Referências Bibliográficas

[Bus87] Samuel R. Buss. Polynomial size proofs of the propositional pigeonhole principle. *Journal of Symbolic Logic*, 52(4):916–927, December 1987. 2.5, 2.5.1, A.4

[Coo76] S.A. Cook. A short proof of the pigeon hole principle using extended resolution. *ACM SIGACT News*, 8(4):28–32, 1976. 3.3.7, 4.4, 4.4.1

[CR79] S. A. Cook and R. A. Reckhow. The relative efficiency of propositional proof systems. *Journal of Symbolic Logic*, 44(1):36–50, March 1979. 1, 2.2, 2.5, A.2, A.4

[dPN01] Maria da Paz Nunes. *Traduções via teoria da prova: aplicações à lógica linear*. PhD thesis, Pontifícia Universidade Católica do Rio de Janeiro, 2001. D

[Fin05] Marcelo Finger. Dag sequents with substitution. In Sergei N. Artëmov, Howard Barringer, Artur S. d'Avila Garcez, Luís C. Lamb, and John Woods, editors, *We Will Show Them! (1)*, pages 671–686. College Publications, 2005. 3.3.7

[Hae90] Edward Hermann Haeusler. *Prova Automática de Teoremas em Dedução Natural: Uma abordagem Abastrata*. PhD thesis, Pontifícia Universidade Católica do Rio de Janeiro, 1990. 3.3

[Hak85] A. Haken. The intractability of resolution. *Theoretical Computer Science*, 39:297–308, 1985. 2.5

[Kra95] Jan Krajíček. *Bounded arithmetic, propositional logic, and complexity theory*, volume 60 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, 1995. 2.6

[Ofmry] Yu. Ofman. On the algorithmic complexity of discrete functions. *Sov. Phys., Dokl.*, 7(7):589–591, 1963, January. 2.5.1

[Pap94] C. H. Papadimitriou. *Computational Complexity*. Addison-Wesley, 1994. 2.2, 2.2

[Pra65] Dag Prawitz. *Natural Deduction, A Proof-Theoretical Study*. Almqvist & Wiksell, 1965. 2

[Sch50] Kurt Schütte. Schluβweissen-Kalküle der Praädikatenlogik. *Mathematische Annalen*, 122:47–65, 1950. 3.3

[TS00] A. S. Troelstra and H. Schwichtenberg. *Basic Proof Theory*. Cambridge University Press, Cambridge, England, 2 edition, 2000. 1

[vD97] Dirk van Dalen. *Logic and Structure*. Springer-Verlag, Berlin, Germany, 2 edition, 1997. 2.1.1

[Wal64] Wallace. A suggestion for a fast multiplier. *IEEETC: IEEE Transactions on Computers*, 13, 1964. 2.5.1

A
Sistemas de Frege

Apresentaremos nesta seção os sistemas de Frege. Mostraremos também que o sistema de dedução natural é um sistema de Frege.

Começaremos, assim, com a apresentação de notações e terminologias para sistemas de provas proposicionais.

A.1
Sistemas de provas proposicionais

Considere κ um conjunto de conectivos proposicionais adequado, binários, unários e zeroários. Adequado significa que toda função verdade pode ser expressa por fórmulas construídas da maneira usual a partir de variáveis proposicionais e conectivos de κ, usando notação infixa.

Se $A_1, \ldots, A_n, B$ são fórmulas, então escrevemos $A_1, \ldots, A_n \models B$ se B é conseqüência lógica de $A_1, \ldots, A_n$ (i. e. toda atribuição de verdade satisfazendo $A_1, \ldots, A_n$ satisfaz B). Cada um dos sistemas de prova proposicional será definido sob algum conjunto de conectivos κ, e será capaz de provar todas as tautologias sobre κ por meio de provas que utilizam as fórmulas construídas usando κ.

Uma *derivação* em tal sistema é uma seqüência finita de *linhas*, terminando na linha provada.

Uma *linha* é sempre uma fórmula, exceto no caso de sistemas de dedução natural (seção A.3). Cada linha deve ser uma hipótese ou *seguir* da linha anterior por meio de regras de inferência.

Se a derivação não tiver hipóteses, ele é dita uma *prova*.

Portanto, para especificar um sistema de prova proposicional, são necessários apenas a especificação κ, a definição de *linha* e a existência de um conjunto finito de *regras de inferência*.

Para que esta noção de sistema de prova se encaixe com a definição (2.13), primeiro devemos notar que as fórmulas podem ser consideradas como strings sobre um alfabeto finito.

O único problema é que uma variável proposicional também deve ser considerada como uma string de forma que exista um suprimento ilimitado de variáveis proposicionais.

Então uma prova π no sistema proposicional que é uma seqüência de fórmulas, pode ser naturalmente considerada como uma string sobre um alfabeto finito que inclui a vírgula como um símbolo separador bem como os símbolos necessários para especificação das fórmulas.

A função f que abstratamente específica o sistema será dada por $f(\pi) = A$ se π provar A, e $f(\pi) = A_0$ para alguma tautologia fixa A_0 se π não é uma string que corresponda a uma prova no sistema.

A notação $A_1 \ldots, A_n \vdash^{\pi}_{\mathscr{S}} B$ significa que π é uma derivação de B a partir das hipóteses $A_1, \ldots, A_n$ no sistema de provas $\mathscr{S}$.

Notação A.1 *Se $L = (A_1, \ldots, A_k) \rightarrow A$ é uma linha, então o comprimento, l, de L, é dado por $l(L) = l(A_1) + \ldots + l(A_k) + l(A)$. Se π é uma derivação, então $\lambda(\pi)$ é o número de linhas em π, e $\rho(\pi)$ é o máximo de $l(L)$, para toda L em π.*

A.2 Sistemas de Frege

Temos, agora, condições de realizar a apresentação da definição de sistema de Frege.

Muitos resultados desta seção serão apresentados sem suas respectivas demonstrações.

Maiores detalhes podem ser encontrados em, por exemplo, (CR79).

Definição A.2 *Se $D_1, \ldots, D_k$ são fórmulas e $P_1, \ldots, P_k$ são variáveis proposicionais distintas, então $\sigma = (D_1, \ldots, D_k)/(P_1, \ldots, P_k)$ é uma* substituição*, e σA é a fórmula resultante da substituição de P_i por D_i, $i = 1, ..., k$, na fórmula A.*

Uma regra de Frege *é um sistema de fórmulas $(C_1, \ldots, C_k)/D$, onde $C_1, \ldots, C_k \models D$. Se $n = 0$, a regra é um* esquema de axioma*. Para qualquer substituição σ dizemos que σD segue de $\sigma C_1, \ldots, \sigma C_n$ pela regra $(C_1, \ldots, C_n)/D$.*

Um sistema de inferência *$\mathcal{F}$ é um conjunto finito de regras de Frege.*

Fica evidenciado pela definição de regra de Frege que se $A_1, \ldots, A_n \vdash_{\mathcal{F}} B$ então $A_1, \ldots, A_n \models_{\mathcal{F}} B$. Ou seja, um sistema de Frege é um sistema de inferência implicacionalmente completo.

Observação A.3 *O sistema de Frege original não encaixa na definição acima, porque ele possui axiomas em vez de esquemas de axiomas, e explicitamente inclui a regra de substituição. Se modificamos a definição original de Frege para a atual, o resultado terá conectivos $\kappa = \{\neg, \rightarrow\}$, a regra de inferência*

$$\frac{A, A \rightarrow B}{B}$$

e os seis esquemas de axiomas

$A \to (B \to A)$,

$(C \to (B \to A)) \to ((C \to B) \to (C \to A))$,

$(D \to (B \to A)) \to (B \to (D \to A))$,

$(B \to A) \to (\neg A \to \neg B)$,

$\neg\neg A \to A$,

$A \to \neg\neg A$.

Teorema A.4 *Para quaisquer dois sistemas de Frege $\mathcal{F}_1$ e $\mathcal{F}_2$ sob κ existe uma função f em $\mathcal{L}$ e constante c tal que para todas fórmulas $A_1, \ldots, A_n, B$ e derivações π, se $A_1, \ldots, A_n \vdash^{\pi}_{\mathcal{F}_1} B$ então $A_1, \ldots, A_n \vdash^{f(\pi)}_{\mathcal{F}_2} B$, e $\lambda(f(\pi)) \leq c\lambda(\pi)$ e $\rho(f(\pi)) \leq c\rho(\pi)$*

Como conseqüência imediata do teorema acima e do teorema (2.18) podemos dizer que:

Corolário A.5 *Quaisquer dois sistemas de Frege sob κ p-simulam um ao outro. Assim um sistema de Frege sob κ é polinomialmente limitado se e somente se todos sistemas de Frege sob κ forem.*

A.3 Dedução Natural

Para o sistema proposicional de Prawitz se adequar à definição de sistema de Frege, é imprescindível que a noção de prova de Prawitz seja mais um grafo acíclico direto do que uma árvore. Isto é, uma vez que uma fórmula é derivada de um conjunto de hipóteses, não será necessário derivá-la novamente se ela for utilizada uma outra vez.

Desta forma, apresentamos as provas em sistema de dedução natural como seqüências de linhas, e cada linha terá a forma $A_1, \ldots, A_n \to A$, onde $A_1, \ldots, A_n$ são hipóteses que implicam A.

Definição A.6 *Um* linha de dedução natural *é um par $\Gamma \to A$, onde Γ é uma seqüência finita de fórmulas, e A é uma fórmula. Se Γ é vazio, escrevemos simplesmente $\to A$.*

Se Δ é uma seqüência $B_1, .., B_n$ de fórmulas e L é a linha $(A_1, \ldots, A_n) \to A$, então ΔL é a linha $(B_1, \ldots, B_2, A_1, \ldots, A_n) \to A$.

Se Λ é um conjunto de linhas, Δ é uma seqüência de fórmulas e σ é uma substituição, então $\Lambda \models L$ implica que $\Delta\sigma(\Lambda) \models \Delta\sigma(L)$, onde as operações Δ e σ são estendidas para conjuntos de linhas de forma natural.

Se Λ é um conjunto finito de linhas e L é uma linha tal que $\Lambda \models L$, então o sistema $R = \Lambda/L$ é uma regra de dedução natural.

A linha L' segue *de Λ' pela regra R se para alguma substituição σ e seqüência Δ, $\Lambda' = \Delta\sigma(\Lambda)$, e $L' = \Delta\sigma(L)$.*

Um sistema de dedução natural *é uma conjunto finito de regras de dedução natural que é completo implicacionalmente*.

Notação A.7 *Dada um linha $L = (A_1, \ldots, A_m) \rightarrow A$ associamos L a fórmula $L^* = \bigvee(\neg A_1, \ldots, \neg A_m, A)$. Se P é uma variável proposicional qualquer então $(PM)^*$ denota $\bigvee(P, \neg A_1, \ldots, \neg A_m, A)$.*

Toda derivação em $\mathcal{F}$, digamos B de $A_1, \ldots, A_n$ pode ser transformada em uma derivação B de $A_1, \ldots, A_n$ em um sistema de dedução natural $nd(\mathcal{F})$ simplesmente adicionando o símbolo $\rightarrow$ à esquerda de todas as fórmulas na derivação.

Inversamente, todo sistema de dedução natural $\mathcal{N}$pode ser transformado em um sistema de Frege $fr(\mathcal{N})$, onde as regras de $fr(\mathcal{N})$ consistem de duas regras $R' = \Lambda^*/L^*$ e $R'' = (P\Lambda)^*/(PL)^*$ para cada regra $R = \Lambda/L$ de $\mathcal{N}$.

Agora se $\pi = L_1, \ldots, L_n$ é qualquer derivação em $\mathcal{N}$, então afirmamos que $\pi^* = L_1^*, \ldots, L_n^*$ é uma derivação em $fr(\mathcal{N})$. Se L_i segue do $L_j's$ anterior por uma regra $R = \Lambda/L$ em $\mathcal{N}$. Então para alguma substituição σ e seqüência Δ. L_1^* segue do L_j^* pela regra Frege $R' = \Lambda^*/L^*$ por σ, desde que, para qualquer linha M, $(\sigma(M))^* = \sigma(M^*)$. Se Δ não é vazio, então L_i^* segue do L_j^* pela regra $R'' = (P\Lambda)^*/(PL)^*$ e substituição σ', onde σ' é a substituição obtida por aplicações simultâneas da substituição σ e $\bigvee(\neg A_1, \ldots, \neg A_k)/P$, onde Δ é $A_1, \ldots, A_k$. Precisamos do fato que para qualquer linha M sem ocorrências de P, $\sigma'((PM)^*) = (\Delta\sigma(M))^*$.

Portanto σ^* é uma derivação em $fr(\mathcal{N})$ para qualquer derivação π em $\mathcal{N}$. Note que desde que $(\rightarrow A)^* = A$, se π é uma derivação em $\mathcal{N}$ de B a partir de $A_1, \ldots, A_l$, então π^* é uma derivação em $fr(\mathcal{N})$ de B de $A_1, \ldots, A_l$. Além disso, é preciso notar que $\lambda(\pi^*) = \lambda(\pi)$ e $\rho(\pi^*) \leq c\rho(\pi)$, onde a constante c depende apenas do conjunto de conectivos κ.

Temos então o seguinte teorema:

Teorema A.8 *Dado os sistemas de dedução natural $\mathcal{N}_1$ e $\mathcal{N}_2$ sobre κ existe uma função f em $\mathcal{L}$ e uma constante c tal que para todas linhas $L_1, \ldots, L_n$, L e derivações π, se $L_1, \ldots, L_n \vdash^{\pi}_{\mathcal{N}_1} L$, então $L_1, \ldots, L_n \vdash^{f(\pi)}_{\mathcal{N}_1} L$, e $\lambda(f(\pi)) \leq c\lambda(\pi)$ e $\rho(f(\pi)) \leq c\rho(\pi)$.*

Corolário A.9 *Seja κ qualquer conjunto de conectivos adequados. Todo sistema de dedução de Frege e sistema de Dedução Natural sobre κ $p-$simula todos os outros*

sistemas de Frege e sistemas de Dedução Natural sobre κ. Assim, tal sistema sobre κ é limitado polinomialmente se e somente se todos tais sistemas sobre κ forem limitados polinomialmente.

A.4 Frege estendido

Cook e Rechkow (CR79) apresentaram uma estensão natural para o sistemas de Frege alegando que tal sistema produziria provas mais curtas.

Foi utilizado o princípio das casas dos pombos para ilustrar a eficiência, em termos de tamanho de prova, do sistema de Frege estendido em relação ao sistema de Frege não estendido.

Contudo, Buss em (Bus87) mostrou que o princípio das casas de pombos não pode ser usado para separar o sistema de Frege do sistema de Frege estendido apresentando, como justificativa, uma prova polinomial do princípio em sistema de Frege.

Teorema A.10 *Se π é uma derivação de B a partir de $A_1, \ldots, A_n$ em $e\mathcal{F}$, então existe uma derivação π' de B a partir de $A_1, \ldots, A_n$ em $\mathcal{F}$ com $\lambda(\pi') \leq \lambda(\pi) + cm$ onde c depende apenas de $\mathcal{F}$ e m é o número de fórmulas definidas em π*

Teorema A.11 *Sejam $e\mathcal{F}$ e $e\mathcal{F}'$ dois sistemas de Frege sob κ e κ', respectivamente, e suponha $L(n) \geq n$ é uma função natural tal que toda tautologia A sob κ tenha uma prova π em $e\mathcal{F}$ com $\lambda(\pi) \leq L(l(A))$. Então toda tautologia A' sob κ' possui uma prova π' em $e\mathcal{F}'$ tal que $\lambda(\pi') \leq cL(cl(A'))$, onde a constante c depende apenas de $\mathcal{F}$ e $\mathcal{F}'$.*

Corolário A.12 *Um sistema de Frege estendido é limitado polinomialmente se e somente se todos os sistemas de Frege estendidos sob todos os conjuntos de conectivos forem limitados polinomialmente. Além disso, um sistema de Frege estendido é polinomialmente limitado se e somente se existir um limite polinomial sob o número de linhas nas provas em $e\mathcal{F}$. Desta forma, se $P \neq NP$, então não existe um limite polinomial sob o número de linhas em provas em sistemas de Frege estendidos, sistemas de Frege ou sistema de Dedução Natural.*

B
Esquema da prova de PHP_2

Faremos a prova de $\neg PHP_2 \rightarrow \neg PHP_1 = \bot$, onde

$PHP_2 =$

$$(p_{00} \vee p_{01}) \wedge (p_{10} \vee p_{11}) \wedge (p_{20} \vee p_{21}) \rightarrow$$
$$(p_{00} \wedge p_{10}) \vee (p_{01} \wedge p_{11}) \vee (p_{00} \wedge p_{20}) \vee (p_{01} \wedge p_{21}) \vee (p_{10} \vee p_{20}) \vee (p_{11} \wedge p_{21})$$

Para facilitar a apresentação das deduções que serão apresentadas a seguir usaremos α para representar o lado esquerdo de PHP_2 e β para representar o lado direito.

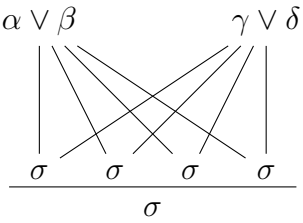
Trabalharemos, sem perda de generalidade, com $\neg PHP_2 \equiv \alpha \wedge \neg\beta$.

A prova de que $PHP_2 \rightarrow PHP_1$, terá o seguinte aspecto:

$$\dfrac{\dfrac{\dfrac{\alpha \wedge \neg\beta}{\neg\beta} \quad \dfrac{\dfrac{\alpha \wedge \neg\beta}{\alpha}}{\beta \vee \sigma}}{\sigma} \quad \dfrac{\dfrac{\dfrac{\alpha \wedge \neg\beta}{\neg\beta}}{\neg\alpha \vee \neg\sigma} \quad \dfrac{\alpha \wedge \neg\beta}{\alpha}}{\neg\sigma}}{\bot}$$

A seguir apresentaremos a prova de $\dfrac{\alpha}{\beta \vee \sigma}$ e de $\dfrac{\neg\beta}{\neg\alpha \vee \neg\sigma}$

Usaremos o seguinte processo para abreviar a representação de $\vee$ encadeados.

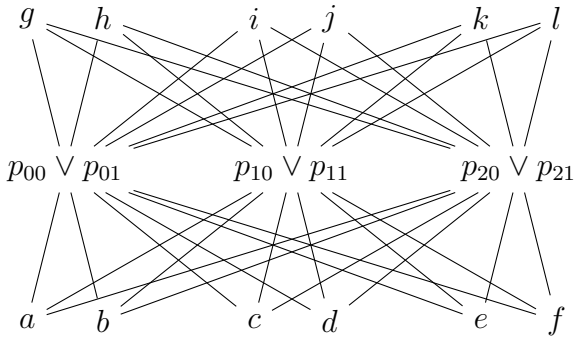


Comecemos com a prova de $\dfrac{\alpha}{\beta \vee \sigma}$:

De α, obtemos as seguintes fórmulas por $\wedge E$.

$$\frac{\alpha}{(p_{00} \vee p_{01})} \qquad \frac{\alpha}{(p_{10} \vee p_{11})} \qquad \frac{\alpha}{(p_{20} \vee p_{21})}$$

Agora, aplicando $\vee E$ produziremos:



onde $a = (p_{00} \wedge p_{10})$, $b = (p_{01} \wedge p_{11})$, $c = (p_{00} \wedge p_{20})$, $d = (p_{01} \wedge p_{21})$, $e = (p_{10} \wedge p_{20})$, $f = (p_{11} \wedge p_{21})$, $g = (p_{00} \wedge p_{11})$, $h = (p_{01} \wedge p_{10})$, $i = (p_{00} \wedge p_{21})$, $j = (p_{01} \wedge p_{20})$, $k = (p_{11} \wedge p_{20})$ e $l = (p_{10} \wedge p_{21})$.

Temos que $\beta = a \vee b \vee c \vee d \vee e \vee f$.

Aplicando $\vee I$ produzimos uma fórmula $\beta \vee \sigma$ onde $\sigma = g \vee h \vee i \vee j \vee k \vee l$.

Ou seja, partindo de α deduzimos $\beta \vee \sigma$, como desejávamos.

A prova de $\dfrac{\neg\beta}{\neg\alpha \vee \neg\sigma}$ segue de modo análogo.

C
Numeral de Church

Seja p uma variável, e defina os tipos iterados por

$$0p := p;$$
$$(k+1)p := kp \to kp$$

Os numerais de Church de tipo kp é definidos por

$$I_k^n = \lambda y^{kp \to kp} x^{kp}.y^n(x)$$

Exemplo C.1 *O exemplo a seguir, representa o numeral de Church* I_0^3

$$\dfrac{\dfrac{\dfrac{\dfrac{}{p}}{p \to p}}{p}\quad \dfrac{\dfrac{\dfrac{}{p}}{p \to p}}{p}}{(p \to p) \to (p \to p)}$$

Figura C.1: I_0^3

A profundidade de I_0^n é $n + 2$.

Notação C.2 *Seja "hyp"a função hiper-exponencial definida por*

$$hyp(x, 0, y) = z, hyp(x, Sx, z) = x^{hyp(x,y,z)}$$

Abreviamos,

$$2_k^i := hyp(2, k, i), \qquad 2_k = hyp(2, k, 1),$$

Um fato interessante dos numerais de Church está na facilidade de gerar exemplos de provas normais com profundidade hyper-exponencial e provas não normais curtas. Por exemplo o numeral $I_0^{2_n}$ tem prova normal de profundidade 2_n+2 enquanto que a prova não normal possui profundidade $n + 3$.

A prova segue diretamente da seguinte redução:

$$I^2_{n-1} I^2_{n-2} \dots I^2_0 =_\beta I^{2_n}_0. \tag{C-1}$$

O lado esquerdo tem profundidade $n + 3$ enquanto o lado esquerdo tem profundidade $2_n + 2$.

Substituindo algumas posições ocupadas por p por variáveis A_i, conseguimos gerar uma nova prova com ramos distintos.

Exemplo C.3 *Considerando os numerais I^2_0 e I^2_1.*

$$\dfrac{\dfrac{\dfrac{p \quad p \to p}{p} \quad p \to p}{p}}{\dfrac{p \to p}{(p \to p) \to (p \to p)}}$$

$$\dfrac{\dfrac{(p \to p) \quad (p \to p) \to (p \to p)}{(p \to p)} \quad (p \to p) \to (p \to p)}{\dfrac{(p \to p)}{(p \to p) \to (p \to p)}}$$

Podemos representar I^4_0 da seguinte forma:

$$\dfrac{\dfrac{\dfrac{(p \to p) \quad I^2_0}{(p \to p)} \quad I^2_0}{(p \to p)}}{(p \to p) \to (p \to p)}$$

A figura abaixo representa o numeral I^4_0 modificado, as partes marcadas na figura representam modificações do numeral I^2_0.

$$\dfrac{\dfrac{[A_1 \to A_2]^5 \quad \dfrac{[A_2 \to A_3]^4 \quad \boxed{\dfrac{\dfrac{[A_1]^1 \quad [A_1 \to A_2]^2}{A_2} \quad [A_2 \to A_3]^3}{\dfrac{A_3}{(A_1 \to A_3)}\,{}^{1}}\,{}^{2}}{(A_2 \to A_3) \to ((A_1 \to A_2) \to (A_1 \to A_3))}\,{}^{3}}{(A_1 \to A_2) \to (A_1 \to A_3)}}{(A_1 \to A_3)} \quad \boxed{\dfrac{\dfrac{\dfrac{[A_4]^6 \quad [A_4 \to A_1]^7}{A_1} \quad [A_1 \to A_3]^8}{\dfrac{A_3}{(A_4 \to A_3)}\,{}^{6}}\,{}^{7}}{(A_1 \to A_3) \to ((A_4 \to A_1) \to (A_4 \to A_3))}\,{}^{8}}}{(A_4 \to A_1) \to (A_4 \to A_3)}}{(A_2 \to A_3) \to ((A_4 \to A_1) \to (A_4 \to A_3))}}{(A_1 \to A_2) \to ((A_2 \to A_3) \to ((A_4 \to A_1) \to (A_4 \to A_3)))}$$

Figura C.2: Numeral I^4_0 modificado.

D
Clássica para Intuicionista

Conforme anunciado na introdução, apresentamos uma versão da prova de normalização de Seldin. Também mostraremos como é possível definir uma tradução da lógica clássica para a lógica intuicionista a partir da normalização de Seldin. Este trabalho encontrasse melhor fundamentado em (dPN01).

Definição D.1 (Profundidade de uma derivação) *A* profunidade de uma derivação π*, denotado por* $d(\pi)$*, é o número de ocorrências de fórmulas de* π*. Mas precisamente* $d(\pi)$ *é definido, por indução, como segue:*

i) *Se* π *é constituída por apenas uma hipótese, então* $l(\pi) = 1$*;*

ii) *Se* π *é* $\dfrac{\begin{matrix}\Sigma_1 & & \Sigma_2\\ A_1 & \cdots & A_n\end{matrix}}{C}$*, então* $d(\pi) = d(\Sigma_1) + \cdots + d(\Sigma_n)$ *para* $n \leq 3$.

Teorema D.2 *Se* π *é uma derivação de C a partir de* Δ *em S, então* π *pode ser transformada em uma derivação* π' *de C a partir de* Δ *em S tal que* π' *contém no máximo uma aplicação da regra de absurdo clássico e, caso esta aplicação ocorra, é a última inferência de* π'*.*

Prova. Prova por indução na profundidade de π.

Se a profundidade de π é igual a 1, é imediato. Nos demais casos, seja π a derivação abaixo e r a sua última inferência.

$$\dfrac{\begin{matrix}\Sigma_1 & \Sigma_2 & \Sigma_3\\ A_1 & A_2 & A_3\end{matrix}}{C}$$

Pela hipótese de indução, as subderivações Σ_1, Σ_2 e Σ_3 podem ser transformadas respectivamente nas derivações Σ_1', Σ_2' e Σ_3' tais que, se existirem aplicações da regra de absurdo clássico em cada uma delas, existe apenas uma e é a última inferência da derivação. Seja π_1 o resultado da substituição de cada Σ_i, $i \leq 3$, por Σ_i' em π.

Se nenhum Σ_i', $i \leq 3$, termina com uma aplicação de absurdo clássico, então π_1 é a derivação desejada. Nos outros casos, mostraremos que a derivação π_1 pode ser transformada em uma derivação π_1' na qual a única aplicação de $\perp_c$ é a sua última inferência.

Caso 1 r é a aplicação de $\rightarrow$-E ou $\wedge$-E.

1. Para algum $i < 2$, Σ'_i termina com uma aplicação de $\bot_c$ Sem perda de generalidade seja $i = 1$.

$$\pi_1 \equiv \dfrac{\dfrac{[\neg A_1]^k \quad \Sigma'_1}{\dfrac{\bot}{A_1}\, k} \quad \dfrac{\Sigma'_2}{A_2}}{C}\, r \qquad \pi'_1 \equiv \dfrac{\dfrac{\dfrac{\Sigma'_2}{\dfrac{[A_1]^k \quad A_2}{C}\, r} \quad [\neg C]^j}{\dfrac{\bot}{[\neg A_1]}\, k} \quad \Sigma'_1}{\dfrac{\bot}{C}\, j}$$

2. Σ'_1 e Σ'_2 terminam com uma aplicação de $\bot_c$

$$\pi_1 \equiv \dfrac{\dfrac{[\neg A'_1]^j \quad \Sigma'_1}{\dfrac{\bot}{A_1}\, i} \quad \dfrac{[\neg A'_2]^j \quad \Sigma'_2}{\dfrac{\bot}{A_2}\, i}}{C}\, r \qquad \pi'_1 \equiv \dfrac{\dfrac{\dfrac{\dfrac{[A_1]^i \quad [A_2]^j}{C}\, r \quad [\neg C]^k}{\dfrac{\bot}{[\neg A_1]}\, i} \quad \dfrac{\bot}{[\neg A_2]}\, j}{\Sigma'_2} \quad \Sigma'_1}{\dfrac{\bot}{C}\, k}$$

Caso 2 r é aplicação de $\rightarrow$-I

$$\pi_1 \equiv \dfrac{\dfrac{[A_1]^i \quad [\neg B]^j}{\dfrac{\Sigma_1}{\dfrac{\bot}{B}\, j}}}{A \rightarrow B}\, r,i \qquad \pi'_1 \equiv \dfrac{\dfrac{\dfrac{[B]^j}{A \rightarrow B}\, r \quad [\neg(A \rightarrow B)]^k}{\dfrac{\bot}{[\neg B]}} \quad [A]^i}{\dfrac{\dfrac{\Sigma_1}{\dfrac{\bot}{B}\, r,i}}{A \rightarrow B} \quad [\neg(A \rightarrow B)]^k}$$

$$\dfrac{\bot}{A \rightarrow B}\, k$$

Caso 3 r é uma aplicação de $\wedge$-E ou $\vee$-I.

$$\pi_1 \equiv \dfrac{\dfrac{[\neg A_1]^i \quad \Sigma'_1}{\dfrac{\bot}{A_1}\, i}}{C}\, r \qquad \pi'_1 \equiv \dfrac{\dfrac{\dfrac{[A_1]^i}{C}\, r \quad [\neg C]^j}{\dfrac{\bot}{[\neg A_1]}\, i} \quad \Sigma'_1}{\dfrac{\bot}{C}\, j}$$

Caso 4 r é uma aplicação de $\wedge$-E

1. Apenas Σ'_1 termina com uma aplicação de $\perp_c$

$$\pi_1 \equiv \dfrac{\dfrac{[\neg(A \vee B)]^i}{\begin{array}{c}\Sigma'_1\\ \bot\end{array}} \quad \begin{array}{cc}[A]^j & [B]^k\\ \Sigma'_2 & \Sigma'_3\\ C & C\end{array}}{A \vee B \qquad\qquad C}\ r,j,k \qquad C$$

$$\pi'_1 \equiv \dfrac{\dfrac{\dfrac{\begin{array}{cc}[A]^l & [B]^k\\ \Sigma'_2 & \Sigma'_3\\ C & C\end{array}}{[A \vee B]^i \qquad C}\ r,j,k \qquad [\neg C]^l}{\dfrac{\bot}{[\neg(A \vee B)]}\ i}}{\begin{array}{c}\Sigma'_1\\ \bot\end{array}}}{C}\ l$$

2. Apenas Σ'_2 termina com uma aplicação de $\perp_c$

$$\pi_1 \equiv \dfrac{\begin{array}{ccc}\Sigma'_1 & [A]^j \quad [\neg C]^i & [B]^k\\ A \vee B & \Sigma'_2 \quad \bot & \Sigma'_3\\ & \overline{C} & C\end{array}}{C}\ r,j,k$$

$$\pi'_1 \equiv \dfrac{\dfrac{\begin{array}{ccc}\Sigma'_1 & [A]^j \quad [\neg C]^i & [B]^k\\ A \vee B & \Sigma'_2 \quad \bot & \Sigma'_3\\ & & C \qquad [\neg C]^i\end{array}}{\bot}\ r,j,k}{\overline{C}\ i}$$

3. Apenas Σ'_3 termina com uma aplicação de $\perp_c$

   Similar ao caso anterior

4. Σ'_1, Σ'_2, Σ'_3 terminam com uma aplicação de $\perp_c$

$$\pi_1 \equiv \dfrac{\begin{array}{cccc}[\neg(A \vee B)]^i & [A]^j \quad [\neg C]^l & [B]^k \quad [\neg C]^l\\ \Sigma'_1 & \Sigma'_2 & \Sigma'_3\\ \dfrac{\bot}{A \vee B}\ i & \dfrac{\bot}{C}\ l & \dfrac{\bot}{C}\ l\end{array}}{C}\ r,j,k$$

$$\pi'_1 \equiv \dfrac{\dfrac{\dfrac{\begin{array}{ccc}[A]^j \quad [\neg C]^l & [B]^k \quad [\neg C]^l\\ \Sigma'_2 & \Sigma'_3\\ \bot & \bot\end{array}}{[A \vee B]^i}\ r,j,k}{\dfrac{\bot}{[\neg(A \vee B)]}\ i}}{\begin{array}{c}\Sigma'_1\\ \bot\end{array}}}{\overline{C}\ l}$$

Caso 5 r é aplicação de absurdo clássico

$$\pi_1 \equiv \dfrac{\dfrac{[\neg\bot]^i \quad [\neg C]^j}{\Sigma_1'}}{\dfrac{\dfrac{\bot}{\bot}\, i}{C}\, r,j} \qquad \pi_1' \equiv \dfrac{\dfrac{\dfrac{[\neg\bot]^i}{\neg\bot}\, i \quad [\neg C]^j}{\Sigma_1'}}{\dfrac{\bot}{C}}$$

■

D.0.1
Tradução da lógica clássica para a lógica intuicionista

De posse do resultado anterior, definiremos uma função que associa fórmulas da linguagem clássica a fórmulas da linguagem intuicionista.

Definição D.3 *Seja h_1 uma função que associa fórmulas da linguagem clássica a fórmulas da linguagem intuicionista definida recursivamente como segue:*

$h_1(A) =_{def} A$*, se A é uma fórmula atômica.*

$h_1(A \to B) =_{def} h_1(A) \to h_1(B)$

$h_1(A \wedge B) =_{def} h_1(A) \wedge h_1(B)$

$h_1(A \vee B) =_{def} h_1(A) \vee h_1(B)$

Definição D.4 *Seja h_2 uma função que associa fórmulas da linguagem clássica a fórmulas da linguagem intuiciontista definida como segue:*

$h_2(A) =_{def} \neg\neg h_1(A)$*, para toda fórmula A pertencente a linguagem clássica.*

h_2 é uma função tradução da lógica clássica na lógica intuicionista, como veremos.

Lema D.5 $\vdash_C A \leftrightarrow h_2(A)$

Prova. Como $(B \leftrightarrow \neg\neg B)$ é teorema em lógica clássica, para qualquer B pertencente a linguagem clássica, temos que $\vdash_c h_1(A) \leftrightarrow \neg\neg h_1(A)$. Assim, para mostrar que $A \leftrightarrow h_2(A)$ é o teorema em lógica clássica, será suficiente provar que:

$$\vdash_C A \leftrightarrow h_1(A) \tag{D-1}$$

Pois, por definição temos que $h_2(A)$ é $\neg\neg h_1(A)$.

A prova de (D-1) segue imediatamente por indução no comprimento da prova A. ■

Lema D.6 $\Gamma \vdash_C A$ *se, e somente se,* $h_2(\Gamma) \vdash h_2(A)$.

Prova. Segue imediatamente do lema anterior. ■

Lema D.7 *Se* $h_2(\Gamma) \vdash_C h_2(A)$*, então* $h_2(\Gamma) \vdash_I h_2(A)$.

Prova. De $h_2(\Gamma) \vdash_C h_2(A)$ temos, pelo teorema D.2, que existe uma derivação pi de $h_2(A)$ a partir de $h_2(\Gamma)$ tal que a única aplicação de $\bot_C$, se existir, é a última inferência de π. Se a última inferência de π não é uma aplicação de $\bot_c$, claramente π é uma derivação em I e conseqüentemente π seria a derivação desejada.

Caso contrário, π seria:

$$\dfrac{\begin{array}{cc} h_2(\Gamma) & [\neg h_2(A)]^i \\ & \Sigma \\ & \bot \end{array}}{h_2(A)}\ \bot_C, i$$

Do fato da subderivação Σ de π não ter aplicações de absurdo clássico e de $(\neg B \rightarrow \neg\neg B)$ ser um teorema da lógica intuicionista, temos a seguinte derivação de $h_2(A)$ a partir de $h_2(\Gamma)$ em I como desejávamos.

$$\dfrac{\begin{array}{cc} & \dfrac{[\neg h_1(A)]^i \quad \neg h_1(A) \rightarrow \neg\neg\neg h_1(A)}{\dfrac{\neg\neg\neg h_1(A)}{\neg h_2(A)}\ def} \\ h_2(\Gamma) & \\ & \Sigma \\ & \bot \end{array}}{\dfrac{\dfrac{\neg\neg h_1(A)}{h_2(A)}\ def}{}\ i}$$

■

Como o sistema intuicionista é um subsistema do sistema clássico, temos:

Lema D.8 *Se* $h_2(\Gamma) \vdash_I h_2(A)$*, então* $h_2(\Gamma) \vdash_C h_2(A)$.

Como conseqüência imediata dos lemas D.6 e D.8, temos.

Teorema D.9 $\Gamma \vdash_C A$ *se, e somente se,* $h_2(\Gamma) \vdash_I h_2(A)$.

Observe que a transformação h_2 é polinomial em relação ao tamanho de A. Além disso a nova derivação de clássica para intuicionista no teorema D.7 é realizada apenas acrescentado 3 linhas a derivação clássica, no pior caso. Ou seja, a transformação de uma prova em sistema clássico para uma prova em sistema intuicionista pode ser realizada polinomialmente.