida pelo duplo traço consiste na aplicação de transbordo de instanciação

é a dedução pretendida.

iv) Analisemos as regras para  $\vee$ <sup>3</sup>:

$$\frac{\vdots}{A} \quad \text{e} \quad \frac{\begin{array}{c} \vdots \\ A \vee B \end{array} \quad \begin{array}{c} [A] \\ \vdots \\ C \end{array} \quad \begin{array}{c} [B] \\ \vdots \\ C \end{array}}{C}$$

Para a 1ª regra, queremos provar que em  $\mathbf{F}_{\text{at}}$  há uma derivação

$$\frac{\vdots}{A^*}}{\forall X((A^* \rightarrow X) \rightarrow ((B^* \rightarrow X) \rightarrow X))}$$

Ora,

$$\frac{\begin{array}{c} \vdots \\ A^* \quad [A^* \rightarrow X] \\ \hline X \\ (B^* \rightarrow X) \rightarrow X \end{array}}{(A^* \rightarrow X) \rightarrow ((B^* \rightarrow X) \rightarrow X)}}{\forall X((A^* \rightarrow X) \rightarrow ((B^* \rightarrow X) \rightarrow X))}$$

é uma dedução em  $\mathbf{F}_{\text{at}}$ .

Para a 2ª regra, queremos provar que em  $\mathbf{F}_{\text{at}}$  é válida uma derivação

$$\frac{\forall X((A^* \rightarrow X) \rightarrow ((B^* \rightarrow X) \rightarrow X)) \quad \begin{array}{c} [A^*] \\ \vdots \\ C^* \end{array} \quad \begin{array}{c} [B^*] \\ \vdots \\ C^* \end{array}}{C^*}}$$

Ora,

$$\frac{\begin{array}{c} \vdots \\ \forall X((A^* \rightarrow X) \rightarrow ((B^* \rightarrow X) \rightarrow X)) \end{array} \quad \begin{array}{c} [A^*] \\ \vdots \\ C^* \end{array}}{\frac{\frac{\frac{\forall X((A^* \rightarrow X) \rightarrow ((B^* \rightarrow X) \rightarrow X))}{(A^* \rightarrow C^*) \rightarrow ((B^* \rightarrow C^*) \rightarrow C^*)} \quad \frac{C^*}{A^* \rightarrow C^*}}{(B^* \rightarrow C^*) \rightarrow C^*}}{\frac{C^*}{B^* \rightarrow C^*}}}$$

é uma dedução em  $\mathbf{F}_{\text{at}}$ . □

**Observação:** O teorema é obviamente válido em  $\mathbf{F}$ , pois todas as regras válidas em  $\mathbf{F}_{\text{at}}$  são válidas em  $\mathbf{F}$ . Em  $\mathbf{F}$  a prova até pode ser simplificada. Em todos os pontos em que

<sup>3</sup>Apresenta-se a regra de introdução da disjunção à direita dado que a regra de introdução à esquerda se analisa de forma análoga.

<sup>4</sup>A derivação omitida pelo duplo traço consiste na aplicação de transbordo de instanciação.



DEMONSTRAÇÃO: A demonstração será feita por indução na complexidade da fórmula  $C$ .

**Caso 1**

Se  $C$  for uma fórmula atômica apenas serão necessárias quatro  $\beta$ -conversões. Usando uma  $\beta$ -conversão universal<sup>6</sup> tem-se

$$\frac{\frac{\frac{\frac{\vdots}{A} \quad [A \rightarrow C]}{C} \quad (B \rightarrow C) \rightarrow C}{(A \rightarrow C) \rightarrow ((B \rightarrow C) \rightarrow C)} \quad \frac{\frac{[A]}{\vdots} \quad C}{A \rightarrow C} \quad \frac{[B]}{\vdots} \quad C}{B \rightarrow C}}{C}$$

com mais uma  $\beta$ -conversão tem-se

$$\frac{\frac{\frac{\frac{\vdots}{A} \quad \frac{[A]}{\vdots} \quad C}{A \rightarrow C} \quad C}{(B \rightarrow C) \rightarrow C} \quad \frac{[B]}{\vdots} \quad C}{B \rightarrow C}}{C}$$

com outra  $\beta$ -conversão tem-se

$$\frac{\frac{\frac{\vdots}{A} \quad \frac{[A]}{\vdots} \quad C}{A \rightarrow C} \quad C}{C}$$

e com mais uma  $\beta$ -conversão tem-se

$$\frac{\vdots}{A} \quad C$$

**Caso 2**

Se  $C: \equiv C_1 \rightarrow C_2$

Queremos provar que uma dedução da forma

---

<sup>6</sup>Com  $C$  fórmula atômica, o traço duplo na dedução corresponde à aplicação de uma simples regra de inferência ( $\forall\mathcal{E}$ )

$$\begin{array}{c}
 \vdots \\
 \frac{A \quad [A \rightarrow X]}{X} \\
 \frac{(B \rightarrow X) \rightarrow X}{(A \rightarrow X) \rightarrow ((B \rightarrow X) \rightarrow X)} \\
 \frac{\forall X[(A \rightarrow X) \rightarrow ((B \rightarrow X) \rightarrow X)]}{(A \rightarrow C_1 \rightarrow C_2) \rightarrow ((B \rightarrow C_1 \rightarrow C_2) \rightarrow C_1 \rightarrow C_2)} \\
 \frac{(A \rightarrow C_1 \rightarrow C_2) \rightarrow ((B \rightarrow C_1 \rightarrow C_2) \rightarrow C_1 \rightarrow C_2)}{(B \rightarrow (C_1 \rightarrow C_2)) \rightarrow (C_1 \rightarrow C_2)} \\
 \hline
 C_1 \rightarrow C_2
 \end{array}
 \quad
 \begin{array}{c}
 [A] \\
 \vdots \\
 C_1 \rightarrow C_2 \\
 \hline
 A \rightarrow (C_1 \rightarrow C_2)
 \end{array}
 \quad
 \begin{array}{c}
 [B] \\
 \vdots \\
 C_1 \rightarrow C_2 \\
 \hline
 B \rightarrow (C_1 \rightarrow C_2)
 \end{array}$$

se converte usando  $\beta\eta$ -conversões, em

$$\begin{array}{c}
 \vdots \\
 A \\
 \vdots \\
 C_1 \rightarrow C_2
 \end{array}$$

Vamos revelar parte da dedução escondida no traço duplo.

$$\begin{array}{c}
 \vdots \\
 \frac{A \quad [A \rightarrow X]}{X} \\
 \frac{(B \rightarrow X) \rightarrow X}{(A \rightarrow X) \rightarrow ((B \rightarrow X) \rightarrow X)} \\
 \frac{\forall X[(A \rightarrow X) \rightarrow ((B \rightarrow X) \rightarrow X)]}{(A \rightarrow C_2) \rightarrow ((B \rightarrow C_2) \rightarrow C_2)} \\
 \frac{(A \rightarrow C_2) \rightarrow ((B \rightarrow C_2) \rightarrow C_2)}{(B \rightarrow C_2) \rightarrow C_2} \\
 \hline
 \frac{C_2}{C_1 \rightarrow C_2} \\
 \frac{(B \rightarrow (C_1 \rightarrow C_2)) \rightarrow (C_1 \rightarrow C_2)}{(A \rightarrow (C_1 \rightarrow C_2)) \rightarrow ((B \rightarrow (C_1 \rightarrow C_2)) \rightarrow (C_1 \rightarrow C_2))}
 \end{array}
 \quad
 \begin{array}{c}
 [A \rightarrow (C_1 \rightarrow C_2)] \quad [A] \\
 \frac{C_1 \rightarrow C_2}{C_2} \quad [C_1] \\
 \hline
 A \rightarrow C_2
 \end{array}
 \quad
 \begin{array}{c}
 [B \rightarrow (C_1 \rightarrow C_2)] \quad [B] \\
 \frac{C_1 \rightarrow C_2}{C_2} \quad [C_1] \\
 \hline
 B \rightarrow C_2
 \end{array}$$

Note-se que por uma questão de espaço omite-se a parte final da demonstração abaixo da fórmula  $(A \rightarrow (C_1 \rightarrow C_2)) \rightarrow ((B \rightarrow (C_1 \rightarrow C_2)) \rightarrow (C_1 \rightarrow C_2))$ .

Como a prova é feita por indução na complexidade em  $C$ , por hipótese de indução (O lema é válido se  $C \equiv C_2$ ) esta dedução converte-se, usando  $\beta\eta$ -conversões, em

$$\begin{array}{c}
 \vdots \\
 \frac{A \quad [A \rightarrow (C_1 \rightarrow C_2)]}{C_1 \rightarrow C_2} \quad [C_1] \\
 \frac{C_2}{C_1 \rightarrow C_2} \\
 \frac{(B \rightarrow (C_1 \rightarrow C_2)) \rightarrow (C_1 \rightarrow C_2)}{(A \rightarrow (C_1 \rightarrow C_2)) \rightarrow ((B \rightarrow (C_1 \rightarrow C_2)) \rightarrow (C_1 \rightarrow C_2))}
 \end{array}$$

Completando a dedução segundo a derivação inicial tem-se

$$\frac{\frac{\frac{\vdots}{A} \quad [A \rightarrow (C_1 \rightarrow C_2)]}{C_1 \rightarrow C_2} \quad [C_1]}{\frac{C_2}{C_1 \rightarrow C_2}} \quad \frac{[A]}{\vdots} \quad \frac{[B]}{\vdots}$$

$$\frac{\frac{(A \rightarrow (C_1 \rightarrow C_2)) \rightarrow ((B \rightarrow (C_1 \rightarrow C_2)) \rightarrow (C_1 \rightarrow C_2))}{(B \rightarrow (C_1 \rightarrow C_2)) \rightarrow (C_1 \rightarrow C_2)} \quad \frac{C_1 \rightarrow C_2}{A \rightarrow (C_1 \rightarrow C_2)} \quad \frac{C_1 \rightarrow C_2}{B \rightarrow (C_1 \rightarrow C_2)}}{C_1 \rightarrow C_2}$$

aplicando uma  $\beta$ -conversão obtem-se

$$\frac{\frac{\frac{[A]}{\vdots} \quad C_1 \rightarrow C_2}{A \rightarrow (C_1 \rightarrow C_2)} \quad [C_1]}{C_1 \rightarrow C_2} \quad \frac{[B]}{\vdots}$$

$$\frac{\frac{C_2}{C_1 \rightarrow C_2} \quad \frac{C_1 \rightarrow C_2}{B \rightarrow (C_1 \rightarrow C_2)}}{(B \rightarrow (C_1 \rightarrow C_2)) \rightarrow (C_1 \rightarrow C_2)} \quad \frac{C_1 \rightarrow C_2}{B \rightarrow (C_1 \rightarrow C_2)}}{C_1 \rightarrow C_2}$$

com mais uma  $\beta$ -conversão obtem-se

$$\frac{\frac{[A]}{\vdots} \quad C_1 \rightarrow C_2}{A \rightarrow (C_1 \rightarrow C_2)} \quad [C_1]}{C_1 \rightarrow C_2} \quad \frac{C_2}{C_1 \rightarrow C_2}$$

com outra  $\beta$ -conversão obtem-se

$$\frac{\frac{\vdots}{A} \quad C_1 \rightarrow C_2 \quad [C_1]}{C_2} \quad \frac{C_2}{C_1 \rightarrow C_2}$$

finalmente com uma  $\eta$ -conversão a dedução converte-se em

$$\frac{\vdots}{A} \quad \frac{C_1 \rightarrow C_2}{C_1 \rightarrow C_2}$$

**Caso 3**

Se  $C: \equiv \forall Y.C_1$

Queremos provar que uma dedução da forma

$$\begin{array}{c}
 \vdots \\
 \frac{A \quad [A \rightarrow X]}{X} \\
 \frac{(B \rightarrow X) \rightarrow X}{(A \rightarrow X) \rightarrow ((B \rightarrow X) \rightarrow X)} \\
 \frac{\forall X[(A \rightarrow X) \rightarrow ((B \rightarrow X) \rightarrow X)]}{(A \rightarrow \forall Y.C_1) \rightarrow ((B \rightarrow \forall Y.C_1) \rightarrow \forall Y.C_1)} \\
 \frac{(A \rightarrow \forall Y.C_1) \rightarrow ((B \rightarrow \forall Y.C_1) \rightarrow \forall Y.C_1)}{(B \rightarrow \forall Y.C_1) \rightarrow \forall Y.C_1} \\
 \forall Y.C_1
 \end{array}
 \quad
 \begin{array}{c}
 [A] \\
 \vdots \\
 \frac{[A]}{\forall Y.C_1} \\
 A \rightarrow \forall Y.C_1
 \end{array}
 \quad
 \begin{array}{c}
 [B] \\
 \vdots \\
 \frac{[B]}{\forall Y.C_1} \\
 B \rightarrow \forall Y.C_1
 \end{array}$$

se converte usando  $\beta\eta$ -conversões, em

$$\begin{array}{c}
 \vdots \\
 A \\
 \vdots \\
 \forall Y.C_1
 \end{array}$$

Vamos revelar parte da dedução escondida no traço duplo

$$\begin{array}{c}
 \vdots \\
 \frac{A \quad [A \rightarrow X]}{X} \\
 \frac{(B \rightarrow X) \rightarrow X}{(A \rightarrow X) \rightarrow ((B \rightarrow X) \rightarrow X)} \\
 \frac{\forall X(A \rightarrow X) \rightarrow ((B \rightarrow X) \rightarrow X)}{(A \rightarrow C_1) \rightarrow ((B \rightarrow C_1) \rightarrow C_1)} \\
 \frac{(A \rightarrow C_1) \rightarrow ((B \rightarrow C_1) \rightarrow C_1)}{(B \rightarrow C_1) \rightarrow C_1} \\
 \frac{C_1}{\forall Y.C_1} \\
 \frac{(B \rightarrow \forall Y.C_1) \rightarrow \forall Y.C_1}{(A \rightarrow \forall Y.C_1) \rightarrow ((B \rightarrow \forall Y.C_1) \rightarrow \forall Y.C_1)}
 \end{array}
 \quad
 \begin{array}{c}
 [A \rightarrow \forall Y.C_1] \quad [A] \\
 \frac{\forall Y.C_1}{C_1} \\
 \frac{C_1}{A \rightarrow C_1} \\
 \frac{C_1}{\forall Y.C_1} \\
 \frac{[B \rightarrow \forall Y.C_1] \quad [B]}{B \rightarrow C_1}
 \end{array}$$

Por uma questão de espaço omite-se a parte final da demonstração abaixo da fórmula  $(A \rightarrow \forall Y.C_1) \rightarrow ((B \rightarrow \forall Y.C_1) \rightarrow \forall Y.C_1)$ .

Por hipótese de indução (O lema é válido se  $C: \equiv C_1$ ) esta dedução converte-se, usando  $\beta\eta$ -conversões, em

$$\begin{array}{c}
 \vdots \\
 \frac{A \quad [A \rightarrow \forall Y.C_1]}{\forall Y.C_1} \\
 \frac{\forall Y.C_1}{C_1} \\
 \frac{C_1}{\forall Y.C_1} \\
 \frac{(B \rightarrow \forall Y.C_1) \rightarrow \forall Y.C_1}{(A \rightarrow \forall Y.C_1) \rightarrow ((B \rightarrow \forall Y.C_1) \rightarrow \forall Y.C_1)}
 \end{array}$$

Voltando à dedução completa tem-se

$$\frac{\frac{\frac{\frac{\vdots}{A} \quad [A \rightarrow \forall Y.C_1]}{\forall Y.C_1} \quad C_1}{\forall Y.C_1} \quad (B \rightarrow \forall Y.C_1) \rightarrow \forall Y.C_1}{(A \rightarrow \forall Y.C_1) \rightarrow ((B \rightarrow \forall Y.C_1) \rightarrow \forall Y.C_1)} \quad \frac{[A]}{\vdots} \quad \frac{[B]}{\vdots}}{\frac{(B \rightarrow \forall Y.C_1) \rightarrow \forall Y.C_1}{\forall Y.C_1} \quad \frac{A \rightarrow \forall Y.C_1}{B \rightarrow \forall Y.C_1}}$$

Usando uma  $\beta$ -conversão implicacionais obtem-se

$$\frac{\frac{\frac{\frac{\vdots}{A} \quad \frac{[A]}{\vdots} \quad \forall Y.C_1}{A \rightarrow \forall Y.C_1}}{\forall Y.C_1} \quad C_1}{\forall Y.C_1} \quad (B \rightarrow \forall Y.C_1) \rightarrow \forall Y.C_1 \quad \frac{[B]}{\vdots} \quad \forall Y.C_1}{B \rightarrow \forall Y.C_1} \quad \forall Y.C_1$$

com outra  $\beta$ -conversão implicacionais obtem-se

$$\frac{\frac{\frac{\frac{[A]}{\vdots} \quad \forall Y.C_1}{A \rightarrow \forall Y.C_1}}{\forall Y.C_1} \quad C_1}{\forall Y.C_1}}$$

e com mais uma  $\beta$ -conversão implicacional obtem-se

$$\frac{\frac{\frac{\vdots}{A} \quad \forall Y.C_1}{\forall Y.C_1} \quad C_1}{\forall Y.C_1}}$$

finalmente com uma  $\eta$ -conversão universal a dedução converte-se em

$$\frac{\frac{\vdots}{A} \quad \forall Y.C_1}{\forall Y.C_1}}$$

O que conclui a demonstração do lema. □

Estamos agora em condições de provar a proposição 5.0.20 uma vez que a tradução canónica do redex da  $\beta$ -conversão para a disjunção tem a forma

$$\frac{\frac{\frac{\frac{\vdots}{A^*} \quad [A^* \rightarrow X]}{X}}{(B^* \rightarrow X) \rightarrow X}}{(A^* \rightarrow X) \rightarrow ((B^* \rightarrow X) \rightarrow X)}}{\forall X[(A^* \rightarrow X) \rightarrow ((B^* \rightarrow X) \rightarrow X)]} \quad \frac{[A^*]}{\vdots} \quad \frac{[B^*]}{\vdots} \quad \frac{C^*}{A^* \rightarrow C^*} \quad \frac{C^*}{B^* \rightarrow C^*}}{(B^* \rightarrow C^*) \rightarrow C^*} \quad C^*$$

e a tradução canónica da contractum tem a forma

$$\frac{\vdots}{A^*} \quad \vdots \quad \frac{\vdots}{C^*}$$

e como caso particular do lema a segunda derivação resulta da primeira usando  $\beta\eta$ -conversões em  $\mathbf{F}_{\text{at}}$ .

Passamos agora ao caso da conjunção.

**PROPOSIÇÃO 5.0.22** *A tradução canónica de*

$$\frac{\frac{\frac{\vdots}{A} \quad \frac{\vdots}{B}}{A \wedge B}}{A}$$

*converte-se, usando  $\beta\eta$ -conversões, na tradução canónica de*

$$\frac{\vdots}{A}$$

Começemos por provar o seguinte lema.

**LEMA 5.0.23** *Uma dedução em  $\mathbf{F}_{\text{at}}$  da forma*

$$\frac{\frac{\frac{\frac{\frac{\vdots}{A} \quad [A \rightarrow (B \rightarrow X)]}{B \rightarrow X}}{X}}{(A \rightarrow (B \rightarrow X)) \rightarrow X}}{\forall X((A \rightarrow (B \rightarrow X)) \rightarrow X)}}{\frac{(A \rightarrow (B \rightarrow C)) \rightarrow C}{C}} \quad \frac{[A]}{\vdots} \quad \frac{C}{B \rightarrow C} \quad \frac{C}{A \rightarrow (B \rightarrow C)}}$$

converte-se, usando  $\beta\eta$ -conversões, em

$$\begin{array}{c} \vdots \\ A \\ \vdots \\ C \end{array}$$

DEMONSTRAÇÃO: A demonstração será feita por indução na complexidade da fórmula  $C$ .

**Caso 1**

Se  $C$  for uma fórmula atômica, aplicando uma  $\beta$ -conversão universal obtem-se

$$\frac{\frac{\frac{\begin{array}{c} \vdots \\ A \end{array} \quad [A \rightarrow (B \rightarrow C)] \quad \begin{array}{c} \vdots \\ B \end{array}}{B \rightarrow C} \quad C}{(A \rightarrow (B \rightarrow C)) \rightarrow C} \quad \frac{\frac{[A] \quad \begin{array}{c} \vdots \\ C \end{array}}{B \rightarrow C}}{A \rightarrow (B \rightarrow C)}}{C}$$

com uma  $\beta$ -conversão obtem-se

$$\frac{\frac{\begin{array}{c} \vdots \\ A \end{array} \quad \frac{\frac{[A] \quad \begin{array}{c} \vdots \\ C \end{array}}{B \rightarrow C}}{A \rightarrow (B \rightarrow C)} \quad \begin{array}{c} \vdots \\ B \end{array}}{B \rightarrow C} \quad C}{C}$$

com outra  $\beta$ -conversão obtem-se

$$\frac{\frac{\begin{array}{c} \vdots \\ A \end{array} \quad \begin{array}{c} \vdots \\ C \end{array}}{B \rightarrow C} \quad \begin{array}{c} \vdots \\ B \end{array}}{C}$$

finalmente com uma quarta  $\beta$ -conversão obtem-se o pretendido

$$\begin{array}{c} \vdots \\ A \\ \vdots \\ C \end{array}$$

**Caso 2**

Se  $C \equiv C_1 \rightarrow C_2$

Queremos provar que a dedução

$$\frac{\frac{\frac{\frac{\vdots}{A} \quad [A \rightarrow (B \rightarrow X)] \quad \vdots}{B \rightarrow X} \quad B}{X} \quad (A \rightarrow (B \rightarrow X)) \rightarrow X}{\forall X((A \rightarrow (B \rightarrow X)) \rightarrow X)} \quad \frac{[A] \quad \vdots \quad C_1 \rightarrow C_2}{B \rightarrow (C_1 \rightarrow C_2)}}{\frac{(A \rightarrow (B \rightarrow (C_1 \rightarrow C_2))) \rightarrow (C_1 \rightarrow C_2)}{C_1 \rightarrow C_2} \quad A \rightarrow (B \rightarrow (C_1 \rightarrow C_2))}$$

se converte, usando  $\beta\eta$ -conversões em

$$\frac{\vdots}{A} \quad \vdots \quad C_1 \rightarrow C_2$$

Vamos agora revelar parte da dedução escondida no traço duplo.

$$\frac{\frac{\frac{\frac{\vdots}{A} \quad [A \rightarrow (B \rightarrow X)] \quad \vdots}{B \rightarrow X} \quad B}{X} \quad (A \rightarrow (B \rightarrow X)) \rightarrow X}{\forall X((A \rightarrow (B \rightarrow X)) \rightarrow X)} \quad \frac{\frac{[A \rightarrow (B \rightarrow (C_1 \rightarrow C_2))] \quad [A]}{B \rightarrow (C_1 \rightarrow C_2)} \quad [B]}{C_1 \rightarrow C_2} \quad [C_1]}{\frac{C_2}{C_1 \rightarrow C_2} \quad \frac{C_2}{B \rightarrow C_2}} \quad \frac{[A] \quad \vdots \quad C_1 \rightarrow C_2}{B \rightarrow (C_1 \rightarrow C_2)}}{\frac{(A \rightarrow (B \rightarrow (C_1 \rightarrow C_2))) \rightarrow (C_1 \rightarrow C_2)}{C_1 \rightarrow C_2} \quad A \rightarrow (B \rightarrow (C_1 \rightarrow C_2))}$$

Por hipótese de indução (o lema é válido para  $C \equiv C_2$ ) temos que a dedução anterior se converte, usando  $\beta\eta$ -conversões em

$$\frac{\frac{\frac{\vdots}{A} \quad [A \rightarrow (B \rightarrow (C_1 \rightarrow C_2))] \quad \vdots}{B \rightarrow (C_1 \rightarrow C_2)} \quad B}{C_1 \rightarrow C_2} \quad [C_1] \quad \frac{[A] \quad \vdots \quad C_1 \rightarrow C_2}{B \rightarrow (C_1 \rightarrow C_2)}}{\frac{C_2}{C_1 \rightarrow C_2} \quad \frac{C_2}{B \rightarrow C_2}} \quad \frac{(A \rightarrow (B \rightarrow (C_1 \rightarrow C_2))) \rightarrow (C_1 \rightarrow C_2)}{C_1 \rightarrow C_2} \quad A \rightarrow (B \rightarrow (C_1 \rightarrow C_2))}$$

Usando uma  $\beta$ -conversão obtem-se

$$\frac{\begin{array}{c} [A] \\ \vdots \\ C_1 \rightarrow C_2 \\ \hline B \rightarrow (C_1 \rightarrow C_2) \\ \hline A \rightarrow (B \rightarrow (C_1 \rightarrow C_2)) \\ \hline A \end{array} \quad \begin{array}{c} \vdots \\ B \end{array}}{\frac{B \rightarrow (C_1 \rightarrow C_2)}{C_1 \rightarrow C_2} \quad [C_1]} \quad \frac{C_2}{C_1 \rightarrow C_2}$$

Com outra  $\beta$ -conversão obtem-se

$$\frac{\begin{array}{c} \vdots \\ A \\ \vdots \\ C_1 \rightarrow C_2 \\ \hline B \rightarrow (C_1 \rightarrow C_2) \\ \hline C_1 \rightarrow C_2 \end{array} \quad \begin{array}{c} \vdots \\ B \\ [C_1] \end{array}}{\frac{C_2}{C_1 \rightarrow C_2}}$$

aplicando uma terceira  $\beta$ -conversão obtem-se

$$\frac{\begin{array}{c} \vdots \\ A \\ \vdots \\ C_1 \rightarrow C_2 \end{array} \quad [C_1]}{\frac{C_2}{C_1 \rightarrow C_2}}$$

finalmente, aplicando uma  $\eta$ -conversão obtem-se

$$\begin{array}{c} \vdots \\ A \\ \vdots \\ C_1 \rightarrow C_2 \end{array}$$



usando agora uma  $\beta$ -conversão obtem-se

$$\frac{\frac{\frac{[A]}{\vdots} \quad \frac{\frac{B \rightarrow \forall Y.C_1}{A \rightarrow (B \rightarrow \forall Y.C_1)}}{\vdots} \quad A}{\vdots} \quad B}{\frac{B \rightarrow \forall Y.C_1}{\forall Y.C_1}} \quad \frac{C_1}{\forall Y.C_1}}$$

com outra  $\beta$ -conversão tem-se

$$\frac{\frac{\frac{A}{\vdots} \quad \frac{\frac{B \rightarrow \forall Y.C_1}{\vdots} \quad B}{\forall Y.C_1}}{\frac{C_1}{\forall Y.C_1}}}{\forall Y.C_1}}$$

aplica-se uma última  $\beta$ -conversão para chegar a

$$\frac{\frac{A}{\vdots} \quad \frac{\frac{C_1}{\forall Y.C_1}}{\forall Y.C_1}}{\forall Y.C_1}}$$

finalmente com uma  $\eta$ -conversão obtemos a dedução pretendida

$$\frac{A}{\vdots} \quad \forall Y.C_1$$

ficando assim concluída a demonstração do lema.  $\square$

Como caso particular do lema anterior, tomando  $C \equiv A$  temos que uma dedução da forma

$$\frac{\frac{\frac{A}{\vdots} \quad \frac{[A \rightarrow (B \rightarrow X)]}{\vdots} \quad B}{\frac{B \rightarrow X}{X}} \quad \frac{[A]}{B \rightarrow A}}{\frac{(A \rightarrow (B \rightarrow X)) \rightarrow X}{\forall X((A \rightarrow (B \rightarrow X)) \rightarrow X)}} \quad \frac{[A]}{B \rightarrow A}}{\frac{(A \rightarrow (B \rightarrow A)) \rightarrow A}{A}} \quad A \rightarrow (B \rightarrow A)$$

converte-se, usando  $\beta\eta$ -conversões em

$$\begin{array}{c} \vdots \\ A \end{array}$$

Estamos agora em condições de provar a proposição 5.0.22 uma vez que a tradução canónica do redex da  $\beta$ -conversão para a conjunção tem a forma

$$\frac{\frac{\frac{\frac{\frac{\vdots}{A^*} \quad [A^* \rightarrow (B^* \rightarrow X)]}{B^* \rightarrow X} \quad \frac{\vdots}{B^*}}{X}}{(A^* \rightarrow (B^* \rightarrow X)) \rightarrow X}}{\forall X((A^* \rightarrow (B^* \rightarrow X)) \rightarrow X)} \quad \frac{[A^*]}{B^* \rightarrow A^*}}{\frac{(A^* \rightarrow (B^* \rightarrow A^*)) \rightarrow A^*}{A^*}} \quad \frac{}{A^* \rightarrow (B^* \rightarrow A^*)}$$

e a tradução canónica do contractum tem a forma

$$\begin{array}{c} \vdots \\ A^* \end{array}$$

e como caso particular do resultado anterior a segunda derivação resulta da primeira usando  $\beta\eta$ -conversões em  $\mathbf{F}_{\text{at}}$ .

# Capítulo 6

## Normalização Forte para o Cálculo Prop. Intuicionista

Como já foi referido, uma ferramenta basilar em Teoria da Demonstração é a normalização de provas (ou eliminação do corte no contexto do cálculo de sequentes). O teorema que se segue permite garantir, de uma forma simples, usando resultados dos dois anteriores Capítulos, que qualquer prova do cálculo proposicional intuicionista é fortemente normalizável considerando  $\beta$ -conversões.

**TEOREMA 6.0.24** *O cálculo proposicional intuicionista, considerando os conetivos  $\vee$ ,  $\wedge$ ,  $\rightarrow$ ,  $\perp$  e  $\beta$ -conversões é fortemente normalizável.*

**DEMONSTRAÇÃO:** Do estudo feito no capítulo 5 e tendo em conta as proposições 5.0.20 e 5.0.22 sabe-se que cada  $\beta$ -conversão do cálculo proposicional intuicionista se traduz em pelo menos uma (número finito)  $\beta\eta$ -conversão no sistema  $\mathbf{F}_{\text{at}}$ . Sendo este sistema fortemente normalizável, capítulo 4, no que respeita a  $\beta\eta$ -conversões fica provado o pretendido.  $\square$

Apresenta-se de seguida um resultado que permite estabelecer um limite máximo para o número de  $\beta$ -conversões e de  $\eta$ -conversões que resultam da tradução das  $\beta$ -conversões do cálculo proposicional intuicionista em  $\mathbf{F}_{\text{at}}$ .

**DEFINIÇÃO 6.0.25** *Seja  $C$  uma fórmula em  $\mathbf{F}_{\text{at}}$ .  $\tau(C)$  define-se por indução na complexidade da fórmula  $C$  da seguinte forma:*

- i) Se  $C$  é atómica,  $\tau(C) := (1, 0, 0)$*
- ii) Se  $C := A \rightarrow B$ ,  $\tau(C) := \tau(B) + (0, 1, 0)$*
- iii) Se  $C := \forall X.A$ ,  $\tau(C) := \tau(A) + (0, 0, 1)$ .*

**DEFINIÇÃO 6.0.26** *Seja  $C$  uma fórmula do cálculo proposicional intuicionista, conclusão de um redex de uma  $\beta$ -conversão e  $C^*$  a sua tradução em  $\mathbf{F}_{\text{at}}$ . Sabemos que a  $\beta$ -conversão do cálculo proposicional intuicionista se traduz em  $\beta\eta$ -conversões em  $\mathbf{F}_{\text{at}}$ . Denotamos por  $\#_{\beta}(C^*)$  (respectivamente  $\#_{\eta}(C^*)$ ) o número máximo de  $\beta$ -conversões (respectivamente de  $\eta$ -conversões) que ocorrem em  $\mathbf{F}_{\text{at}}$  como resultado da tradução da  $\beta$ -conversão.*

**PROPOSIÇÃO 6.0.27**  $\#_{\beta}(C^*) = \tau(C^*)|(4, 3, 3)$  e  $\#_{\eta}(C^*) = \tau(C^*)|(0, 1, 1)$

DEMONSTRAÇÃO:

As coordenadas do vetor  $(4, 3, 3)$  correspondem ao número de  $\beta$ -conversões que foram aplicadas nas demonstrações dos lemas 5.0.21 e 5.0.23, nos Casos 1, 2 e 3, respetivamente. As coordenadas do vetor  $(0, 1, 1)$  correspondem ao número de  $\eta$ -conversões que foram aplicadas nas mesmas demonstrações nos três respectivos casos.

$\tau(A)$ , com  $A$  fórmula em  $\mathbf{F}_{\text{at}}$ , é um vetor  $(n_1, n_2, n_3)$  em que  $n_1, n_2$  e  $n_3$  correspondem ao número de fórmulas atómicas, implicações e quantificações universais respetivamente que ocorrem na fórmula  $A$  e são relevantes para o transbordo de instanciação e consequentemente para contagem das  $\beta\eta$ -conversões em  $\mathbf{F}_{\text{at}}$ .

Assim,

$\#_{\beta}(C^*)$ , o produto interno de  $\tau(C^*)$  com  $(4, 3, 3)$ , contabiliza o número máximo de  $\beta$ -conversões que ocorrem em  $\mathbf{F}_{\text{at}}$  como resultado da tradução da  $\beta$ -conversão.

Da mesma forma,

$\#_{\eta}(C^*)$ , o produto interno de  $\tau(C^*)$  com  $(0, 1, 1)$ , contabiliza o número máximo de  $\eta$ -conversões que ocorrem em  $\mathbf{F}_{\text{at}}$  como resultado da tradução da  $\beta$ -conversão.

□

# Bibliografia

- [1] Abreu A. F. E., *Fundamentos Matemáticos da Programação Funcional*, tese de mestrado, Univ. Aveiro, 2009.
- [2] Barker-Plummer D, Barwise J. and Etchemendy J., *Language, Proof and Logic*, University of Chicago Press, 2011.
- [3] Barreto F. M. N., *Análise estruturada e formal das Provas*, tese de mestrado, Univ. Aveiro, 2009.
- [4] Bianconi R., *Lógicas Construtivas: Intuicionismo, uma introdução*, disponível em <http://www.ime.usp.br/~bianconi/recursos/in.pdf>.
- [5] Buss S. R., *Handbook of Proof Theory*, Studies in Logic, Elsevier B.V., vol. 137, 1998.
- [6] Costa D. Gomes, *Sistemas de Lógica Modal em Dedução Natural*, tese de mestrado, Univ. Federal do Rio Grande do Norte, 2010.
- [7] Ferreira F. and Ferreira G., *Atomic Polymorphism*, Journal of Symbolic Logic, vol. 78, nº1, pp.260-274, 2013.
- [8] Ferreira F. and Ferreira G., *Commuting Conversions vs. the standard Conversions of the “Good” Connectives*, Studia Logica, vol.92, pp 63-84, 2009.
- [9] Ferreira F., *Comments on Predicative Logic*, Journal of Philosophical Logic, vol. 35, pp 1-8, 2006.
- [10] Gentzen G., *The collected papers of Gerhard Gentzen*, Szabo ed., 1969.
- [11] Girard J-Y., Lafond Y. and Taylor P., *Proofs and Types*, Cambridge University Press, 1989.
- [12] Girard J-Y., *Une extension de l’interpretation de Gödel à l’analyse, et son application à l’élimination des coupures dans l’analyse et la théorie des types*, Studies in Logic and the Foundations of Mathematics North-Holland, pp. 63-92, 1971.
- [13] Meré M.C., *Lógicas Relevantes: Formalismo e Semântica*, tese de doutoramento, Univ. Católica do Rio Grande, 1993.
- [14] Prawitz D., *Ideas and results in Proof Theory*, Proceedings of the second scandinavian logic symposium, J. E. Fenstad ed., pp. 235-307, 1971.
- [15] Prawitz D., *Natural Deduction*, Dover Publications, 1965.
- [16] Reynolds J. C., *Towards a Theory of Type Structure*, Colloque sur la programmation, LNCS 19, B. Robinet Ed., Sringer-Verlag, 1974.

- [17] Sorensen M. H. and Urzyczin P., *Lectures on the Curry-Howard Isomorphism*, Studies in Logic, vol. 149, 2006.
- [18] Stalmarck G., *Normalization Theorems for full First Order Classical Natural Deduction*, The Journal of Symbolic Logic, vol. 56, Num 1, 1991.
- [19] Troelstra A.S., Schwichtenberg H., *Basic Proof Theory*, Cambridge University Press, 1996.
- [20] Van Dalen D., *Logic and Structure*, Springer, 1994.