Aritmética Computável em Espaço Polinomial

Dissertação de Mestrado da Licenciada
Gilda Maria Saraiva Dias Ferreira

Orientador: Professor Fernando Ferreira

Faculdade de Ciências da Universidade de Lisboa

Novembro 2001

Resumo

O principal objectivo desta dissertação é apresentar uma teoria de análise, cujas funções demonstravelmente totais, com gráfico apropriado, sejam as funções computáveis em espaço polinomial.

Na dissertação "*Bounded Arithmetic*", Buss introduz várias teorias que permitem fornecer caracterizações alternativas de algumas classes de complexidade computacional, nomeadamente uma teoria de 2^a ordem, U_2^1, cujas funções demonstravelmente totais, com gráfico apropriado, são as funções de $PSPACE$. Visto todo o nosso trabalho girar em torno de $PSPACE$, começamos por estudar, com algum detalhe, várias versões de máquinas de Turing, nomeadamente deterministas, não deterministas, com oráculo e alternadas, e algumas classes de complexidade computacional a elas associadas (resultantes da imposição de limites sobre o tempo e o espaço). De seguida introduzimos duas teorias, uma de 1^a ordem $PSCA$ (acrónimo para *Polynomial Space Computable Arithmetic*) na linguagem $\mathcal{L}_{PS}$, que além de alguns axiomas básicos e definidores tem indução na notação para matrizes decidíveis em espaço polinomial e outra de 2^a ordem $\Sigma_1^{1,b}$-NIA, na linguagem $\mathcal{L}_2^b$, constituída por alguns axiomas básicos, por um esquema de indução na notação para fórmulas $\Sigma_1^{1,b}$ e por esquemas de compreensão e substituição para fórmulas $\Sigma_0^{1,b}$. São demonstrados vários resultados nesta última teoria, nomeadamente o facto de que substituindo os esquemas de indução na notação para fórmulas $\Sigma_1^{1,b}$ e substituição para fórmulas $\Sigma_0^{1,b}$ por indução na notação para fórmulas $\Sigma_1^{1,b}$-*estendidas*, continuamos na presença da mesma teoria. Vemos assim que $\Sigma_1^{1,b}$-NIA corresponde, na linguagem por nós adoptada (cuja interpretação intencionada é a árvore binária $2^{<\omega}$), à teoria U_2^1 de Buss. Embora as teorias tenham diferentes linguagens, demonstramos que existe uma imersão de $PSCA$ em $\Sigma_1^{1,b}$-NIA. A estratégia utilizada para conseguir tal intento consiste em "introduzir" em $\Sigma_1^{1,b}$-NIA os símbolos funcionais de $\mathcal{L}_{PS}$, i.e. as funções computáveis em espaço polinomial, através de fórmulas apropriadas de $\mathcal{L}_2^b$. Em ambas as teorias provamos que as suas funções demonstravelmente totais são as funções de $PSPACE$. Contudo, enquanto no caso de $PSCA$ tal resultado é uma consequência quase imediata do teorema de Herbrand, na teoria $\Sigma_1^{1,b}$-NIA um outro tipo de abordagem é necessário, tendo nós recorrido ao cálculo de sequentes de Gentzen e a uma versão do teorema da eliminação do corte.

Definimos ainda uma terceira teoria, $\Sigma_1^{1,b}$-$NIA + B\Sigma_\infty^{1,b} + B^1\Sigma_\infty^{1,b}$, que resulta do enriquecimento de $\Sigma_1^{1,b}$-NIA com os seguintes dois esquemas de colecção:

- $\forall x \preceq t \exists y \varphi(x,y) \rightarrow \exists z \forall x \preceq t \exists y \preceq z \varphi(x,y)$ e
- $\forall X^t \exists y \varphi(y, X^t) \rightarrow \exists z \forall X^t \exists y \preceq z \varphi(y, X^t)$

em que φ é uma fórmula $\Sigma^{1,b}_\infty$.

Formulando a teoria assim enriquecida no cálculo de sequentes, demonstramos que esta é $\forall\exists\Sigma^{1,b}_\infty$-*conservativa* sobre $\Sigma^{1,b}_1$-NIA, continuando portanto a ter como funções demonstravelmente totais, com gráfico apropriado, as funções de $PSPACE$.

Por último apresentamos uma teoria de análise, designada por $BTPSA$ (acrónimo para *Base Theory for Polynomial Space Analysis*), que uma vez mais permite caracterizar as funções de $PSPACE$ como as demonstravelmente totais nessa teoria. Acreditamos que em $BTPSA$ se pode desenvolver alguma análise.

PALAVRAS CHAVE

Sistemas formais, $PSPACE$, aritmética limitada, análise fraca.

Abstract

The basic aim of this dissertation is to set up a theory for analysis where provably total functions, having appropriate graphs, are the polynomial space computable functions.

In the dissertation *"Bounded Arithmetic"*, Buss has already introduced a second-order theory, U_2^1, whose provably total functions, having appropriate graphs, are the $PSPACE$ functions. We start by studying, in some detail, different versions of Turing machines, such as deterministic, nondeterministic, oracle and alternative Turing machines and some computational complexity classes connected to them (resulting from the imposition of limits in time and space). We introduce two theories. Firstly, the first-order theory $PSCA$ (an acronym for *Polynomial Space Computable Arithmetic*) in the language $\mathcal{L}_{PS}$, which in addition to some basic axioms and defining axioms has induction on notation for polynomial space decidable matrices. Secondly, the second-order theory, $\Sigma_1^{1,b}$-NIA, in the language $\mathcal{L}_2^b$, formed by basic axioms, scheme of induction on notation for $\Sigma_1^{1,b}$-formulas and schemes of comprehension and substitution for $\Sigma_0^{1,b}$-formulas.

In this last theory, several results are proved, for instance the fact that by substituting the scheme of induction on notation for $\Sigma_1^{1,b}$-formulas and the scheme of substitution for $\Sigma_0^{1,b}$-formulas by induction on notation for *extended* $\Sigma_1^{1,b}$-formulas, we still have the same theory. So, we can see that $\Sigma_1^{1,b}$-NIA is the analogue, in our language (whose intended interpretation is the binary tree $2^{<\omega}$), of Buss' theory U_2^1.

Although the teories have different languages, we can prove the existence of an immersion of $PSCA$ into $\Sigma_1^{1,b}$-NIA. The strategy that we use to prove this consists in "introducing" in $\Sigma_1^{1,b}$-NIA the functional symbols of $\mathcal{L}_{PS}$, namely, the polynomial space computable functions, through appropriate formulas of $\mathcal{L}_2^b$. In both theories, we show that their provably total functions are the functions of $PSPACE$. However, whereas in case of $PSCA$ such result is an almost immediate consequence of Herbrand's theorem, in the case of the theory $\Sigma_1^{1,b}$-NIA, another kind of approach is necessary, viz to use Gentzen's sequent calculus and a version of the cut elimination theorem.

We have also defined a third theory, $\Sigma_1^{1,b}$-$NIA + B\Sigma_\infty^{1,b} + B^1\Sigma_\infty^{1,b}$, an enrichment of $\Sigma_1^{1,b}$-NIA with the two following schemes of collection:

- $\forall x \preceq t \exists y \varphi(x, y) \rightarrow \exists z \forall x \preceq t \exists y \preceq z \varphi(x, y)$ and
- $\forall X^t \exists y \varphi(y, X^t) \rightarrow \exists z \forall X^t \exists y \preceq z \varphi(y, X^t)$

where φ is a $\Sigma^{1,b}_{\infty}$-formula.

Once again, by formulating the theory $\Sigma^{1,b}_{1}$-NIA+$B\Sigma^{1,b}_{\infty}$+$B^{1}\Sigma^{1,b}_{\infty}$ in the sequent calculus, we show it is $\forall\exists\Sigma^{1,b}_{\infty}$-*conservative* over $\Sigma^{1,b}_{1}$-NIA, and so its provably total functions, having appropriate graphs, are still the functions of $PSPACE$.

Finally, we introduce a theory of analysis, called $BTPSA$ (an acronym for *Base Theory for Polynomial Space Analysis*), that once again characterizes the $PSPACE$ functions as the provably total functions of this theory. We believe that some analysis can be developed in $BTPSA$.

KEY WORDS

Formal systems, $PSPACE$, bounded arithmetic, weak analysis.

Agradecimentos

As minhas primeiras palavras de agradecimento são dirigidas ao Professor Fernando Ferreira pela sua orientação, absolutamente essencial na realização deste trabalho, pelo incansável e simpático apoio com que sempre pude contar e pela forma entusiasta, admirável e exemplar com que se dedica à Lógica e a transmite aos outros.

Agradeço também à FCT (Fundação para a Ciência e Tecnologia) que através duma Bolsa de Mestrado me suportou financeiramente durante este último ano.

Grata estou ainda a vários professores da FCUL (Faculdade de Ciências da Universidade de Lisboa) que tive o privilégio de ter como mestres, dos quais destaco o Professor José Dias da Silva e as Professoras Luísa Galvão e Catarina Gomes pela amabilidade e disponibilidade que sempre tiveram para comigo.

Por último um agradecimento especial às minhas colegas (em particular à Ana Cristina Casimiro, que tal como o meu irmão, sempre se prontificou a tentar solucionar dificuldades relacionadas com processamento de texto) e à minha família pelo seu apoio e encorajamento.

Conteúdo

Capítulo 1
INTRODUÇÃO

A partir do momento em que se estabelece uma definição formal de algoritmo e de função computável importa adequar estes conceitos à nossa realidade, i.e. estudar tal temática à luz do que é praticável no "mundo real" onde existem limitações de recursos, nomeadamente tempo e espaço. Surgem assim as chamadas classes de complexidade computacional.

Este trabalho gira em torno duma dessas classes, conhecida por $PSPACE$, que é a classe constituída por todas as funções computáveis em espaço polinomial.

Após a introdução de alguma notação e definições que nos acompanharão ao longo de todo este estudo, surgem no capítulo 2 a apresentação das máquinas de Turing como o processo mecânico por nós adoptado para formalizar rigorosamente o conceito de computabilidade; a descrição de várias versões dessas máquinas com diferentes graus de eficiência; a apresentação de duas caracterizações da classe $PSPACE$, uma delas independente de máquinas e a demonstração de alguns resultados relativos a computações de 2^a ordem em espaço polinomial.

À semelhança do trabalho de Buss na sua dissertação "*Bounded Arithmetic*", em que são apresentadas várias teorias com o propósito de através delas caracterizar determinadas classes de complexidade computacional como sendo as classes de funções demonstravelmente totais nessas teorias, também nós introduzimos algumas teorias com a finalidade de fornecer caracterizações alternativas de $PSPACE$.

Prescindiremos, contudo, da linguagem da aritmética (adoptada por Buss) em favor da linguagem cuja interpretação intencionada é a árvore binária $2^{<\omega}$, ou seja, a classe das sequências finitas de 0's e 1's, linguagem essa introduzida por Fernando Ferreira na dissertação "*Polynomial Time Computable Arithmetic and Conservative Extensions*".

Nos capítulos 3 e 4 são desenvolvidas as teorias $PSCA$ (teoria de 1^a ordem) e $\Sigma_1^{1,b}$-NIA (teoria de 2^a ordem) respectivamente, cujas funções demonstravelmente totais (com gráficos apropriados) são as funções de $PSPACE$.

Para obtermos este resultado em relação à 2^a teoria, necessitámos introduzir um sistema rigoroso de demonstração, tendo optado por uma variante do cálculo de sequentes de Gentzen. Assim sendo no capítulo 5 apresentamos, de forma breve, este sistema de demonstração e formulamos $\Sigma_1^{1,b}$-NIA no cálculo de sequentes.

No capítulo 6 introduzimos a teoria $\Sigma_1^{1,b}$-$NIA + B\Sigma_\infty^{1,b} + B^1\Sigma_\infty^{1,b}$ que resulta do enriquecimento de $\Sigma_1^{1,b}$-NIA com dois novos esquemas de colecção e apresentamos um resultado de conservação.

O 7º capítulo, onde definimos a teoria de 2ª ordem $BTPSA$, pretende apontar o caminho que tencionamos seguir futuramente, na procura de desenvolver noções de análise em sistemas fracos de aritmética de 2ª ordem computáveis em espaço polinomial.

1.1 Notação

Representamos por $2^{<w}$ o conjunto de todas as sequências finitas de zeros e uns. A cada uma dessas sequências está associado um comprimento (notamos o comprimento da sequência x por $|x|$) que indica o número de dígitos que a constitui. $2^{<w}$ é, portanto, a família das palavras de comprimento finito no alfabeto $\{0,1\}$. A palavra vazia, isto é, a que tem comprimento zero, será notada por ε.

Consideremos a bijecção $2^{<w} \to \mathbb{N}$, esquematizada pela árvore abaixo

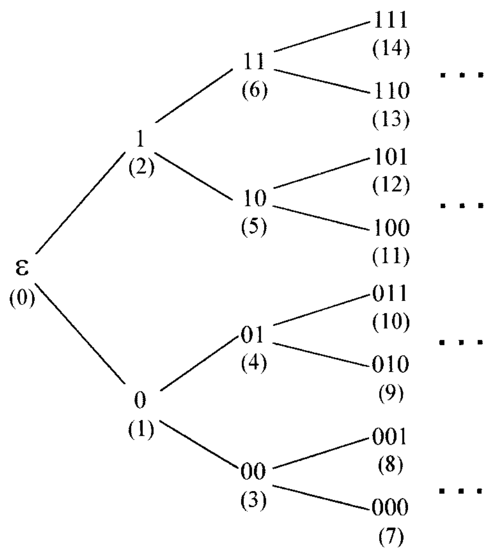


Fig. 1

Esta bijecção permite identificar os elementos de $2^{<w}$ com os números naturais.

Sendo x e y elementos de $2^{<w}$ representamos por:

- $x \frown y$ a **concatenação** de x com y (abreviada por xy);
- $x \subseteq y$, x é **subpalavra inicial** de y, i.e. $\exists z \; x \frown z = y$;
- $x \subseteq^* y$, x é **subpalavra** de y, i.e. $\exists z \; z \frown x \subseteq y$;
- $x_{|y}$ a **truncatura** de x a y, i.e.

$$x_{|y} = \begin{cases} x & se \quad |x| \leq |y| \\ z & se \quad z \subseteq x \text{ e } |z| = |y| \end{cases};$$

- $x \times y$ o **produto** de x por y, definido do seguinte modo:

$x \times y = \underbrace{x \frown \ldots \frown x}_{|y| \text{ vezes}};$

- $x \preccurlyeq y$, o comprimento de x é menor ou igual que o comprimento de y ($|x| \leq |y|$), i.e. $1 \times x \subseteq 1 \times y$.
- $x \equiv y$, o comprimento de x é igual ao comprimento de y, i.e. $1 \times x = 1 \times y$.

Nos capítulos que se seguem vamos trabalhar com duas linguagens, uma de primeira, outra de segunda ordem, que passamos a definir.

Seja $\mathcal{L}$ a linguagem de 1^a ordem com igualdade, que tem três constantes 0, 1 e ε, dois símbolos funcionais binários $\frown$ e $\times$ e dois símbolos relacionais binários $\subseteq$ e $=$.

Seja $\mathcal{L}_2^b$ a linguagem de 2^a ordem que inclui a anterior linguagem $\mathcal{L}$ e que contém ainda um símbolo relacional binário que opera entre um termo de $\mathcal{L}$ e uma variável de 2^a ordem, denotado por $\in$. Além de variáveis de 1^a ordem notadas por $x, y, z, \ldots$ $\mathcal{L}_2^b$ contém, portanto, também variáveis de 2^a ordem representadas por $F^t, G^r, \ldots$ com t, r,... termos de $\mathcal{L}$.

A ideia é fazer com que as variáveis de 1^a ordem tomem valores em $2^{<\omega}$ e as de 2^a ordem F^t variem entre os subconjuntos de $2^{<\omega}$ que verifiquem $x \in F^t \rightarrow x \preccurlyeq t$, onde t é um termo que não depende de x.

Observação 1 *Os **termos** de $\mathcal{L}_2^b$ coincidem com os termos de $\mathcal{L}$.*

Definição 1 *A classe das **fórmulas** de $\mathcal{L}_2^b$ é a menor classe de expressões, tais que:*

1. Se t_1 e t_2 são termos e F^t é uma variável de 2^a ordem então $t_1 \subseteq t_2$, $t_1 = t_2$ e $t_1 \in F^t$ são fórmulas (fórmulas atómicas).

2. Se P e Q são fórmulas então $\neg P$, $(P \wedge Q)$, $(P \vee Q)$ e $(P \rightarrow Q)$ são fórmulas.

3. Se P é uma fórmula, x é uma variável de 1^a ordem, F^t é uma variável de 2^a ordem e q é um termo então $\forall x P$, $\exists x P$, $(\forall x \preccurlyeq q)P$, $(\exists x \preccurlyeq q)P$, $(\forall\ F^t)P$ e $(\exists\ F^t)P$ são fórmulas.

Observação 2 *Em $\mathcal{L}_2^b$, introduzimos $(\forall x \preccurlyeq q)P$ e $(\exists x \preccurlyeq q)P$ como novas fórmulas e não como abreviações de $\forall x(x \preccurlyeq q \rightarrow P)$ e $\exists x(x \preccurlyeq q \wedge P)$ respectivamente, por motivos técnicos ligados ao cálculo de sequentes, que se tornarão mais claros em capítulos posteriores.*

Definição 2 *Uma **fórmula** $\Sigma_0^{1,b}$ é uma fórmula de $\mathcal{L}_2^b$ sem quantificações de 2^a ordem e em que todas as quantificações de 1^a ordem são limitadas*. Estas fórmulas podem, obviamente, ter parâmetros de 2^a ordem.*

---

*Quantificações limitadas são as quantificações da forma $(\forall x \preccurlyeq q)$ e $(\exists x \preccurlyeq q)$, com x variável de 1^a ordem e q um termo em que x não ocorre.

Capítulo 2
EM TORNO DE PSPACE

2.1 Máquinas de Turing deterministas

Em sentido informal, uma função computável é aquela cujas imagens se podem obter através de um processo mecânico, de acordo com um algoritmo.

Existem várias formas de tornar rigorosa a noção de computabilidade, mediante a escolha de diferentes máquinas abstractas. Entre as mais utilizadas encontra-se a chamada máquina de Turing, que ficou a dever o seu nome a Alan Mathison Turing que a concebeu em 1936. Como existe uma grande diversidade de descrições de máquinas de Turing passamos a estabelecer a versão usada ao longo deste capítulo.

Definição 3 *Uma* ***máquina de Turing determinista*** *com k fitas (das quais k_1 são de leitura, k_2 de escrita e as restantes de leitura/escrita) é um quintuplo $M = \; =< Q, \Sigma, \delta, q_0, F >$ onde*

1. *Q é o conjunto finito de estados*
2. *Σ é o alfabeto*
3. *$q_0 \in Q$ é o estado inicial*
4. *F é o conjunto de estados de aceitação*
5. *$\delta : Q \times \Sigma^{k-k_2} \rightarrow Q \times \Sigma^{k-k_1} \times \{D, P, E\}^{k-k_2} \times \{D, P\}^{k_2}$ é uma função parcial chamada função transição de M.*

Interpretaremos uma máquina de Turing como sendo constituída por k fitas, das quais k_1 são fitas de *input*, k_2 de *output* e as restantes são fitas de trabalho.

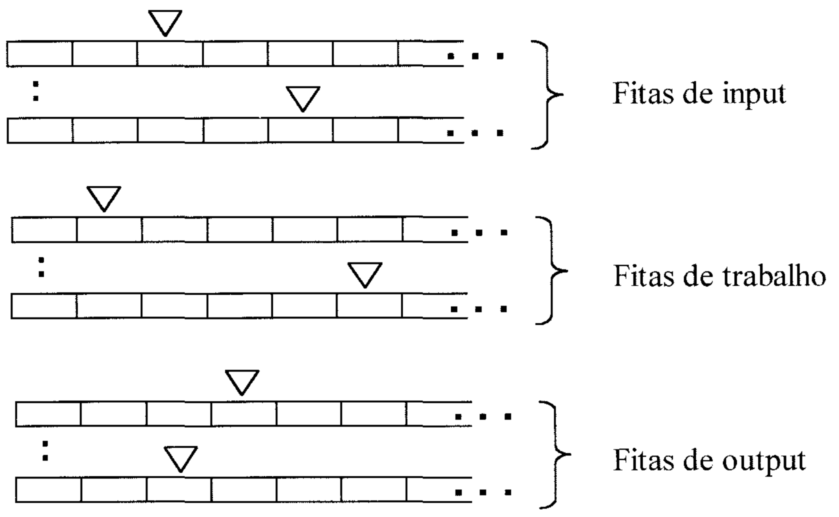


Fig. 2

Todas as fitas são semi-infinitas, i.e. são constituídas por um número infinito de células, existindo a célula mais à esquerda, mas não existindo a célula mais à direita.

Cada fita possui uma cabeça que, em cada instante, aponta para uma e uma só célula. As fitas de trabalho possuem cabeças de leitura/escrita, as fitas de *input* possuem cabeças de leitura e as de *output* cabeças de escrita.

Vejamos então como se processa o funcionamento desta máquina.

Em cada momento vemos qual o estado da máquina e os elementos que estão a ser apontados nas várias fitas pelas cabeças de leitura e de leitura/escrita. Mediante esta informação, a função δ "diz-nos" que alterações se irão dar. A primeira componente da imagem indica qual o novo estado da máquina; a segunda componente quais os elementos que se escreverão nas células apontadas pelas cabeças de leitura/escrita e de escrita; a terceira componente descreve-nos o movimento de cada uma das cabeças das fitas de *input* e de trabalho podendo estas deslocar-se uma célula para a esquerda (E), uma para a direita (D) ou manterem a posição (P) e a quarta componente informa-nos sobre o movimento (D ou P) das cabeças das fitas de *output*. Vemos, portanto, que enquanto nas fitas de *input* e de trabalho a cabeça se pode mover em ambos os sentidos, nas fitas de *output* não se pode deslocar para a esquerda. Obviamente, em qualquer tipo de fitas, estando a cabeça a apontar para a primeira célula, esta não se pode deslocar para a esquerda.

As alterações implementadas segundo a função δ constituem um **passo**.

Se para determinado estado e elementos apontados a função transição não está definida, a máquina pára.

O nosso alfabeto será $\Sigma = \{0, 1, B\}$.

A máquina M começa a operar no estado q_0 e tendo certo *input* $w_1, ..., w_{k_1}$* colocado respectivamente nas primeiras k_1 fitas (fitas de *input*), disposto da esquerda

*O *input* pertence a $\{0,1\}^*$ i.e., ao conjunto de todas as sequências finitas binárias.

para a direita, de tal forma que cada célula apenas contenha um símbolo (0 ou 1) e figurando B nas restantes células das fitas, B esse interpretado como estando a célula em Branco. As fitas de trabalho e de *output* são iniciadas todas com B. A máquina inicia então o funcionamento atrás descrito segundo a sua função transição.

Dizemos que M aceita o *input* $w_1, ..., w_{k_1}$ se a máquina pára num estado de aceitação.

Dizemos que M computa uma função $f : (2^{<w})^{k_1} \to (2^{<w})^{k_2}$ se sempre que iniciarmos a máquina com *input* $(w_1, ..., w_{k_1}) \in (2^{<w})^{k_1}$ esta pára em estado de aceitação e $f(w_1, ..., w_{k_1})$ figura nas fitas de *output*.

Definição 4 *Dada uma máquina M, uma* ***configuração de M*** *é a descrição num dado momento dos elementos que estão nas fitas, das posições das cabeças nessas mesmas fitas e do estado da máquina.*

Se M tem k fitas, uma configuração de M é um $k+1$*-uplo* $(q, x_1, x_2, ..., x_k)$ *em que q é o estado de M e cada* $x_j \in \Sigma^*\#\Sigma^{*\dagger}$ *descreve os elementos que estão na fita j nesse momento. O símbolo* $\# \notin \Sigma$ *serve para marcar a célula apontada pela cabeça. Por convenção, a cabeça aponta para o símbolo imediatamente à direita de #. Todos os símbolos nas fitas semi-infinitas que não aparecem descritos em* x_j *supõem-se B.*

Definição 5 *A configuração inicial de uma máquina M iniciada com input* $w_1, ..., w_{k_1}$ *é* $(q_0, \#w_1, ..., \#w_{k_1}, \#, ..., \#)$.

Definição 6 *Dada uma máquina M e um input* $\bar{w}$*, uma* ***computação*** *é uma sequência de configurações de M, que começa com a configuração inicial de M em* $\bar{w}$*, em que a passagem duma configuração à seguinte obedece à função transição e que termina numa configuração (configuração terminal) em que não se podem dar mais passos.*

As máquinas de Turing, com que temos lidado até aqui, são chamadas deterministas uma vez que a acção, por estas perpetrada, está perfeitamente determinada a partir de qualquer configuração. Existem, contudo, outros modelos de máquinas de Turing em que tal não se verifica e que serão, de seguida, alvo da nossa atenção.

2.2 Máquinas de Turing não deterministas

A única diferença entre as máquinas de Turing deterministas e as não deterministas é que, enquanto nas primeiras cada passo é completamente determinado pelo estado e pelos símbolos nas células apontadas pelas cabeças de leitura e de leitura/escrita, nas segundas o próximo passo pode, por vezes, ser "escolhido" dentre várias possibilidades.

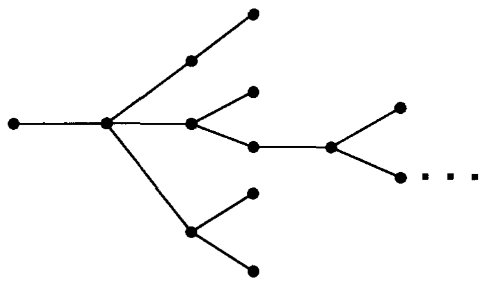
Formalmente, temos a seguinte definição:

$^\dagger\Sigma^*$ é o conjunto de todas as sequências finitas de elementos de Σ.

Definição 7 *Uma* ***máquina de Turing não determinista*** *com k fitas (das quais k_1 são de leitura, k_2 de escrita e as restantes de leitura/escrita) é um quintuplo $M =< Q, \Sigma, \delta, q_0, F >$ exactamente como as máquinas de Turing deterministas, mas em que a função transição δ passa a ser:*

$$\delta : Q \times \Sigma^{k-k_2} \rightarrow \mathcal{P}(Q \times \Sigma^{k-k_1} \times \{D, P, E\}^{k-k_2} \times \{D, P\}^{k_2})^{\ddagger}$$

As anteriores definições de configuração e de computação continuam válidas para este tipo de máquinas, se bem que agora, a partir de determinado *input* $\bar{w}$ não existe, em geral, uma única computação, i.e. não existe apenas uma sequência "linear" de configurações, mas um conjunto de possíveis computações que podem ser esquematizadas numa árvore,



onde cada nodo representa uma configuração da máquina, representando a raíz da árvore (nodo inicial) a configuração inicial e sendo os descendentes[§] dum certo nodo c, as configurações que, a partir de c, podem ser alcançadas de acordo com a função transição.

Uma máquina de Turing não determinista, M, aceita determinado *input* se existe uma computação de M nesse *input* terminando num estado de aceitação, ou seja, se no esquema em árvore existe um caminho finito que termine num estado de aceitação.

2.3 Máquinas de Turing com oráculo

Existe uma versão mais complexa de máquinas de Turing que permite recorrer, em sentido que vamos precisar já a seguir, a uma certa ajuda externa, são as chamadas máquinas de Turing com oráculo.

Definição 8 *Uma* ***máquina de Turing*** *(determinista ou não determinista)* ***com oráculo*** *é uma máquina de Turing (determinista ou não determinista) M, com algumas fitas especiais, apenas de escrita, chamadas fitas de oráculo, e três novos estados: Interrogativo, Sim e Não.*

[‡]Para qualquer conjunto A, $\mathcal{P}(A)$ denota as partes de A.

[§]Designamos por descendentes dum nodo c os nodos que na árvore se encontram imediatamente à direita de c.

Para trabalhar com uma máquina de Turing com oráculo precisamos fixar à partida um conjunto, chamado **conjunto de oráculo**.

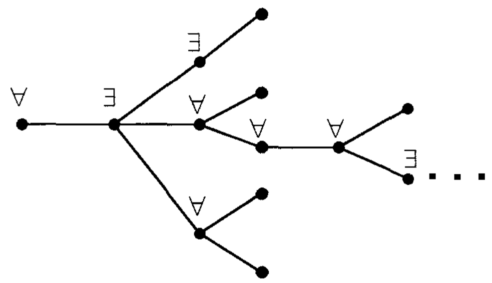
Em determinado momento da computação podemos entrar no estado Interrogativo. Nessa altura se nas fitas do oráculo estiver $\bar{w}$ pertencente ao conjunto, passamos para o estado Sim, caso contrário passamos para o estado Não. Em qualquer dos casos as fitas de oráculo são instantaneamente apagadas, não se dando outras alterações na configuração da máquina.

2.4 Máquinas de Turing alternadas

A última versão de máquina de Turing que vamos apresentar é bastante poderosa, na medida em que combina o não determinismo anteriormente estudado com um certo paralelismo, ou seja a possibilidade de ocorrerem computações em "simultâneo".

Definição 9 *Uma **máquina de Turing alternada** com k fitas é um quíntuplo $M =< Q, \Sigma, \delta, q_0, g >$ onde Q, Σ, δ e q_0 são definidos como para as máquinas de Turing não deterministas e $g : Q \longrightarrow \{\forall, \exists, ace, rej\}$ é uma função que "cataloga" os estados de Q em estados universais, existenciais, de aceitação e de rejeição.*

Tal como no caso das máquinas de Turing não deterministas, também representaremos as computações das máquinas de Turing alteradas, a partir de determinado *input*, através duma árvore. Porém agora, associado a cada nodo não terminal temos um símbolo $\forall$ ou $\exists$, conforme o estado, na configuração representada por esse nodo, for universal ou existencial.



Para que uma máquina de Turing alternada aceite um *input*, não basta que, na árvore das computações a partir desse *input*, exista um caminho finito que termine num estado de aceitação, é necessário que exista uma etiquetagem (segundo o processo a seguir descrito) que atribua 1 ao nodo de partida (raíz da árvore). As atribuições de 1's são feitas, a partir dos nodos terminais até chegar ao nodo inicial, do seguinte modo:

• Os únicos nodos terminais que podem ser rotulados com 1 são os que correspondem a configurações com estado de aceitação.

• Um nodo interno existencial é marcado com 1 se pelo menos um dos seus descendentes tiver rótulo 1.

• Um nodo interno universal é marcado com 1 se todos os seus descendentes tiverem rótulo 1.

Se a máquina aceita um *input*, para cada etiquetagem que atribua 1 ao nodo inicial, podemos pensar na sub-árvore da árvore das computações que tem todos os nodos rotulados com 1. Essas sub-árvores são chamadas **árvores de aceitação**.

Observação 3 *Todas as árvores de aceitação são sub-árvores da árvore de aceitação que se obtém rotulando com 1 todos os nodos terminais que correspondem a configurações com estado de aceitação.*

Observação 4 *Uma máquina de Turing não determinista é um caso particular duma máquina de Turing alternada, em que todos os nodos são existenciais.*

2.5 Computações com recursos limitados

Quando pensamos numa função computável, uma questão que se levanta de imediato, é a de saber que recursos, em termos de tempo e espaço, são necessários para a computar. Quanto à aceitação de *inputs*, problemas idênticos se colocam, sendo óbvio que os recursos necessários dependem da versão da máquina de Turing que escolhermos.

Da imposição de limites sobre o tempo e o espaço e da escolha da máquina de Turing surgem as chamadas **classes de complexidade computacional**. Iremos limitar-nos às classes $PTIME$, $PSPACE$ e $APTIME$ pois são as que intervêm no decorrer deste trabalho.

Definição 10 *Uma função $f : (2^{<w})^{k_1} \to (2^{<w})^{k_2}$ é **computável por uma máquina de Turing determinista em tempo polinomial** se existirem uma máquina de Turing determinista, M, que compute f e um polinómio, $p \in \mathbb{N}[x]$, tais que, para todo $\bar{w} = (w_1, ..., w_{k_1}) \in (2^{<w})^{k_1}$ o número de passos executados por M, até a máquina parar, quando o input é $\bar{w}$, é menor ou igual que $p(n)$, sendo $n = \max\{|w_1|, ..., |w_{k_1}|\}$.*

Definição 11 *Uma função $f : (2^{<w})^{k_1} \to (2^{<w})^{k_2}$ é **computável por uma máquina de Turing determinista em espaço polinomial** se existirem uma máquina de Turing determinista, M, que compute f e um polinómio, $p \in \mathbb{N}[x]$, tais que, para todo $\bar{w} = (w_1, ..., w_{k_1}) \in (2^{<w})^{k_1}$ o número das células de M alguma vez visitadas ou ocupadas durante a computação a partir de $\bar{w}$, é menor ou igual que $p(n)$, sendo $n = \max\{|w_1|, ..., |w_{k_1}|\}$.*

Definição 12 *Um conjunto $C \subseteq (2^{<w})^{k_1}$ é **decidível por uma máquina de Turing determinista em tempo** (respectivamente **espaço**) polinomial, se a sua função característica χ_C for computável por uma máquina de Turing determinista em tempo (respectivamente espaço) polinomial.*

Definição 13 *Um conjunto $C \subseteq (2^{<w})^{k_1}$ é* ***aceite por uma máquina de Turing alternada em tempo polinomial*** *se existirem uma máquina de Turing alternada, M, e um polinómio, $p \in \mathbb{N}[x]$, tais que:*

1) para todo $\bar{w} = (w_1, ..., w_{k_1}) \in (2^{<w})^{k_1}$, $\bar{w} \in C$ sse M aceita $\bar{w}$,

2) para todo o $\bar{w} \in C$ existe uma árvore de aceitação (iniciando M com input $\bar{w}$) de comprimento¶ menor ou igual que $p(n)$, sendo $n = \max\{|w_1|, ..., |w_{k_1}|\}$.

Estamos agora em condições de definir as três classes de complexidade computacional anteriormente referidas.

Definição 14 • *PTIME é a classe das funções computáveis por uma máquina de Turing determinista em tempo polinomial. Por vezes, PTIME é também usado para designar a classe dos conjuntos decidíveis por uma máquina de Turing determinista em tempo polinomial.*

• *PSPACE é a classe das funções computáveis por uma máquina de Turing determinista em espaço polinomial. Por vezes, PSPACE é também usado para designar a classe dos conjuntos decidíveis por uma máquina de Turing determinista em espaço polinomial.*

• *APTIME é a classe dos conjuntos aceites por uma máquina de Turing alternada em tempo polinomial.*

Um resultado conhecido, que pode ser encontrado, por exemplo, no livro [2] "*Structural Complexity II*" estabelece a seguinte igualdade:

$$\boxed{PSPACE = APTIME}$$

considerando $PSPACE$ como classe de conjuntos.

2.6 Computações de 2^a ordem

Nas secções anteriores, as máquinas trabalhavam com *inputs* e *outputs* de 1^a ordem, i.e sequências binárias de um certo comprimento n, que podem ser interpretadas como números naturais através da bijecção $2^{<w} \to \mathbb{N}$, apresentada na fig.1.

Estamos, porém, interessados em que as máquinas também possam trabalhar com *inputs* e *outputs* de 2^a ordem, i.e. sequências finitas binárias que podem ser interpretadas, mediante codificação apropriada que introduziremos adiante, como subconjuntos finitos de $2^{<w}$ cujos elementos têm comprimento menor ou igual que um certo n, ou seja, novamente pela bijecção da fig.1, subconjuntos finitos de $\mathbb{N}$.

A única diferença em relação às máquinas atrás descritas é que, agora, umas fitas de *input* são para *inputs* de 1^a ordem e outras para *inputs* de 2^a ordem, convenientemente codificados, e o mesmo se passa nas fitas de *output* e nas fitas de oráculo (caso se trate duma máquina de Turing com oráculo).

¶Comprimento de uma árvore é o comprimento do seu maior ramo, i.e. é o maior número de passos que se podem dar entre o nodo inicial e um terminal.

Os elementos de 2^a ordem são denotados por F^s, sendo F^s um subconjunto finito de $2^{<\omega}$ em que todas as palavras têm comprimento menor ou igual que o comprimento de s.

• Dado o *input* de 1^a ordem $x = 11010$, já sabemos que este é colocado numa fita de *input* de 1^a ordem do seguinte modo:

1	1	0	1	0	B	...

• Dado o *input* de 2^a ordem F^s, este é colocado numa fita de *input* de 2^a ordem do seguinte modo: na célula j colocamos 1 ou 0 conforme a sequência binária correspondente ao número j pertence ou não pertence a F^s, sempre que $0 \leq j < < 2^{|s|+1} - 1$. Nas restantes células colocamos B.

Definição 15 *Seja* $Q(\bar{x}, \bar{F}^s) = Q(x_1, ..., x_k, F_1^{s_1}, ..., F_r^{s_r})$ *um oráculo de 2^a ordem, com $\bar{x}$ de 1^a ordem e $\bar{F}^s$ de 2^a ordem. Uma máquina de Turing determinista, M, com tempo exponencial limitado por $p \in \mathbb{N}[x]$, com inputs de 1^a e de 2^a ordem e com oráculo Q, satisfaz as seguintes condições:*

1. M tem fitas de input apenas de leitura: umas de 1^a ordem com inputs de comprimento $\leq n$ e outras de 2^a ordem com inputs de comprimento $\leq 2^{p(n)}$.

2. M escreve as perguntas ao oráculo nas fitas de oráculo, apenas de escrita. Nas fitas de 1^a ordem M escreve respectivamente $x_1, ..., x_k$ onde cada x_i tem comprimento $\leq p(n)$ ($1 \leq i \leq k$), nas fitas de 2^a ordem escreve respectivamente $F_1^{s_1}, ..., F_r^{s_r}$ onde cada $F_i^{s_i}$ tem comprimento $\leq 2^{p(n)}$. O oráculo responde Sim ou Não conforme $Q(\bar{x}, \bar{F}^s)$ se verifica ou não, e apaga as fitas de oráculo.

3. O tempo computacional total é limitado por $2^{p(n)}$.

4. M escreve os outputs em fitas de output apenas de escrita: umas para outputs de 1^a ordem que podem ter comprimento quando muito $p(n)$ e outras para outputs de 2^a ordem com comprimento $\leq 2^{p(n)}$.

$TIME(2^{p(n)})^Q$:= classe dos funcionais computáveis por uma máquina de Turing satisfazendo as condições anteriores.

O **espaço** usado na computação é o espaço total usado nas fitas de trabalho de M.

$SPACE(r(n))^Q$:= classe dos funcionais computáveis por uma máquina de Turing satisfazendo as condições anteriores em espaço $\leq r(n)$.

$$PSPACE^{\Sigma_0^{1,b}} := \bigcup_{Q \in \Sigma_0^{1,b}} \bigcup_{k \in \mathbb{N}} SPACE(n^k)^Q.$$

Dizemos que uma máquina, como na definição anterior, computa uma **função** se não tem *inputs* nem *outputs* de 2^a ordem, podendo, no entanto, fazer perguntas de 2^a ordem ao oráculo.

Estamos agora em condições de enunciar alguns resultados relativos ao espaço polinomial e de apresentar esboços das respectivas demonstrações.

Proposição 1 *Os funcionais da classe* $PSPACE^{\Sigma_0^{1,b}}$, *que são funções, são precisamente as funções de* $PSPACE$.

Dem. Sem perda de generalidade, vamos considerar que existem apenas duas fitas de oráculo, uma para 1^a ordem e outra para 2^a ordem.

$\boxed{\supseteq}$ Se $f \in PSPACE$ então existe M, uma máquina de Turing determinista, que computa f em espaço polinomial.

M pode ser encarada como uma máquina de Turing nas condições da definição anterior, em que as fitas de 2^a ordem ficam em branco, e o oráculo nunca é chamado a intervir.

Logo $f \in PSPACE^{\Sigma_0^{1,b}}$.

$\boxed{\subseteq}$ Seja $f \in PSPACE^{\Sigma_0^{1,b}}$ uma função.

Então existe M_1, uma máquina de Turing determinista que trabalha em espaço polinomial e recorre a oráculo $Q(x, F^s)$ em $\Sigma_0^{1,b}$ e que, quando o *input* é $\bar{w}$, o *output* é $f(\bar{w})$.

Seja M_2 uma máquina de Turing determinista, sem fitas de 2^a ordem, que iniciamos em $\bar{w}$ e que vai operando os mesmos passos que M_1, excepto quando em M_1 se escrevem símbolos na fita de oráculo de 1^a ordem, em M_2 escrevem-se numa fita de trabalho e quando em M_1 se escrevem símbolos na 2^a fita de oráculo (fita de 2^a ordem), em M_2 não se faz nada.

Vejamos que fazer quando em M_1 se consulta o oráculo pela primeira vez.

Se $Q(x, F^s) \in \Sigma_0^{1,b}$ é um oráculo de 1^a ordem, i.e. F^s não intervém, como a fórmula é limitada, é decidível em espaço polinomial, logo em M_2 basta introduzir os passos que decidem $Q(x)$.

Se F^s ocorre em $Q(x, F^s)$ suponhamos, sem perda de generalidade, que $Q(x, F^s)$ é da forma $(\exists z_1 \preccurlyeq t_1(x))(\forall z_2 \preccurlyeq t_2(x))\ r(x, z_1, z_2) \in F^s$.

Vejamos que existe uma máquina de Turing alternada, trabalhando em tempo polinomial, que, com input x, aceita $Q(x, F^s)$.

Começamos por computar t_1 e t_2, o que pode ser feito em $PSPACE$.

Como nas máquinas de Turing alternadas existem estados existenciais e estados universais, é fácil convencermo-nos que se conseguirmos decidir $r \in F^s$ em $PSPACE$ (que como sabemos é equivalente a tempo polinomial em máquinas de Turing alternadas), temos uma máquina de Turing alternada que aceita $Q(x, F^s)$ em tempo polinomial.

A partir de x, z_1 e z_2, podemos computar r em $PSPACE$.

Para decidir $r \in F^s$ pensamos numa máquina iniciada em $\bar{w}$, que opera como M_1, mas em que, sempre que em M_1 se escreve um elemento na 1^a fita de oráculo, nesta nova máquina escrevemo-lo numa fita de trabalho e sempre que em M_1 se escreve um elemento na 2^a fita de oráculo, nesta nova máquina colocamos em notação binária o número de elementos que já deveriam ter sido escritos na 2^a fita de oráculo em M_1. Quando esse número for r, lê-se o próximo elemento a ser colocado na fita de oráculo de 2^a ordem de M_1. Se for 0 temos que $r \notin F^s$, se for 1 temos que $r \in F^s$. Logo $r \in F^s$ decide-se em $PSPACE$.

$\therefore$ $Q(x, F^s)$ é aceite, a partir de x, por uma máquina de Turing alternada operando em tempo polinomial, logo é decidível em $PSPACE$.

Assim, em M_2 introduzimos os passos que permitem decidir $Q(x, F^s)$.

Repetindo o processo sempre que em M_1 se consulta o oráculo, temos que M_2 é uma máquina de Turing que computa f em espaço polinomial.

$\therefore f \in PSPACE$. ■

Corolário 1 *Seja ϕ um funcional da classe $PSPACE^{\Sigma_0^{1,b}}$ sem inputs de 2^a ordem e com um único output, que é de 2^a ordem.*

Então a função

$$\varphi(\bar{x}, i) = \begin{cases} 1 & se \quad i \in \phi(\bar{x}) \\ 0 & se \quad i \notin \phi(\bar{x}) \end{cases}$$

está em $PSPACE$.

Dem. Seja M' a máquina que computa ϕ em espaço polinomial, recorrendo a oráculo em $\Sigma_0^{1,b}$, i.e. quando nas fitas de *input* de M' colocamos $\bar{x}$, a máquina trabalhando em espaço polinomial, usando fitas de oráculo de 1^a e 2^a ordem, coloca na fita de *output* (de 2^a ordem) $\phi(\bar{x})$.

Seja M uma máquina com mais uma fita de *input* de 1^a ordem do que M' e com uma única fita de *output* de 1^a ordem, que quando iniciada com $\bar{x}$, i vai realizar os mesmos passos que M' (quando iniciada em $\bar{x}$), mas em vez de colocar $\phi(\bar{x})$ na fita de *output*, coloca-o numa fita de oráculo de 2^a ordem e coloca i numa fita de oráculo de 1^a ordem. Em seguida, vai perguntar ao oráculo se $i \in \phi(\bar{x})$. Se a resposta for Sim, coloca 1 na fita de *output* (de 1^a ordem). Se a resposta for Não, coloca 0 na fita de *output* (de 1^a ordem).

Temos que $\varphi(\bar{x}, i) \in PSPACE^{\Sigma_0^{1,b}}$.

Como $\varphi(\bar{x}, i)$ é uma função, sabemos pela proposição anterior que $\varphi(\bar{x}, i)$ está em $PSPACE$. ■

Proposição 2 *A composição de funcionais de $PSPACE^{\Sigma_0^{1,b}}$ ainda é um funcional de $PSPACE^{\Sigma_0^{1,b}}$.*

Dem. Sejam $\mathcal{F}$, $\mathcal{G} \in PSPACE^{\Sigma_0^{1,b}}$. Vejamos que $\mathcal{F} \circ \mathcal{G} \in PSPACE^{\Sigma_0^{1,b}}$.

Suponhamos que $\mathcal{F}$ é computável por uma máquina M', que trabalha em espaço polinomial, com oráculo em $\Sigma_0^{1,b}$, e que $\mathcal{G}$ é computável por uma máquina M", que também trabalha em espaço polinomial, com oráculo em $\Sigma_0^{1,b}$.

Suponhamos, sem perda de generalidade, que quer em M' quer em M" só existem duas fitas de *input*, uma de 1^a ordem e outra de 2^a ordem e duas fitas de *output*, uma de 1^a ordem e outra de 2^a ordem.

Seja M a máquina que, quando iniciada com *input* de 1^a ordem x e *input* de 2^a ordem X^t, vai efectuar os mesmos passos que M", mas em vez de colocar o *output* de 1^a ordem, y, na fita de *output*, coloca-o numa fita de trabalho, e quando M" escreve na fita de *output* de 2^a ordem, M não faz nada.

Em seguida M vai operar segundo os passos da máquina M' quando esta é iniciada com y. Como não temos o *input* de 2^a ordem, sempre que em M' é necessário ler a célula i da fita de *input* de 2^a ordem, vamos realizar novamente os passos de M", iniciada em x, X^t e quando se deveriam escrever elementos na fita de *output* de 2^a ordem, apenas escrevemos em notação binária, numa fita de trabalho, o número de elementos que já deveriam ter sido escritos nessa fita de *output* de 2^a ordem. Quando o número for i vemos qual seria o próximo elemento a ser escrito na fita de *output* de 2^a ordem por M". Continuamos a computar segundo M', como se o resultado da leitura da célula i da fita de *input* de 2^a ordem tivesse sido esse elemento.

M é uma máquina que computa $\mathcal{F} \circ \mathcal{G}$ em espaço polinomial, recorrendo a oráculo em $\Sigma_0^{1,b}$.

$\therefore \mathcal{F} \circ \mathcal{G} \in PSPACE^{\Sigma_0^{1,b}}$. ∎

Proposição 3 *Se f se obtém, por recursão limitada na notação, a partir de funcionais de $PSPACE^{\Sigma_0^{1,b}}$ então f ainda é um funcional de $PSPACE^{\Sigma_0^{1,b}}$, i.e. se*

$$f(\bar{x}, \bar{X}^t, \varepsilon) = g(\bar{x}, \bar{X}^t)$$
$$f(\bar{x}, \bar{X}^t, y0) = h_0(\bar{x}, \bar{X}^t, y, f(\bar{x}, \bar{X}^t, y))_{|t(\bar{x},y)}$$
$$f(\bar{x}, \bar{X}^t, y1) = h_1(\bar{x}, \bar{X}^t, y, f(\bar{x}, \bar{X}^t, y))_{|t(\bar{x},y)}$$

com $g, h_0, h_1 \in PSPACE^{\Sigma_0^{1,b}}$, t uma função limitativa[‖] *e onde $_{|t(\bar{x},y)}$ significa que as imagens de 1^a ordem de h_0 e h_1 são truncadas pelo comprimento de $t(\bar{x}, y)$ e as palavras das imagens de 2^a ordem, Z, de h_0 e h_1 também são truncadas pelo comprimento de $t(\bar{x}, y)$, i.e. as imagens de 2^a ordem são Z^t,*
então $f \in PSPACE^{\Sigma_0^{1,b}}$.

Dem. A demonstração segue a técnica que usámos para a proposição anterior, mas agora iterada tantas vezes quanto necessário.

Ou seja, uma máquina M que computa $f(\bar{x}, \bar{X}^t, y)$, vai agir do seguinte modo:

· se y for ε, faz as operações da máquina que computa g;

· se $y = z \frown 0$ ou $y = z \frown 1$ faz respectivamente as operações da máquina que computa h_0 ou h_1, mas sempre que é necessário usar $f(\bar{x}, \bar{X}^t, z)$, i.e. sempre que precisa conhecer o conteúdo, digamos $i_{|z|}$, de determinada célula duma das fitas que contêm a informação $f(\bar{x}, \bar{X}^t, z)$, reinicializa o processo, usando a máquina que computa g, h_0 ou h_1 conforme z for ε, terminar em 0 ou em 1 respectivamente... Este processo é iterado até se chegar ao ponto em que $f(\bar{x}, \bar{X}^t, \varepsilon)$ é o *input* desconhecido, donde eventualmente necessita conhecer o valor i_0 duma das células para que a computação

[‖] A classe das funções limitativas é a menor classe de funções que contém as projecções, a concatenação e o "produto" de funções e é fechada para a composição e "substituição" de variáveis por constantes. Alternativamente, podemos pensar em $t(\bar{x}, y)$ como um termo da linguagem $\mathcal{L}$.

possa prosseguir. Então opera segundo a máquina que computa g, retirando a informação que pretende, não escrevendo em fitas de *output*, mas por um sistema de contagem binária, análogo ao usado na proposição anterior, que indica o número de elementos que já deveriam ter sido escritos nas fitas de *output* de 2^a ordem, permitindo assim identificar o elemento i_0 que pretendia. O número máximo de "máquinas" a operar em cadeia, para encontrar de forma faseada os elementos ($i_{|z|}$, $i_{|z|-1}$,... ..., i_1, i_0), é $|z|+2$. Na posse de i_0 e com vista a encontrar i_1, continua a computação da penúltima "máquina", voltando a recorrer à última ("máquina" que computa g) se for necessário identificar outros elementos nas fitas de *input* que contêm a informação $f(\bar{x}, \bar{X}^t, \varepsilon)$. O processo continua desta forma até se encontrar $i_{|z|}$, repetindo-se todo este raciocínio sempre que na computação da primeira "máquina" novos elementos, das fitas com a informação $f(\bar{x}, \bar{X}^t, z)$, forem necessários.

Pode-se ver que M (que engloba as $|z|+2$ "máquinas") trabalha em espaço polinomial.

$\therefore f \in PSPACE^{\Sigma_0^{1,b}}$. ■

2.7 Outra caracterização de PSPACE

Definimos $PSPACE$ como sendo a classe das funções computáveis por uma máquina de Turing determinista em espaço polinomial. Apresentamos de seguida uma outra caracterização de $PSPACE$, desta vez não recorrendo a máquinas.

Proposição 4 *$PSPACE$ é a menor classe de funções que contém as **funções iniciais**:*

1) $E(x) = \varepsilon$

2) $P_i^n(x_1, ..., x_n) = x_i \quad , 1 \leq i \leq n$

3) $C_0(x) = x0$

4) $C_1(x) = x1$

5) $Q(x,y) = \begin{cases} 1 & se \quad x \subseteq y \\ 0 & caso \quad contrário \end{cases}$

e é fechada para os seguintes esquemas:

Esq.1-Composição

$f(x_1, ..., x_n) = g(h_1(x_1, ..., x_n), ..., h_k(x_1, ..., x_n))$

Esq.2-Recursão limitada na notação

$f(\bar{x}, \varepsilon) = g(\bar{x})$

$f(\bar{x}, y0) = h_0(\bar{x}, y, f(\bar{x}, y))_{|t(\bar{x},y)}$

$f(\bar{x}, y1) = h_1(\bar{x}, y, f(\bar{x}, y))_{|t(\bar{x},y)}$

onde t é uma função limitativa

Esq.3-Recursão limitada

$f(\bar{x}, \varepsilon) = g(\bar{x})$

$f(\bar{x}, S(y)) = h(\bar{x}, y, f(\bar{x}, y))_{|t(\bar{x},y)}$

onde t é uma função limitativa e S é a função sucessor definida por $S(\varepsilon) = 0$, $S(x0) = x1$ e $S(x1) = S(x)0$.

A caracterização de $PSPACE$ aqui apresentada é, no essencial, a exposta na tese de mestrado [14] de Isabel Oitavem, onde é apresentado um esboço da verificação de que, de facto, $PSPACE$ coincide com esta classe de funções.

Observação 5 *Para obtermos uma caracterização de $PTIME$ também independente de máquinas, basta, na anterior classe de funções, omitir o esquema 3 (Recursão limitada). Este resultado encontra-se demonstrado na tese anteriormente referida e na tese [7] de Fernando Ferreira "Polynomial Time Computable Arithmetic and Conservative Extensions".*

Capítulo 3
FUNDAMENTOS DA ARITMÉTICA COMPUTÁVEL EM ESPAÇO POLINOMIAL I

3.1 Teoria PSCA

Seja $\mathcal{L}_{PS}$ a linguagem de 1^a ordem com igualdade, que se obtém de $\mathcal{L}$ (linguagem definida no capítulo 1) adicionando um símbolo funcional para cada descrição duma função computável em espaço polinomial, de acordo com o esquema apresentado na proposição 4 do capítulo anterior, que como observámos, gera todas as funções de $PSPACE$.

Definição 16 *A classe das **matrizes decidíveis em espaço polinomial** é a menor classe de fórmulas de $\mathcal{L}_{PS}$ que contém as fórmulas atómicas e é fechada para as operações booleanas e quantificações da forma: $\forall x(x \preceq t \rightarrow ...)$ e $\exists x(x \preceq t \wedge ...)$, onde t é um termo de $\mathcal{L}_{PS}$ que não contém a variável x.**

Vamos de seguida definir uma teoria de 1^a ordem em $\mathcal{L}_{PS}$, que designaremos por **PSCA** (acrónimo para *Polynomial Space Computable Arithmetic*). Para facilitar a notação escreveremos $x_{|z} = y$ para abreviar a fórmula $(1 \times z \subseteq 1 \times x \wedge y \subseteq x \wedge$ $\wedge 1 \times z = 1 \times y) \vee (1 \times x \subseteq 1 \times z \wedge x = y)$ que indica que y é a truncatura de x pelo comprimento de z.

Para não sobrecarregar as fórmulas, omitimos o símbolo da concatenação $\frown$ e convencionamos que esta tem precedência sobre o produto, o que, por exemplo, permite escrever $x \times y0$ em vez de $x \times (y \frown 0)$.

Definição 17 **PSCA** *é a teoria de 1^a ordem, na linguagem $\mathcal{L}_{PS}$, constituída pelos seguintes axiomas:*

- ***Axiomas básicos***

1. $x\varepsilon = x$

2. $x(y0) = (xy)0$

3. $x(y1) = (xy)1$

4. $x \times \varepsilon = \varepsilon$

5. $x \times y0 = (x \times y)x$

---

*$x \preceq t$ está na linguagem $\mathcal{L}_{PS}$ pois é uma abreviação de $1 \times x \subseteq 1 \times t$.

6. $x \times y1 = (x \times y)x$
7. $x \subseteq \varepsilon \longleftrightarrow x = \varepsilon$
8. $x \subseteq y0 \longleftrightarrow x \subseteq y \vee x = y0$
9. $x \subseteq y1 \longleftrightarrow x \subseteq y \vee x = y1$
10. $x0 = y0 \rightarrow x = y$
11. $x1 = y1 \rightarrow x = y$
12. $x0 \neq y1$
13. $x0 \neq \varepsilon$
14. $x1 \neq \varepsilon$

• ***Axiomas definidores***

a. Funções iniciais
1. $E(x) = \varepsilon$
2. $P_i^n(x_1, ..., x_n) = x_i \quad , 1 \leq i \leq n$
3. $C_0(x) = x0$
4. $C_1(x) = x1$
5. $Q(x, y) = 1 \longleftrightarrow x \subseteq y$
$Q(x, y) = 0 \vee Q(x, y) = 1$

b. Funções derivadas
1. $f(x_1, ..., x_n) = g(h_1(x_1, ..., x_n), ..., h_k(x_1, ..., x_n))$,
onde f *é a descrição da composição definida a partir de* $g, h_1, ..., h_k$.
2. $f(\bar{x}, \varepsilon) = g(\bar{x})$
$f(\bar{x}, y0) = h_0(\bar{x}, y, f(\bar{x}, y))_{|t(\bar{x},y)}$
$f(\bar{x}, y1) = h_1(\bar{x}, y, f(\bar{x}, y))_{|t(\bar{x},y)}$,
onde t *é um termo da linguagem* $\mathcal{L}$ *e* f *é a descrição da recursão limitada na notação a partir de* g, h_0 *e* h_1.
3. $f(\bar{x}, \varepsilon) = g(\bar{x})$
$f(\bar{x}, S(y)) = h(\bar{x}, y, f(\bar{x}, y))_{|t(\bar{x},y)}$,
onde t *é um termo de* $\mathcal{L}$, S *é a função sucessor e* f *é a descrição da recursão limitada a partir de* g *e* h.

• ***Axiomas de indução na notação para matrizes decidíveis em espaço polinomial***

$A(\varepsilon) \wedge \forall x(A(x) \rightarrow A(x0) \wedge A(x1)) \rightarrow \forall x A(x)$,
com A *uma matriz decidível em espaço polinomial, podendo ter outras variáveis livres além de* x.[†]

Observação 6 *A teoria* $PSCA$ *foi inspirada na teoria* **PTCA** *(acrónimo para Polynomial Time Computable Arithmetic) que é a teoria de 1ª ordem na linguagem* $\mathcal{L}_{PT}$ *(linguagem de 1ª ordem que se obtém de* $\mathcal{L}$ *adicionando um símbolo funcional para*

[†]A indução na notação corresponde em notação numérica à indução $PIND$, definida por Buss na dissertação [4] "*Bounded Arithmetic*".

cada descrição duma função computável em tempo polinomial, de acordo com a observação 5 do capítulo anterior) cujos axiomas são:

- *Axiomas básicos*
- *Axiomas definidores excluindo os axiomas b.3*
- *Axiomas de indução na notação para matrizes decidíveis em tempo polinomial.*[†]

Um estudo detalhado de PTCA pode ser encontrado na tese [7] de Fernando Ferreira "Polynomial Time Computable Arithmetic and Conservative Extensions".

Observação 7 *$PTIME \subseteq PSPACE$ logo $PTCA \subseteq$ [‡]$PSCA$. Assim todos os resultados acerca de $PTCA$, demonstrados na tese anteriormente referida, continuam válidos em $PSCA$.*

Observação 8 *A **indução "lenta"** para matrizes decidíveis em espaço polinomial é válida em $PSCA$, i.e. $PSCA \vdash A(\varepsilon) \wedge \forall x(A(x) \rightarrow A(S(x))) \rightarrow \forall x A(x)$ onde A é uma matriz decidível em espaço polinomial possivelmente com outras variáveis livres além de x.*[§]

A demonstração deste resultado no contexto de $PTCA$ (i.e. $PTCA \vdash A(\varepsilon) \wedge$ $\wedge \forall x(A(x) \rightarrow A(S(x))) \rightarrow \forall x A(x)$ onde A é uma matriz decidível em tempo polinomial), pode ser encontrada na tese atrás mencionada, demonstração essa que também funciona para o resultado em $PSCA$.

3.2 Caracterização das funções demonstravelmente totais de PSCA

A teoria $PSCA$ não foi apresentada como uma teoria universal, devido aos axiomas de indução. Vamos porém provar que, de facto, esta teoria é universal.

Lema 1 *Dadas matrizes decidíveis em espaço polinomial $A_1(\bar{x}),\ldots, A_n(\bar{x})$ para as quais existem símbolos funcionais $K_{A_1},\ldots, K_{A_n}$ tais que,*

$PSCA \vdash (A_i(\bar{x}) \rightarrow K_{A_i}(\bar{x}) = 1) \wedge (\neg A_i(\bar{x}) \rightarrow K_{A_i}(\bar{x}) = 0)$ *com* $1 \leq i \leq n$ *e dados símbolos funcionais $f_1(\bar{x}),\ldots, f_n(\bar{x})$, $f_{n+1}(\bar{x})$, existe um símbolo funcional $f(\bar{x})$ tal que,*

$$PSCA \vdash (A_1(\bar{x}) \wedge f(\bar{x}) = f_1(\bar{x})) \vee (\neg A_1(\bar{x}) \wedge A_2(\bar{x}) \wedge f(\bar{x}) = f_2(\bar{x})) \vee \ldots$$
$$\ldots \vee (\neg A_1(\bar{x}) \wedge \ldots \wedge \neg A_n(\bar{x}) \wedge f(\bar{x}) = f_{n+1}(\bar{x})).$$

Dem. Demonstremos o resultado para $n = 1$.

[†]A classe das matrizes decidíveis em tempo polinomial é a menor classe de fórmulas de $\mathcal{L}_{PT}$ que contém as fórmulas atómicas e é fechada para as operações booleanas e quantificações da forma: $\forall x(x \subseteq t \rightarrow \ldots)$ e $\exists x(x \subseteq t \wedge \ldots)$, onde t é um termo de $\mathcal{L}_{PT}$ que não contém a variável x.

[‡]$PTCA \subseteq PSCA$ no sentido em que, a partir de qualquer modelo de $PSCA$, podemos criar um modelo de $PTCA$ mantendo o domínio e as interpretações das constantes e dos símbolos funcionais e relacionais de $\mathcal{L}_{PT}$.

[§]A indução "lenta" corresponde em notação numérica à usual indução "+1".

Seja $h(y, \varepsilon) = y$
$h(y, x0) = y$
$h(y, x1) = x$.

Temos que $PSCA \vdash h(y,x)1 = x \vee ((\forall z \subseteq x\ z1 \neq x) \wedge h(y,x) = y)$. Tomando $f(\bar{x}) = h(f_2(\bar{x}), f_1(\bar{x})K_A(\bar{x}))$ temos o pretendido. O caso geral prova-se facilmente por indução em n. ■

Proposição 5 *Para cada matriz decidível em espaço polinomial A existe um símbolo funcional K_A em $\mathcal{L}_{PS} \backslash \mathcal{L}$ tal que,*
$PSCA \vdash (A(\bar{x}) \rightarrow K_A(\bar{x}) = 1) \wedge (\neg A(\bar{x}) \rightarrow K_A(\bar{x}) = 0)$.

Dem. Comecemos por demonstrar que para cada termo t de $\mathcal{L}_{PS}$ existe um símbolo funcional f em $\mathcal{L}_{PS} \backslash \mathcal{L}$ tal que $PSCA \vdash \forall \bar{x}(f(\bar{x}) = t(\bar{x}))$. Pelo axioma definidor b.1 de $PSCA$ basta estudar os casos em que t é uma constante, uma variável, a concatenação e o produto.

Para as constantes ε, 0 e 1, os símbolos funcionais pretendidos são $E(x)$, $C_0(E(x))$ e $C_1(E(x))$ respectivamente. Se t é a variável x, basta tomar $f(x)$ como sendo $P_1^1(x)$.

Sejam $C(x, \varepsilon) = P_1^1(x)$ e $P(x, \varepsilon) = E(x)$
$C(x, y0) = C_0(C(x, y))$ $P(x, y0) = C(P(x, y), x)$
$C(x, y1) = C_1(C(x, y))$ $P(x, y1) = C(P(x, y), x)$.

Facilmente se arranjam funções limitativas e se prova, por indução na notação em y, fixando x, que $C(x,y) = x \frown y$ e $P(x,y) = x \times y$.

Provemos então a proposição por indução na complexidade de A. No caso de A ser uma fórmula atómica tomamos $K_{\subseteq}$ como sendo Q e $K_{=}(x,y)$ como sendo $Q(11, Q(x,y)Q(y,x))$.

Definimos $K_{\neg B} := K_{=}(0, K_B)$ e $K_{B \wedge C} := K_{=}(11, K_B K_C)$.

Seja $A(\bar{z}, x)$ a fórmula $\forall y(y \preceq x \rightarrow B(\bar{z}, y))$. Por hipótese de indução temos $K_B(\bar{z}, y)$. Definimos
$f(\bar{z}, \varepsilon) = K_B(\bar{z}, \varepsilon)$
$$f(\bar{z}, S(x)) = \begin{cases} f(\bar{z}, x) & se \quad K_B(\bar{z}, S(x)) = 1 \\ 0 & se \quad K_B(\bar{z}, S(x)) = 0. \end{cases}$$

Seja $\leq_l$ a ordem lexicográfica, i.e. $x \leq_l y$ abrevia $(x \preceq y \wedge \neg(x \equiv y)) \vee$ $\vee (x \equiv y \wedge \exists z \subseteq x(z0 \subseteq x \wedge z1 \subseteq y)) \vee (x = y)$. É fácil provar, por indução "lenta" em x, que $\forall y(y \leq_l x \rightarrow B(\bar{z}, y)) \longleftrightarrow f(\bar{z}, x) = 1$. Logo, visto $y \preceq x \longleftrightarrow y \leq_l 1 \times x$, temos que $\forall y(y \preceq x \rightarrow B(\bar{z}, y)) \longleftrightarrow f(\bar{z}, 1 \times x) = 1$.

Tomando $K_A(\bar{z}, x)$ como sendo $K_{=}(1, f(\bar{z}, 1 \times x))$ temos o pretendido. ■

Corolário 2 *Dadas matrizes decidíveis em espaço polinomial $A_1(\bar{x}), \ldots, A_n(\bar{x})$ e símbolos funcionais $f_1(\bar{x}), \ldots, f_n(\bar{x}), f_{n+1}(\bar{x})$, existe um símbolo funcional $f(\bar{x})$ tal que,*
$PSCA \vdash (A_1(\bar{x}) \wedge f(\bar{x}) = f_1(\bar{x})) \vee (\neg A_1(\bar{x}) \wedge A_2(\bar{x}) \wedge f(\bar{x}) = f_2(\bar{x})) \vee \ldots$
$\ldots \vee (\neg A_1(\bar{x}) \wedge \ldots \wedge \neg A_n(\bar{x}) \wedge f(\bar{x}) = f_{n+1}(\bar{x}))$.

Dem. O corolário resulta imediatamente do lema e proposição anteriores. ■

Lema 2 *Para cada matriz decidível em espaço polinomial $A(\bar{z},x)$ existe um símbolo funcional g em $\mathcal{L}_{PS}\backslash\mathcal{L}$ tal que,*
$PSCA \vdash (\exists y \preceq xA(\bar{z},y)) \rightarrow g(\bar{z},x) \preceq x \wedge A(\bar{z},g(\bar{z},x)).$

Dem. Seja

$$f(\bar{z},\varepsilon)=\begin{cases}\varepsilon & se\ \ A(\bar{z},\varepsilon)\\ 1 & caso\ contr\acute{a}rio\end{cases}$$

$$f(\bar{z},S(y))=\begin{cases}f(\bar{z},y) & se\ \ f(\bar{z},y)\preceq y\\ S(y) & se\ \ f(\bar{z},y)\not\preceq y \text{ e } A(\bar{z},S(y))\\ S(y)1 & se\ \ f(\bar{z},y)\not\preceq y \text{ e } \neg A(\bar{z},S(y)).\end{cases}$$

Como função limitativa podemos tomar $1\times y11$. Seja $g(\bar{z},x) := f(\bar{z},1\times x)$. Pode provar-se, por indução "lenta" em y, que $f(\bar{z},y)\preceq y \rightarrow A(\bar{z},f(\bar{z},y))$. Logo, visto $g(\bar{z},y)\preceq y \rightarrow g(\bar{z},y)\preceq 1\times y$ vem que (*) $g(\bar{z},y)\preceq y \rightarrow A(\bar{z},g(\bar{z},y))$. Novamente por um raciocínio de indução "lenta", desta vez em x, pode provar-se que $(\exists y \leq_l x\ A(\bar{z},y)) \rightarrow f(\bar{z},x)\preceq x$. Como $y\preceq x \rightarrow y \leq_l 1\times x$ e $g(\bar{z},x)\preceq 1\times x \rightarrow$ $\rightarrow g(\bar{z},x)\preceq x$, vem que (**) $(\exists y\preceq x\ A(\bar{z},y)) \rightarrow g(\bar{z},x)\preceq x$.

De (*) e (**) conclui-se o pretendido. ∎

Proposição 6 *Seja M um modelo de $PSCA$ e N uma subestrutura de M.*

As matrizes decidíveis em espaço polinomial são absolutas entre N e M, i.e. se $A(\bar{x})$ é uma matriz decidível em espaço polinomial e $\bar{a}$ são elementos em N então $N\models A(\bar{a})$ sse $M\models A(\bar{a})$.

Dem. A demonstração é feita por indução na complexidade de A.

Todos os casos são triviais à excepção das quantificações limitadas. Suponhamos que $A(\bar{z},x)$ tem a forma $\forall y \preceq xB(\bar{z},y)$. Sejam $\bar{a}$ e b elementos em N. Queremos provar que $N\models A(\bar{a},b)$ sse $M\models A(\bar{a},b)$.

Se $M\models A(\bar{a},b)$, usando a hipótese de indução e o facto de N ser subestrutura de M, temos que $N\models A(\bar{a},b)$.

Reciprocamente, suponhamos que $M\not\models A(\bar{a},b)$, logo $M\models \exists y\preceq b(\neg B(\bar{a},y))$. Pelo lema anterior, sabemos que existe um símbolo funcional g em $\mathcal{L}_{PS}\backslash\mathcal{L}$ tal que $M\models g(\bar{a},b)\preceq b$ e $M\not\models B(\bar{a},g(\bar{a},b))$. Como $g(\bar{a},b)$ está em N, usando a hipótese de indução, temos $N\models g(\bar{a},b)\preceq b \wedge (\neg B(\bar{a},g(\bar{a},b)))$ ou seja $N\not\models A(\bar{a},b)$.

O caso $\exists y\preceq xB(\bar{z},y)$ num sentido é óbvio e no outro torna-se imediato usando o lema anterior. ∎

Proposição 7 *Se M é um modelo de $PSCA$ e N é uma subestrutura de M, então N é um modelo de $PSCA$.*

Dem. Obviamente os axiomas básicos e os axiomas definidores são válidos em N. Vejamos que os axiomas de indução também se verificam em N. Seja A uma matriz decidível em espaço polinomial e a um elemento em N. Como M é modelo de $PSCA$ é fácil ver que $M \models A(\varepsilon) \wedge \forall y \subseteq a(A(y) \rightarrow A(y0) \wedge A(y1)) \rightarrow A(a)$, o que implica, visto as matrizes decidíveis em espaço polinomial serem absolutas entre M e N e a ser um elemento arbitrário de N, que $N \models A(\varepsilon) \wedge \forall x(A(x) \rightarrow A(x0) \wedge A(x1)) \rightarrow$ $\rightarrow \forall x A(x)$. Logo os axiomas de indução na notação para matrizes decidíveis em espaço polinomial são válidos em N.

$\therefore N$ é modelo de $PSCA$. ∎

Observação 9 *Por um resultado bem conhecido de Lós e Tarski*[‡], *que garante que uma teoria é preservada por subestruturas sse é constituída por axiomas universais, vemos que* $PSCA$ *é uma teoria universal.*

Recordemos o Teorema de Herbrand (1930), cuja demonstração pode ser encontrada no livro [5] "*Handbook of Proof Theory*" num artigo de Samuel Buss.

Teorema 1 (Herbrand) *Seja* T *uma teoria axiomatizada por fórmulas puramente universais. Suponhamos que* $T \models (\forall \bar{x})\exists y_1 ... \exists y_k B(\bar{x}, \bar{y})$ *com* $B(\bar{x}, \bar{y})$ *uma fórmula sem quantificações.*

Então existe uma sequência finita de termos $t_{i,j} = t_{i,j}(\bar{x})$ *com* $1 \leq i \leq r$ *e* $1 \leq j \leq k$ *tal que* $T \vdash (\forall \bar{x})(\bigvee_{i=1}^{r} B(\bar{x}, t_{i,1}, ..., t_{i,k}))$.

Estamos agora em condições de caracterizar as funções demonstravelmente totais de $PSCA$.

Teorema 2 *Suponhamos que* $PSCA \vdash \forall \bar{x} \exists y A(\bar{x}, y)$, *onde* A *é uma matriz decidível em espaço polinomial sendo* $\bar{x}$ *e* y *as suas únicas variáveis livres.*

Então existe um símbolo funcional f *de* $\mathcal{L}_{PS}$ *tal que* $PSCA \vdash \forall \bar{x} A(\bar{x}, f(\bar{x}))$.

Dem. Tendo em conta a observação 9, a proposição 5 e o corolário 2, a demonstração do teorema resulta imediatamente do Teorema de Herbrand. ∎

[‡]Esse resultado pode ser encontrado, por exemplo, no livro [6] "*Model Theory*" de Chang e Keisler.

Capítulo 4
FUNDAMENTOS DA ARITMÉTICA COMPUTÁVEL EM ESPAÇO POLINOMIAL II

4.1 Teoria $\Sigma_1^{1,b}$-NIA

Relembremos que notamos por $\mathcal{L}_2^b$ a linguagem de 2^a ordem (com variáveis de 1^a ordem x, y, z,... e variáveis de 2^a ordem $F^t, G^r, \ldots$ com t, r,... termos de $\mathcal{L}$) que resulta de $\mathcal{L}$ adicionando $\in$ (símbolo relacional binário que opera entre um termo de $\mathcal{L}$ e uma variável de 2^a ordem). Com $t \in F^s$ pretende-se significar que a palavra representada pelo termo t pertence ao subconjunto finito de $2^{<\omega}$ representado por F^s.

O propósito principal desta secção é definir uma teoria de 2^a ordem em $\mathcal{L}_2^b$, que será notada por $\Sigma_1^{1,b}$-NIA ('NIA' é o acrónimo para *Notation Induction Axioms*) que corresponde à teoria U_2^1 introduzida por Buss em [4] e que desempenhará um papel fundamental no nosso trabalho. Para isso precisamos da seguinte definição.

Definição 18 *Uma **fórmula** $\Sigma_1^{1,b}$ é uma fórmula de $\mathcal{L}_2^b$ da forma:*
$$\exists F_1^{t_1} \ldots \exists F_k^{t_k} \varphi(F_1^{t_1}, \ldots, F_k^{t_k}, \bar{p}, \bar{G}^r)$$
onde φ é uma fórmula de $\mathcal{L}_2^b$ sem quantificações de 2^a ordem e em que todas as quantificações de 1^a ordem são limitadas, i.e. φ é uma fórmula $\Sigma_0^{1,b}$.

Definição 19 $\Sigma_1^{1,b}$**-NIA** *é a teoria de 2^a ordem, na linguagem $\mathcal{L}_2^b$, constituída pelos seguintes axiomas:*

- ***Axiomas básicos.****

- $\forall y \forall F^t (y \in F^t \rightarrow y \preceq t)$

  onde t é um termo em que y não ocorre.

- ***Esquema de compreensão para fórmulas*** $\Sigma_0^{1,b}$*:*

  $\forall x \exists F^x \forall y \preceq x (y \in F^x \longleftrightarrow A(y))$

  onde A é uma fórmula $\Sigma_0^{1,b}$ que pode ter outras variáveis livres além de y mas em que a variável F^x não ocorre.

- ***Esquema de indução na notação para fórmulas*** $\Sigma_1^{1,b}$*:*

  $B(\varepsilon) \wedge \forall x (B(x) \rightarrow B(x0) \wedge B(x1)) \rightarrow \forall x B(x)$

  onde B é uma fórmula $\Sigma_1^{1,b}$ que pode ter outras variáveis livres além de x.

- ***Esquema de substituição para fórmulas*** $\Sigma_0^{1,b}$*:*

*São os primeiros 14 axiomas da definição 17, apresentados aquando da descrição da teoria PSCA.

$\forall x \preceq t \exists F^q \varphi(x, F^q) \rightarrow \exists G^{(tq'1)(tq'1)} \forall x \preceq t\ \bar{\varphi}(x, G^{(tq'1)(tq'1)})$
onde φ é uma fórmula $\Sigma_0^{1,b}$ que pode ter outras variáveis livres além de x e F^q, t é um termo onde x não ocorre, $q' := q(t/x)$[†] *e $\bar{\varphi}$ se obtém de φ substituindo todas as ocorrências de $s \in F^q$ por $< x, s > \in G^{(tq'1)(tq'1)}$.*[‡]

4.2 Alguns resultados em $\Sigma_1^{1,b}$-NIA

Definição 20 *Uma* ***fórmula*** **$\Sigma_1^{1,b}$-estendida** *é uma fórmula de $\mathcal{L}_2^b$ que pode ser construída num número finito de passos, começando por fórmulas $\Sigma_0^{1,b}$ e permitindo conjunções, disjunções, quantificações limitadas de 1ª ordem e quantificações existenciais de 2ª ordem.*

Proposição 8 *Em $\Sigma_1^{1,b}$-NIA uma fórmula $\Sigma_1^{1,b}$-estendida é equivalente a uma fórmula $\Sigma_1^{1,b}$.*

Dem. Comecemos por observar que dois quantificadores existenciais de 2ª ordem podem ser transformados num só, do seguinte modo:

$$\exists F^t \exists H^q \varphi(F^t, H^q) \longleftrightarrow \exists G^{(1tq1)(1tq1)} \bar{\varphi}(G^{(1tq1)(1tq1)})$$

onde $\bar{\varphi}$ se obtém de φ substituindo todas as ocorrências de $s \in F^t$ por $< \varepsilon, s > \in G^{(1tq1)(1tq1)}$ e as ocorrências de $s \in H^q$ por $< 0, s > \in G^{(1tq1)(1tq1)}$.

Estudemos o caso da fórmula $\Sigma_1^{1,b}$-*estendida* ser da forma $\forall x \preceq t \exists F^q \varphi(x, F^q)$ com φ uma fórmula $\Sigma_0^{1,b}$. Pelo esquema de substituição temos que $\forall x \preceq t \exists F^q \varphi(x, F^q) \rightarrow \exists G^{(tq'1)(tq'1)} \forall x \preceq t\ \bar{\varphi}(x, G^{(tq'1)(tq'1)})$ onde $\bar{\varphi}$ se obtém de φ substituindo todas as ocorrências de $s \in F^q$ por $< x, s > \in G^{(tq'1)(tq'1)}$. Como a implicação contrária também é válida e $\exists G^{(tq'1)(tq'1)} \forall x \preceq t\ \bar{\varphi}$ é uma fórmula $\Sigma_1^{1,b}$ temos o pretendido.

Os restantes casos são triviais. ■

Como consequência da proposição anterior temos o corolário que enunciamos de seguida e que garante que em $\Sigma_1^{1,b}$-NIA é válida a indução na notação para fórmulas $\Sigma_1^{1,b}$-*estendidas*.

Corolário 3 $\Sigma_1^{1,b}$-$NIA \vdash B(\varepsilon) \wedge \forall x (B(x) \rightarrow B(x0) \wedge B(x1)) \rightarrow \forall x B(x)$
onde B é uma fórmula $\Sigma_1^{1,b}$-estendida.

[†] $q' := q(t/x)$ significa que q' é o termo que se obtém de q substituindo todas as ocorrências de x pelo termo t.

[‡] Por $< x, s >$ representamos a codificação de (x, s) feita do seguinte modo:
$< x, s > = (cod(x))11(cod(s))$ onde
$cod(\varepsilon) = \varepsilon$
$cod(x0) = cod(x)01_{|11 \times x1}$
$cod(x1) = cod(x)10_{|11 \times x1}$.
$< x, s > \in G^{(tq'1)(tq'1)}$ é a abreviação de $\exists u \preceq (xs1)(xs1)\ (H_{<,>}(x, s, u) \wedge u \in G^{(tq'1)(tq'1)})$ onde $H_{<,>}$ é a fórmula $\Sigma_0^{1,b}$ de $\mathcal{L}_2^b$, da primeira proposição em Apêndice, que existe visto a codificação $<,>$ ser feita em $PTIME$. Logo o axioma está na linguagem $\mathcal{L}_2^b$.

Para facilitar a notação vamos introduzir mais algumas abreviações.

- Escrevemos $n \in T$ para abreviar $n = 1 \times n$. Um n nestas condições é usualmente designado por número unário ou de talha (tally), sendo T conhecido como o conjunto dos números unários.
- Escrevemos $\forall n \in T\ \varphi$ para abreviar $\forall n(n \in T \rightarrow \varphi)$.
- Escrevemos $\forall x \equiv n\ \varphi$ para abreviar $\forall x(x \equiv n \rightarrow \varphi)$.
- Escrevemos $x \prec y$ para abreviar $x \preceq y \wedge \neg(x \equiv y)$.
- Escrevemos $x \notin F^q$ para abreviar $\neg(x \in F^q)$.
- Escrevemos $\exists^1 x\varphi(x)$ para abreviar $\exists x(\varphi(x) \wedge \forall y(\varphi(y) \rightarrow y = x))$.
- Dados $m, n \in T$ com $m \preceq n$, escrevemos $n \dot{-} m = x$ para abreviar $x \in T \wedge$ $\wedge mx = n$ e escrevemos $x \equiv n \dot{-} m$ para abreviar $\exists y \preceq n(y = n \dot{-} m \wedge x \equiv y)$.

Observação 10 *É fácil convencermo-nos que "indução na notação $\rightarrow$ indução em talha (indução tally)", onde por indução em talha entendemos o seguinte esquema:*
$\varphi(\varepsilon) \wedge \forall n \in T(\varphi(n) \rightarrow \varphi(n1)) \rightarrow \forall n \in T\varphi(n)$.
Logo temos que $\Sigma_1^{1,b}$*-NIA* $\vdash \varphi(\varepsilon) \wedge \forall n \in T(\varphi(n) \rightarrow \varphi(n1)) \rightarrow \forall n \in T\varphi(n)$ *onde* φ *é uma fórmula* $\Sigma_1^{1,b}$*-estendida.*

Lema 3 *Se na definição 19 substituirmos os dois últimos esquemas (indução na notação para fórmulas* $\Sigma_1^{1,b}$ *e substituição para fórmulas* $\Sigma_0^{1,b}$*) por indução na notação para fórmulas* $\Sigma_1^{1,b}$*-estendidas, continua válido o esquema de substituição para fórmulas* $\Sigma_0^{1,b}$*.*

Dem. Suponhamos que $\forall x \preceq y \exists F^q \varphi(x, F^q)$, com φ uma fórmula $\Sigma_0^{1,b}$. Queremos provar que $\exists G^{(yq'1)(yq'1)} \forall x \preceq y\ \bar{\varphi}(x, G^{(yq'1)(yq'1)})$, onde $q' := q(y/x)$ e $\bar{\varphi}$ se obtém de φ substituindo todas as ocorrências de $s \in F^q$ por $< x, s > \in G^{(yq'1)(yq'1)}$.

Fixemos y. Seja $m := 1 \times y$ e $r := (yq'1)(yq'1)$. Provemos, por indução em talha em $n \preceq m$, que $\forall n \preceq m \forall z \equiv m \dot{-} n \exists G^r \forall x \preceq m(z \subseteq x \rightarrow \bar{\varphi}(x, G^r))$.

Para $n = \varepsilon$, fixando $z \equiv m \dot{-} n$, basta tomar $G^r = \{< z, \omega >: \omega \in F^q\}$ sendo F^q o conjunto que verifica $\varphi(z, F^q)$ que existe por hipótese.

Suponhamos que, por hipótese de indução, para um certo $n \prec m$ arbitrário, se tem $\forall z \equiv m \dot{-} n \exists G^r \forall x \preceq m(z \subseteq x \rightarrow \bar{\varphi}(x, G^r))$. Queremos provar que se verifica que $\forall z \equiv m \dot{-} (n1) \exists G^r \forall x \preceq m(z \subseteq x \rightarrow \bar{\varphi}(x, G^r))$.

Seja $z \equiv m \dot{-} (n1)$. Por hipótese de indução, visto $z0$ e $z1$ terem comprimento $m \dot{-} n$, existem G_0^r e G_1^r tais que $\forall x \preceq m(z0 \subseteq x \rightarrow \bar{\varphi}(x, G_0^r))$ e $\forall x \preceq m(z1 \subseteq x \rightarrow$ $\rightarrow \bar{\varphi}(x, G_1^r))$. Definindo G^r como sendo $(G_0^r \cap \{< u, v >: z0 \subseteq u \wedge u \preceq r \wedge v \preceq r\}) \cup$ $\cup (G_1^r \cap \{< u, v >: z1 \subseteq u \wedge u \preceq r \wedge v \preceq r\}) \cup \{< z, \omega >: \omega \in F^q\}$ sendo F^q o conjunto que verifica $\varphi(z, F^q)$ que existe por hipótese, temos o que se pretende. Provámos, assim, por indução em talha, que $\forall n \preceq m \forall z \equiv m \dot{-} n \exists G^r \forall x \preceq m(z \subseteq x \rightarrow \bar{\varphi}(x, G^r))$.

Tomando $n = m$ temos que $\exists G^r \forall x \preceq m\bar{\varphi}(x, G^r)$ logo, visto $y \equiv m$, temos $\exists G^r \forall x \preceq y\bar{\varphi}(x, G^r)$. ∎

Observação 11 *À semelhança da teoria U_2^1 de Buss, também poderíamos, na definição de $\Sigma_1^{1,b}$-NIA ter substituído os dois últimos esquemas (indução na notação para fórmulas $\Sigma_1^{1,b}$ e substituição para fórmulas $\Sigma_0^{1,b}$) pelo esquema de indução na notação para fórmulas $\Sigma_1^{1,b}$-estendidas. O motivo por que o não fizemos, optando assim por uma descrição da teoria aparentemente mais complicada, prende-se com o facto de facilitar algumas demonstrações no decorrer deste trabalho.*

Definição 21 *Uma* ***fórmula*** $\mathbf{\Pi_1^{1,b}}$ *é uma fórmula de $\mathcal{L}_2^b$ da forma:*
$\forall F_1^{t_1}...\forall F_k^{t_k}\varphi(F_1^{t_1},...,F_k^{t_k},\bar{p},\bar{G}^r)$
onde φ é uma fórmula de $\mathcal{L}_2^b$ sem quantificações de 2ª ordem e em que todas as quantificações de 1ª ordem são limitadas, i.e. φ é uma fórmula $\Sigma_0^{1,b}$.

À semelhança do que fizemos para as fórmulas $\Sigma_1^{1,b}$, também definimos uma ***fórmula*** $\mathbf{\Pi_1^{1,b}}$**-estendida** *como sendo uma fórmula de $\mathcal{L}_2^b$ que pode ser construída num número finito de passos, começando por fórmulas $\Sigma_0^{1,b}$ e permitindo conjunções, disjunções, quantificações limitadas de 1ª ordem e quantificações universais de 2ª ordem.*

Definição 22 *Uma fórmula $\Sigma_1^{1,b}$ (respectivamente $\Sigma_1^{1,b}$-estendida), ϕ, é* $\mathbf{\Delta_1^{1,b}}$ *(respectivamente* $\mathbf{\Delta_1^{1,b}}$**-estendida***) em $\Sigma_1^{1,b}$-NIA se existir uma fórmula $\Pi_1^{1,b}$ (respectivamente $\Pi_1^{1,b}$-estendida), ψ, tal que $\Sigma_1^{1,b}$-$NIA \vdash \phi \longleftrightarrow \psi$.*

Lema 4 $\Sigma_1^{1,b}$-$NIA \vdash \neg\exists x(A(x) \wedge B(x)) \rightarrow$
$$\rightarrow \forall n \in T\exists F^n \forall x \equiv n((A(x) \rightarrow x \in F^n) \wedge (B(x) \rightarrow x \notin F^n))$$
com A e B fórmulas $\Pi_1^{1,b}$-estendidas.

Dem. Suponhamos que $\neg\exists x(A(x) \wedge B(x))$. Queremos provar que se tem que $\forall n \in T\exists F^n\forall x \equiv n((A(x) \rightarrow x \in F^n) \wedge (B(x) \rightarrow x \notin F^n))$. Fixemos n elemento de talha. Vamos demonstrar, por indução em talha para fórmulas $\Sigma_1^{1,b}$-*estendidas* em $m \preceq n$, que:
$$\forall m \preceq n \underbrace{\forall x' \equiv n\dot{-}m \exists F^n \forall x \equiv n(x' \subseteq x \rightarrow ((A(x) \rightarrow x \in F^n) \wedge (B(x) \rightarrow x \notin F^n)))}_{(*)}.$$

Para $m = \varepsilon$ basta pensar em $F^n = \{x'\}$ se $A(x')$ e $F^n = \varnothing$ se $\neg A(x')$.

Suponhamos que, por hipótese de indução, (*) se verifica para certo $m \prec n$. Queremos ver que $\forall x' \equiv n\dot{-}m1\exists F^n\forall x \equiv n(x' \subseteq x \rightarrow ((A(x) \rightarrow x \in F^n) \wedge (B(x) \rightarrow x \notin F^n)))$. Seja $x' \equiv n\dot{-}m1$. Ora $x'0$ e $x'1$ têm comprimento $n\dot{-}m$, logo, por hipótese de indução, existem F_0^n e F_1^n que verificam $\forall x \equiv n(x'0 \subseteq x \rightarrow ((A(x) \rightarrow x \in F_0^n) \wedge (B(x) \rightarrow x \notin F_0^n)))$ e $\forall x \equiv n(x'1 \subseteq x \rightarrow ((A(x) \rightarrow x \in F_1^n) \wedge (B(x) \rightarrow x \notin F_1^n)))$ respectivamente.

Seja $F^n = (F_0^n \cap \{x : x \equiv n \wedge x'0 \subseteq x\}) \cup (F_1^n \cap \{x : x \equiv n \wedge x'1 \subseteq x\})$. Vejamos que $\forall x \equiv n(x' \subseteq x \rightarrow ((A(x) \rightarrow x \in F^n) \wedge (B(x) \rightarrow x \notin F^n)))$. Seja $x \equiv n$ e suponhamos que $x' \subseteq x$. Como $\neg(x' \equiv x)$ temos que $x'0 \subseteq x$ ou $x'1 \subseteq x$. Se $x'0 \subseteq x$ então $(A(x) \rightarrow x \in F_0^n) \wedge (B(x) \rightarrow x \notin F_0^n)$. Logo $A(x) \rightarrow x \in F^n$. Se $x'1 \subseteq x$ então $(A(x) \rightarrow x \in F_1^n) \wedge (B(x) \rightarrow x \notin F_1^n)$. Logo $A(x) \rightarrow x \in F^n$. Vejamos agora que

$B(x) \rightarrow x \notin F^n$. Suponhamos que temos $B(x)$ e $x \in F^n$. Sem perda de generalidade, seja $x \in F_0^n \cap \{x : x \equiv n \wedge x'0 \subseteq x\}$. Logo $x \notin F_0^n$, visto se ter $B(x)$, o que é absurdo. Logo $B(x) \rightarrow x \notin F^n$.

Provámos assim que
$\forall x' \equiv n \dot{-} m1 \exists F^n \forall x \equiv n(x' \subseteq x \rightarrow ((A(x) \rightarrow x \in F^n) \wedge (B(x) \rightarrow x \notin F^n)))$. Logo, pela indução em talha atrás referida, temos (*) sempre que $m \preceq n$.

Em particular, para $m = n$ temos que
$\exists F^n \forall x \equiv n((A(x) \rightarrow x \in F^n) \wedge (B(x) \rightarrow x \notin F^n))$. ∎

O resultado que se segue estabelece a validade do esquema de separação para fórmulas $\Pi_1^{1,b}$*-estendidas*.

Proposição 9 $\Sigma_1^{1,b}$*-NIA* $\vdash \neg\exists x(A(x) \wedge B(x)) \rightarrow$
$\rightarrow \forall \omega \exists F^\omega \forall x \preceq \omega((A(x) \rightarrow x \in F^\omega) \wedge (B(x) \rightarrow x \notin F^\omega))$
onde A *e* B *são fórmulas* $\Pi_1^{1,b}$*-estendidas.*

Dem. Consideremos $<_l$ a ordem linear (ordem lexicográfica) em $2^{<\omega}$ definida por $x <_l y \Longleftrightarrow (x \preceq y \wedge \neg(x \equiv y)) \vee (x \equiv y \wedge \exists z \subseteq x(z0 \subseteq x \wedge z1 \subseteq y))$.

Como referido no artigo [10] de Fernando Ferreira "*A Feasible Theory for Analysis*", em modelos de Σ_1^b*-NIA* é possível introduzir a operação $+_l$ que vem da anterior ordem linear e que verifica as seguintes propriedades:

P_1) Σ_1^b*-NIA* $\vdash x \preceq a \rightarrow (0 \times a1) +_l x \equiv a1 \wedge (0 \times a1) +_l x \neq 1 \times a1$

P_2) Σ_1^b*-NIA* $\vdash \omega \equiv a1 \rightarrow \omega = 1 \times a1 \vee \exists^1 x \preceq a\ (0 \times a1) +_l x = \omega$.

Logo em $\Sigma_1^{1,b}$*-NIA* tais propriedades continuam válidas.

Suponhamos que $\neg\exists x(A(x) \wedge B(x))$. Queremos ver que $\forall \omega \exists F^\omega \forall x \preceq \omega((A(x) \rightarrow$ $\rightarrow x \in F^\omega) \wedge (B(x) \rightarrow x \notin F^\omega))$. Fixemos ω. Seja $n := 1 \times \omega 1$. Sejam $A'(y)$ a fórmula $\exists x \prec n\ ((0 \times n) +_l x = y \wedge A(x))$ e $B'(y)$ a fórmula $\exists x \prec n\ ((0 \times n) +_l x = y \wedge B(x))$. Como $\neg\exists x(A(x) \wedge B(x))$ temos que $\neg\exists y(A'(y) \wedge B'(y))$. Logo pelo lema anterior $\exists F^n \forall y \equiv n((A'(y) \rightarrow y \in F^n) \wedge (B'(y) \rightarrow y \notin F^n))$.

Seja $F^\omega := \{x \prec n : (0 \times n) +_l x \in F^n\}$. Seja $x \preceq w$. Se temos $A(x)$ temos $A'((0 \times n) +_l x)$, logo $(0 \times n) +_l x \in F^n$. Portanto $x \in F^\omega$. Se temos $B(x)$ temos $B'((0 \times n) +_l x)$, logo $(0 \times n) +_l x \notin F^n$. Portanto $x \notin F^\omega$. ∎

A proposição seguinte garante que, em $\Sigma_1^{1,b}$*-NIA*, se tem compreensão para fórmulas $\Delta_1^{1,b}$*-estendidas*.

Proposição 10 $\Sigma_1^{1,b}$*-NIA* $\vdash \forall x(A(x) \longleftrightarrow B(x)) \rightarrow$
$\rightarrow \forall \omega \exists F^\omega \forall x \preceq \omega\ (x \in F^\omega \longleftrightarrow A(x))$
onde A *é uma fórmula* $\Sigma_1^{1,b}$*-estendida e* B *é uma fórmula* $\Pi_1^{1,b}$*-estendida.*

Dem. Suponhamos que $\forall x(A(x) \longleftrightarrow B(x))$. Queremos mostrar que se tem que $\forall \omega \exists F^\omega \forall x \preceq \omega\ (x \in F^\omega \longleftrightarrow A(x))$.

Fixemos ω. B e $\neg A$ são fórmulas $\Pi_1^{1,b}$*-estendidas*. Por hipótese $\forall x(A(x) \longleftrightarrow$ $\longleftrightarrow B(x))$, logo temos que $\neg\exists x(B(x) \wedge \neg A(x))$ e portanto a proposição anterior garante que $\exists F^\omega \forall x \preceq \omega((B(x) \to x \in F^\omega) \wedge (\neg A(x) \to x \notin F^\omega))$. Assim constatamos que $\exists F^\omega \forall x \preceq \omega((A(x) \to x \in F^\omega) \wedge (x \in F^\omega \to A(x)))$.

$\therefore \exists F^\omega \forall x \preceq \omega(A(x) \longleftrightarrow x \in F^\omega)$. ■

Proposição 11 *Em $\Sigma_1^{1,b}$-NIA é válida indução "lenta" para fórmulas $\Delta_1^{1,b}$-estendidas.*

Dem. Queremos provar que $\forall x(A(x) \longleftrightarrow B(x)) \to$
$\to ((A(\varepsilon) \wedge \forall x(A(x) \to A(S(x))) \to \forall x A(x))$ com A uma fórmula $\Sigma_1^{1,b}$-*estendida* e B uma fórmula $\Pi_1^{1,b}$-*estendida*.

Suponhamos que $\forall x(A(x) \longleftrightarrow B(x))$ e $A(\varepsilon) \wedge \forall x(A(x) \to A(S(x)))$. Vejamos que $\forall x A(x)$. Fixemos x. Seja $\omega := x1$. De $\forall x(A(x) \longleftrightarrow B(x))$ temos, por compreensão para fórmulas $\Delta_1^{1,b}$-*estendidas*, que $\exists F^\omega \forall y \preceq \omega(A(y) \longleftrightarrow y \in F^\omega)$.

Seja $\psi(z) := z \in F^\omega \vee \omega \preceq z$. Temos $\psi(\varepsilon)$ e $\forall z(\psi(z) \to \psi(S(z)))$. Ora sabe-se que em $\Sigma_1^{1,b}$-NIA é válida indução "lenta" para fórmulas $\Sigma_0^{1,b}$ (ver dissertação de Buss [4]) logo $\forall z \psi(z)$. Em particular temos $\psi(x)$ e uma vez que $\neg(\omega \preceq x)$ vem $x \in F^\omega$, logo temos $A(x)$. ■

Proposição 12 *O esquema de minimização para fórmulas $\Delta_1^{1,b}$-estendidas é válido em $\Sigma_1^{1,b}$-NIA, i.e. $\Sigma_1^{1,b}$-$NIA \vdash \exists x A(x) \to \exists x(A(x) \wedge \forall y < x \neg A(y))$, com A uma fórmula $\Delta_1^{1,b}$-estendida.*[§]

Dem. Sendo A uma fórmula $\Delta_1^{1,b}$-*estendida* temos que $\forall y < x \neg A(y)$ é equivalente a uma fórmula $\Delta_1^{1,b}$-*estendida*, logo pela proposição anterior temos indução "lenta" para $B(x) :\longleftrightarrow \forall y < x \neg A(y)$, i.e. $B(\varepsilon) \wedge \forall x(B(x) \to B(S(x))) \to \forall x B(x)$.

Suponhamos que $\exists x A(x)$. Seja b tal que $A(b)$. Queremos provar que $\exists x(A(x) \wedge \forall y < x \neg A(y))$.

Se $\forall y < b \neg A(y)$, b é o elemento pretendido.

Se $\neg(\forall y < b \neg A(y))$, i.e. $\neg B(b)$, como temos $B(\varepsilon)$ vem que $\neg(\forall x(B(x) \to$
$\to B(S(x))))$. Logo $\exists x(B(x) \wedge \neg B(S(x)))$ ou seja $\exists x((\forall y < x \neg A(y)) \wedge$
$\wedge (\exists y < S(x) A(y)))$. Temos portanto que $\exists x(\forall y < x \neg A(y) \wedge A(x))$. ■

4.3 Imersão de PSCA em $\Sigma_1^{1,b}$-NIA

À semelhança do primeiro resultado em apêndice, que permite "introduzir" em Σ_1^b-NIA[¶] os símbolos funcionais de $\mathcal{L}_{PT}$, i.e. as funções computáveis em tempo polinomial, através de fórmulas em $\mathcal{L}$ apropriadas, vamos estabelecer um resultado análogo, agora no contexto da teoria $\Sigma_1^{1,b}$-NIA e com os símbolos funcionais de $\mathcal{L}_{PS}$, ou seja com as funções computáveis em espaço polinomial.

[§]O símbolo $<$ corresponde ao símbolo $<_l$ introduzido anteriormente e é o correspondente em $\Sigma_1^{1,b}$-NIA à relação $<$ da teoria S_2^1 de Buss. (Notar que a teoria Σ_1^b-NIA definida em apêndice e S_2^1 são bi-interpretáveis considerando a bijecção da Fig.1.)

[¶]Teoria de 1ª ordem definida em apêndice.

Proposição 13 *Para cada símbolo funcional* f *de* $\mathcal{L}_{PS} \setminus \mathcal{L}$ *existem uma fórmula* $\Sigma_1^{1,b}$*-estendida* φ_f^Σ *em* $\mathcal{L}_2^b$ *e um termo* b_f *em* $\mathcal{L}$ *tais que:*

$\Sigma_1^{1,b}\text{-}NIA \vdash \forall \bar{x} \exists z \preceq b_f(\bar{x})\ \varphi_f^\Sigma(\bar{x}, z)$

$\Sigma_1^{1,b}\text{-}NIA \vdash \varphi_f^\Sigma(\bar{x}, z) \wedge \varphi_f^\Sigma(\bar{x}, y) \rightarrow z = y$

e

a) em $\Sigma_1^{1,b}$*-NIA tem-se que*

1. $\varphi_E^\Sigma(x, \varepsilon)$

2. $\varphi_{P_i^n}^\Sigma(x_1, ..., x_n, x_i)$ *com* $1 \leq i \leq n$

3. $\varphi_{C_0}^\Sigma(x, x0)$

4. $\varphi_{C_1}^\Sigma(x, x1)$

5. $\varphi_Q^\Sigma(x, y, 1) \longleftrightarrow x \subseteq y$

$\varphi_Q^\Sigma(x, y, 0) \vee \varphi_Q^\Sigma(x, y, 1)$

b)

1. se f *é definida a partir de* $g, h_1, ..., h_k$ *por composição então*

$\Sigma_1^{1,b}\text{-}NIA \vdash \varphi_{h_1}^\Sigma(\bar{x}, y_1) \wedge ... \wedge \varphi_{h_k}^\Sigma(\bar{x}, y_k) \wedge \varphi_g^\Sigma(y_1, ..., y_k, z) \rightarrow \varphi_f^\Sigma(\bar{x}, z)$

2. se f *é definida a partir de* g, h_0 *e* h_1 *por recursão limitada na notação com limite* t *então*

$\Sigma_1^{1,b}\text{-}NIA \vdash \varphi_g^\Sigma(\bar{x}, z) \rightarrow \varphi_f^\Sigma(\bar{x}, \varepsilon, z)$

$\Sigma_1^{1,b}\text{-}NIA \vdash \varphi_f^\Sigma(\bar{x}, y, r) \wedge \varphi_{h_0}^\Sigma(\bar{x}, y, r, u) \wedge z = u_{|t(\bar{x}, y)} \rightarrow \varphi_f^\Sigma(\bar{x}, y0, z)$

$\Sigma_1^{1,b}\text{-}NIA \vdash \varphi_f^\Sigma(\bar{x}, y, r) \wedge \varphi_{h_1}^\Sigma(\bar{x}, y, r, u) \wedge z = u_{|t(\bar{x}, y)} \rightarrow \varphi_f^\Sigma(\bar{x}, y1, z)$

3. se f *é definida a partir de* g *e* h *por recursão limitada com limite* t *então*

$\Sigma_1^{1,b}\text{-}NIA \vdash \varphi_g^\Sigma(\bar{x}, z) \rightarrow \varphi_f^\Sigma(\bar{x}, \varepsilon, z)$

$\Sigma_1^{1,b}\text{-}NIA \vdash \varphi_f^\Sigma(\bar{x}, y, r) \wedge \varphi_h^\Sigma(\bar{x}, y, r, u) \wedge z = u_{|t(\bar{x}, y)} \rightarrow \varphi_f^\Sigma(\bar{x}, S(y), z).$

Dem. A demonstração é feita por indução na complexidade da descrição do símbolo funcional f. Nos casos em que f é uma função inicial ou resulta de composição ou de recursão limitada na notação, a demonstração é análoga à da primeira proposição em apêndice e pode ser encontrada no artigo [8] "*Polynomial Time Computable Arithmetic*" de Fernando Ferreira.

Resta estudar o caso em que f resulta de recursão limitada (b. 3).

Para facilitar a notação vamos considerar que $\mathcal{L}_2^b$ contém todos os símbolos funcionais de $\mathcal{L}_{PT}$ (possível pela proposição 19 em apêndice).

Na demonstração da proposição 9, introduzimos em $\Sigma_1^{1,b}$-NIA, $<_l$ e $+_l$, que em $2^{<\omega}$ "correspondem" respectivamente a $<$ e $+$ em $\mathbb{N}$ (considerando a bijecção da Fig.1 do primeiro capítulo). $<_l$ e $+_l$ passarão a ser notados por $<$ e $+$. Como S_2^1 (teoria introduzida por Buss na tese [4] "Bounded Arithmetic") e Σ_1^b-NIA (teoria definida em apêndice) são bi-interpretáveis de forma natural, além de $<$ e $+$, podem ser introduzidas em $\Sigma_1^{1,b}$-NIA a relação $\leq$ e as operações $-$ e $\cdot$, que "correspondem" à relação de menor ou igual, à subtracção truncada[‖] e ao produto em $\mathbb{N}$ (considerando

[‖]Subtracção truncada, $-_t$, é a seguinte operação em $\mathbb{N}$:

$$x -_t y := \begin{cases} x - y & se \quad x \geq y \\ 0 & se \quad x < y \end{cases}$$

a bijecção da Fig.1). Por exemplo em $2^{<\omega}$

• $x - y = z$ significa que z é a palavra que, segundo a bijecção anterior, corresponde ao número natural que resulta da subtracção dos números correspondentes às palavras x e y;

• $2 \cdot x = y$ significa que y é a palavra que corresponde ao dobro do número correspondente à palavra x;

• $x - 1$ poderia ser ambíguo, uma vez que poderiamos considerar 1 como número natural ou como elemento de $2^{<\omega}$ (que corresponde ao número natural 2). Para evitar a ambiguidade convencionamos que nesta situação 1 é o número natural que corresponde à palavra 0.

Sendo T o conjunto dos números unários, pensemos na bijecção:

$$\begin{array}{ccc} T & \rightarrow & \mathbb{N} \\ \varepsilon & \mapsto & 0 \\ 1 & \mapsto & 1 \\ 11 & \mapsto & 2 \\ 111 & \mapsto & 3 \\ & \ldots & \end{array}$$

Através desta bijecção, das operações usuais de adição e subtracção truncada em $\mathbb{N}$, surgem operações análogas em T, que serão notadas por $\dot{+}$ e $\dot{-}$ respectivamente. Sendo n um elemento de talha, $n \neq \varepsilon$, notamos por 2^n a palavra $\underbrace{0........0}_{|n\dot{-}1|\ vezes}1$. Notamos por 2^ε a palavra 0.

Temos que $\forall y \exists^1 n \in T(2^{n\dot{-}1} \leq y < 2^n)$. Notemos por $\phi(y)$ tal n. Sendo f definida por recursão limitada a partir de g e h, com limite t, queremos encontrar uma fórmula de $\mathcal{L}_2^b$, $\Sigma_1^{1,b}$-*estendida*, φ_f^Σ, e um termo de $\mathcal{L}$, b_f, nas condições do enunciado.

Temos que $f(\bar{x}, \varepsilon) = g(\bar{x}) \preceq b_g(\bar{x})$ e $f(\bar{x}, S(y)) \preceq t(\bar{x}, y)$. Seja $t'(\bar{x}, n) = b_g(\bar{x}) \frown t(\bar{x}, 2^n)$. Temos que $\forall n \in T \forall y < 2^n(f(\bar{x}, y) \preceq t'(\bar{x}, n))$. Seja $cod(\varepsilon) = \varepsilon$, $cod(x0) = cod(x)01$, $cod(x1) = cod(x)10$. Definamos $q(\bar{x}, n)$ como sendo $t'(\bar{x}, n) \frown t'(\bar{x}, n)$. Temos que $\forall n \in T \forall y < 2^n\ cod(f(\bar{x}, y)) \preceq q(\bar{x}, n)$.

Com vista a definir φ_f^Σ vamos introduzir algumas abreviações.

• $seq(F^\theta) := \forall i \preceq \theta(2 \cdot i \in F^\theta \rightarrow 2 \cdot i + 1 \notin F^\theta)$. A ideia é que, colocando 1 ou 0 conforme as palavras pertençam ou não a F^θ, se obtenha uma sequência de códigos: $cod(f(\bar{x}, 0))$, $cod(f(\bar{x}, 1))$, $cod(f(\bar{x}, 2)), ...,$ $cod(f(\bar{x}, y))$, intercalados com pares de zeros de modo a uniformizar os comprimentos dos códigos, formando uma sequência de blocos de comprimento sempre igual ao comprimento de $q(\bar{x}, n)$.

• $lh(\varepsilon) = \varepsilon$, $lh(x0) = lh(x1) = S(lh(x))$, i.e. $lh(x)$ é a palavra que através da bijecção da Fig.1 corresponde ao comprimento de x.

• $bit(x, k, j) := k \leq lh(x) - 1 \wedge (\exists y \subseteq x\ (lh(y) = k \wedge y0 \subseteq x) \rightarrow j = 0) \wedge (\exists y \subseteq x\ (lh(y) = k \wedge y1 \subseteq x) \rightarrow j = 1) \wedge x \neq \varepsilon$. "$x$ tem na posição k o número binário j".

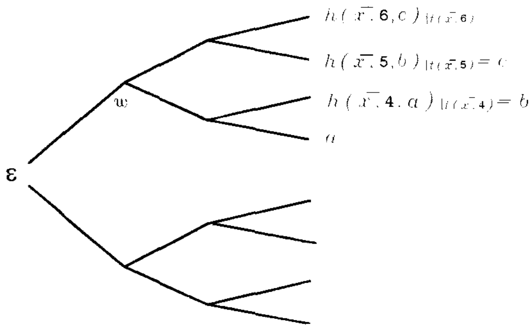
• $bit(F^\theta, k, j) := (k \notin F^\theta \wedge j = 0) \vee (k \in F^\theta \wedge j = 1)$. "$F^\theta$ tem na posição k o número binário j."

• $pal(w,i,F^\theta,\bar{x},n) := n \in T \wedge \forall k \leq (i+1)\cdot lh(q(\bar{x},n)) - 1(i\cdot lh(q(\bar{x},n)) \leq k \rightarrow ((bit(F^\theta,k,0) \longleftrightarrow bit(w,k - i\cdot lh(q(\bar{x},n)),0)) \wedge (bit(F^\theta,k,1) \longleftrightarrow bit(w,k - i\cdot lh(q(\bar{x},n)),1))) \wedge w \equiv q(\bar{x},n)$. "$w$ é a *i-ésima* palavra (bloco) gerado por F^θ."

• $sig(w,z) := \exists z' \subseteq^* w(w = zz' \wedge z' = 0 \times z' \wedge (bit(z,lh(z)-1,0) \rightarrow bit(z,lh(z)-2,1)) \wedge \exists i \leq lh(z)\exists j \leq lh(z')(lh(z) = 2\cdot i \wedge lh(z') = 2\cdot j)$.
"z é a parte significativa de w, i.e. sendo w um bloco gerado por F^θ, z é o código."

• $chave(F^\theta,w,a,\bar{x},n) := seq(F^\theta)\wedge\exists r \equiv q(\bar{x},n)\exists t \preceq q(\bar{x},n)pal(r,0,F^\theta,\bar{x},n)\wedge sig(r,t)\wedge cod(a) = t\wedge\forall i < 2^{n\dot{-}(1\times w)}-1(\exists v \equiv q(\bar{x},n)\, pal(v,i,F^\theta,\bar{x},n) \rightarrow \exists u,u',v' \preceq q(\bar{x},n)\exists p,r \preceq t'(\bar{x},n)\exists s \preceq b_h(\bar{x},\underbrace{(w \frown (0\times(n\dot{-}(1\times w)))) - (2^n-1)+i}_{j},r)$
$(pal(u,i+1,F^\theta,\bar{x},n) \wedge sig(u,u') \wedge sig(v,v') \wedge cod(r) = v' \wedge \varphi_h^\Sigma(\bar{x},j,r,s)\wedge s_{|t(\bar{x},j)} = p \wedge cod(p) = u')$.

"Nas partes significativas dos primeiros $2^{n\dot{-}(1\times w)}$ blocos gerados por F^θ temos os códigos de $a, \underbrace{h(\bar{x},j,a)_{|t(\bar{x},j)}}_{b}, h(\bar{x},j+1,b)_{|t(\bar{x},j+1)},\ldots$ respectivamente." Por exemplo, quando w é a palavra 1 temos os códigos das palavras apresentadas na figura que se segue.



Seja $\theta := 2^{\phi(y)}\cdot lh(q(\bar{x},\phi(y))) - 1$ definimos $\varphi_f^\Sigma(\bar{x},y,z)$ como sendo a fórmula $\exists F^\theta\exists z' \preceq b_g(\bar{x})\varphi_g^\Sigma(\bar{x},z')\wedge chave(F^\theta,\varepsilon,z',\bar{x},\phi(y))\wedge\exists r \equiv q(\bar{x},\phi(y))\,(pal(r,y,F^\theta,\bar{x},\phi(y))\wedge sig(r,cod(z)))$ e $b_f(\bar{x},y)$ como sendo $t'(\bar{x},\phi(y))$.

Vejamos agora que φ_f^Σ e b_f satisfazem o pretendido.

Começamos por demonstrar o seguinte facto:

$\boxed{\forall\bar{x}\forall n \in T\forall w \preceq n\forall a \preceq t'(\bar{x},n)\exists F^\theta chave(F^\theta,w,a,\bar{x},n)}$ com $\theta = 2^n\cdot lh(q(\bar{x},n)) - 1$.

Fixemos $\bar{x}$ e n. Queremos ver que $\forall w \preceq n\forall a \preceq t'(\bar{x},n)\exists F^\theta chave(F^\theta,w,a,\bar{x},n)$.

Provemos por indução em talha em m, para fórmulas $\Sigma_1^{1,b}$-*estendidas*, que $\forall m \subseteq n\forall w \equiv n\dot{-}m\forall a \preceq t'(\bar{x},n)\exists F^\theta chave(F^\theta,w,a,\bar{x},n)$.

Para $m = \varepsilon$, basta pensar em $F^\theta = \{x : bit(cod(a),x,1)\}$.

Dado $m \subset n$ suponhamos, por hipótese de indução, que $\forall w \equiv n\dot{-}m\forall a \preceq t'(\bar{x},n)\exists F^\theta chave(F^\theta,w,a,\bar{x},n)$.

Queremos provar que $\forall w \equiv n\dot{-}(m\dot{+}1)\forall a \preceq t'(\bar{x},n)\exists F^\theta chave(F^\theta,w,a,\bar{x},n)$.

Seja $w \equiv n\dot{-}(m\dot{+}1)$ e $a \preceq t'(\bar{x}, n)$. Temos que $w0 \equiv n\dot{-}m$, logo, por hipótese de indução, $\exists F_0^\theta chave(F_0^\theta, w0, a, \bar{x}, n)$.

Seja $b \equiv q(\bar{x}, n)$ tal que $pal(b, 2^{n\dot{-}(1\times w0)} - 1, F_0^\theta, \bar{x}, n)$. Sejam b', b'' tais que $b' \preceq q(\bar{x}, n)$, $b'' \preceq t'(\bar{x}, n)$ e $sig(b, b') \wedge cod(b'') = b'$.

Seja $a^* \preceq b_h(\bar{x}, (w1 \frown (0 \times (n\dot{-}(1 \times w1)))) - 2^n, b'')$ tal que $\varphi_h^\Sigma(\bar{x}, (w1 \frown (0 \times (n\dot{-}(1 \times w1)))) - 2^n, b'', a^*)$. Seja $a' = a^*_{|t(\bar{x},(w1\frown(0\times(n\dot{-}(1\times w1))))-2^n)}$, temos que $a' \preceq t'(\bar{x}, n)$. Como $w1 \equiv n\dot{-}m$, por hipótese de indução, vem que $\exists F_1^\theta chave(F_1^\theta, w1, a', \bar{x}, n)$.

Seja $F^\theta = \{i : (i \in F_0^\theta \wedge i \leq 2^{n\dot{-}(1\times w0)} \cdot lh(q(\bar{x}, n)) - 1)\vee$ $\vee(i - 2^{n\dot{-}(1\times w0)} \cdot lh(q(\bar{x}, n)) \in F_1^\theta)\}$. Por construção de F^θ é fácil ver que temos $chave(F^\theta, \omega, a, \bar{x}, n)$.

Provámos assim, por indução, que $\forall m \subseteq n \forall w \equiv n\dot{-}m \forall a \preceq t'(\bar{x}, n) \exists F^\theta$ $chave(F^\theta, w, a, \bar{x}, n)$.

$\therefore \forall w \preceq n \forall a \preceq t'(\bar{x}, n) \exists F^\theta chave(F^\theta, w, a, \bar{x}, n)$.

c.q.d.

Para $w = \varepsilon$ temos que $\forall a \preceq t'(\bar{x}, n) \exists F^\theta chave(F^\theta, \varepsilon, a, \bar{x}, n)$, logo $\exists F^\theta \exists z' \preceq b_g(\bar{x}) \varphi_g^\Sigma(\bar{x}, z') \wedge chave(F^\theta, \varepsilon, z', \bar{x}, n)$.

(*) $\therefore \forall \bar{x} \forall n \in T \exists F^\theta \exists z' \preceq b_g(\bar{x}) \varphi_g^\Sigma(\bar{x}, z') \wedge chave(F^\theta, \varepsilon, z', \bar{x}, n)$.

Provemos agora que

$$\boxed{\Sigma_1^{1,b}\text{-}NIA \vdash \forall \bar{x} \forall y \exists z \preceq b_f(\bar{x}, y)\ \varphi_f^\Sigma(\bar{x}, y, z)}$$

Fixemos $\bar{x}$ e y. Seja $n = \phi(y)$. Logo $2^{n\dot{-}1} \leq y < 2^n$.

Por (*) sabemos que $\exists F^\theta \exists z' \preceq b_g(\bar{x}) \varphi_g^\Sigma(\bar{x}, z') \wedge chave(F^\theta, \varepsilon, z', \bar{x}, n)$.

Seja $z^* \equiv q(\bar{x}, n)$ tal que $pal(z^*, y, F^\theta, \bar{x}, n)$, que existe por definição de *chave*. Seja $z \preceq t'(\bar{x}, n)$ tal que $sig(z^*, cod(z))$, (existe por definição de *chave*). Logo temos que $\exists z \preceq b_f(\bar{x}, y)\ \varphi_f^\Sigma(\bar{x}, y, z)$.

c.q.d.

Demonstremos, de seguida, que

$$\boxed{\Sigma_1^{1,b}\text{-}NIA \vdash \varphi_f^\Sigma(\bar{x}, y, z_1) \wedge \varphi_f^\Sigma(\bar{x}, y, z_2) \rightarrow z_1 = z_2}$$

Dados $\bar{x}$ e y, seja $n = \phi(y)$. De $\varphi_f^\Sigma(\bar{x}, y, z_1)$ temos que $\exists F_1^\theta \exists z' \preceq b_g(\bar{x}) \varphi_g^\Sigma(\bar{x}, z') \wedge$ $\wedge chave(F_1^\theta, \varepsilon, z', \bar{x}, n) \wedge \exists r \equiv q(\bar{x}, n)\, pal(r, y, F_1^\theta, \bar{x}, n) \wedge sig(r, cod(z_1))$. De $\varphi_f^\Sigma(\bar{x}, y, z_2)$ temos que $\exists F_2^\theta \exists z'' \preceq b_g(\bar{x}) \varphi_g^\Sigma(\bar{x}, z'') \wedge chave(F_2^\theta, \varepsilon, z'', \bar{x}, n) \wedge \exists r' \equiv q(\bar{x}, n)$ $pal(r', y, F_2^\theta, \bar{x}, n) \wedge sig(r', cod(z_2))$. $\varphi_g^\Sigma(\bar{x}, z') \wedge \varphi_g^\Sigma(\bar{x}, z'') \rightarrow z' = z''$, logo temos $chave(F_2^\theta, \varepsilon, z', \bar{x}, n)$.

Vejamos por indução lenta em i, para fórmulas $\Sigma_0^{1,b}$, que $\forall i \leq y \forall w \preceq q(\bar{x}, n)\ (pal(w, i, F_1^\theta, \bar{x}, n) \longleftrightarrow pal(w, i, F_2^\theta, \bar{x}, n))$.

Caso $i = 0$.

Se $pal(w_1, 0, F_1^\theta, \bar{x}, n)$ e $pal(w_2, 0, F_2^\theta, \bar{x}, n)$ então existem $t_1, t_2 \preceq q(\bar{x}, n)$ tais que $sig(w_1, t_1) \wedge sig(w_2, t_2) \wedge cod(z') = t_1 \wedge cod(z') = t_2$, logo $t_1 = t_2$ e portanto $w_1 = w_2$.

Dado $i < y$ suponhamos, por hipótese de indução, que
$\forall w \preceq q(\bar{x}, n)\ (pal(w, i, F_1^\theta, \bar{x}, n) \longleftrightarrow pal(w, i, F_2^\theta, \bar{x}, n))$. Queremos provar que
$\forall w \preceq q(\bar{x}, n)\ (pal(w, i+1, F_1^\theta, \bar{x}, n) \longleftrightarrow pal(w, i+1, F_2^\theta, \bar{x}, n))$.

Suponhamos que $pal(w_1, i{+}1, F_1^\theta, \bar{x}, n)$, $pal(w_2, i{+}1, F_2^\theta, \bar{x}, n)$ e $pal(v, i, F_1^\theta, \bar{x}, n)$. Sendo $sig(v, v')$ e $cod(v'') = v'$; $sig(w_1, w_1')$ e $cod(w_1'') = w_1'$ temos que $w_1'' = s_{|t(\bar{x},i)}$ com $\varphi_h^\Sigma(\bar{x}, \underbrace{0 \times n - (2^n - 1) + i}_{i}, v'', s)$. Por hipótese de indução temos $pal(v, i, F_2^\theta, \bar{x}, n)$. Logo sendo $sig(w_2, w_2')$ e $cod(w_2'') = w_2'$ temos $w_2'' = s_{|t(\bar{x},i)}$. Logo $w_1'' = w_2''$.

$\therefore\ w_1' = w_2'$ e $w_1 = w_2$.

Em particular temos que $\forall w \preceq q(\bar{x}, n)\ (pal(w, y, F_1^\theta, \bar{x}, n) \longleftrightarrow pal(w, y, F_2^\theta, \bar{x}, n))$.

$\therefore\ r = r'$. Como $sig(r, cod(z_1))$ e $sig(r', cod(z_2))$ temos que $cod(z_1) = cod(z_2)$.

$\therefore\ z_1 = z_2$.

c.q.d.

Vejamos que

$$\boxed{\Sigma_1^{1,b}\text{-}NIA \vdash \varphi_g^\Sigma(\bar{x}, z) \to \varphi_f^\Sigma(\bar{x}, \varepsilon, z)}$$

Suponhamos que $\varphi_g^\Sigma(\bar{x}, z)$. Fixemos $y \geq \varepsilon$ e seja $n = \phi(y)$. Por (*) $\exists F^\theta \exists z' \preceq b_g(\bar{x}) \varphi_g^\Sigma(\bar{x}, z') \wedge chave(F^\theta, \varepsilon, z', \bar{x}, n)$. $\varphi_g^\Sigma(\bar{x}, z) \wedge \varphi_g^\Sigma(\bar{x}, z') \to z = z'$. Logo $\exists F^\theta \exists z \preceq b_g(\bar{x}) \varphi_g^\Sigma(\bar{x}, z) \wedge chave(F^\theta, \varepsilon, z, \bar{x}, n)$.

Seja $w \equiv q(\bar{x}, n)$ tal que $pal(w, 0, F^\theta, \bar{x}, n)$. Então $sig(w, cod(z))$. Temos, portanto, $\varphi_f^\Sigma(\bar{x}, \varepsilon, z)$.

c.q.d.

Provemos finalmente que

$$\boxed{\Sigma_1^{1,b}\text{-}NIA \vdash \varphi_f^\Sigma(\bar{x}, y, r) \wedge \varphi_h^\Sigma(\bar{x}, y, r, u) \wedge z = u_{|t(\bar{x},y)} \to \varphi_f^\Sigma(\bar{x}, S(y), z)}$$

Dados $\bar{x}, y$, seja $n = \phi(y)$, logo $2^{n \dot{-} 1} \leq y < 2^n$.

De $\varphi_f^\Sigma(\bar{x}, y, r)$ temos que $\exists F_1^\theta \exists z' \preceq b_g(\bar{x}) \varphi_g^\Sigma(\bar{x}, z') \wedge chave(F_1^\theta, \varepsilon, z', \bar{x}, n) \wedge$
$\wedge \exists s \equiv q(\bar{x}, n)\ pal(s, y, F_1^\theta, \bar{x}, n) \wedge sig(s, cod(r))$.

Suponhamos que $\varphi_h^\Sigma(\bar{x}, y, r, u)$ e $z = u_{|t(\bar{x},y)}$.

Se $\underline{y < 2^n - 1}$ fazendo $F^\theta = F_1^\theta$ temos que $\exists F^\theta \exists z' \preceq b_g(\bar{x}) \varphi_g^\Sigma(\bar{x}, z') \wedge$
$\wedge chave(F^\theta, \varepsilon, z', \bar{x}, n)$ e sendo $pal(w, y+1, F^\theta, \bar{x}, n)$, por definição de *chave*, sabemos que $w \equiv q(\bar{x}, n)$ e $sig(w, cod(z))$.

$\therefore\ \varphi_f^\Sigma(\bar{x}, S(y), z)$.

Se $\underline{y = 2^n - 1}$ então $S(y) = 2^n$, logo $\phi(S(y)) = n \dot{+} 1$. Por (*) sabemos que $\exists F_2^\theta \exists z' \preceq b_g(\bar{x}) \varphi_g^\Sigma(\bar{x}, z') \wedge chave(F_2^\theta, \varepsilon, z', \bar{x}, n \dot{+} 1)$.

Vejamos por indução lenta em i, para fórmulas $\Sigma_0^{1,b}$, que
$\forall i < 2^n \forall w_1 \preceq q(\bar{x}, n) \forall w_2 \preceq q(\bar{x}, n \dot{+} 1) \forall v \preceq q(\bar{x}, n \dot{+} 1)(pal(w_1, i, F_1^\theta, \bar{x}, n) \wedge$
$\wedge pal(w_2, i, F_2^\theta, \bar{x}, n \dot{+} 1) \to (sig(w_1, v) \longleftrightarrow sig(w_2, v)))$.

Caso $i = 0$ é imediato, pois se $pal(w_1, 0, F_1^\theta, \bar{x}, n)$ e $pal(w_2, 0, F_2^\theta, \bar{x}, n \dot{+} 1)$, então $sig(w_1, cod(z'))$ e $sig(w_2, cod(z'))$.

Por hipótese de indução, admitamos que o resultado é válido para i, sendo $i < 2^n - 1$. Queremos provar que é válido para $i + 1$.

Suponhamos que $pal(w_1, i+1, F_1^\theta, \bar{x}, n)$ e $pal(w_2, i+1, F_2^\theta, \bar{x}, n\dot{+}1)$. Seja $sig(w_1, v_1)$ e $sig(w_2, v_2)$. Admitamos que $pal(u_1, i, F_1^\theta, \bar{x}, n)$ e $pal(u_2, i, F_2^\theta, \bar{x}, n\dot{+}1)$. Seja $sig(u_1, v)$. Por hipótese de indução temos $sig(u_2, v)$. Suponhamos que $cod(p) = v$. Se $\varphi_h^\Sigma(\bar{x}, i, p, k)$ e $k_{|t(\bar{x},i)} = k'$ então, por definição de *chave*, temos que $cod(k') = v_1$ e $cod(k') = v_2$.

$\therefore v_1 = v_2$.

Provámos assim que
$\forall i < 2^n \forall w_1 \preceq q(\bar{x}, n) \forall w_2 \preceq q(\bar{x}, n\dot{+}1) \forall v \preceq q(\bar{x}, n\dot{+}1)(pal(w_1, i, F_1^\theta, \bar{x}, n) \wedge$
$\wedge pal(w_2, i, F_2^\theta, \bar{x}, n\dot{+}1) \rightarrow (sig(w_1, v) \longleftrightarrow sig(w_2, v)))$.

Logo, sendo $pal(s_2, y, F_2^\theta, \bar{x}, n\dot{+}1)$ temos $sig(s_2, cod(r))$. Por definição de *chave* e visto que $\varphi_h^\Sigma(\bar{x}, y, r, u)$ e $u_{|t(\bar{x},y)} = z$ temos que sendo $pal(w, y+1, F_2^\theta, \bar{x}, n\dot{+}1)$ se tem $sig(w, cod(z))$.

Obviamente $w \equiv q(\bar{x}, n\dot{+}1)$. Logo fazendo $F^\theta = F_2^\theta$ sabemos que
$\exists F^\theta \exists z' \preceq b_g(\bar{x}) \varphi_g^\Sigma(\bar{x}, z') \wedge chave(F^\theta, \varepsilon, z', \bar{x}, n\dot{+}1) \wedge \exists w \equiv q(\bar{x}, n\dot{+}1)$
$pal(w, y+1, F^\theta, \bar{x}, n\dot{+}1) \wedge sig(w, cod(z))$.

$\therefore \varphi_f^\Sigma(\bar{x}, S(y), z)$.

c.q.d.

Concluimos assim a demonstração da proposição. ∎

Observação 12 *Se no enunciado da proposição anterior substituirmos "fórmula $\Sigma_1^{1,b}$-estendida" por "fórmula $\Pi_1^{1,b}$-estendida" o resultado continua válido, bastando tomar $\varphi_f^\Pi(\bar{x}, z)$ como sendo $\forall w \preceq b_f(\bar{x})(\varphi_f^\Sigma(\bar{x}, w) \rightarrow w = z)$.*

Observação 13 *O resultado da proposição anterior pode ser estendido a todos os termos, t, de $\mathcal{L}_{PS}$ de tal modo que:*

a. $\Sigma_1^{1,b}$-$NIA \vdash \forall \bar{x} \exists z \preceq b_t(\bar{x})\ \varphi_t^\Sigma(\bar{x}, z)$

b. $\Sigma_1^{1,b}$-$NIA \vdash \varphi_t^\Sigma(\bar{x}, z) \wedge \varphi_t^\Sigma(\bar{x}, y) \rightarrow z = y$

c. Em $\Sigma_1^{1,b}$-NIA *o seguinte é válido:*

1) $\varphi_\frown^\Sigma(x, y, x \frown y)$

2) $\varphi_\times^\Sigma(x, y, x \times y)$

3) Se $t(\bar{x}) = q(t_1(\bar{x}), ..., t_k(\bar{x}))$, *com* $q, t_1, ...t_k$ *termos de* $\mathcal{L}_{PS}$, *então*
$\Sigma_1^{1,b}$-$NIA \vdash \varphi_{t_1}^\Sigma(\bar{x}, y_1) \wedge ... \wedge \varphi_{t_k}^\Sigma(\bar{x}, y_k) \wedge \varphi_q^\Sigma(y_1, ..., y_k, z) \rightarrow \varphi_t^\Sigma(\bar{x}, z)$.

Estamos agora em condições de demonstrar que, em sentido a seguir especificado, $PSCA \subseteq \Sigma_1^{1,b}$-$NIA$.

Proposição 14 *Todo o modelo M de $\Sigma_1^{1,b}$-NIA pode ser estendido a um modelo M' de $PSCA$ mantendo o domínio de 1ª ordem e as interpretações dos símbolos de $\mathcal{L}$ e definindo a interpretação de cada símbolo funcional f de $\mathcal{L}_{PS} \setminus \mathcal{L}$ segundo φ_f^Σ. Isto é, interpretando f como sendo a função $\{(\bar{a}, b) : M \models \varphi_f^\Sigma(\bar{a}, b)\}$.*

Dem. Pelo estudo anteriormente efectuado, é fácil ver que M' é uma estrutura bem definida e satisfaz os axiomas básicos e os axiomas definidores. Para mostrar que

M' também verifica o esquema de indução é suficiente provar que para toda a matriz decidível em espaço polinomial, $A'(\bar{x})$, existe uma fórmula $\Sigma_1^{1,b}$-*estendida*, $A(\bar{x})$, tal que para todos os parâmetros $\bar{a}$ de M' se tem $M' \vDash A'(\bar{a})$ *sse* $M \vDash A(\bar{a})$.

Como consequência da última observação temos que, para todo o termo t de $\mathcal{L}_{PS}$ e parâmetros $\bar{a}$ e b de M', $M' \vDash t(\bar{a}) = b$ *sse* $M \vDash \varphi_t^{\Sigma}(\bar{a}, b)$. (Pode ser provado por indução na complexidade de t.)

Seja $A'(\bar{x})$ uma matriz decidível em espaço polinomial. Evidentemente $A'(\bar{x})$ é equivalente a uma fórmula que contém uma sequência de quantificações da forma $\forall x \preceq t(\bar{y})$ e/ou $\exists x \preceq t(\bar{y})$ com t um termo de $\mathcal{L}_{PS}$ em que x não ocorre, seguida por uma fórmula aberta na forma normal conjuntiva.**

Vejamos como alterar esta fórmula de modo a pertencer à linguagem $\mathcal{L}_2^b$, criando assim a fórmula $A(\bar{x})$ pretendida.

Substituimos $\forall x \preceq t(\bar{y})...$ por $\exists z \preceq b_t(\bar{y})(\ \varphi_t^{\Sigma}(\bar{y}, z) \wedge \forall x \preceq z...)$ e substituimos $\exists x \preceq t(\bar{y})...$ por $\exists z \preceq b_t(\bar{y})\ (\varphi_t^{\Sigma}(\bar{y}, z) \wedge \exists x \preceq z...)$.

Se em A' aparecem fórmulas atómicas, $t(\bar{x}) = q(\bar{x})$ ou $t(\bar{x}) \subseteq q(\bar{x})$ com t, q termos de $\mathcal{L}_{PS}$ definimos A como tendo $\exists z \preceq b_t(\bar{x})\ (\varphi_t^{\Sigma}(\bar{x}, z) \wedge\ \varphi_q^{\Sigma}(\bar{x}, z))$ ou $\exists z \preceq b_t(\bar{x})$ $\exists w \preceq b_q(\bar{x})\ (\varphi_t^{\Sigma}(\bar{x}, z) \wedge\ \varphi_q^{\Sigma}(\bar{x}, w) \wedge z \subseteq w)$ respectivamente.

Se em A' figuram negações de fórmulas atómicas, $t(\bar{x}) \neq q(\bar{x})$, $\neg(t(\bar{x}) \subseteq q(\bar{x}))$ substituimo-las em A pelas fórmulas $\exists z \preceq b_t(\bar{x})\ \exists \omega \preceq b_q(\bar{x})(\varphi_t^{\Sigma}(\bar{x}, z) \wedge\ \varphi_q^{\Sigma}(\bar{x}, w) \wedge$ $\wedge z \neq w)$, $\exists z \preceq b_t(\bar{x})\ \exists w \preceq b_q(\bar{x})\ (\varphi_t^{\Sigma}(\bar{x}, z) \wedge\ \varphi_q^{\Sigma}(\bar{x}, w) \wedge \neg(z \subseteq w))$ respectivamente. Facilmente se vê que as fórmulas $A(\bar{x})$ assim construídas são fórmulas $\Sigma_1^{1,b}$-*estendidas* que verificam o pretendido. ∎

**Fórmula de $\mathcal{L}_{PS}$, sem quantificadores, que é uma conjunção de disjunções de literais.

Capítulo 5
SISTEMAS BASEADOS NO CÁLCULO DE SEQUENTES

O objectivo principal deste capítulo é apresentar uma caracterização das funções demonstravelmente totais de $\Sigma_1^{1,b}$-NIA. Para tal necessitaremos de definir, com rigor, a nossa sintaxe e as regras de dedução. O sistema de demonstração que vamos adoptar é uma variante do cálculo de sequentes introduzido por Gentzen em 1935, enriquecido com novas regras relacionadas com quantificações de 1^a e 2^a ordem e que continuará a ser notado por LK. A secção que se segue apresenta de forma breve este cálculo de sequentes, estabelecendo as regras de dedução que o regem.

5.1 Cálculo de sequentes

A linguagem adoptada será $\mathcal{L}_2^b$. Em relação às variáveis quer de 1^a, quer de 2^a ordem diremos que ocorrem **mudas** ou **livres**, conforme apareçam ou não quantificadas.

No cálculo sequencial, cada linha numa demonstração é constituída por **sequentes**, i.e. estruturas da forma:

$$A_1, ..., A_k \Longrightarrow B_1, ..., B_r$$

com A_i $(1 \leq i \leq k)$ e B_j $(1 \leq j \leq r)$ fórmulas, tendo o significado intuitivo de que "*a conjunção dos* A_i's *implica a disjunção dos* B_j's". $A_1, ..., A_k$ será chamado o **antecedente** e $B_1, ..., B_r$ o **consequente** do sequente apresentado.

Uma demonstração segundo o sistema do cálculo sequencial LK tem o aspecto de uma árvore, em que os nodos de cima (folhas) são os axiomas, também conhecidos por sequentes iniciais, e em que cada sequente da demonstração que não seja um desses axiomas é inferido do(s) sequente(s) imediatamente acima através das chamadas **Regras de dedução** ou **Regras de inferência**, apresentadas a seguir. Os axiomas de LK são da forma $A \Longrightarrow A$ com A fórmula atómica.

Sendo $\mathcal{S}$ um conjunto de sequentes, podemos permitir que os axiomas sejam também sequentes de $\mathcal{S}$, passando o sistema de sequentes a ser notado por $LK_{\mathcal{S}}$ e as demonstrações neste sistema a serem designadas por $LK_{\mathcal{S}}$-demonstrações.

REGRAS DE INFERÊNCIA

No que se segue, Γ, Π, Λ e Δ denotam conjuntos de fórmulas, A e B fórmulas e t e s termos quaisquer. As regras de dedução são representadas por $\frac{S_1}{S}$ ou $\frac{S_1 \quad\quad S_2}{S}$

indicando que o sequente S se deduz de S_1 ou do par S_1 e S_2.

- **Regras estruturais fracas**

(permutação) p:e $\frac{\Gamma,A,B,\Pi\Longrightarrow\Delta}{\Gamma,B,A,\Pi\Longrightarrow\Delta}$ p:d $\frac{\Gamma\Longrightarrow\Delta,A,B,\Lambda}{\Gamma\Longrightarrow\Delta,B,A,\Lambda}$

(contracção) c:e $\frac{A,A,\Gamma\Longrightarrow\Delta}{A,\Gamma\Longrightarrow\Delta}$ c:d $\frac{\Gamma\Longrightarrow\Delta,A,A}{\Gamma\Longrightarrow\Delta,A}$

(enfraquecimento) e:e $\frac{\Gamma\Longrightarrow\Delta}{A,\Gamma\Longrightarrow\Delta}$ e:d $\frac{\Gamma\Longrightarrow\Delta}{\Gamma\Longrightarrow\Delta,A}$

- **Regra do corte**

$$\frac{\Gamma\Longrightarrow\Delta,A \qquad A,\Gamma\Longrightarrow\Delta}{\Gamma\Longrightarrow\Delta}$$

- **Regras proposicionais**

$\neg$:e $\frac{\Gamma\Longrightarrow\Delta,A}{\neg A,\Gamma\Longrightarrow\Delta}$ $\neg$:d $\frac{A,\Gamma\Longrightarrow\Delta}{\Gamma\Longrightarrow\Delta,\neg A}$

$\wedge$:e $\frac{A,B,\Gamma\Longrightarrow\Delta}{A\wedge B,\Gamma\Longrightarrow\Delta}$ $\wedge$:d $\frac{\Gamma\Longrightarrow\Delta,A \qquad \Gamma\Longrightarrow\Delta,B}{\Gamma\Longrightarrow\Delta,A\wedge B}$

$\vee$:e $\frac{A,\Gamma\Longrightarrow\Delta \qquad B,\Gamma\Longrightarrow\Delta}{A\vee B,\Gamma\Longrightarrow\Delta}$ $\vee$:d $\frac{\Gamma\Longrightarrow\Delta,A,B}{\Gamma\Longrightarrow\Delta,A\vee B}$

$\rightarrow$:e $\frac{\Gamma\Longrightarrow\Delta,A \qquad B,\Gamma\Longrightarrow\Delta}{A\rightarrow B,\Gamma\Longrightarrow\Delta}$ $\rightarrow$:d $\frac{A,\Gamma\Longrightarrow\Delta,B}{\Gamma\Longrightarrow\Delta,A\rightarrow B}$

- **Regras de quantificação**

$\forall$:e $\frac{A(t),\Gamma\Longrightarrow\Delta}{\forall xA(x),\Gamma\Longrightarrow\Delta}$ $\forall$:d $\frac{\Gamma\Longrightarrow\Delta,A(b)}{\Gamma\Longrightarrow\Delta,\forall xA(x)}$

$\exists$:e $\frac{A(b),\Gamma\Longrightarrow\Delta}{\exists xA(x),\Gamma\Longrightarrow\Delta}$ $\exists$:d $\frac{\Gamma\Longrightarrow\Delta,A(t)}{\Gamma\Longrightarrow\Delta,\exists xA(x)}$

$\forall_{\preceq}$:e $\frac{A(t),\Gamma\Longrightarrow\Delta}{t\preceq s,\forall x\preceq sA(x),\Gamma\Longrightarrow\Delta}$ $\forall_{\preceq}$:d $\frac{b\preceq t,\Gamma\Longrightarrow\Delta,A(b)}{\Gamma\Longrightarrow\Delta,\forall x\preceq tA(x)}$

$\exists_{\preceq}$:e $\frac{b\preceq t,A(b),\Gamma\Longrightarrow\Delta}{\exists x\preceq tA(x),\Gamma\Longrightarrow\Delta}$ $\exists_{\preceq}$:d $\frac{\Gamma\Longrightarrow\Delta,A(t)}{t\preceq s,\Gamma\Longrightarrow\Delta,\exists x\preceq sA(x)}$

$\forall_{2^a}$:e $\frac{A(F^t),\Gamma\Longrightarrow\Delta}{\forall X^tA(X^t),\Gamma\Longrightarrow\Delta}$ $\forall_{2^a}$:d $\frac{\Gamma\Longrightarrow\Delta,A(C^t)}{\Gamma\Longrightarrow\Delta,\forall X^tA(X^t)}$

$\exists_{2^a}$:e $\frac{A(C^t),\Gamma\Longrightarrow\Delta}{\exists X^tA(X^t),\Gamma\Longrightarrow\Delta}$ $\exists_{2^a}$:d $\frac{\Gamma\Longrightarrow\Delta,A(F^t)}{\Gamma\Longrightarrow\Delta,\exists X^tA(X^t)}$

com b **variável própria de 1^a ordem** e C^t **variável própria de 2^a ordem**, i.e. variáveis livres que não ocorrem no sequente de baixo.

Observação 14 *Por indução na complexidade da fórmula é fácil ver que, para qualquer fórmula A, o sequente $A \Longrightarrow A$ se deduz em LK, sem usar a regra do corte.*

Proposição 15 *LK prova que* $\forall x \preceq tA(x) \Longrightarrow \forall x(x \preceq t \to A(x))$ *e* $\forall x(x \preceq t \to A(x)) \Longrightarrow \forall x \preceq tA(x)$.

Dem.

$$\dfrac{\dfrac{\dfrac{A(a) \Longrightarrow A(a)}{a \preceq t, \forall x \preceq tA(x) \Longrightarrow A(a)}\;(\forall_{\preceq}\text{:e})}{\forall x \preceq tA(x) \Longrightarrow a \preceq t \to A(a)}\;(\to\text{:d})}{\forall x \preceq tA(x) \Longrightarrow \forall x(x \preceq t \to A(x))}\;(\forall\text{:d})$$

$$\dfrac{\dfrac{\dfrac{a \preceq t \Longrightarrow a \preceq t \qquad A(a) \Longrightarrow A(a)}{a \preceq t \to A(a), a \preceq t \Longrightarrow A(a)}\;(\to\text{:e})^*}{\forall x(x \preceq t \to A(x)), a \preceq t \Longrightarrow A(a)}\;(\forall\text{:e})}{\forall x(x \preceq t \to A(x)) \Longrightarrow \forall x \preceq tA(x)}\;(\forall_{\preceq}\text{:d})$$

■

Observação 15 *De forma análoga se prova que existem LK-demonstrações de* $\exists x \preceq tA(x) \Longrightarrow \exists x(x \preceq t \wedge A(x))$ *e de* $\exists x(x \preceq t \wedge A(x)) \Longrightarrow \exists x \preceq tA(x)$.

O teorema da eliminação do corte, também conhecido por Gentzen's Hauptsatz, é um resultado fundamental do cálculo de sequentes e está na base de grande parte das demonstrações deste capítulo. Com vista a enunciar uma generalização deste teorema, o teorema da eliminação do corte livre em LK_S, necessitamos de apresentar algumas definições.

Definição 23 • *Numa inferência, as fórmulas que ocorrem no sequente de baixo e não estão em* Γ, Δ, Λ *ou* Π *nem são* $t \preceq s$, *são chamadas* ***fórmulas principais***.

• *Numa inferência, as fórmulas* A *e* B *que ocorrem nos sequentes de cima são chamadas* ***fórmulas auxiliares***.

Definição 24 • *Se* C *é a i-ésima fórmula de* Γ, Δ, Λ *ou* Π *que figura na parte de cima de uma inferência, então o* ***descendente imediato*** *de* C *é a ocorrência dessa mesma fórmula na parte de baixo da inferência, ocupando a mesma posição no* Γ, Δ, Λ *ou* Π *respectivo.*

• *Se* C *é uma fórmula auxiliar de qualquer inferência excepto permutação e regra do corte, então a fórmula principal da inferência é o seu* ***descendente imediato***.

---

*Entre parêntesis indicam-se as regras utilizadas. O duplo traço horizontal significa que, além da regra que figura à direita, se utilizaram algumas regras de inferência fracas. Na passagem em questão omitiram-se duas regras de enfraquecimento e duas regras de permutação.

• *Na inferência de permutação, os* ***descendentes imediatos*** *das fórmulas auxiliares* A *e* B *são respectivamente as fórmulas principais* A *e* B.

• *Na regra do corte,* A *não tem* ***descendente imediato.***

• *Nas regras* $\forall_{\preceq}$*:d e* $\exists_{\preceq}$*:e,* $b \preceq t$ *tem como* ***descendente imediato*** *a fórmula principal.*

Definição 25 C *é um* ***ascendente imediato*** *de* D *se* D *for um descendente imediato de* C.

Definição 26 • C *é um* ***ascendente*** *de* D *se existir uma cadeia de ascendentes imediatos de* D *para* C.

• *Um* ***ascendente directo*** *de* D *é um ascendente* C *de* D *tal que* C *é a mesma fórmula que* D.

• *De forma análoga se definem* ***descendentes*** *e* ***descendentes directos.***

Definição 27 *Seja* S *um conjunto de sequentes e seja* P *uma* LK_S*-demonstração.*

• *Uma fórmula que ocorre em* P *diz-se* ***ancorada*** *(por um sequente de* S*) se for um descendente directo de uma fórmula que ocorra num sequente inicial de* S.

• *Uma inferência de corte em* P *diz-se* ***ancorada*** *se pelo menos uma das duas ocorrências da fórmula auxiliar do corte (também conhecida como fórmula do corte) estiver ancorada.*

• *Uma inferência de corte que não esteja ancorada diz-se* ***livre.***

Teorema 3 *(Teorema da Eliminação do Corte Livre)*

Seja S *um conjunto de sequentes fechado para a substituição*†.

Se $\Gamma \Longrightarrow \Delta$ *se deduz em* LK_S *então existe uma demonstração de* $\Gamma \Longrightarrow \Delta$ *em* LK_S *sem cortes livres.*

Dem. A demonstração deste resultado é apresentada no livro [5] *"Handbook of Proof Theory"* no artigo de Samuel Buss e no livro [16] "*Proof Theory*" de Takeuti, bastando acrescentar novos casos para as regras de inferência que adicionámos. ■

5.2 Formulação de $\Sigma_1^{1,b}$-NIA no cálculo de sequentes

A teoria $\Sigma_1^{1,b}$-NIA será formulada no cálculo de sequentes dum modo específico, que passamos a descrever.

O cálculo de sequentes para $\Sigma_1^{1,b}$-NIA, que notaremos por LK_{PS}, além dos sequentes iniciais (axiomas) da forma $A \Longrightarrow A$, com A fórmula atómica, admite ainda os seguintes axiomas:

1) $\Longrightarrow A(\bar{s})$ com A axioma básico de $\Sigma_1^{1,b}$-NIA, e $\bar{s}$ termos quaisquer;

†Um conjunto de sequentes S diz-se fechado para a substituição se sempre que $\Gamma(a) \Longrightarrow \Delta(a)$ está em S, com a uma variável livre de 1^a ordem, também $\Gamma(t) \Longrightarrow \Delta(t)$ está em S, sendo t um termo qualquer.

2) $s \in F^t \Longrightarrow s \preceq t$ em que as variáveis no termo s não ocorrem em t;

3) $\Longrightarrow \exists F^s \forall y \preceq s(y \in F^s \longleftrightarrow A(y))$ com A uma fórmula $\Sigma_0^{1,b}$ em que F^s não ocorre.

Além das regras de inferência usuais para o cálculo de sequentes de 2^a ordem, apresentadas na secção anterior, LK_{PS} contém ainda as seguintes regras:

a) **Regra de indução**

$$\frac{\Gamma, A(a) \Longrightarrow A(a0) \qquad \Gamma, A(a) \Longrightarrow A(a1)}{\Gamma, A(\varepsilon) \Longrightarrow A(s)}$$

onde s é um termo qualquer, a é uma variável própria e A é uma fórmula $\Sigma_1^{1,b}$ que pode ter outras variáveis livres além de a;

b) **Regra de substituição**

$$\frac{\Gamma, a \preceq t \Longrightarrow \exists F^q \varphi(a, F^q)}{\Gamma \Longrightarrow \exists G^{\bar{q}} \forall x \preceq t \bar{\varphi}(x, G^{\bar{q}})}$$

onde a é uma variável própria, φ é uma fórmula $\Sigma_0^{1,b}$ que pode ter outras variáveis livres além de a e F^q, $\bar{q} = (tq'1)(tq'1)$ com $q' = q(t/x)$ e $\bar{\varphi}$ se obtém de φ substituindo todas as ocorrências de $s \in F^q$ por $< x, s > \in G^{\bar{q}}$.

Observação 16 *Obviamente* $\Sigma_1^{1,b}$*-*NIA *pode ser formulada no cálculo de sequentes de Gentzen através de* LK_S *onde* S *é o conjunto de todos os sequentes da forma* $\Longrightarrow A$ *com* A *axioma de* $\Sigma_1^{1,b}$*-*NIA.

Para vermos que LK_{PS} *é ainda uma formulação da teoria* $\Sigma_1^{1,b}$*-*NIA, *basta provar que:*

a) de $\Longrightarrow A(s)$, *com* s *termo qualquer, se obtém* $\Longrightarrow \forall x A(x)$ *e vice-versa;*

b) de $s \in F^t \Longrightarrow s \preceq t$ *se obtém* $\Longrightarrow s \in F^t \rightarrow s \preceq t$ *e vice-versa;*

c) sendo válida a regra de indução temos $\Longrightarrow A(\varepsilon) \wedge \forall x(A(x) \rightarrow A(x0) \wedge \wedge A(x1)) \rightarrow \forall x A(x)$ *e reciprocamente, do sequente anterior segue-se a regra de indução;*

d) sendo válida a regra de substituição temos $\Longrightarrow \forall x \preceq t \exists F^q \varphi(x, F^q) \rightarrow \rightarrow \exists G^{\bar{q}} \forall x \preceq t\ \bar{\varphi}(x, G^{\bar{q}})$ *e reciprocamente, do sequente anterior segue-se a regra de substituição.*

Passemos à demonstração de cada uma das alíneas anteriores.

Dem. *a)* Tendo $\Longrightarrow A(s)$, com s termo qualquer, temos em particular $\Longrightarrow A(a)$.

$$\frac{\Longrightarrow A(a)}{\Longrightarrow \forall x A(x)} \ (\forall\text{:d}).$$

Reciprocamente

$$\frac{\Longrightarrow \forall x A(x) \qquad \dfrac{A(s) \Longrightarrow A(s)}{\forall x A(x) \Longrightarrow A(s)} \ (\forall\text{:e})}{\Longrightarrow A(s)} \ (\textit{corte}).$$

b)

$$\dfrac{s \in F^t \Longrightarrow s \preceq t}{\Longrightarrow s \in F^t \to s \preceq t}\ (\to :\text{d})$$

Reciprocamente

$$\dfrac{\dfrac{\dfrac{\dfrac{s \in F^t \Longrightarrow s \in F^t}{s \in F^t \Longrightarrow s \preceq t, s \in F^t} \qquad \dfrac{s \preceq t \Longrightarrow s \preceq t}{s \preceq t, s \in F^t \Longrightarrow s \preceq t}}{s \in F^t \to s \preceq t, s \in F^t \Longrightarrow s \preceq t}\ (\to :\text{e}) \qquad \Longrightarrow s \in F^t \to s \preceq t}{}\ (\mathit{corte})}{s \in F^t \Longrightarrow s \preceq t}$$

c) Seja P a demonstração do sequente
$S_0)$ $\forall x(A(x) \to A(x0) \wedge A(x1)), A(a) \Longrightarrow A(a0)$

$$\dfrac{\dfrac{\dfrac{A(a) \Longrightarrow A(a)}{A(a) \Longrightarrow A(a0), A(a)} \qquad \dfrac{\dfrac{A(a0) \Longrightarrow A(a0)}{A(a0), A(a1), A(a) \Longrightarrow A(a0)}}{A(a0) \wedge A(a1), A(a) \Longrightarrow A(a0)}}{A(a) \to A(a0) \wedge A(a1), A(a) \Longrightarrow A(a0)}\ (\to :\text{e})}{\forall x(A(x) \to A(x0) \wedge A(x1)), A(a) \Longrightarrow A(a0)}\ (\forall\text{:e})$$

Seja R a demonstração do sequente
$S_1)$ $\forall x(A(x) \to A(x0) \wedge A(x1)), A(a) \Longrightarrow A(a1)$

$$\dfrac{\dfrac{\dfrac{A(a) \Longrightarrow A(a)}{A(a) \Longrightarrow A(a1), A(a)} \qquad \dfrac{\dfrac{A(a1) \Longrightarrow A(a1)}{A(a0), A(a1), A(a) \Longrightarrow A(a1)}}{A(a0) \wedge A(a1), A(a) \Longrightarrow A(a1)}}{A(a) \to A(a0) \wedge A(a1), A(a) \Longrightarrow A(a1)}\ (\to :\text{e})}{\forall x(A(x) \to A(x0) \wedge A(x1)), A(a) \Longrightarrow A(a1)}\ (\forall\text{:e})$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\overbrace{S_0)}^{P} \qquad \overbrace{S_1)}^{R}}{\forall x(A(x) \to A(x0) \wedge A(x1)), A(\varepsilon) \Longrightarrow A(b)}\ \mathit{R.I.}}{\forall x(A(x) \to A(x0) \wedge A(x1)), A(\varepsilon) \Longrightarrow \forall x A(x)}\ (\forall\text{:d})}{A(\varepsilon) \wedge \forall x(A(x) \to A(x0) \wedge A(x1)) \Longrightarrow \forall x A(x)}\ (\wedge\text{:e})}{\Longrightarrow A(\varepsilon) \wedge \forall x(A(x) \to A(x0) \wedge A(x1)) \to \forall x A(x)}\ (\to :\text{d})$$

Reciprocamente, seja $S)$ o sequente
$A(\varepsilon) \wedge \forall x(A(x) \to A(x0) \wedge A(x1)) \Longrightarrow \forall x A(x)$

$$\dfrac{\Longrightarrow A(\varepsilon) \wedge \forall x(A(x) \to A(x0) \wedge A(x1)) \to \forall x A(x) \quad (\text{alínea } b))}{A(\varepsilon) \wedge \forall x(A(x) \to A(x0) \wedge A(x1)) \Longrightarrow \forall x A(x)}$$

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\Gamma, A(a) \Longrightarrow A(a0) \qquad \Gamma, A(a) \Longrightarrow A(a1)}{\Gamma, A(a) \Longrightarrow A(a0) \wedge A(a1)}}{\Gamma \Longrightarrow A(a) \to A(a0) \wedge A(a1)}}{\Gamma \Longrightarrow \forall x(A(x) \to A(x0) \wedge A(x1))} \qquad \dfrac{A(\varepsilon) \Longrightarrow A(\varepsilon)}{A(\varepsilon), \Gamma \Longrightarrow A(\varepsilon)}}{S) \quad A(\varepsilon), \Gamma \Longrightarrow A(\varepsilon) \wedge \forall x(A(x) \to A(x0) \wedge A(x1))}}{\dfrac{A(\varepsilon), \Gamma \Longrightarrow \forall x A(x)}{\Gamma, A(\varepsilon) \Longrightarrow A(s)}}
\qquad
\begin{array}{l} (\wedge\text{:d}) \\ (\to\text{:d}) \\ \\ (\wedge\text{:d}) \\ (\mathit{corte}) \\ (\text{alínea } a)) \end{array}
$$

d)

$$
\dfrac{\dfrac{\dfrac{\exists F^q \varphi(a, F^q) \Longrightarrow \exists F^q \varphi(a, F^q)}{\forall x \preceq t \exists F^q \varphi(x, F^q), a \preceq t \Longrightarrow \exists F^q \varphi(a, F^q)}}{\forall x \preceq t \exists F^q \varphi(x, F^q) \Longrightarrow \exists G^{\bar{q}} \forall x \preceq t \bar{\varphi}(x, G^{\bar{q}})}}{\Longrightarrow \forall x \preceq t \exists F^q \varphi(x, F^q) \to \exists G^{\bar{q}} \forall x \preceq t \bar{\varphi}(x, G^{\bar{q}})}
\qquad
\begin{array}{l} (\forall_{\preceq}\text{:e}) \\ (R.S.) \\ (\to\text{:d}) \end{array}
$$

Reciprocamente, seja $S)$ o sequente $\forall x \preceq t \exists F^q \varphi(x, F^q) \Longrightarrow \exists G^{\bar{q}} \forall x \preceq t \bar{\varphi}(x, G^{\bar{q}})$, que pode ser obtido por:

$$
\dfrac{\Longrightarrow \forall x \preceq t \exists F^q \varphi(x, F^q) \to \exists G^{\bar{q}} \forall x \preceq t \bar{\varphi}(x, G^{\bar{q}}) \quad (\text{alínea } b))}{\forall x \preceq t \exists F^q \varphi(x, F^q) \Longrightarrow \exists G^{\bar{q}} \forall x \preceq t \bar{\varphi}(x, G^{\bar{q}})}
$$

$$
\begin{array}{l} (\forall_{\preceq}\text{:d}) \\ (\mathit{corte}) \end{array}
\quad
\dfrac{\dfrac{\Gamma, a \preceq t \Longrightarrow \exists F^q \varphi(a, F^q)}{\Gamma \Longrightarrow \forall x \preceq t \exists F^q \varphi(x, F^q)} \qquad S)}{\Gamma \Longrightarrow \exists G^{\bar{q}} \forall x \preceq t \bar{\varphi}(x, G^{\bar{q}})}
\quad \blacksquare
$$

Alterando ligeiramente a definição de fórmula ancorada, é fácil vermos que em LK_{PS} ainda é válido o teorema da eliminação do corte livre.

Definição 28 • *As **fórmulas principais** da regra de indução são $A(\varepsilon)$ e $A(s)$ e a **fórmula principal** da regra de substituição é $\exists G^{\bar{q}} \forall x \preceq t \bar{\varphi}(x, G^{\bar{q}})$.*

• *Seja P uma LK_{PS}-demonstração.*

*Uma ocorrência de uma fórmula em P diz-se **ancorada** se for descendente directo de uma fórmula que ocorra num sequente inicial do tipo 1), 2) ou 3)[‡] ou se for descendente directo duma fórmula principal duma inferência de indução ou de substituição.*

• *Com esta noção de fórmula ancorada definimos similarmente a noção de **corte livre** e **corte ancorado**.*

Munidos destas novas definições temos o seguinte teorema, cuja demonstração é análoga à demonstração do teorema da eliminação do corte livre em LK_S.

Teorema 4 *(Teorema da Eliminação do corte livre em LK_{PS})*

Se $\Gamma \Longrightarrow \Delta$ se deduz em LK_{PS} então existe uma demonstração de $\Gamma \Longrightarrow \Delta$ em LK_{PS} sem cortes livres.

[‡]Apresentados aquando da descrição de LK_{PS}.

5.3 Caracterização das funções demonstravelmente totais de $\Sigma_1^{1,b}$-NIA

Com vista a caracterizar as funções demonstravelmente totais de $\Sigma_1^{1,b}$-NIA, começamos por apresentar algumas propriedades de LK_{PS}.

Proposição 16 *Se $LK_{PS} \vdash \Gamma \Longrightarrow \Delta$, com Γ e Δ constituídos por fórmulas $\Sigma_1^{1,b}$, então existe uma LK_{PS}-demonstração de $\Gamma \Longrightarrow \Delta$ em que todos os sequentes da demonstração são constituídos por fórmulas $\Sigma_1^{1,b}$.*

Dem. Seja P uma LK_{PS}-demonstração de $\Gamma \Longrightarrow \Delta$.

Pelo teorema da eliminação do corte livre, existe P^* uma LK_{PS}-demonstração de $\Gamma \Longrightarrow \Delta$ sem cortes livres.

As fórmulas que ocorrem em P^* ou são ascendentes de fórmulas de Γ ou Δ, ou são ascendentes de fórmulas do corte. Sendo ascendentes de fórmulas de Γ ou Δ são fórmulas $\Sigma_1^{1,b}$, isto porque todas as regras à excepção do corte fazem aumentar ou manter a complexidade das fórmulas. Como em P^* todos os cortes são ancorados, as fórmulas do corte que aí figuram estão nos sequentes iniciais do tipo 1), 2) ou 3), ou são fórmulas principais da regra de indução ou de substituição. Em qualquer dos casos são fórmulas $\Sigma_1^{1,b}$, ainda o sendo obviamente os seus ascendentes. ■

Para não sobrecarregar a notação, no resultado que se segue, sempre que não seja indispensável, nas variáveis de 2^a ordem omitimos os termos, por exemplo X^t será representada por X.

Teorema 5 *(Teorema Fundamental)*

Suponhamos que $LK_{PS} \vdash \Gamma \Longrightarrow \Delta$, onde Γ e Δ são constituídos por fórmulas $\Sigma_1^{1,b}$. Seja $\Gamma := \exists\bar{X}\varphi_1(\bar{x},\bar{F},\bar{X}),...,\exists\bar{X}\varphi_n(\bar{x},\bar{F},\bar{X})$, com φ_i fórmulas $\Sigma_0^{1,b}$; $\Delta := \exists\bar{Y}\psi_1(\bar{x},\bar{F},\bar{Y}),...,\exists\bar{Y}\psi_m(\bar{x},\bar{F},\bar{Y})$, com ψ_i fórmulas $\Sigma_0^{1,b}$ e com $\bar{Y} = Y_1,...,Y_k$; $\boldsymbol{\varphi}(\bar{x},\bar{F},\bar{X}) := \bigwedge_{j=1}^{n}\varphi_j$; $\Psi(\bar{x},\bar{F},\bar{Y}) := \bigvee_{i=1}^{m}\psi_i$ e notemos por $\Theta(\bar{x},\bar{F},\bar{X},\bar{Y})$ a fórmula $\boldsymbol{\varphi}(\bar{x},\bar{F},\bar{X}) \to \Psi(\bar{x},\bar{F},\bar{Y})$.

Então existem termos $t_i(\bar{x}) \in \mathcal{L}$ $(1 \le i \le k)$; existem $M_i^{\Sigma}(\omega,\bar{x},\bar{F},\bar{X})$ fórmulas $\Sigma_1^{1,b}$-estendidas $(1 \le i \le k)$; existem $M_i^{\Pi}(\omega,\bar{x},\bar{F},\bar{X})$ fórmulas $\Pi_1^{1,b}$-estendidas $(1 \le i \le k)$ e existem $\Phi_i(\bar{x},\bar{F},\bar{X})$ funcionais de $PSPACE^{\Sigma_0^{1,b}}$ $(1 \le i \le k)$ tais que:

(1) $\Sigma_1^{1,b}$-$NIA \vdash \forall\bar{x}\forall\bar{F}\forall\bar{X}\Theta(\bar{x},\bar{F},\bar{X},\{\omega \preceq t_1(\bar{x}) : M_1^{\Sigma}(\omega,\bar{x},\bar{F},\bar{X})\},...$ $...,\{\omega \preceq t_k(\bar{x}) : M_k^{\Sigma}(\omega,\bar{x},\bar{F},\bar{X})\})$;

(2) $\Sigma_1^{1,b}$-$NIA \vdash \forall\bar{x}\forall\bar{F}\forall\bar{X}\forall\omega \preceq t_i(\bar{x})(M_i^{\Sigma}(\omega,\bar{x},\bar{F},\bar{X}) \longleftrightarrow M_i^{\Pi}(\omega,\bar{x},\bar{F},\bar{X}))$, com $1 \le i \le k$;

(3) $\Phi_i(\bar{x},\bar{F},\bar{X}) = \{\omega \preceq t_i(\bar{x}) : M_i^{\Sigma}(\omega,\bar{x},\bar{F},\bar{X})\}$, com $1 \le i \le k$.

Observação 17 • *Na alínea (1) do teorema anterior, representamos por $\Theta(\bar{x},\bar{F},\bar{X},\{\omega \preceq t_1(\bar{x}) : M_1^{\Sigma}(\omega,\bar{x},\bar{F},\bar{X})\},...)$ a fórmula $\Theta(\bar{x},\bar{F},\bar{X},G_1,...)$ em que sempre que nesta última aparece $r \in G_1$ se substitui por $r \preceq t_1(\bar{x}) \wedge M_1^{\Sigma}(r,\bar{x},\bar{F},\bar{X})$.*

• *Como $\Theta(\bar{x},\bar{F},\bar{X},\bar{Y})$ é uma fórmula $\Sigma_0^{1,b}$, provando que $\Sigma_1^{1,b}$-$NIA \vdash \forall\bar{x}\forall\bar{F}\forall\bar{X}\forall\omega \preceq t_i(\bar{x})(M_i^{\Sigma}(\omega,\bar{x},\bar{F},\bar{X}) \longleftrightarrow M_i^{\Pi}(\omega,\bar{x},\bar{F},\bar{X}))$, com*

$1 \leq i \leq k$, *podemos escrever* $\Theta(\bar{x}, \bar{F}, \bar{X}, \{\omega \preceq t_1(\bar{x}) : M_1^{\Sigma}(\omega, \bar{x}, \bar{F}, \bar{X})\}, \ldots$ $\ldots, \{\omega \preceq t_k(\bar{x}) : M_k^{\Sigma}(\omega, \bar{x}, \bar{F}, \bar{X})\})$ *como uma fórmula* $\Sigma_1^{1,b}$*-estendidas, bastando para o efeito substituir* $r \in G_i$ *por* $r \preceq t_i(\bar{x}) \wedge M_i^{\Sigma}(r, \bar{x}, \bar{F}, \bar{X})$ *e* $r \notin G_i$ *por* $\neg(r \preceq t_i(\bar{x}) \wedge M_i^{\Pi}(r, \bar{x}, \bar{F}, \bar{X}))$. *Analogamente podemos escrever* $\Theta(\bar{x}, \bar{F}, \bar{X}, \{\omega \preceq t_1(\bar{x}) : M_1^{\Sigma}(\omega, \bar{x}, \bar{F}, \bar{X})\}, \ldots, \{\omega \preceq t_k(\bar{x}) : M_k^{\Sigma}(\omega, \bar{x}, \bar{F}, \bar{X})\})$ *como uma fórmula* $\Pi_1^{1,b}$*-estendidas. Sempre que quisermos notar que, na fórmula, a escolha duma ocorrência de* M_i^{Σ} *ou* M_i^{Π} *é feita de modo a que esta seja* $\Sigma_1^{1,b}$*-estendida ou* $\Pi_1^{1,b}$*-estendida, conforme nos seja conveniente, colocamos* $\Theta(\bar{x}, \bar{F}, \bar{X}, \{\omega \preceq t_1(\bar{x}) : M_1^{\Delta}(\omega, \bar{x}, \bar{F}, \bar{X})\}, \ldots, \{\omega \preceq t_k(\bar{x}) : M_k^{\Delta}(\omega, \bar{x}, \bar{F}, \bar{X})\})$.

Dem. Como $LK_{PS} \vdash \Gamma \Longrightarrow \Delta$, com Γ e Δ constituídos por fórmulas $\Sigma_1^{1,b}$, pela proposição anterior existe P, uma LK_{PS}-demonstração de $\Gamma \Longrightarrow \Delta$, em que todos os sequentes da demonstração são constituídos por fórmulas $\Sigma_1^{1,b}$.

Vamos provar por indução no número de linhas da demonstração que, para qualquer sequente $\Pi \Longrightarrow \Lambda$ de P, existem os termos, as fórmulas e os funcionais testemunhas nas condições pretendidas.

• Se $\Pi \Longrightarrow \Lambda$ é um sequente inicial da forma $A \Longrightarrow A$ com A fórmula atómica, ou é um sequente dos tipos 1) ou 2)[§], nada há a demonstrar.

• Se $\Pi \Longrightarrow \Lambda$ é um sequente inicial do tipo 3), i.e. $\Pi \Longrightarrow \Lambda$ tem a forma $\Longrightarrow \exists F^s \forall y \preceq s(y \in F^s \longleftrightarrow A(y, \bar{x}, \bar{X}))$ com A uma fórmula $\Sigma_0^{1,b}$, definimos $M_1^{\Sigma}(\omega, \bar{x}, \bar{X})$ como sendo $A(\omega, \bar{x}, \bar{X})$ que é uma fórmula $\Sigma_0^{1,b}$ logo é $\Sigma_1^{1,b}$-*estendida*; definimos $M_1^{\Pi}(\omega, \bar{x}, \bar{X})$ como sendo $A(\omega, \bar{x}, \bar{X})$ que é uma fórmula $\Sigma_0^{1,b}$ logo é $\Pi_1^{1,b}$-*estendida*; tomamos $t_1 := s$ e $\Phi_1(\bar{x}, \bar{X}) := \{\omega \preceq s : A(\omega, \bar{x}, \bar{X})\}$.

Para vermos que $\Phi_1 \in PSPACE^{\Sigma_0^{1,b}}$ basta pensarmos na máquina de Turing que iniciada com *input's* de 1ª ordem $\bar{x}$ e de 2ª ordem $\bar{X}$, na célula ω da única fita de *output* (que é de 2ª ordem) coloca 1 ou 0 conforme se tenha $\omega \preceq s \wedge A(\omega, \bar{x}, \bar{X})$ ou $\neg(\omega \preceq s \wedge A(\omega, \bar{x}, \bar{X}))$, cuja resposta é dada pelo oráculo visto serem fórmulas $\Sigma_0^{1,b}$. Facilmente constatamos que M_1^{Σ}, M_1^{Π}, t_1 e Φ_1 verificam as condições pretendidas.

• Os casos em que $\Pi \Longrightarrow \Lambda$ se obtém por p:e, p:d, c:e, c:d, e:e, e:d, $\neg$:e, $\neg$:d, $\wedge$:e, $\vee$:d, $\rightarrow$:d, $\forall_{\preceq}$:e, $\exists_{\preceq}$:d e $\exists_{2^a}$:e são triviais.

• Se $\Pi \Longrightarrow \Lambda$ se obtém por $\wedge$:d, $\Pi \Longrightarrow \Lambda$ é da forma $\Gamma' \Longrightarrow \Delta', A \wedge B$. $\left(\frac{\Gamma' \Longrightarrow \Delta', A \qquad \Gamma' \Longrightarrow \Delta', B}{\Gamma' \Longrightarrow \Delta', A \wedge B}\right)$

Como $A \wedge B$ é uma fórmula $\Sigma_1^{1,b}$, temos que A e B são fórmulas $\Sigma_0^{1,b}$.

Por hipótese de indução, para $\Gamma' \Longrightarrow \Delta', A$ existem $M_i'^{\Sigma}(\omega, \bar{x}, \bar{X})$, $M_i'^{\Pi}(\omega, \bar{x}, \bar{X})$, $t_i'(\bar{x})$, $\Phi_i'(\bar{x}, \bar{X})$ nas condições pretendidas e para $\Gamma' \Longrightarrow \Delta', B$ existem $M_i''^{\Sigma}(\omega, \bar{x}, \bar{X})$, $M_i''^{\Pi}(\omega, \bar{x}, \bar{X})$, $t_i''(\bar{x})$, $\Phi_i''(\bar{x}, \bar{X})$ nas condições pretendidas.

Para $\Gamma' \Longrightarrow \Delta', A \wedge B$ fazemos:

$M_i^{\Sigma}(\omega, \bar{x}, \bar{X}) :\longleftrightarrow (A \vee (\omega \preceq t_i' \wedge M_i'^{\Sigma}(\omega, \bar{x}, \bar{X}))) \wedge (\neg A \vee B \vee (\omega \preceq t_i'' \wedge \wedge M_i''^{\Sigma}(\omega, \bar{x}, \bar{X}))) \wedge (\neg A \vee \neg B)$ que é uma fórmula $\Sigma_1^{1,b}$-*estendida*,

§Estes sequentes foram apresentados aquando da formulação de $\Sigma_1^{1,b}$-NIA no cálculo de sequentes LK_{PS}.

$M_i^\Pi(\omega,\bar{x},\bar{X}) :\longleftrightarrow (A \vee (\omega \preceq t_i' \wedge M_i'^\Pi(\omega,\bar{x},\bar{X}))) \wedge (\neg A \vee B \vee (\omega \preceq t_i'' \wedge \wedge M_i''^\Pi(\omega,\bar{x},\bar{X}))) \wedge (\neg A \vee \neg B)$ que é uma fórmula $\Pi_1^{1,b}$-*estendida*,

$t_i := t_i' \frown t_i''$,

$$\Phi_i(\bar{x},\bar{X}) := \begin{cases} \Phi_i'(\bar{x},\bar{X}) & se \quad \neg A \\ \Phi_i''(\bar{x},\bar{X}) & se \quad A \wedge \neg B \\ \emptyset & se \quad A \wedge B \end{cases}.$$

• Se $\Pi \Longrightarrow \Lambda$ se obtém por $\vee$:e, $\Pi \Longrightarrow \Lambda$ é da forma $A \vee B, \Gamma' \Longrightarrow \Delta'$.
$\left(\frac{A,\Gamma' \Longrightarrow \Delta' \qquad B,\Gamma' \Longrightarrow \Delta'}{A \vee B, \Gamma' \Longrightarrow \Delta'}\right)$

Como $A \vee B$ é uma fórmula $\Sigma_1^{1,b}$, temos que A e B são fórmulas $\Sigma_0^{1,b}$.

Por hipótese de indução, para $A, \Gamma' \Longrightarrow \Delta'$ existem $M_i'^\Sigma(\omega,\bar{x},\bar{X})$, $M_i'^\Pi(\omega,\bar{x},\bar{X})$, $t_i'(\bar{x})$, $\Phi_i'(\bar{x},\bar{X})$ nas condições pretendidas e para $B, \Gamma' \Longrightarrow \Delta'$ existem $M_i''^\Sigma(\omega,\bar{x},\bar{X})$, $M_i''^\Pi(\omega,\bar{x},\bar{X})$, $t_i''(\bar{x})$, $\Phi_i''(\bar{x},\bar{X})$ nas condições pretendidas.

Para $A \vee B, \Gamma' \Longrightarrow \Delta'$ fazemos:

$M_i^\Sigma(\omega,\bar{x},\bar{X}) :\longleftrightarrow (\neg A \vee (\omega \preceq t_i' \wedge M_i'^\Sigma(\omega,\bar{x},\bar{X}))) \wedge (A \vee \neg B \vee (\omega \preceq t_i'' \wedge$
$\wedge M_i''^\Sigma(\omega,\bar{x},\bar{X}))) \wedge (A \vee B)$,

$M_i^\Pi(\omega,\bar{x},\bar{X}) :\longleftrightarrow (\neg A \vee (\omega \preceq t_i' \wedge M_i'^\Pi(\omega,\bar{x},\bar{X}))) \wedge (A \vee \neg B \vee (\omega \preceq t_i'' \wedge$
$\wedge M_i''^\Pi(\omega,\bar{x},\bar{X}))) \wedge (A \vee B)$,

$t_i := t_i' \frown t_i''$,

$$\Phi_i(\bar{x},\bar{X}) := \begin{cases} \Phi_i'(\bar{x},\bar{X}) & se \quad A \\ \Phi_i''(\bar{x},\bar{X}) & se \quad \neg A \wedge B \\ \emptyset & se \quad \neg A \wedge \neg B \end{cases}.$$

• Se $\Pi \Longrightarrow \Lambda$ se obtém por $\rightarrow$:e, $\Pi \Longrightarrow \Lambda$ é da forma $A \rightarrow B, \Gamma' \Longrightarrow \Delta'$.
$\left(\frac{\Gamma' \Longrightarrow \Delta', A \qquad B,\Gamma' \Longrightarrow \Delta'}{A \rightarrow B, \Gamma' \Longrightarrow \Delta'}\right)$

Como $A \rightarrow B$ é uma fórmula $\Sigma_1^{1,b}$, temos que A e B são fórmulas $\Sigma_0^{1,b}$.

Por hipótese de indução, para $\Gamma' \Longrightarrow \Delta', A$ existem $M_i'^\Sigma(\omega,\bar{x},\bar{X})$, $M_i'^\Pi(\omega,\bar{x},\bar{X})$, $t_i'(\bar{x})$, $\Phi_i'(\bar{x},\bar{X})$ e para $B, \Gamma' \Longrightarrow \Delta'$ existem $M_i''^\Sigma(\omega,\bar{x},\bar{X})$, $M_i''^\Pi(\omega,\bar{x},\bar{X})$, $t_i''(\bar{x})$, $\Phi_i''(\bar{x},\bar{X})$ nas condições pretendidas.

Para $A \rightarrow B, \Gamma' \Longrightarrow \Delta'$ fazemos:

$M_i^\Sigma(\omega,\bar{x},\bar{X}) :\longleftrightarrow (\neg B \vee (\omega \preceq t_i'' \wedge M_i''^\Sigma(\omega,\bar{x},\bar{X}))) \wedge (B \vee \neg A) \wedge$
$\wedge (B \vee A \vee (\omega \preceq t_i' \wedge M_i'^\Sigma(\omega,\bar{x},\bar{X})))$,

$M_i^\Pi(\omega,\bar{x},\bar{X}) :\longleftrightarrow (\neg B \vee (\omega \preceq t_i'' \wedge M_i''^\Pi(\omega,\bar{x},\bar{X}))) \wedge (B \vee \neg A) \wedge$
$\wedge (B \vee A \vee (\omega \preceq t_i' \wedge M_i'^\Pi(\omega,\bar{x},\bar{X})))$,

$t_i := t_i' \frown t_i''$,

$$\Phi_i(\bar{x},\bar{X}) := \begin{cases} \Phi_i''(\bar{x},\bar{X}) & se \quad B \\ \emptyset & se \quad \neg B \wedge A \\ \Phi_i'(\bar{x},\bar{X}) & se \quad \neg B \wedge \neg A \end{cases}.$$

• Obviamente $\Pi \Longrightarrow \Lambda$ não se pode obter por $\forall$:e, $\forall$:d, $\exists$:e, $\exists$:d, $\forall_{2^a}$:e nem $\forall_{2^a}$:d pois todas as fórmulas na demonstração são $\Sigma_1^{1,b}$.

• Se $\Pi \Longrightarrow \Lambda$ se obtém por $\forall_\preceq$:d, $\Pi \Longrightarrow \Lambda$ é da forma $\Gamma' \Longrightarrow \Delta', \forall x \preceq t A(x)$.
$\left(\frac{b \preceq t, \Gamma' \Longrightarrow \Delta', A(b)}{\Gamma' \Longrightarrow \Delta', \forall x \preceq t A(x)}\right)$

Como $\forall x \preceq t A(x)$ é uma fórmula $\Sigma_1^{1,b}$, temos que $A(x)$ é uma fórmula $\Sigma_0^{1,b}$.

Por hipótese de indução, para $b \preceq t, \Gamma' \Longrightarrow \Delta', A(b)$ existem $M_i'^{\Sigma}(\omega, x, \bar{x}, \bar{X})$, $M_i'^{\Pi}(\omega, x, \bar{x}, \bar{X})$, $t_i'(x, \bar{x})$, $\Phi_i'(x, \bar{x}, \bar{X})$ nas condições pretendidas.

Para $\Gamma' \Longrightarrow \Delta', \forall x \preceq tA(x)$ fazemos:

$M_i^{\Sigma}(\omega, \bar{x}, \bar{X}) :\longleftrightarrow \exists x \preceq t(\neg A(x) \wedge \forall x' < xA(x') \wedge \omega \preceq t_i'(x, \bar{x}) \wedge M_i'^{\Sigma}(\omega, x, \bar{x}, \bar{X}))$,

$M_i^{\Pi}(\omega, \bar{x}, \bar{X}) :\longleftrightarrow \exists x \preceq t(\neg A(x) \wedge \forall x' < xA(x') \wedge \omega \preceq t_i'(x, \bar{x}) \wedge M_i'^{\Pi}(\omega, x, \bar{x}, \bar{X}))$,

$t_i(\bar{x}) := t_i'(t(\bar{x}), \bar{x})$,

$$\Phi_i(\bar{x}, \bar{X}) := \begin{cases} \emptyset & se \quad \forall x \preceq tA(x) \\ \Phi_i'(\mu x \preceq t\neg A(x), \bar{x}, \bar{X}) & se \quad \exists x \preceq t\neg A(x) \end{cases},$$

onde $\mu x \preceq t\neg A(x)$ é o menor elemento, pela ordem lexicográfica, de comprimento menor ou igual que t que verifica $\neg A(x)$.

Facilmente se vê que temos o pretendido, uma vez que, segundo a proposição 12, em $\Sigma_1^{1,b}$-NIA é válido o esquema de minimização para fórmulas $\Delta_1^{1,b}$.

• Se $\Pi \Longrightarrow \Lambda$ se obtém por $\exists_{\preceq}$:e, $\Pi \Longrightarrow \Lambda$ é da forma $\exists x \preceq tA(x), \Gamma' \Longrightarrow \Delta'$.

$\left(\frac{b \preceq t, A(b), \Gamma' \Longrightarrow \Delta'}{\exists x \preceq tA(x), \Gamma' \Longrightarrow \Delta'}\right)$

Como $\exists x \preceq tA(x)$ é uma fórmula $\Sigma_1^{1,b}$, temos que $A(x)$ é uma fórmula $\Sigma_0^{1,b}$.

Por hipótese de indução, para $b \preceq t, A(b), \Gamma' \Longrightarrow \Delta'$ existem $M_i'^{\Sigma}(\omega, x, \bar{x}, \bar{X})$, $M_i'^{\Pi}(\omega, x, \bar{x}, \bar{X})$, $t_i'(x, \bar{x})$, $\Phi_i'(x, \bar{x}, \bar{X})$ nas condições pretendidas.

Para $\exists x \preceq tA(x), \Gamma' \Longrightarrow \Delta'$ fazemos:

$M_i^{\Sigma}(\omega, \bar{x}, \bar{X}) :\longleftrightarrow \exists x \preceq t(A(x) \wedge \forall x' < x\neg A(x') \wedge \omega \preceq t_i'(x, \bar{x}) \wedge M_i'^{\Sigma}(\omega, x, \bar{x}, \bar{X}))$,

$M_i^{\Pi}(\omega, \bar{x}, \bar{X}) :\longleftrightarrow \exists x \preceq t(A(x) \wedge \forall x' < x\neg A(x') \wedge \omega \preceq t_i'(x, \bar{x}) \wedge M_i'^{\Pi}(\omega, x, \bar{x}, \bar{X}))$,

$t_i(\bar{x}) := t_i'(t(\bar{x}), \bar{x})$,

$$\Phi_i(\bar{x}, \bar{X}) := \begin{cases} \emptyset & se \quad \forall x \preceq t\neg A(x) \\ \Phi_i'(\mu x \preceq tA(x), \bar{x}, \bar{X}) & se \quad \exists x \preceq tA(x) \end{cases}.$$

• Se $\Pi \Longrightarrow \Lambda$ se obtém por $\exists_{2^a}$:d, $\Pi \Longrightarrow \Lambda$ é da forma $\Gamma' \Longrightarrow \Delta', \exists F\ A(F)$.

$\left(\frac{\Gamma' \Longrightarrow \Delta', A(Z^q)}{\Gamma' \Longrightarrow \Delta', \exists F A(F)}\right)$

Suponhamos que $\Gamma' := \exists \bar{X}\varphi_1(\bar{x}, \bar{F}, Z^q, \bar{X}), ..., \exists \bar{X}\varphi_n(\bar{x}, \bar{F}, Z^q, \bar{X})$, com φ_i fórmulas $\Sigma_0^{1,b}$; $\Delta' := \exists \bar{Y}\psi_1(\bar{x}, \bar{F}, Z^q, \bar{Y}), ..., \exists \bar{Y}\psi_m(\bar{x}, \bar{F}, Z^q, \bar{Y})$, com ψ_i fórmulas $\Sigma_0^{1,b}$ e $\bar{Y} = Y_1, ..., Y_k$ e $A(Z^q) := \exists \bar{Y}\ \underbrace{\gamma(\bar{x}, \bar{F}, Z^q, \bar{Y})}_{\text{fórmula } \Sigma_0^{1,b}}$.

Por hipótese de indução, para $\Gamma' \Longrightarrow \Delta', A(Z^q)$ existem $M_i'^{\Sigma}(\omega, \bar{x}, \bar{F}, Z^q, \bar{X})$, $M_i'^{\Pi}(\omega, \bar{x}, \bar{F}, Z^q, \bar{X})$, $t_i'(\bar{x})$, $\Phi_i'(\bar{x}, \bar{F}, Z^q, \bar{X})$ nas condições pretendidas.

Para $\Gamma' \Longrightarrow \Delta', \exists F A(F)$ fazemos:

$$M_i^{\Sigma}(\omega, \bar{x}, \bar{F}, Z^q, \bar{X}) :\longleftrightarrow \begin{cases} M_i'^{\Sigma}(\omega, \bar{x}, \bar{F}, Z^q, \bar{X}) & se \quad 1 \leq i \leq k \\ \omega \in Z^q & se \quad i = k+1 \end{cases},$$

$$M_i^{\Pi}(\omega, \bar{x}, \bar{F}, Z^q, \bar{X}) :\longleftrightarrow \begin{cases} M_i'^{\Pi}(\omega, \bar{x}, \bar{F}, Z^q, \bar{X}) & se \quad 1 \leq i \leq k \\ \omega \in Z^q & se \quad i = k+1 \end{cases},$$

$$t_i(\bar{x}) := \begin{cases} t_i'(\bar{x}) & se \quad 1 \leq i \leq k \\ q(\bar{x}) & se \quad i = k+1 \end{cases},$$

$$\Phi_i(\bar{x}, \bar{F}, Z^q, \bar{X}) := \begin{cases} \Phi_i'(\bar{x}, \bar{F}, Z^q, \bar{X}) & se \quad 1 \leq i \leq k \\ Z^q & se \quad i = k+1 \end{cases}.$$

• Se $\Pi \Longrightarrow \Lambda$ se obtém pela regra do corte, $\Pi \Longrightarrow \Lambda$ é da forma $\Gamma' \Longrightarrow \Delta'$.

$(\frac{\Gamma' \Longrightarrow \Delta', A \quad A, \Gamma' \Longrightarrow \Delta'}{\Gamma' \Longrightarrow \Delta'})$

Seja $A(\bar{x}, \bar{F}) \; :\longleftrightarrow \; \exists G_1 ... \exists G_r \underbrace{\gamma(\bar{x}, \bar{F}, \bar{G})}_{\text{fórmula } \Sigma_0^{1,b}}$, seja $\Gamma' := \exists \bar{X} \varphi_1(\bar{x}, \bar{F}, \bar{X}), ...$ $..., \exists \bar{X} \varphi_n(\bar{x}, \bar{F}, \bar{X})$, com φ_i fórmulas $\Sigma_0^{1,b}$ e $\Delta' := \exists \bar{Y} \psi_1(\bar{x}, \bar{F}, \bar{Y}), ..., \exists \bar{Y} \psi_m(\bar{x}, \bar{F}, \bar{Y})$, com ψ_i fórmulas $\Sigma_0^{1,b}$ e $\bar{Y} = Y_1, ..., Y_k$.

Por hipótese de indução, para $\Gamma' \Longrightarrow \Delta', A$ sabemos que existem $M_i'^{\Sigma}(\omega, \bar{x}, \bar{F}, \bar{X})$, $M_i'^{\Pi}(\omega, \bar{x}, \bar{F}, \bar{X})$, $t_i'(\bar{x})$, $\Phi_i'(\bar{x}, \bar{F}, \bar{X})$, com $1 \leq i \leq k + r$ e para $A, \Gamma' \Longrightarrow \Delta'$ existem $M_i''^{\Sigma}(\omega, \bar{x}, \bar{F}, \bar{X}, \bar{G})$, $M_i''^{\Pi}(\omega, \bar{x}, \bar{F}, \bar{X}, \bar{G})$, $t_i''(\bar{x})$, $\Phi_i''(\bar{x}, \bar{F}, \bar{X}, \bar{G})$, com $1 \leq i \leq k$, nas condições pretendidas.

Para $\Gamma' \Longrightarrow \Delta'$ e para $1 \leq i \leq k$ fazemos:

$M_i^{\Sigma}(\omega, \bar{x}, \bar{F}, \bar{X}) :\longleftrightarrow (\neg(\bigvee_{j=1}^{m} \psi_j(\bar{x}, \bar{F}, \{\omega \preceq t_1' : M_1'^{\Delta}(\omega, \bar{x}, \bar{F}, \bar{X})\}, ...$[¶]

$..., \{\omega \preceq t_k' : M_k'^{\Delta}(\omega, \bar{x}, \bar{F}, \bar{X})\})) \vee (\omega \preceq t_i' \wedge M_i'^{\Sigma}(\omega, \bar{x}, \bar{F}, \bar{X}))) \wedge$
$\wedge(\bigvee_{j=1}^{m} \psi_j(\bar{x}, \bar{F}, \{\omega \preceq t_1' : M_1'^{\Delta}(\omega, \bar{x}, \bar{F}, \bar{X})\}, ..., \{\omega \preceq t_k' : M_k'^{\Delta}(\omega, \bar{x}, \bar{F}, \bar{X})\}) \vee$
$\vee(\omega \preceq t_i'' \wedge M_i''^{\Sigma}(\omega, \bar{x}, \bar{F}, \bar{X}, \{\omega \preceq t_{k+1}' : M_{k+1}'^{\Delta}(\omega, \bar{x}, \bar{F}, \bar{X})\}, ...$
$..., \{\omega \preceq t_{k+r}' : M_{k+r}'^{\Delta}(\omega, \bar{x}, \bar{F}, \bar{X})\}))),$

$M_i^{\Pi}(\omega, \bar{x}, \bar{F}, \bar{X})$ é análogo, bastando na fórmula anterior substituir $M_i'^{\Sigma}$ por $M_i'^{\Pi}$ e $M_i''^{\Sigma}$ por $M_i''^{\Pi}$,

$t_i := t_i' \frown t_i''$,

$$\Phi_i(\bar{x}, \bar{F}, \bar{X}) := \begin{cases} \Phi_i'(\bar{x}, \bar{F}, \bar{X}) & se \quad \bigvee_{j=1}^{m} \psi_j(\bar{x}, \bar{F}, \Phi_1'(\bar{x}, \bar{F}, \bar{X}), ... \\ & \qquad ..., \Phi_k'(\bar{x}, \bar{F}, \bar{X})) \\ \Phi_i''(\bar{x}, \bar{F}, \bar{X}, \Phi_{k+1}'(\bar{x}, \bar{F}, \bar{X}), ... & se \quad \neg(\bigvee_{j=1}^{m} \psi_j(\bar{x}, \bar{F}, \Phi_1'(\bar{x}, \bar{F}, \bar{X}), ... \\ ..., \Phi_{k+r}'(\bar{x}, \bar{F}, \bar{X})) & \qquad ..., \Phi_k'(\bar{x}, \bar{F}, \bar{X}))) \end{cases} .$$

$\Phi_i(\bar{x}, \bar{F}, \bar{X}) \in PSPACE^{\Sigma_0^{1,b}}$, pois como provámos no capítulo 2, a classe $PSPACE^{\Sigma_0^{1,b}}$ é fechada para a composição.

• Se $\Pi \Longrightarrow \Lambda$ se obtém pela regra de substituição, $\Pi \Longrightarrow \Lambda$ é da forma $\Gamma' \Longrightarrow \exists G \forall x \preceq t \bar{\varphi}(x, G)$.

$(\frac{\Gamma', a \preceq t \Longrightarrow \exists F \varphi(a, F)}{\Gamma' \Longrightarrow \exists G \forall x \preceq t \bar{\varphi}(x, G)})$

$\exists G \forall x \preceq t \bar{\varphi}(x, G)$ é uma fórmula $\Sigma_1^{1,b}$, logo $\bar{\varphi}$ é uma fórmula $\Sigma_0^{1,b}$ e portanto, φ é também uma fórmula $\Sigma_0^{1,b}$. (Aliás só a estas fórmulas se aplica a regra de substituição.)

Por hipótese de indução, para $\Gamma', a \preceq t \Longrightarrow \exists F \varphi(a, F)$ existem $M_1'^{\Sigma}(\omega, \bar{x}, y, \bar{X})$, $M_1'^{\Pi}(\omega, \bar{x}, y, \bar{X})$, $t_1'(\bar{x}, y)$, $\Phi_1'(\bar{x}, y, \bar{X})$ nas condições pretendidas.

Para $\Gamma' \Longrightarrow \exists G \forall x \preceq t \bar{\varphi}(x, G)$ fazemos:

$M_1^{\Sigma}(\omega, \bar{x}, \bar{X}) :\longleftrightarrow \exists y \preceq t \exists s \preceq t_1' M_1'^{\Sigma}(s, \bar{x}, y, \bar{X}) \wedge \omega =< y, s >$,

$M_1^{\Pi}(\omega, \bar{x}, \bar{X}) :\longleftrightarrow \exists y \preceq t \exists s \preceq t_1' M_1'^{\Pi}(s, \bar{x}, y, \bar{X}) \wedge \omega =< y, s >$,

$t_1(\bar{x}) := t(\bar{x}) \frown t_1'(\bar{x}, t(\bar{x})) 1 \times 11$,

$\Phi_1(\bar{x}, \bar{X}) := \{< y, s >: y \preceq t \wedge s \preceq t_1' \wedge s \in \Phi_1'(\bar{x}, y, \bar{X})\}$.

[¶] M^{Δ} foram definidos na observação anterior.

• Se $\Pi \Longrightarrow \Lambda$ se obtém pela regra de indução, $\Pi \Longrightarrow \Lambda$ é da forma $\Gamma', A(\varepsilon) \Longrightarrow$ $\Longrightarrow A(s)$.

$\left(\frac{\Gamma', A(a) \Longrightarrow A(a0) \qquad \Gamma', A(a) \Longrightarrow A(a1)}{\Gamma', A(\varepsilon) \Longrightarrow A(s)}\right)$

Seja $A(z) :\longleftrightarrow \exists \bar{W}\ \gamma(\bar{x}, z, \bar{X}, \bar{W})$ com γ uma fórmula $\Sigma_0^{1,b}$ e $\bar{W} = W_1, ..., W_m$.

Por hipótese de indução, para $\Gamma', A(a) \Longrightarrow A(a0)$ existem $M_i'^{\Sigma}(\omega, \bar{x}, z, \bar{X}, \bar{W})$, $M_i'^{\Pi}(\omega, \bar{x}, z, \bar{X}, \bar{W})$, $t_i'(\bar{x}, z)$, $\Phi_i'(\bar{x}, z, \bar{X}, \bar{W})$ com $1 \leq i \leq m$, e para $\Gamma', A(a) \Longrightarrow A(a1)$ existem $M_i''^{\Sigma}(\omega, \bar{x}, z, \bar{X}, \bar{W})$, $M_i''^{\Pi}(\omega, \bar{x}, z, \bar{X}, \bar{W})$, $t_i''(\bar{x}, z)$, $\Phi_i''(\bar{x}, z, \bar{X}, \bar{W})$ com $1 \leq i \leq$ $\leq m$, nas condições pretendidas.

Para $\Gamma', A(\varepsilon) \Longrightarrow A(s)$ e para $1 \leq i \leq m$ pensemos em

$\tilde{\phi}_i(\bar{x}, \bar{X}, \bar{W}, \varepsilon) := W_i$

$\tilde{\phi}_i(\bar{x}, \bar{X}, \bar{W}, z0) := \Phi_i'(\bar{x}, z, \bar{X}, \tilde{\phi}_1(\bar{x}, \bar{X}, \bar{W}, z), ..., \tilde{\phi}_m(\bar{x}, \bar{X}, \bar{W}, z))_{|t_i'(\bar{x}, z)}$

$\tilde{\phi}_i(\bar{x}, \bar{X}, \bar{W}, z1) := \Phi_i''(\bar{x}, z, \bar{X}, \tilde{\phi}_1(\bar{x}, \bar{X}, \bar{W}, z), ..., \tilde{\phi}_m(\bar{x}, \bar{X}, \bar{W}, z))_{|t_i''(\bar{x}, z)}$.

Pelo estudo efectuado no capítulo 2, facilmente se vê que $\tilde{\phi}_i \in PSPACE^{\Sigma_0^{1,b}}$. Façamos $\Phi_i(\bar{x}, \bar{X}, \bar{W}) := \tilde{\phi}_i(\bar{x}, \bar{X}, \bar{W}, s(\bar{x}))$, para $1 \leq i \leq m$, que são ainda funcionais de $PSPACE^{\Sigma_0^{1,b}}$. Consideremos as seguintes fórmulas: $\Psi^i(\omega, \bar{x}, \bar{X}, \bar{W}) :\longleftrightarrow$ $\longleftrightarrow \omega \in W_i$, $N_0^{iQ}(\omega, \bar{x}, \bar{X}, \bar{W}, z, T_1, ..., T_m) :\longleftrightarrow \omega \preceq t_i'(\bar{x}, z) \wedge M_i'^{Q}(\omega, \bar{x}, z, \bar{X}, T_1, ..., T_m)$ e $N_1^{iQ}(\omega, \bar{x}, \bar{X}, \bar{W}, z, T_1, ..., T_m) :\longleftrightarrow \omega \preceq t_i''(\bar{x}, z) \wedge M_i''^{Q}(\omega, \bar{x}, z, \bar{X}, T_1, ..., T_m)$ com $1 \leq$ $\leq i \leq m$ e $Q \in \{\Sigma, \Pi\}$. Pelo último lema e observação que figuram em apêndice, sabemos que existem fórmulas $\Sigma_1^{1,b}$-*estendidas*, $\gamma_i^{\Sigma}(\omega, \bar{x}, \bar{X}, \bar{W}, z)$, fórmulas $\Pi_1^{1,b}$-*estendidas*, $\gamma_i^{\Pi}(\omega, \bar{x}, \bar{X}, \bar{W}, z)$ e termos $q_i(\bar{x}, z)$ de $\mathcal{L}$, com $1 \leq i \leq m$, tais que $\tilde{\phi}_i(\bar{x}, \bar{X}, \bar{W}, z) =$ $= \{\omega \preceq q_i(\bar{x}, z) : \gamma_i^{Q}(\omega, \bar{x}, \bar{X}, \bar{W}, z)\}$. Logo definimos $M_i^{\Sigma}(\omega, \bar{x}, \bar{X}, \bar{W})$ como sendo $\gamma_i^{\Sigma}(\omega, \bar{x}, \bar{X}, \bar{W}, s(\bar{x}))$, $M_i^{\Pi}(\omega, \bar{x}, \bar{X}, \bar{W})$ como sendo $\gamma_i^{\Pi}(\omega, \bar{x}, \bar{X}, \bar{W}, s(\bar{x}))$ e $t_i(\bar{x})$ como sendo $q_i(\bar{x}, s(\bar{x}))$. ■

Lema 5 *Seja* $\varphi(\bar{x}, y)$ *uma fórmula* $\Sigma_1^{1,b}$ *e suponhamos que* $\Sigma_1^{1,b}$-$NIA \vdash \forall \bar{x} \exists y \varphi(\bar{x}, y)$. *Então existe um termo* $t(\bar{x})$ *de* $\mathcal{L}$ *tal que* $\Sigma_1^{1,b}$-$NIA \vdash \forall \bar{x} \exists y \preceq t(\bar{x}) \varphi(\bar{x}, y)$.

Dem. Uma vez que $\Sigma_1^{1,b}$-$NIA \vdash \forall \bar{x} \exists y \varphi(\bar{x}, y)$, existe uma demonstração de $\Longrightarrow \exists y \varphi(\bar{x}, y)$ em LK_{PS}. Logo, pelo teorema da eliminação do corte livre, existe uma LK_{PS}-demonstração, P, do sequente $\Longrightarrow \exists y \varphi(\bar{x}, y)$ sem cortes livres. É fácil constatar que todo o sequente da demonstração P é, a menos de uma permutação do consequente, da forma (*) $\Gamma \Longrightarrow \Delta, \exists y \varphi(\bar{x}, y), ..., \exists y \varphi(\bar{x}, y)$ onde Γ e Δ são constituídos por fórmulas $\Sigma_1^{1,b}$.

Por indução no número de linhas da demonstração prova-se que, para qualquer sequente (*) em P, existe um termo, t, tal que $\Gamma \Longrightarrow \Delta, \exists y \preceq t \varphi(\bar{x}, y), ...$ $..., \exists y \preceq t \varphi(\bar{x}, y)$ se deduz em LK_{PS}.

O único caso a estudar é a regra $\exists$:d $\left(\frac{\Gamma \Longrightarrow \Delta, \exists y \varphi(\bar{x}, y), ..., \exists y \varphi(\bar{x}, y), \varphi(\bar{x}, r)}{\Gamma \Longrightarrow \Delta, \exists y \varphi(\bar{x}, y), ..., \exists y \varphi(\bar{x}, y), \exists y \varphi(\bar{x}, y)}\right)$ com r um termo qualquer.

Por hipótese de indução existe um termo q tal que $\Gamma \Longrightarrow \Delta, \exists y \preceq q \varphi(\bar{x}, y), ...$ $..., \exists y \preceq q \varphi(\bar{x}, y), \varphi(\bar{x}, r)$. Basta tomar t como sendo $q \frown r$.

Prova-se assim que existe um termo, t, tal que LK_{PS} demonstra o sequente $\Longrightarrow \exists y \preceq t \varphi(\bar{x}, y)$. Pode supôr-se que t só depende de $\bar{x}$, pois se dependesse dum certo $\bar{b}$, tomávamo-lo como sendo $\bar{b} = \bar{0}$. Obtemos assim um termo $t(\bar{x})$ que verifica $\Sigma_1^{1,b}$-$NIA \vdash \forall \bar{x} \exists y \preceq t(\bar{x}) \varphi(\bar{x}, y)$. ∎

Teorema 6 *Se* $\Sigma_1^{1,b}$-$NIA \vdash \forall \bar{x} \exists y \varphi(\bar{x}, y)$ *com* φ *uma fórmula* $\Sigma_1^{1,b}$, *então existe uma função* $f \in PSPACE$ *tal que, para todo* $\bar{\sigma}$ *em* $2^{<\omega}$ *se tem* $\varphi(\bar{\sigma}, f(\bar{\sigma}))$.

Além disso existe uma fórmula $\Delta_1^{1,b}$-*estendida,* Θ, *em* $\Sigma_1^{1,b}$-NIA *e um termo* $t(\bar{x})$ *tais que*

1) $f(\bar{\sigma}) = \tau \longleftrightarrow \Theta(\bar{\sigma}, \tau)$;

2) $\Sigma_1^{1,b}$-$NIA \vdash \forall \bar{x} \forall y (\Theta(\bar{x}, y) \rightarrow \varphi(\bar{x}, y))$;

3) $\Sigma_1^{1,b}$-$NIA \vdash \forall \bar{x} \exists y \preceq t \Theta(\bar{x}, y)$;

4) $\Sigma_1^{1,b}$-$NIA \vdash \forall \bar{x} \exists^1 y \Theta(\bar{x}, y)$.

Dem. Pelo lema anterior, como $\Sigma_1^{1,b}$-$NIA \vdash \forall \bar{x} \exists y \varphi(\bar{x}, y)$ com φ uma fórmula $\Sigma_1^{1,b}$, temos garantida a existência de um termo $t'(\bar{x})$ tal que

$\Sigma_1^{1,b}$-$NIA \vdash \forall \bar{x} \exists y \preceq t'(\bar{x}) \varphi(\bar{x}, y)$. Logo LK_{PS} deduz $\Longrightarrow \forall \bar{x} \exists y \preceq t'(\bar{x}) \varphi(\bar{x}, y)$, e portanto também deduz o sequente $\Longrightarrow \exists y \preceq t'(\bar{x}) \varphi(\bar{x}, y)$.

Seja $\varphi(\bar{x}, y) :\longleftrightarrow \exists U_1 ... \exists U_k \tilde{\varphi}(\bar{x}, y, U_1, ..., U_k)$ com $\tilde{\varphi}$ uma fórmula $\Sigma_0^{1,b}$. Temos então que LK_{PS} deduz o sequente $\Longrightarrow \exists U_1 ... \exists U_k \underbrace{\exists y \preceq t'(\bar{x}) \tilde{\varphi}(\bar{x}, y, U_1, ..., U_k)}_{\textit{fórmula } \Sigma_0^{1,b}}$. Pelo teorema fundamental existem funcionais em $PSPACE^{\Sigma_0^{1,b}}$, $\phi_1, ..., \phi_k$, que verificam $\forall \bar{\sigma} \exists y \preceq t'(\bar{\sigma}) \tilde{\varphi}(\bar{\sigma}, y, \phi_1(\bar{\sigma}), ..., \phi_k(\bar{\sigma}))$ e existem M_i^{Σ}, fórmulas $\Sigma_1^{1,b}$-*estendidas*, M_i^{Π}, fórmulas $\Pi_1^{1,b}$-*estendidas* e termos t_i, com $1 \leq i \leq k$, que verificam o seguinte: $\phi_i(\bar{x}) = \{\omega \preceq t_i(\bar{x}) : M_i^{\Sigma}(\omega, \bar{x})\}$, $\Sigma_1^{1,b}$-$NIA \vdash \forall \bar{x} \exists y \preceq t'(\bar{x}) \tilde{\varphi}(\bar{x}, y, \{\omega \preceq t_1(\bar{x}) : M_1^{\Sigma}(\omega, \bar{x})\}, ..., \{\omega \preceq t_k(\bar{x}) : M_k^{\Sigma}(\omega, \bar{x})\})$ e $\Sigma_1^{1,b}$-$NIA \vdash \forall \bar{x} \forall \omega \preceq t_i(\bar{x}) (M_i^{\Sigma}(\omega, \bar{x}) \longleftrightarrow$ $\longleftrightarrow M_i^{\Pi}(\omega, \bar{x}))$.

Seja $f(\bar{\sigma}) := \mu y \preceq t'(\bar{\sigma}) \tilde{\varphi}(\bar{\sigma}, y, \phi_1(\bar{\sigma}), ..., \phi_k(\bar{\sigma}))$. Como $\phi_1, ..., \phi_k$ são funcionais de $PSPACE^{\Sigma_0^{1,b}}$, temos que $f \in PSPACE^{\Sigma_0^{1,b}}$. Pela proposição 1 do capítulo 2, uma vez que f é uma função, sabemos que $f \in PSPACE$. Obviamente temos $\forall \bar{\sigma} \varphi(\bar{\sigma}, f(\bar{\sigma}))$. Seja $\Theta(\bar{x}, y) :\longleftrightarrow \tilde{\varphi}(\bar{x}, y, \{\omega \preceq t_1(\bar{x}) : M_1^{\Delta}(\omega, \bar{x})\}, ..., \{\omega \preceq t_k(\bar{x}) : M_k^{\Delta}(\omega, \bar{x})\}) \wedge \forall y' < y \neg \tilde{\varphi}(\bar{x}, y', \{\omega \preceq t_1(\bar{x}) : M_1^{\Delta}(\omega, \bar{x})\}, ..., \{\omega \preceq t_k(\bar{x}) : M_k^{\Delta}(\omega, \bar{x})\})$, que pela observação ao teorema fundamental sabemos que é $\Delta_1^{1,b}$-*estendida*. Seja $t(\bar{x}) := t'(\bar{x})$.

Obviamente as propriedades 1) e 2) verificam-se.

Por outro lado, $\Sigma_1^{1,b}$-$NIA \vdash \forall \bar{x} \exists y \preceq t \Theta(\bar{x}, y)$, pois em $\Sigma_1^{1,b}$-NIA é válida minimização para fórmulas $\Delta_1^{1,b}$-*estendidas*. A unicidade resulta da definição de Θ. ∎

Capítulo 6
COLECÇÃO LIMITADA

O objectivo deste capítulo é estudar a teoria $\Sigma_1^{1,b}$-NIA enriquecida com dois esquemas de colecção, e apresentar um resultado de conservação.

6.1 Teoria $\Sigma_1^{1,b}$-NIA + B$\Sigma_\infty^{1,b}$+B$^1\Sigma_\infty^{1,b}$

Definição 29 *Uma fórmula diz-se* $\Sigma_\infty^{1,b}$ *se pertence à menor classe de fórmulas, na linguagem* $\mathcal{L}_2^b$*, que contém as fórmulas* $\Sigma_0^{1,b}$ *e é fechada para* $\neg$, $\wedge$, $\vee$, $\exists X^t$, $\forall X^t$, $\exists x \preceq t$ *e* $\forall x \preceq t$.

Consideremos os seguintes esquemas:

- **Esquema B$\Sigma_\infty^{1,b}$**

$\forall x \preceq t \exists y \varphi(x, y) \rightarrow \exists z \forall x \preceq t \exists y \preceq z \varphi(x, y)$

com t um termo onde x não ocorre e φ uma fórmula $\Sigma_\infty^{1,b}$ que pode ter outras variáveis livres além de x e y;

- **Esquema B$^1\Sigma_\infty^{1,b}$**

$\forall X^t \exists y \varphi(y, X^t) \rightarrow \exists z \forall X^t \exists y \preceq z \varphi(y, X^t)$

com φ uma fórmula $\Sigma_\infty^{1,b}$ que pode ter outras variáveis livres além de y e X^t.

Observação 18 *A teoria designada por* $\Sigma_1^{1,b}$-$NIA + B\Sigma_\infty^{1,b} + B^1\Sigma_\infty^{1,b}$, *que é obtida da teoria* $\Sigma_1^{1,b}$-NIA *acrescentando os dois esquemas anteriores, também pode ser formulada no cálculo de sequentes de Gentzen. Esse cálculo de sequentes, que designaremos por* LK'_{PS}, *será* LK_{PS} *(o cálculo de sequentes para* $\Sigma_1^{1,b}$-NIA*) com mais duas regras de inferência:*

- ***Regra*** **B$\Sigma_\infty^{1,b}$**

$$\frac{a \preceq t, \Gamma \Longrightarrow \exists y \varphi(a, y)}{\Gamma \Longrightarrow \exists z \forall x \preceq t \exists y \preceq z \varphi(x, y)}$$

onde a *é uma variável própria e* φ *é uma fórmula* $\Sigma_\infty^{1,b}$ *que pode ter outras variáveis livres além das apresentadas;*

- ***Regra*** **B$^1\Sigma_\infty^{1,b}$**

$$\frac{\Gamma \Longrightarrow \exists y \varphi(y, C^t)}{\Gamma \Longrightarrow \exists z \forall X^t \exists y \preceq z \varphi(y, X^t)}$$

onde C^t *é uma variável própria,* t *é um termo onde* y *não ocorre e* φ *é uma fórmula* $\Sigma_\infty^{1,b}$ *que pode ter outras variáveis livres além das apresentadas.*

Vejamos que, de facto, sendo válida a regra $B\Sigma^{1,b}_{\infty}$ é válido o sequente $\Longrightarrow \forall x \preceq t\exists y\varphi(x,y) \rightarrow \exists z\forall x \preceq t\exists y \preceq z\varphi(x,y)$ e reciprocamente do sequente anterior segue-se a regra $B\Sigma^{1,b}_{\infty}$; e sendo válida a regra $B^1\Sigma^{1,b}_{\infty}$ é válido o sequente $\Longrightarrow \forall X^t\exists y\varphi(y,X^t) \rightarrow \exists z\forall X^t\exists y \preceq z\varphi(y,X^t)$ e reciprocamente do sequente anterior segue-se a regra $B^1\Sigma^{1,b}_{\infty}$.

Dem. Da regra $B\Sigma^{1,b}_{\infty}$ segue-se o esquema $B\Sigma^{1,b}_{\infty}$:

$$\begin{array}{c l}
\exists y\varphi(a,y) \Longrightarrow \exists y\varphi(a,y) & (\forall_{\preceq}\text{:e}) \\ \hline
a \preceq t, \forall x \preceq t\exists y\varphi(x,y) \Longrightarrow \exists y\varphi(a,y) & (R.B\Sigma^{1,b}_{\infty}) \\ \hline
\forall x \preceq t\exists y\varphi(x,y) \Longrightarrow \exists z\forall x \preceq t\exists y \preceq z\varphi(x,y) & (\rightarrow\text{:d}) \\ \hline
\Longrightarrow \forall x \preceq t\exists y\varphi(x,y) \rightarrow \exists z\forall x \preceq t\exists y \preceq z\varphi(x,y) &
\end{array}$$

Do esquema $B\Sigma^{1,b}_{\infty}$ segue-se a regra $B\Sigma^{1,b}_{\infty}$:

$$\begin{array}{l}
(\forall_{\preceq}\text{:d}) \\
(corte)
\end{array}
\dfrac{\dfrac{a \preceq t, \Gamma \Longrightarrow \exists y\varphi(a,y)}{\Gamma \Longrightarrow \forall x \preceq t\exists y\varphi(x,y)} \qquad \dfrac{\Longrightarrow \forall x \preceq t\exists y\varphi(x,y) \rightarrow \exists z\forall x \preceq t\exists y \preceq z\varphi(x,y)}{\forall x \preceq t\exists y\varphi(x,y) \Longrightarrow \exists z\forall x \preceq t\exists y \preceq z\varphi(x,y)}}{\Gamma \Longrightarrow \exists z\forall x \preceq t\exists y \preceq z\varphi(x,y)}$$

Da regra $B^1\Sigma^{1,b}_{\infty}$ segue-se o esquema $B^1\Sigma^{1,b}_{\infty}$:

$$\begin{array}{c l}
\exists y\varphi(y,C^t) \Longrightarrow \exists y\varphi(y,C^t) & (\forall_{2^a}\text{:e}) \\ \hline
\forall X^t\exists y\varphi(y,X^t) \Longrightarrow \exists y\varphi(y,C^t) & (R.B^1\Sigma^{1,b}_{\infty}) \\ \hline
\forall X^t\exists y\varphi(y,X^t) \Longrightarrow \exists z\forall X^t\exists y \preceq z\varphi(y,X^t) & (\rightarrow\text{:d}) \\ \hline
\Longrightarrow \forall X^t\exists y\varphi(y,X^t) \rightarrow \exists z\forall X^t\exists y \preceq z\varphi(y,X^t) &
\end{array}$$

Do esquema $B^1\Sigma^{1,b}_{\infty}$ segue-se a regra $B^1\Sigma^{1,b}_{\infty}$:

$$\begin{array}{l}
(\forall_{2^a}\text{:d}) \\
(corte)
\end{array}
\dfrac{\dfrac{\Gamma \Longrightarrow \exists y\varphi(y,C^t)}{\Gamma \Longrightarrow \forall X^t\exists y\varphi(y,X^t)} \qquad \dfrac{\Longrightarrow \forall X^t\exists y\varphi(y,X^t) \rightarrow \exists z\forall X^t\exists y \preceq z\varphi(y,X^t)}{\forall X^t\exists y\varphi(y,X^t) \Longrightarrow \exists z\forall X^t\exists y \preceq z\varphi(y,X^t)}}{\Gamma \Longrightarrow \exists z\forall X^t\exists y \preceq z\varphi(y,X^t)}$$

■

6.2 Um resultado de conservação

Definição 30 *Sejam T_1 e T_2 teorias na linguagem $\mathcal{L}^b_2$, tais que $T_1 \supseteq T_2$.*

Diz-se que T_1 é uma teoria $\forall\exists\Sigma^{\mathbf{1,b}}_{\infty}$**-conservativa** *sobre T_2 se sempre que uma sentença Ψ da forma $\forall\bar{x}\exists y\varphi(\bar{x},y)$, com φ uma fórmula $\Sigma^{1,b}_{\infty}$, é tal que $T_1 \vdash \Psi$ então $T_2 \vdash \Psi$.*

Proposição 17 *A teoria $\Sigma^{1,b}_1$-NIA + $B\Sigma^{1,b}_{\infty}$ + $B^1\Sigma^{1,b}_{\infty}$ é $\forall\exists\Sigma^{1,b}_{\infty}$-conservativa sobre $\Sigma^{1,b}_1$-NIA.*

Dem. Suponhamos que $\Sigma_1^{1,b}$-$NIA + B\Sigma_\infty^{1,b} + B^1\Sigma_\infty^{1,b} \vdash \forall\bar{x}\exists y\varphi(\bar{x}, y)$ com φ uma fórmula $\Sigma_\infty^{1,b}$. Então existe uma LK'_{PS}-demonstração do sequente $\Longrightarrow \forall\bar{x}\exists y\varphi(\bar{x}, y)$ e, portanto, em LK'_{PS} demonstra-se $\Longrightarrow \exists y\varphi(\bar{x}, y)$.

O teorema da eliminação do corte livre*, garante a existência de uma LK'_{PS}-demonstração P do sequente $\Longrightarrow \exists y\varphi(\bar{x}, y)$ sem cortes livres. Logo todo o sequente da demonstração P é da forma $\Gamma \Longrightarrow \Delta$ em que Γ e Δ são constituídos por fórmulas $\exists x\Theta(x, \bar{x}, \bar{X}^p)$, com Θ fórmulas $\Sigma_\infty^{1,b}$, podendo obviamente $\exists x$ não aparecer.

Seja $\Gamma := \exists x_1\varphi_1(x_1, \bar{x}, \bar{X}^{p(\bar{x})}), \dots, \exists x_n\varphi_n(x_n, \bar{x}, \bar{X}^{p(\bar{x})})$ com $\varphi_1,\dots,\varphi_n$ fórmulas $\Sigma_\infty^{1,b}$ e seja $\Delta := \exists y_1\psi_1(y_1, \bar{x}, \bar{X}^{p(\bar{x})}), \dots, \exists y_k\psi_k(y_k, \bar{x}, \bar{X}^{p(\bar{x})})$ com $\psi_1,\dots,\psi_k$ fórmulas $\Sigma_\infty^{1,b}$.

Demonstra-se, por indução no número de linhas da demonstração P, que para qualquer sequente $\Gamma \Longrightarrow \Delta$ em P se tem

(*) $\Sigma_1^{1,b}$-$NIA \vdash \forall u\exists v\forall\bar{x} \preceq u\forall\bar{X}^{p(\bar{x})}(\Gamma^{\preceq u} \to \Delta^{\preceq v})$,

onde $\Gamma^{\preceq u}$ abrevia $\exists x_1 \preceq u\varphi_1(x_1, \bar{x}, \bar{X}^{p(\bar{x})}) \wedge \dots \wedge \exists x_n \preceq u\varphi_n(x_n, \bar{x}, \bar{X}^{p(\bar{x})})$ e $\Delta^{\preceq v}$ abrevia $\exists y_1 \preceq v\psi_1(y_1, \bar{x}, \bar{X}^{p(\bar{x})}) \vee \dots \vee \exists y_k \preceq v\psi_k(y_k, \bar{x}, \bar{X}^{p(\bar{x})})$.

Uma vez efectuada esta demonstração por indução no número de linhas temos o que se pretende, pois aplicando (*) ao último sequente da demonstração P vem que $\Sigma_1^{1,b}$-NIA demonstra que $\forall u\exists v\forall\bar{x} \preceq u\exists y \preceq v\varphi(\bar{x}, y)$. Dado $\bar{x}$, pensando em u como a concatenação dos elementos em $\bar{x}$, temos que $\Sigma_1^{1,b}$-$NIA \vdash \exists v\exists y \preceq v\varphi(\bar{x}, y)$. Em particular $\Sigma_1^{1,b}$-$NIA \vdash \exists y\varphi(\bar{x}, y)$. Logo $\Sigma_1^{1,b}$-$NIA \vdash \forall\bar{x}\exists y\varphi(\bar{x}, y)$.

Vejamos que (*) se verifica.

- Para os sequentes iniciais, para os sequentes obtidos pelas regras estruturais fracas, pelas regras proposicionais, por $\exists$:e, $\forall_\preceq$:e, $\exists_\preceq$:d, $\forall_{2^a}$:e, $\forall_{2^a}$:d, $\exists_{2^a}$:e, $\exists_{2^a}$:d e pelas regras de indução e substituição o resultado é óbvio.
- As regras $\forall$:e e $\forall$:d não ocorrem na demonstração P.

Estudemos as restantes regras.

- Suponhamos que $\Gamma \Longrightarrow \Delta$ se obtém pela regra do corte.

$\left(\dfrac{\Gamma\Longrightarrow\Delta, A \qquad A, \Gamma\Longrightarrow\Delta}{\Gamma\Longrightarrow\Delta}\right)$

Se A é uma fórmula $\Sigma_\infty^{1,b}$ o resultado sai imediatamente fazendo $v := v_1 \frown v_2$ sendo v_1 e v_2 os $v's$ que existem por hipótese de indução.

Suponhamos que $A :\longleftrightarrow \exists z\Theta(z, \bar{x}, \bar{X}^{p(\bar{x})})$ com Θ uma fórmula $\Sigma_\infty^{1,b}$. Por hipótese de indução sabemos que:

1) $\Sigma_1^{1,b}$-$NIA \vdash \forall u\exists v\forall\bar{x} \preceq u\forall\bar{X}^{p(\bar{x})}(\Gamma^{\preceq u} \to \Delta^{\preceq v} \vee \exists z \preceq v\Theta(z, \bar{x}, \bar{X}^{p(\bar{x})}))$ e

2) $\Sigma_1^{1,b}$-$NIA \vdash \forall u\exists v\forall\bar{x} \preceq u\forall\bar{X}^{p(\bar{x})}(\exists z \preceq u\Theta(z, \bar{x}, \bar{X}^{p(\bar{x})}) \wedge \Gamma^{\preceq u} \to \Delta^{\preceq v})$.

Queremos ver que $\Sigma_1^{1,b}$-$NIA \vdash \forall u\exists v\forall\bar{x} \preceq u\forall\bar{X}^{p(\bar{x})}(\Gamma^{\preceq u} \to \Delta^{\preceq v})$. Raciocinemos em $\Sigma_1^{1,b}$-NIA. Seja u dado. A condição 1) garante a existência de um v_1 que verifica $\forall\bar{x} \preceq u\forall\bar{X}^{p(\bar{x})}(\Gamma^{\preceq u} \to \Delta^{\preceq v_1} \vee \exists z \preceq v_1\Theta(z, \bar{x}, \bar{X}^{p(\bar{x})}))$. Obviamente podemos supôr que $u \preceq v_1$, pois se isso não acontecer, substituimos v_1 por $v_1 \frown u$ que a sentença acima continua válida, uma vez que $v \preceq v' \to (\exists y \preceq v\gamma(y) \to \exists y \preceq v'\gamma(y))$.

*O teorema da eliminação do corte livre continua válido em LK'_{PS}, bastando para isso considerar que as fórmulas que ocorrem ancoradas passem também a ser os descendentes directos das fórmulas principais das Regras de colecção $B\Sigma_\infty^{1,b}$ e $B^1\Sigma_\infty^{1,b}$, que são as fórmulas $\exists z\forall x \preceq t\exists y \preceq z\varphi(x, y)$ e $\exists z\forall X^t\exists y \preceq z\varphi(y, X^t)$ respectivamente.

Por 2) sabemos que existe v_2 tal que $\forall\bar{x} \preceq v_1 \forall \bar{X}^{p(\bar{x})}(\exists z \preceq v_1 \Theta(z, \bar{x}, \bar{X}^{p(\bar{x})}) \wedge \Gamma^{\preceq v_1} \rightarrow$ $\rightarrow \Delta^{\preceq v_2})$. Logo $\forall\bar{x} \preceq u \forall \bar{X}^{p(\bar{x})}(\exists z \preceq v_1 \Theta(z, \bar{x}, \bar{X}^{p(\bar{x})}) \wedge \Gamma^{\preceq u} \rightarrow \Delta^{\preceq v_2})$ uma vez que se verifica a implicação $u \preceq u' \rightarrow (\Gamma^{\preceq u} \rightarrow \Gamma^{\preceq u'})$. Fazendo $v := v_1 \frown v_2$ temos que $\forall\bar{x} \preceq u \forall \bar{X}^{p(\bar{x})}(\Gamma^{\preceq u} \rightarrow \Delta^{\preceq v})$.

• Suponhamos que o sequente se obtém pela regra $\exists$:d.
$\left(\frac{\Gamma \Longrightarrow \Delta, A(t)}{\Gamma \Longrightarrow \Delta, \exists x A(x)}\right)$
Pela forma como construímos a demonstração P, sabemos que A é uma fórmula $\Sigma^{1,b}_\infty$.

Por hipótese de indução, $\Sigma^{1,b}_1$-$NIA \vdash \forall u \exists v \forall \bar{x} \preceq u \forall \bar{X}^{p(\bar{x})}(\Gamma^{\preceq u} \rightarrow \Delta^{\preceq v} \vee A(t))$. Vejamos que $\Sigma^{1,b}_1$-$NIA \vdash \forall u \exists v \forall \bar{x} \preceq u \forall \bar{X}^{p(\bar{x})}(\Gamma^{\preceq u} \rightarrow \Delta^{\preceq v} \vee \exists x \preceq v A(x))$. Seja u dado. Sabemos que existe v_1 tal que $\forall \bar{x} \preceq u \forall \bar{X}^{p(\bar{x})}(\Gamma^{\preceq u} \rightarrow \Delta^{\preceq v_1} \vee A(t))$. Seja $v := v_1 \frown t(\bar{u})$, temos que $\forall\bar{x} \preceq u \forall \bar{X}^{p(\bar{x})}(\Gamma^{\preceq u} \rightarrow \Delta^{\preceq v} \vee \exists x \preceq v A(x))$.

• Suponhamos que o sequente se obtém pela regra $\forall_{\preceq}$:d.
$\left(\frac{a \preceq t, \Gamma \Longrightarrow \Delta, A(a)}{\Gamma \Longrightarrow \Delta, \forall x \preceq t A(x)}\right)$ com a uma variável própria e $A(x)$ uma fórmula $\Sigma^{1,b}_\infty$.

Por hipótese de indução, $\Sigma^{1,b}_1$-$NIA \vdash \forall u \exists v \forall \bar{x} \preceq u \forall \bar{X}^{p(\bar{x})} \forall y \preceq u(y \preceq t \wedge$ $\wedge \Gamma^{\preceq u} \rightarrow \Delta^{\preceq v} \vee A(y))$. Queremos ver que $\Sigma^{1,b}_1$-$NIA \vdash \forall u \exists v \forall \bar{x} \preceq u \forall \bar{X}^{p(\bar{x})}(\Gamma^{\preceq u} \rightarrow$ $\rightarrow \Delta^{\preceq v} \vee \forall x \preceq t A(x))$. Seja u dado. Tomemos $u' = t(\bar{u}) \frown u$. Por hipótese de indução sabemos que existe v' tal que $\forall\bar{x} \preceq u' \forall \bar{X}^{p(\bar{x})} \forall y \preceq u'(y \preceq t \wedge \Gamma^{\preceq u'} \rightarrow \Delta^{\preceq v'} \vee A(y))$. Logo $\forall\bar{x} \preceq u \forall \bar{X}^{p(\bar{x})} \forall y \preceq u'(y \preceq t \wedge \Gamma^{\preceq u} \rightarrow \Delta^{\preceq v'} \vee A(y))$. Fazendo $v := v'$ temos que $\forall\bar{x} \preceq u \forall \bar{X}^{p(\bar{x})}(\Gamma^{\preceq u} \rightarrow \Delta^{\preceq v} \vee \forall y \preceq t A(y))$.

• Se o sequente é obtido pela regra $\exists_{\preceq}$:e o argumento é inteiramente análogo ao anterior.

• Suponhamos que o sequente se obtém pela regra $B\Sigma^{1,b}_\infty$.
$\left(\frac{a \preceq t, \Gamma \Longrightarrow \exists y \varphi(a,y)}{\Gamma \Longrightarrow \exists z \forall x \preceq t \exists y \preceq z \varphi(x,y)}\right)$ com a uma variável própria e φ uma fórmula $\Sigma^{1,b}_\infty$.

Por hipótese de indução, $\Sigma^{1,b}_1$-$NIA \vdash \forall u \exists v \forall \bar{x} \preceq u \forall \bar{X}^{p(\bar{x})} \forall z \preceq u(z \preceq t \wedge$ $\wedge \Gamma^{\preceq u} \rightarrow \exists y \preceq v \varphi(z,y))$. Queremos ver que $\Sigma^{1,b}_1$-$NIA \vdash \forall u \exists v \forall \bar{x} \preceq u \forall \bar{X}^{p(\bar{x})}(\Gamma^{\preceq u} \rightarrow$ $\rightarrow \exists z \preceq v \forall x \preceq t \exists y \preceq z \varphi(x,y))$. Seja u dado. Consideremos $u' = t(\bar{u}) \frown u$. Por hipótese de indução existe v' tal que $\forall\bar{x} \preceq u' \forall \bar{X}^{p(\bar{x})} \forall z \preceq u'(z \preceq t \wedge \Gamma^{\preceq u'} \rightarrow$ $\rightarrow \exists y \preceq v' \varphi(z,y))$. Logo $\forall\bar{x} \preceq u \forall \bar{X}^{p(\bar{x})} \forall z \preceq u'(z \preceq t \wedge \Gamma^{\preceq u} \rightarrow \exists y \preceq v' \varphi(z,y))$. Temos portanto $\forall\bar{x} \preceq u \forall \bar{X}^{p(\bar{x})}(\Gamma^{\preceq u} \rightarrow \forall z \preceq t \exists y \preceq v' \varphi(z,y))$. Fazendo $v := v'$ temos que $\forall\bar{x} \preceq u \forall \bar{X}^{p(\bar{x})}(\Gamma^{\preceq u} \rightarrow \forall z \preceq t \exists y \preceq v \varphi(z,y))$. Pensando em $z = v$ temos, como se pretendia, que $\forall\bar{x} \preceq u \forall \bar{X}^{p(\bar{x})}(\Gamma^{\preceq u} \rightarrow \exists z \preceq v \forall x \preceq t \exists y \preceq z \varphi(x,y))$.

• Suponhamos que o sequente é deduzido pela regra $B^1\Sigma^{1,b}_\infty$.
$\left(\frac{\Gamma \Longrightarrow \exists y \varphi(y, C^t)}{\Gamma \Longrightarrow \exists z \forall X^t \exists y \preceq z \varphi(y, X^t)}\right)$ com C^t uma variável própria e φ uma fórmula $\Sigma^{1,b}_\infty$.

Por hipótese de indução, vem que $\Sigma^{1,b}_1$-$NIA \vdash \forall u \exists v \forall \bar{x} \preceq u \forall \bar{X}^{p(\bar{x})} \forall X^{t(\bar{x})}(\Gamma^{\preceq u} \rightarrow$ $\rightarrow \exists y \preceq v \varphi(y, X^{t(\bar{x})}))$. Para demonstrar, como se pretende, que $\Sigma^{1,b}_1$-$NIA \vdash \forall u \exists v$ $\forall\bar{x} \preceq u \forall \bar{X}^{p(\bar{x})}(\Gamma^{\preceq u} \rightarrow \exists z \preceq v \forall X^{t(\bar{x})} \exists y \preceq z \varphi(y, X^{t(\bar{x})}))$, basta pensar em v como sendo o que existe por hipótese de indução e tomar $z := v$.

Obtemos assim o pretendido. ∎

Torna-se agora imediato provar que, as funções demonstravelmente totais de $\Sigma^{1,b}_1$-$NIA + B\Sigma^{1,b}_\infty + B^1\Sigma^{1,b}_\infty$ com gráfico $\Sigma^{1,b}_1$, são ainda as funções de $PSPACE$.

Teorema 7 *Se* $\Sigma_1^{1,b}$-$NIA + B\Sigma_\infty^{1,b} + B^1\Sigma_\infty^{1,b} \vdash \forall\bar{x}\exists y\varphi(\bar{x},y)$ *com* φ *uma fórmula* $\Sigma_1^{1,b}$*, então existe uma função* $f \in PSPACE$ *tal que, para todo* $\bar{\sigma}$ *em* $2^{<\omega}$ *se tem* $\varphi(\bar{\sigma}, f(\bar{\sigma}))$.

Além disso existem uma fórmula $\Delta_1^{1,b}$*-estendida,* Θ*, em* $\Sigma_1^{1,b}$-$NIA + B\Sigma_\infty^{1,b} + B^1\Sigma_\infty^{1,b}$ *e um termo* $t(\bar{x})$ *tais que*

1) $f(\bar{\sigma}) = \tau \longleftrightarrow \Theta(\bar{\sigma},\tau)$;

2) $\Sigma_1^{1,b}$-$NIA + B\Sigma_\infty^{1,b} + B^1\Sigma_\infty^{1,b} \vdash \forall\bar{x}\forall y(\Theta(\bar{x},y) \to \varphi(\bar{x},y))$;

3) $\Sigma_1^{1,b}$-$NIA + B\Sigma_\infty^{1,b} + B^1\Sigma_\infty^{1,b} \vdash \forall\bar{x}\exists y \preceq t\Theta(\bar{x},y)$;

4) $\Sigma_1^{1,b}$-$NIA + B\Sigma_\infty^{1,b} + B^1\Sigma_\infty^{1,b} \vdash \forall\bar{x}\exists^1 y\Theta(\bar{x},y)$.

Dem. Se $\Sigma_1^{1,b}$-$NIA + B\Sigma_\infty^{1,b} + B^1\Sigma_\infty^{1,b} \vdash \forall\bar{x}\exists y\varphi(\bar{x},y)$, com φ uma fórmula $\Sigma_1^{1,b}$, então pela proposição anterior temos que $\Sigma_1^{1,b}$-$NIA \vdash \forall\bar{x}\exists y\varphi(\bar{x},y)$, uma vez que as fórmulas $\Sigma_1^{1,b}$ são em particular fórmulas $\Sigma_\infty^{1,b}$. O resultado segue imediatamente do teorema 6 apresentado no capítulo anterior. ■

Capítulo 7
EM DIRECÇÃO A UMA TEORIA DE ANÁLISE COMPUTÁVEL EM ESPAÇO POLINOMIAL

Este último capítulo tem como propósito fundamental apresentar uma teoria de 2^a ordem, designada por $BTPSA$ (acrónimo para *Base Theory for Polynomial Space Analysis*), cujas funções demonstravelmente totais são exactamente as funções computáveis em espaço polinomial e na qual acreditamos que se possam desenvolver algumas noções de análise.

7.1 Teoria BTPSA

Seja $\mathcal{L}_2$ a linguagem de 2^a ordem que inclui a linguagem $\mathcal{L}$ (linguagem de 1^a ordem que contém três constantes $0, 1$ e ε, dois símbolos funcionais binários $\frown$ e $\times$ e dois símbolos relacionais binários $=$ e $\subseteq$) e que contém ainda variáveis de 2^a ordem denotadas por $F, G, C, X, Y...$ e um símbolo relacional binário $\in$, que opera entre um termo de $\mathcal{L}$ e uma variável de 2^a ordem.

Os **termos** da linguagem $\mathcal{L}_2$ coincidem com os termos de $\mathcal{L}$.

Definição 31 *A classe das **fórmulas** de $\mathcal{L}_2$ é a menor classe de expressões tais que:*

1. Se t_1 e t_2 são termos e X é uma variável de 2^a ordem então $t_1 \subseteq t_2$, $t_1 = t_2$ e $t_1 \in X$ são fórmulas (fórmulas atómicas).

2. Se P e Q são fórmulas então $\neg P$, $(P \wedge Q)$, $(P \vee Q)$ e $(P \rightarrow Q)$ são fórmulas.

3. Se P é uma fórmula, x é uma variável de 1^a ordem e X é uma variável de 2^a ordem então $\forall x P$, $\exists x P$, $(\forall X)P$ e $(\exists X)P$ são fórmulas.

Observação 19 • *Por convenção, sendo P uma fórmula e t um termo, $(\forall x \preceq t)P$ abrevia $\forall x(x \preceq t \rightarrow P)$ e $(\exists x \preceq t)P$ abrevia $\exists x(x \preceq t \wedge P)$.*

• *$X \preceq t$ abrevia $\forall z(z \in X \rightarrow z \preceq t)$. Logo $(\forall X \preceq t)\varphi$ tem na linguagem $\mathcal{L}_2$ o mesmo significado que $\forall X^t \varphi$ tem na linguagem $\mathcal{L}_2^b$. Podemos assim considerar que $\mathcal{L}_2^b \subseteq \mathcal{L}_2$, querendo com isto significar que $\mathcal{L}_2$ tem maior poder expressivo que $\mathcal{L}_2^b$, uma vez que X^t pode ser representado por $X \preceq t$.*

No âmbito desta nova linguagem $\mathcal{L}_2$, vamos introduzir definições análogas às já apresentadas para a linguagem $\mathcal{L}_2^b$.

Definição 32 • *Uma **fórmula** $\Sigma_0^{1,b}$ é uma fórmula de $\mathcal{L}_2$ sem quantificações de 2ª ordem e em que todas as quantificações de 1ª ordem são limitadas, podendo obviamente ter parâmetros de 2ª ordem.*

• *Uma **fórmula** $\Sigma_1^{1,b}$ é uma fórmula de $\mathcal{L}_2$ da forma:*
$\exists X_1 \preceq t_1 ... \exists X_k \preceq t_k \varphi(\bar{x}, \bar{Y}, X_1, ..., X_k)$, *onde φ é uma fórmula $\Sigma_0^{1,b}$.*

• *Uma **fórmula** $\Pi_1^{1,b}$ é uma fórmula de $\mathcal{L}_2$ da forma:*
$\forall X_1 \preceq t_1 ... \forall X_k \preceq t_k \varphi(\bar{x}, \bar{Y}, X_1, ..., X_k)$, *onde φ é uma fórmula $\Sigma_0^{1,b}$.*

• *Uma **fórmula** $\Sigma_1^{1,b}$**-estendida** (respectivamente $\Pi_1^{1,b}$**-estendida**) é uma fórmula de $\mathcal{L}_2$ que pode ser construída num número finito de passos, começando por fórmulas $\Sigma_0^{1,b}$ e permitindo conjunções, disjunções, quantificações limitadas de 1ª ordem e quantificações existenciais limitadas de 2ª ordem (respectivamente quantificações universais limitadas de 2ª ordem).*

• *Uma **fórmula** $\Sigma_\infty^{1,b}$ é uma fórmula de $\mathcal{L}_2$ em que todas as quantificações de 1ª e 2ª ordem são limitadas.*

Definição 33 BTPSA *é a teoria de 2ª ordem, na linguagem $\mathcal{L}_2$, cujos axiomas são:*

• ***Axiomas básicos****;*

• ***Esquema de indução na notação para fórmulas*** $\Sigma_1^{1,b}$*-estendidas*
$$B(\varepsilon) \wedge \forall x(B(x) \rightarrow B(x0) \wedge B(x1)) \rightarrow \forall x B(x)$$
com B uma fórmula $\Sigma_1^{1,b}$-estendida que pode ter outras variáveis livres além de x;

• ***Esquema*** $\mathrm{B}\Sigma_\infty^{1,b}$
$$\forall x \preceq t \exists y \varphi(x,y) \rightarrow \exists z \forall x \preceq t \exists y \preceq z \varphi(x,y)$$
com t um termo onde x não ocorre e φ uma fórmula $\Sigma_\infty^{1,b}$ que pode ter outras variáveis livres além de x e y;

• ***Esquema*** $\mathrm{B}^1\Sigma_\infty^{1,b}$
$$\forall X \preceq t \exists y \varphi(y,X) \rightarrow \exists z \forall X \preceq t \exists y \preceq z \varphi(y,X)$$
com φ uma fórmula $\Sigma_\infty^{1,b}$ que pode ter outras variáveis livres além de y e X;

• ***Esquema*** $\Delta_1^0(\mathbf{PS})$
$$\forall x(\exists y \varphi(x,y) \longleftrightarrow \forall y \psi(x,y)) \rightarrow \exists X \forall x(x \in X \longleftrightarrow \exists y \varphi(x,y))$$
com φ uma fórmula $\Sigma_1^{1,b}$ e ψ uma fórmula $\Pi_1^{1,b}$ que podem ter outras variáveis livres além de x e y.

Proposição 18 *Em BTPSA é válida a seguinte implicação:*
$$\forall X \preceq t \forall x \preceq t \exists y \varphi(x,y,X) \rightarrow \exists z \forall X \preceq t \forall x \preceq t \exists y \preceq z \varphi(x,y,X)$$
sendo t um termo onde x não ocorre e φ uma fórmula $\Sigma_\infty^{1,b}$ que pode ter outras variáveis livres além de x, y e X.

Dem. Raciocinemos em $BTPSA$.

Suponhamos que $\forall X \preceq t \forall x \preceq t \exists y \varphi(x,y,X)$. Pelo esquema $B\Sigma_\infty^{1,b}$ temos que $\forall X \preceq t \exists z' \forall x \preceq t \exists y \preceq z' \varphi(x,y,X)$. Uma vez que $\forall x \preceq t \exists y \preceq z' \varphi(x,y,X)$ é uma fórmula $\Sigma_\infty^{1,b}$, o esquema $B^1\Sigma_\infty^{1,b}$ garante que $\exists z \forall X \preceq t \exists z' \preceq z \forall x \preceq t \exists y \preceq z' \varphi(x,y,X)$. Logo $\exists z \forall X \preceq t \forall x \preceq t \exists y \preceq z \varphi(x,y,X)$. ∎

---

*Apresentados na definição 17, no capítulo 3, aquando da definição da teoria $PSCA$.

Observação 20 *Tendo em conta que $\mathcal{L}_2^b \subseteq \mathcal{L}_2$, as teorias anteriormente estudadas, $\Sigma_1^{1,b}$-NIA e $\Sigma_1^{1,b}$-$NIA + B\Sigma_\infty^{1,b} + B^1\Sigma_\infty^{1,b}$, estão "contidas" em $BTPSA$, no sentido em que, todo o modelo de $BTPSA$ satisfaz os axiomas de $\Sigma_1^{1,b}$-$NIA + B\Sigma_\infty^{1,b} + B^1\Sigma_\infty^{1,b}$.*

Para nos convencermos da asserção anterior basta provar que o esquema de compreensão para fórmulas $\Sigma_0^{1,b}$ é válido em $BTPSA$. Seja, então, $A(x)$ uma fórmula $\Sigma_0^{1,b}$ que pode ter outras variáveis livres além de x, mas na qual y não ocorre. A fórmula $x \preceq a \wedge A(x)$, com a variável livre, é simultaneamente $\Sigma_1^{1,b}$ e $\Pi_1^{1,b}$ e como $BTPSA \vdash \forall a \forall x(\exists y(x \preceq a \wedge A(x)) \longleftrightarrow \forall y\ (x \preceq a \wedge A(x)))$ temos, pelo esquema $\Delta_1^0(PS)$ que $BTPSA \vdash \forall a \exists X \forall x(x \in X \longleftrightarrow \exists y(x \preceq a \wedge A(x)))$. Logo temos que $BTPSA \vdash \forall a \exists X \preceq a \forall x \preceq a(x \in X \longleftrightarrow A(x))$ como pretendiamos demonstrar.

7.2 Caracterização das funções demonstravelmente totais de BTPSA

Seja $\mathcal{M}$ um modelo de $BTPSA$. O seu domínio, notado por $|\mathcal{M}| = (M, S)$, indica que as variáveis de 1^a ordem tomam valores em M e as de 2^a ordem tomam valores em S, um subconjunto de $\mathcal{P}(M)$. O modelo intencionado de $BTPSA$ é $\mathcal{M}$ tal que $|\mathcal{M}| = (2^{<\omega}, \mathcal{P}(2^{<\omega}))$ e com as interpretações usuais.

Lema 6 *(Lema Principal)*
Se $\mathcal{M}$, com domínio $|\mathcal{M}| = (M, S_b)$, é um modelo da teoria $\Sigma_1^{1,b}$-$NIA + B\Sigma_\infty^{1,b} + B^1\Sigma_\infty^{1,b}$ (na linguagem $\mathcal{L}_2^b$) então existe $S \subseteq \mathcal{P}(M)$ tal que $\mathcal{M}^*$, com domínio $|\mathcal{M}^*| = (M, S)$, é um modelo da teoria $BTPSA$ (na linguagem $\mathcal{L}_2$) tendo-se que $S_b = \{X^a : X \in S$ e $a \in M\}$.

Dem. Seja S constituído pelos subconjuntos $X \subseteq M$ para os quais existem fórmulas $\varphi(x, y, \bar{q}, \bar{Q}^{p(x,y,\bar{q})})$ e $\psi(x, y, \bar{p}, \bar{P}^{u(x,y,\bar{p})})$ respectivamente $\Sigma_1^{1,b}$ e $\Pi_1^{1,b}$ e elementos $\bar{a}$, $\bar{b}$ em M e $\bar{A}^p$, $\bar{B}^u$ em S_b tais que $X = \{x \in M : \mathcal{M} \models \exists y \varphi(x, y, \bar{a}, \bar{A}^{p(x,y,\bar{a})})\} = \{x \in M : \mathcal{M} \models \forall y \psi(x, y, \bar{b}, \bar{B}^{u(x,y,\bar{b})})\}$.

$\boxed{\text{Vejamos que } S_b = \{X^a : X \in S \text{ e } a \in M\}}$

$\boxed{\subseteq}$ Dado $A \in S_b$ existe $a \in M$ tal que $\forall x(x \in A \to x \preceq a)$. Logo $A = A^a$. Seja $\varphi(x) := x \in A^a$, que é uma fórmula $\Sigma_0^{1,b}$, logo $\Sigma_1^{1,b}$, e seja $\psi(x) := x \in A^a$, que é uma fórmula $\Pi_0^{1,b}$, logo $\Pi_1^{1,b}$. Temos que $A = \{x \in M : \mathcal{M} \models \exists y(x \in A^a)\} = \{x \in M : \mathcal{M} \models \forall y(x \in A^a)\}$. Logo $A \in S$.

$\boxed{\supseteq}$ Seja $C \in S$ e $c \in M$. Demonstremos que $C^c \in S_b$.

Como $C \in S$ existem fórmulas $\Sigma_1^{1,b}$, φ, e $\Pi_1^{1,b}$, ψ e existem $\bar{a}$, $\bar{b}$ em M e $\bar{A}$, $\bar{B}$ em S_b tais que $C = \{x \in M : \mathcal{M} \models \exists y \varphi(x, y, \bar{a}, \bar{A})\} = \{x \in M : \mathcal{M} \models \forall y \psi(x, y, \bar{b}, \bar{B})\}$. Portanto $\mathcal{M} \models \forall x(\exists y \varphi(x, y, \bar{a}, \bar{A}) \longleftrightarrow \forall y \psi(x, y, \bar{b}, \bar{B}))$. Assim temos:

1) $\mathcal{M} \models \forall x \forall y \forall z(\varphi(x, y, \bar{a}, \bar{A}) \to \psi(x, z, \bar{b}, \bar{B}))$ e

2) $\mathcal{M} \models \forall x \exists y \exists z(\psi(x, y, \bar{b}, \bar{B}) \to \varphi(x, z, \bar{a}, \bar{A}))$.

De 2) sai em particular que $\mathcal{M} \models \forall x \preceq c \exists y \exists z(\psi(x, y, \bar{b}, \bar{B}) \to \varphi(x, z, \bar{a}, \bar{A}))$. Logo $\mathcal{M} \models \forall x \preceq c \underbrace{\exists \omega \exists y \preceq \omega \exists z \preceq \omega(\psi(x, y, \bar{b}, \bar{B}) \to \varphi(x, z, \bar{a}, \bar{A}))}_{\text{fórmula } \Sigma_\infty^{1,b}}$. Por $B\Sigma_\infty^{1,b}$ temos

que $\mathcal{M} \models \exists d \forall x \preceq c \exists \omega \preceq d \exists y \preceq \omega \exists z \preceq \omega(\psi(x,y,\bar{b},\bar{B}) \rightarrow \varphi(x,z,\bar{a},\bar{A}))$. Logo $\mathcal{M} \models \exists d \forall x \preceq c \exists y \preceq d \exists z \preceq d(\psi(x,y,\bar{b},\bar{B}) \rightarrow \varphi(x,z,\bar{a},\bar{A}))$. Temos assim que $\mathcal{M} \models \exists d \forall x \preceq c(\forall y \preceq d\psi(x,y,\bar{b},\bar{B}) \rightarrow \exists y \preceq d\varphi(x,y,\bar{a},\bar{A}))$. Seja $d \in M$ tal que (*) $\mathcal{M} \models \forall x \preceq c(\forall y \preceq d\psi(x,y,\bar{b},\bar{B}) \rightarrow \exists y \preceq d\varphi(x,y,\bar{a},\bar{A}))$. De 1) temos que $\mathcal{M} \models \forall x \preceq c \forall y \preceq d \forall z \preceq d(\varphi(x,y,\bar{a},\bar{A}) \rightarrow \psi(x,z,\bar{b},\bar{B}))$. Logo temos (**) $\mathcal{M} \models$ $\models \forall x \preceq c(\exists y \preceq d\varphi(x,y,\bar{a},\bar{A}) \rightarrow \forall y \preceq d\psi(x,y,\bar{b},\bar{B}))$.
De (*) e (**) temos que $\mathcal{M} \models \forall x \preceq c(\underbrace{\exists y \preceq d\varphi(x,y,\bar{a},\bar{A})}_{\text{fórmula } \Sigma_1^{1,b}\text{-}estendida} \longleftrightarrow \underbrace{\forall y \preceq d\psi(x,y,\bar{b},\bar{B})}_{\text{fórmula } \Pi_1^{1,b}\text{-}estendida})$.

Como em $\Sigma_1^{1,b}$-NIA temos compreensão para fórmulas $\Delta_1^{1,b}$-*estendidas* vem que $\mathcal{M} \models \exists F^c \forall x \preceq c(x \in F^c \longleftrightarrow \exists y \preceq d\varphi(x,y,\bar{a},\bar{A}))$.

$F^c = \{x \preceq c : \exists y \preceq d\varphi(x,y,\bar{a},\bar{A})\} = \{x \preceq c : \exists y\varphi(x,y,\bar{a},\bar{A})\} = C^c$. Vejamos que a segunda igualdade é de facto válida.

$\boxed{\subseteq}$ imediato.

$\boxed{\supseteq}$ Seja $x \preceq c$ tal que $\exists y\varphi(x,y,\bar{a},\bar{A})$. Como $\exists y\varphi(x,y,\bar{a},\bar{A}) \rightarrow \forall y\psi(x,y,\bar{b},\bar{B})$, temos, em particular, que $\forall y \preceq d\psi(x,y,\bar{b},\bar{B})$. Pela forma como definimos d sabemos que $\exists y \preceq d\varphi(x,y,\bar{a},\bar{A})$, provando-se assim a inclusão pretendida.

$\therefore C^c \in S_b$.

$\boxed{\text{Sendo } |\mathcal{M}^*| = (M,S)\text{, vejamos que } \mathcal{M}^* \text{ é modelo de } BTPSA}$

Como em $\mathcal{M}^*$ as constantes, os símbolos funcionais e os relacionais são interpretados do mesmo modo que em $\mathcal{M}$ (com $|\mathcal{M}| = (M, S_b)$) e como a parte de 1^a ordem em ambos os modelos coincide, temos que os axiomas básicos são verificados em $\mathcal{M}^*$ (visto o serem em $\mathcal{M}$).

FACTO: Dada $\varphi(\bar{u},\bar{U})$ uma fórmula $\Sigma_\infty^{1,b}$, existe um termo $t(\bar{u})$ com a seguinte propriedade: dados $\bar{c}$ em M e $\bar{C}$ em S então $\mathcal{M}^* \models \varphi(\bar{c},\bar{C}) \Longleftrightarrow \mathcal{M} \models \varphi(\bar{c},\bar{C}^b)$ sempre que $t(\bar{c}) \preceq b$.

DEM. DO FACTO:

A demonstração é feita por indução na complexidade de φ.

• Seja $\varphi :\longleftrightarrow t_1 = t_2$ com t_1 e t_2 termos. Temos $\mathcal{M}^* \models \varphi \Longleftrightarrow \mathcal{M} \models \varphi$.

• Seja $\varphi :\longleftrightarrow t_1 \subseteq t_2$ com t_1 e t_2 termos. Temos $\mathcal{M}^* \models \varphi \Longleftrightarrow \mathcal{M} \models \varphi$.

• Seja $\varphi(\bar{u},U) :\longleftrightarrow t(\bar{u}) \in U$. Dados $\bar{c}$ em M e C em S temos que $\mathcal{M}^* \models t(\bar{c}) \in C \Longleftrightarrow \mathcal{M} \models t(\bar{c}) \in C^b$ sempre que $t(\bar{c}) \preceq b$.

• Seja $\varphi(\bar{u},\bar{U}) :\longleftrightarrow \neg\psi(\bar{u},\bar{U})$. Por hipótese de indução existe $t(\bar{u})$ tal que, dados $\bar{c}$ em M e $\bar{C}$ em S se tem $\mathcal{M}^* \models \psi(\bar{c},\bar{C}) \Longleftrightarrow \mathcal{M} \models \psi(\bar{c},\bar{C}^b)$ sempre que $t(\bar{c}) \preceq b$. Logo

$$\begin{aligned} \mathcal{M}^* \models \varphi(\bar{c},\bar{C}) &\Longleftrightarrow \mathcal{M}^* \models \neg\psi(\bar{c},\bar{C}) \\ &\Longleftrightarrow \mathcal{M}^* \not\models \psi(\bar{c},\bar{C}) \\ &\underset{H.I.}{\Longleftrightarrow} \mathcal{M} \not\models \psi(\bar{c},\bar{C}^b) \text{ sempre que } t(\bar{c}) \preceq b \\ &\Longleftrightarrow \mathcal{M} \models \neg\psi(\bar{c},\bar{C}^b) \text{ sempre que } t(\bar{c}) \preceq b \\ &\Longleftrightarrow \mathcal{M} \models \varphi(\bar{c},\bar{C}^b) \text{ sempre que } t(\bar{c}) \preceq b. \end{aligned}$$

• Seja $\varphi(\bar{u},\bar{U}) :\longleftrightarrow (\psi \wedge \theta)(\bar{u},\bar{U})$. Por hipótese de indução existem termos $t_1(\bar{u})$ e $t_2(\bar{u})$ tais que, dados $\bar{c}$ em M e $\bar{C}$ em S se tem $\mathcal{M}^* \models \psi(\bar{c},\bar{C}) \Longleftrightarrow$

$\iff \mathcal{M} \models \psi(\bar{c}, \bar{C}^{b_1})$ sempre que $t_1(\bar{c}) \preceq b_1$ e $\mathcal{M}^* \models \theta(\bar{c}, \bar{C}) \iff \mathcal{M} \models \theta(\bar{c}, \bar{C}^{b_2})$ sempre que $t_2(\bar{c}) \preceq b_2$. Logo, sendo $t(\bar{u}) := t_1(\bar{u}) \frown t_2(\bar{u})$ temos que $\mathcal{M}^* \models \psi(\bar{c}, \bar{C}) \iff$ $\iff \mathcal{M} \models \psi(\bar{c}, \bar{C}^b)$ sempre que $t(\bar{c}) \preceq b$ e $\mathcal{M}^* \models \theta(\bar{c}, \bar{C}) \iff \mathcal{M} \models \theta(\bar{c}, \bar{C}^b)$ sempre que $t(\bar{c}) \preceq b$.

$$\begin{aligned}
\mathcal{M}^* \models (\psi \wedge \theta)(\bar{c}, \bar{C}) &\iff \mathcal{M}^* \models \psi(\bar{c}, \bar{C}) \text{ e } \mathcal{M}^* \models \theta(\bar{c}, \bar{C}) \\
&\underset{H.I.}{\iff} \mathcal{M} \models \psi(\bar{c}, \bar{C}^b) \text{ e } \mathcal{M} \models \theta(\bar{c}, \bar{C}^b) \text{ sempre que } t(\bar{c}) \preceq b \\
&\iff \mathcal{M} \models (\psi \wedge \theta)(\bar{c}, \bar{C}^b) \text{ sempre que } t(\bar{c}) \preceq b.
\end{aligned}$$

- Caso $\varphi :\longleftrightarrow \psi \vee \theta$ é análogo ao anterior.
- Caso $\varphi :\longleftrightarrow \psi \to \theta$ sai dos anteriores.
- Seja $\varphi(\bar{u}, \bar{U}) :\longleftrightarrow \forall x \preceq q(\bar{u})\psi(x, \bar{u}, \bar{U})$. Consideremos $\theta(x, \bar{u}, \bar{U})$ a fórmula $x \preceq q(\bar{u}) \to \psi(x, \bar{u}, \bar{U})$. A hipótese de indução garante a existência de um termo $t'(x, \bar{u})$ tal que, dados $a, \bar{c}$ em M e $\bar{C}$ em S se tem $\mathcal{M}^* \models a \preceq q(\bar{c}) \to \psi(a, \bar{c}, \bar{C}) \iff$ $\iff \mathcal{M} \models a \preceq q(\bar{c}) \to \psi(a, \bar{c}, \bar{C}^b)$ sempre que $t'(a, \bar{c}) \preceq b$. Seja $t(\bar{u}) := t'(q(\bar{u}), \bar{u})$, temos que $\mathcal{M}^* \models a \preceq q(\bar{c}) \to \psi(a, \bar{c}, \bar{C}) \iff \mathcal{M} \models a \preceq q(\bar{c}) \to \psi(a, \bar{c}, \bar{C}^b)$ sempre que $t(\bar{c}) \preceq b$. Logo

$$\begin{aligned}
\mathcal{M}^* \models \forall x \preceq q(\bar{c})\psi(x, \bar{c}, \bar{C}) &\iff \text{para todo } a \in M,\ \mathcal{M}^* \models a \preceq q(\bar{c}) \to \psi(a, \bar{c}, \bar{C}) \\
&\underset{H.I.}{\iff} \text{para todo } a \in M,\ \mathcal{M} \models a \preceq q(\bar{c}) \to \psi(a, \bar{c}, \bar{C}^b) \\
&\qquad \text{sempre que } t(\bar{c}) \preceq b \\
&\iff \mathcal{M} \models \forall x \preceq q(\bar{c})\psi(x, \bar{c}, \bar{C}^b) \text{ sempre que } t(\bar{c}) \preceq b.
\end{aligned}$$

- Caso $\varphi(\bar{u}, \bar{U}) :\longleftrightarrow \exists x \preceq q(\bar{u})\psi(x, \bar{u}, \bar{U})$ é análogo ao anterior.
- Seja $\varphi(\bar{u}, \bar{U}) :\longleftrightarrow \forall X \preceq q(\bar{u})\psi(\bar{u}, X, \bar{U})$. Consideremos $\theta(\bar{u}, X, \bar{U})$ como sendo a fórmula $X \preceq q(\bar{u}) \to \psi(\bar{u}, X, \bar{U})$. Por hipótese de indução existe um termo $t'(\bar{u})$ tal que, dados $\bar{c}$ em M e $A, \bar{C}$ em S se tem $\mathcal{M}^* \models A \preceq q(\bar{c}) \to \psi(\bar{c}, A, \bar{C}) \iff$ $\iff \mathcal{M} \models A^b \preceq q(\bar{c}) \to \psi(\bar{c}, A^b, \bar{C}^b)$ sempre que $t'(\bar{c}) \preceq b$. Seja $t(\bar{u}) := t'(\bar{u}) \frown q(\bar{u})$. Temos então que $\mathcal{M}^* \models A \preceq q(\bar{c}) \to \psi(\bar{c}, A, \bar{C}) \iff \mathcal{M} \models A^b \preceq q(\bar{c}) \to \psi(\bar{c}, A^b, \bar{C}^b)$ sempre que $t(\bar{c}) \preceq b$. Logo $\mathcal{M}^* \models A \preceq q(\bar{c}) \to \psi(\bar{c}, A, \bar{C}) \iff \mathcal{M} \models A \preceq q(\bar{c}) \to$ $\to \psi(\bar{c}, A, \bar{C}^b)$ sempre que $t(\bar{c}) \preceq b$.

$$\begin{aligned}
\mathcal{M}^* \models \forall X \preceq q(\bar{c})\psi(\bar{c}, X, \bar{C}) &\iff \text{para todo } A \in S,\ \mathcal{M}^* \models A \preceq q(\bar{c}) \to \psi(\bar{c}, A, \bar{C}) \\
&\underset{H.I.}{\iff} \text{para todo } A \in S,\ \mathcal{M} \models A \preceq q(\bar{c}) \to \psi(\bar{c}, A, \bar{C}^b) \\
&\qquad \text{sempre que } t(\bar{c}) \preceq b \\
&\iff \text{para todo } A \in S_b,\ \mathcal{M} \models A \preceq q(\bar{c}) \to \psi(\bar{c}, A, \bar{C}^b) \\
&\qquad \text{sempre que } t(\bar{c}) \preceq b \\
&\iff \mathcal{M} \models \forall X^{q(\bar{c})}\psi(\bar{c}, X^{q(\bar{c})}, \bar{C}^b) \text{ sempre que } t(\bar{c}) \preceq b.
\end{aligned}$$

- Caso $\varphi(\bar{u}, \bar{U}) :\longleftrightarrow \exists X \preceq q(\bar{u})\psi(\bar{u}, X, \bar{U})$ é análogo ao anterior.

c.q.d.

$\boxed{\text{Vejamos que em } \mathcal{M}^* \text{ é válida indução na notação para fórmulas } \Sigma_1^{1,b}\textit{-estendidas}}$

Suponhamos que $\mathcal{M}^* \models B(\varepsilon, \bar{a}, \bar{A}) \wedge \forall x(B(x, \bar{a}, \bar{A}) \to B(x0, \bar{a}, \bar{A}) \wedge B(x1, \bar{a}, \bar{A}))$ com B uma fórmula $\Sigma_1^{1,b}$-*estendida*. Queremos provar que $\mathcal{M}^* \models \forall x B(x, \bar{a}, \bar{A})$. Fixemos c em M. Temos que $\mathcal{M}^* \models B(\varepsilon, \bar{a}, \bar{A}) \wedge \forall x \preceq c(B(x, \bar{a}, \bar{A}) \to B(x0, \bar{a}, \bar{A}) \wedge$ $\wedge B(x1, \bar{a}, \bar{A}))$. Considerando $\varphi(v, \bar{u}, \bar{U})$ a fórmula $\Sigma_\infty^{1,b}$ $B(\varepsilon, \bar{u}, \bar{U}) \wedge \forall x \preceq v(B(x, \bar{u}, \bar{U}) \to$

$\to B(x0,\bar{u},\bar{U}) \wedge B(x1,\bar{u},\bar{U}))$, pelo facto atrás demonstrado, existe um termo $t(v,\bar{u})$ tal que, dados c, $\bar{a}$ em M e $\bar{A}$ em S se tem $\mathcal{M} \models B(\varepsilon,\bar{a},\bar{A}^b) \wedge \forall x \preceq c(B(x,\bar{a},\bar{A}^b) \to$ $\to B(x0,\bar{a},\bar{A}^b) \wedge B(x1,\bar{a},\bar{A}^b))$ sempre que $t(c,\bar{a}) \preceq b$.

Pelo esquema de indução na notação para fórmulas $\Sigma_1^{1,b}$-*estendidas* (válido em $\mathcal{M}$) temos que $\mathcal{M} \models \forall x \preceq cB(x,\bar{a},\bar{A}^b)$ sempre que $t(c,\bar{a}) \preceq b$. Considerando a fórmula $\Sigma_\infty^{1,b}$ $\varphi'(v,\bar{u},\bar{U}) :\longleftrightarrow \forall x \preceq vB(x,\bar{u},\bar{U})$, novamente pelo facto anterior, existe $t'(v,\bar{u})$ tal que, dados c, $\bar{a}$ em M e $\bar{A}$ em S se tem $\mathcal{M}^* \models \varphi'(c,\bar{a},\bar{A}) \iff \mathcal{M} \models$ $\models \varphi'(c,\bar{a},\bar{A}^{b'})$ sempre que $t'(c,\bar{a}) \preceq b'$. Seja $b'' := t(c,\bar{a}) \frown t'(c,\bar{a})$. Como evidentemente se tem que $\mathcal{M} \models \forall x \preceq cB(x,\bar{a},\bar{A}^{b''})$ vem que $\mathcal{M}^* \models \forall x \preceq cB(x,\bar{a},\bar{A})$. Logo $\mathcal{M}^* \models B(c,\bar{a},\bar{A})$. Como c era um elemento arbitrário de M, temos que $\mathcal{M}^* \models \forall x B(x,\bar{a},\bar{A})$.

$\boxed{\text{Vejamos que o esquema } B\Sigma_\infty^{1,b} \text{ é válido em } \mathcal{M}^*}$

Suponhamos que $\mathcal{M}^* \models \forall x \preceq q(\bar{a})\exists y\varphi(x,y,\bar{a},\bar{A})$ com φ uma fórmula $\Sigma_\infty^{1,b}$. Queremos provar que $\mathcal{M}^* \models \exists z\forall x \preceq q(\bar{a})\exists y \preceq z\varphi(x,y,\bar{a},\bar{A})$. Aplicando o facto anterior a $\varphi(x,y,\bar{u},\bar{U})$ sabemos que existe um termo $t(x,y,\bar{u})$ tal que, dados $s,r,\bar{a}$ em M e $\bar{A}$ em S se tem $\mathcal{M}^* \models \varphi(s,r,\bar{a},\bar{A})$ sse $\mathcal{M} \models \varphi(s,r,\bar{a},\bar{A}^b)$ sempre que $t(s,r,\bar{a}) \preceq b$. Logo

(*) $\mathcal{M} \models \forall x \preceq q(\bar{a})\exists y\varphi(x,y,\bar{a},\bar{A}^{t(q(\bar{a}),y,\bar{a})})$.

Notemos que, de facto, até se tem $\mathcal{M} \models \forall x \preceq q(\bar{a})\exists y\forall b(t(q(\bar{a}),y,\bar{a}) \preceq b \to$ $\to \varphi(x,y,\bar{a},\bar{A}^b))$. Pelo esquema $B\Sigma_\infty^{1,b}$ (que sabemos ser válido em $\mathcal{M}$), de (*) vem que $\mathcal{M} \models \exists z\forall x \preceq q(\bar{a})\exists y \preceq z\varphi(x,y,\bar{a},\bar{A}^{t(q(\bar{a}),y,\bar{a})})$.

Seja $z \in M$ tal que $\mathcal{M} \models \forall x \preceq q(\bar{a})\exists y \preceq z\varphi(x,y,\bar{a},\bar{A}^{t(q(\bar{a}),y,\bar{a})})$. Seja $\varphi'(v,\bar{u},\bar{U}) :\longleftrightarrow \underbrace{\forall x \preceq q(\bar{u})\exists y \preceq v\varphi(x,y,\bar{u},\bar{U})}_{\text{fórmula } \Sigma_\infty^{1,b}}$. Pelo facto anterior, sabemos que existe $t'(v,\bar{u})$ tal que, dados $z,\bar{a}$ em M e $\bar{A}$ em S se tem $\mathcal{M}^* \models \varphi'(z,\bar{a},\bar{A})$ sse $\mathcal{M} \models \varphi'(z,\bar{a},\bar{A}^{b'})$ sempre que $t'(z,\bar{a}) \preceq b'$. Seja $b' := t(q(\bar{a}),z,\bar{a}) \frown t'(z,\bar{a})$. Sabemos que $\mathcal{M} \models \forall x \preceq q(\bar{a})\exists y \preceq z\varphi(x,y,\bar{a},\bar{A}^{t(q(\bar{a}),y,\bar{a})})$ e também $\mathcal{M} \models \forall x \preceq q(\bar{a})\exists y \preceq z$ $\varphi(x,y,\bar{a},\bar{A}^{b'})$. Logo temos $\mathcal{M}^* \models \forall x \preceq q(\bar{a})\exists y \preceq z\varphi(x,y,\bar{a},\bar{A})$.

$\therefore \mathcal{M}^* \models \exists z\forall x \preceq q(\bar{a})\exists y \preceq z\varphi(x,y,\bar{a},\bar{A})$.

$\boxed{\text{Vejamos que o esquema } B^1\Sigma_\infty^{1,b} \text{ é válido em } \mathcal{M}^*}$

Suponhamos que $\mathcal{M}^* \models \forall X \preceq q(\bar{a})\exists y\varphi(y,X,\bar{a},\bar{A})$ com φ uma fórmula $\Sigma_\infty^{1,b}$. Queremos provar que $\mathcal{M}^* \models \exists z\forall X \preceq q(\bar{a})\exists y \preceq z\varphi(y,X,\bar{a},\bar{A})$. Aplicando o facto anterior a $\varphi(y,X,\bar{u},\bar{U})$ sabemos que existe um termo $t(y,\bar{u})$ tal que, dados $s,\bar{a}$ em M e $C,\bar{A}$ em S se tem $\mathcal{M}^* \models \varphi(s,C,\bar{a},\bar{A})$ sse $\mathcal{M} \models \varphi(s,C^b,\bar{a},\bar{A}^b)$ sempre que $t(s,\bar{a}) \preceq b$, em particular sempre que $t(s,\bar{a}) \frown q(\bar{a}) \preceq b$. Logo

(*) $\mathcal{M} \models \forall X^{q(\bar{a})}\exists y\varphi(y,X^{q(\bar{a})},\bar{a},\bar{A}^{t(y,\bar{a})\frown q(\bar{a})})$.

Mas notemos que, de facto, até se tem $\mathcal{M} \models \forall X^{q(\bar{a})}\exists y\forall b(t(y,\bar{a}) \frown q(\bar{a}) \preceq b \to$ $\to \varphi(y,X^{q(\bar{a})},\bar{a},\bar{A}^b))$. Pelo esquema $B^1\Sigma_\infty^{1,b}$ (que sabemos ser válido em $\mathcal{M}$), de (*) vem que $\mathcal{M} \models \exists z\forall X^{q(\bar{a})}\exists y \preceq z\varphi(y,X^{q(\bar{a})},\bar{a},\bar{A}^{t(y,\bar{a})\frown q(\bar{a})})$.

Seja $z \in M$ tal que $\mathcal{M} \models \forall X^{q(\bar{a})} \exists y \preceq z\varphi(y, X^{q(\bar{a})}, \bar{a}, \bar{A}^{t(y,\bar{a})\frown q(\bar{a})})$. Consideremos $\varphi'(v, \bar{u}, \bar{U}) :\longleftrightarrow \underbrace{\forall X \preceq q(\bar{u}) \exists y \preceq v\varphi(y, X, \bar{u}, \bar{U})}_{\text{fórmula } \Sigma^{1,b}_{\infty}}$. Pelo facto anterior, sabemos que existe um termo $t'(v, \bar{u})$ tal que, dados $z, \bar{a}$ em M e $\bar{A}$ em S se tem que $\mathcal{M}^* \models$ $\models \forall X \preceq q(\bar{a}) \exists y \preceq z\varphi(y, X, \bar{a}, \bar{A})$ sse $\mathcal{M} \models \forall X^{q(\bar{a})} \exists y \preceq z\varphi(y, X^{q(\bar{a})}, \bar{a}, \bar{A}^{b'})$ sempre que $t'(z, \bar{a}) \preceq b'$. Seja $b' := t(z, \bar{a}) \frown q(\bar{a}) \frown t'(z, \bar{a})$. Sabemos que $\mathcal{M} \models \forall X^{q(\bar{a})} \exists y \preceq$ $\preceq z\varphi(y, X^{q(\bar{a})}, \bar{a}, \bar{A}^{t(y,\bar{a})\frown q(\bar{a})})$ e também que $\mathcal{M} \models \forall X^{q(\bar{a})} \exists y \preceq z\ \varphi(y, X^{q(\bar{a})}, \bar{a}, \bar{A}^{b'})$. Logo vem que $\mathcal{M}^* \models \forall X \preceq q(\bar{a}) \exists y \preceq z\varphi(y, X, \bar{a}, \bar{A})$ e portanto $\mathcal{M}^* \models \exists z \forall X \preceq q(\bar{a})$ $\exists y \preceq z\varphi(y, X, \bar{a}, \bar{A})$.

$\boxed{\text{Vejamos que o esquema } \Delta^0_1(PS) \text{ é válido em } \mathcal{M}^*}$

Suponhamos que $\mathcal{M}^* \models \forall x(\exists y\varphi(x, y, \bar{a}, \bar{A}) \longleftrightarrow \forall y\psi(x, y, \bar{b}, \bar{B}))$ com φ uma fórmula $\Sigma^{1,b}_1$ e ψ uma fórmula $\Pi^{1,b}_1$. Queremos provar que $\mathcal{M}^* \models \exists X \forall x(x \in X \longleftrightarrow$ $\longleftrightarrow \exists y\varphi(x, y, \bar{a}, \bar{A}))$. Consideremos $\varphi(x, y, \bar{u}, \bar{U})$ que sendo uma fórmula $\Sigma^{1,b}_1$ é, em particular, $\Sigma^{1,b}_{\infty}$ e $\psi(x, y, \bar{u}, \bar{U})$ que sendo uma fórmula $\Pi^{1,b}_1$ também é $\Sigma^{1,b}_{\infty}$. Aplicando o facto atrás demonstrado a φ, temos garantida a existência de um termo $p(x, y, \bar{u})$ tal que, dados $s, r, \bar{a}$ em M e $\bar{A}$ em S se tem

(*) $\mathcal{M}^* \models \varphi(s, r, \bar{a}, \bar{A}) \iff \mathcal{M} \models \varphi(s, r, \bar{a}, \bar{A}^b)$ sempre que $p(s, r, \bar{a}) \preceq b$. Aplicando o mesmo facto agora à fórmula ψ sabemos que existe um termo $u(x, y, \bar{u})$ tal que, dados $s, r, \bar{b}$ em M e $\bar{B}$ em S se tem $\mathcal{M}^* \models \psi(s, r, \bar{b}, \bar{B}) \iff \mathcal{M} \models \psi(s, r, \bar{b}, \bar{B}^{b'})$ sempre que $u(s, r, \bar{b}) \preceq b'$. Logo de $\mathcal{M}^* \models \forall x(\exists y\varphi(x, y, \bar{a}, \bar{A}) \longleftrightarrow \forall y\psi(x, y, \bar{b}, \bar{B}))$ temos que $\mathcal{M} \models \forall x(\exists y\varphi(x, y, \bar{a}, \bar{A}^{p(x,y,\bar{a})}) \longleftrightarrow \forall y\psi(x, y, \bar{b}, \bar{B}^{u(x,y,\bar{b})}))$. Seja $X =$ $= \{x \in M : \mathcal{M} \models \exists y\varphi(x, y, \bar{a}, \bar{A}^{p(x,y,\bar{a})})\} = \{x \in M : \mathcal{M} \models \forall y\psi(x, y, \bar{b}, \bar{B}^{u(x,y,\bar{b})})\}$. Pela forma como S foi definido temos que $X \in S$. Como por (*) sabemos que $\mathcal{M}^* \models \exists y\varphi(s, y, \bar{a}, \bar{A}) \iff \mathcal{M} \models \exists y\varphi(s, y, \bar{a}, \bar{A}^{p(s,y,\bar{a})})$ vem que $X = \{x \in M : \mathcal{M}^* \models$ $\models \exists y\varphi(x, y, \bar{a}, \bar{A})\}$. Logo $\mathcal{M}^* \models \exists X \forall x(x \in X \longleftrightarrow \exists y\varphi(x, y, \bar{a}, \bar{A}))$.

Provámos assim que $\mathcal{M}^*$ é modelo de $BTPSA$. ∎

Teorema 8 *Se $BTPSA \models \forall \bar{x} \exists y\varphi(\bar{x}, y)$ com φ uma fórmula $\Sigma^{1,b}_{\infty}$ na linguagem $\mathcal{L}^b_2$ então $\Sigma^{1,b}_1$-$NIA \models \forall \bar{x} \exists y\varphi(\bar{x}, y)$.*

Dem. Seja φ uma fórmula $\Sigma^{1,b}_{\infty}$ na linguagem $\mathcal{L}^b_2$ tal que $BTPSA \models \forall \bar{x} \exists y\varphi(\bar{x}, y)$. Suponhamos com vista a absurdo que $\Sigma^{1,b}_1$-$NIA + B\Sigma^{1,b}_{\infty} + B^1\Sigma^{1,b}_{\infty} \not\models \forall \bar{x} \exists y\varphi(\bar{x}, y)$. Então existe $\mathcal{M}$ um modelo de $\Sigma^{1,b}_1$-$NIA + B\Sigma^{1,b}_{\infty} + B^1\Sigma^{1,b}_{\infty}$, com $|\mathcal{M}| = (M, S_b)$, tal que $\mathcal{M} \not\models \forall \bar{x} \exists y\varphi(\bar{x}, y)$ ou seja $\mathcal{M} \models \exists \bar{x} \forall y \neg\varphi(\bar{x}, y)$.

Pelo lema principal sabemos que existe $S \subseteq \mathcal{P}(M)$ tal que $\mathcal{M}^*$, com $|\mathcal{M}^*| =$ $= (M, S)$, é modelo de $BTPSA$ e $S_b = \{X^a : X \in S \text{ e } a \in M\}$.

Vejamos que de $\mathcal{M} \models \exists \bar{x} \forall y \neg\varphi(\bar{x}, y)$ se tem que $\mathcal{M}^* \models \exists \bar{x} \forall y \neg\varphi(\bar{x}, y)$.

Considerando $\bar{a}$ como sendo elementos de M tais que $\mathcal{M} \models \forall y \neg\varphi(\bar{a}, y)$, basta provar que $\mathcal{M}^* \models \forall y \neg\varphi(\bar{a}, y)$. Ora isso é óbvio uma vez que, dado $c \in M$ fixo, se tem $\mathcal{M} \models \neg\varphi(\bar{a}, c) \underset{Facto}{\iff} \mathcal{M}^* \models \neg\varphi(\bar{a}, c)$.

Temos assim que $\mathcal{M}^* \models \exists \bar{x} \forall y \neg\varphi(\bar{x}, y)$, o que é <u>absurdo</u> pois $\mathcal{M}^*$ é modelo de $BTPSA$ e por hipótese $BTPSA \models \forall \bar{x} \exists y\varphi(\bar{x}, y)$.

$\therefore\ \Sigma_1^{1,b}\text{-}NIA + B\Sigma_\infty^{1,b} + B^1\Sigma_\infty^{1,b} \models \forall\bar{x}\exists y\varphi(\bar{x}, y)$.

Como $\Sigma_1^{1,b}\text{-}NIA + B\Sigma_\infty^{1,b} + B^1\Sigma_\infty^{1,b}$ é $\forall\exists\Sigma_\infty^{1,b}$-*conservativa* sobre $\Sigma_1^{1,b}\text{-}NIA$ (provado na proposição 17 do capítulo anterior) temos que $\Sigma_1^{1,b}\text{-}NIA \models \forall\bar{x}\exists y\varphi(\bar{x}, y)$. ■

Como, em particular, o teorema anterior é válido para fórmulas $\Sigma_1^{1,b}$ na linguagem $\mathcal{L}_2^b$, temos que as funções demonstravelmente totais de $BTPSA$ com gráfico $\Sigma_1^{1,b}$ em $\mathcal{L}_2^b$ continuam a ser as funções de $PSPACE$.

Capítulo 8
APÊNDICE

8.1 Teoria Σ_1^b-NIA

Definição 34 *A classe das **fórmulas com quantificações de subpalavras** é a menor classe de fórmulas de $\mathcal{L}$ que contém as fórmulas atómicas e é fechada para os conectivos Booleanos e quantificações de subpalavras, i.e. quantificações da forma $\forall x(x \subseteq^* t \to \phi)$ ou $\exists x(x \subseteq^* t \land \phi)$ em que t é um termo onde x não ocorre.*

Definição 35 *Uma **fórmula** Σ_1^b é uma fórmula de $\mathcal{L}$ da forma $\exists x(x \preceq t \land \phi)$ onde ϕ é uma fórmula com quantificações de subpalavras e x não ocorre em t.*

Estamos agora em condições de definir a teoria Σ_1^b-NIA.

Definição 36 **Σ_1^b-NIA** *é a teoria de 1ª ordem, na linguagem $\mathcal{L}$, constituída pelos seguintes axiomas:*

- ***Axiomas básicos,****[*]
- ***Esquema de indução na notação para fórmulas** Σ_1^b*
  $\phi(\varepsilon) \land \forall x(\phi(x) \to \phi(x0) \land \phi(x1)) \to \forall x\phi(x)$
  onde ϕ é uma fórmula Σ_1^b, que pode ter outras variáveis livres além de x.

Um estudo detalhado desta teoria, incluindo o resultado que se segue, pode ser encontrado na tese [7] de Fernando Ferreira "*Polynomial Time Computable Arithmetic and Conservative Extensions*". A demonstração da proposição seguinte pode ser vista no artigo [8] "*Polynomial Time Computable Arithmetic*" do mesmo autor.[†]

Proposição 19 *Para cada símbolo funcional f de $\mathcal{L}_{PT} \setminus \mathcal{L}$ existem uma fórmula Σ_1^b-estendida*[‡] *H_f e um termo b_f em $\mathcal{L}$ tais que:*
Σ_1^b-$NIA \vdash \forall \bar{x} \exists z \preceq b_f(\bar{x})\ H_f(\bar{x}, z)$

---

[*] Apresentados na definição 17.

[†] A teoria Σ_1^b-NIA, na tese e no artigo mencionados, é designada por Σ_1^b-$PIND$ e "corresponde", embora em diferente notação, à teoria S_2^1 introduzida por Samuel Buss na dissertação [4] "*Bounded Arithmetic*".

[‡] Fórmula de $\mathcal{L}$ que pode ser construída num número finito de passos começando com fórmulas com quantificações de subpalavras e permitindo conjunções, disjunções, quantificações de subpalavras e quantificações existenciais limitadas.

Σ_1^b-$NIA \vdash H_f(\bar{x}, z) \wedge H_f(\bar{x}, y) \rightarrow z = y$

e

a) em Σ_1^b-NIA *tem-se que*

1. $H_E(x, \varepsilon)$

2. $H_{P_i^n}(x_1, ..., x_n, x_i)$ *com* $1 \leq i \leq n$

3. $H_{C_0}(x, x0)$

4. $H_{C_1}(x, x1)$

5. $H_Q(x, y, 1) \longleftrightarrow x \subseteq y$

$H_Q(x, y, 0) \vee H_Q(x, y, 1)$

b)

1. se f *é definida a partir de* $g, h_1, ..., h_k$ *por composição então*

Σ_1^b-$NIA \vdash H_{h_1}(\bar{x}, y_1) \wedge ... \wedge H_{h_k}(\bar{x}, y_k) \wedge H_g(y_1, ..., y_k, z) \rightarrow H_f(\bar{x}, z)$

2. se f *é definida a partir de* g, h_0 *e* h_1 *por recursão limitada na notação com limite* t *então*

Σ_1^b-$NIA \vdash H_g(\bar{x}, z) \rightarrow H_f(\bar{x}, \varepsilon, z)$

Σ_1^b-$NIA \vdash H_f(\bar{x}, y, r) \wedge H_{h_0}(\bar{x}, y, r, u) \wedge z = u_{|t(\bar{x}, y)} \rightarrow H_f(\bar{x}, y0, z)$

Σ_1^b-$NIA \vdash H_f(\bar{x}, y, r) \wedge H_{h_1}(\bar{x}, y, r, u) \wedge z = u_{|t(\bar{x}, y)} \rightarrow H_f(\bar{x}, y1, z)$.

8.2 Um resultado técnico

O lema que se segue é usado na demonstração do teorema fundamental no capítulo 5, capítulo esse dedicado ao cálculo de sequentes, aquando do estudo da regra de indução. Uma vez que a sua demonstração é bastante técnica, limitar-nos-emos a esboçá-la, omitindo alguns detalhes. A observação que precede a demonstração do lema dá uma ideia precisa do modo como este é usado na demonstração do teorema fundamental. Tal como aconteceu no enunciado e demonstração desse teorema, também aqui, por motivos de simplificação da notação, notaremos as variáveis de 2^a ordem, X^t, apenas por X.

Lema 7 *Consideremos* $\Psi^\Sigma(\omega, \bar{x}, \bar{X})$, $N_0^\Sigma(\omega, \bar{x}, \bar{X}, z, W)$ *e* $N_1^\Sigma(\omega, \bar{x}, \bar{X}, z, W)$ *fórmulas* $\Sigma_1^{1,b}$*-estendidas,* $\Psi^\Pi(\omega, \bar{x}, \bar{X})$, $N_0^\Pi(\omega, \bar{x}, \bar{X}, z, W)$ *e* $N_1^\Pi(\omega, \bar{x}, \bar{X}, z, W)$ *fórmulas* $\Pi_1^{1,b}$*-estendidas e* $t(\bar{x})$, $t_0(\bar{x}, z)$ *e* $t_1(\bar{x}, z)$ *termos de* $\mathcal{L}$ *tais que em* $\Sigma_1^{1,b}$-NIA *se demonstra:*

a) $\forall \bar{x} \forall \bar{X} \forall \omega \preceq t(\bar{x})\ (\Psi^\Sigma(\omega, \bar{x}, \bar{X}) \longleftrightarrow \Psi^\Pi(\omega, \bar{x}, \bar{X}))$;

b) $\forall \bar{x} \forall z \forall \bar{X} \forall W \forall \omega \preceq t_0(\bar{x}, z)\ (N_0^\Sigma(\omega, \bar{x}, \bar{X}, z, W) \longleftrightarrow N_0^\Pi(\omega, \bar{x}, \bar{X}, z, W))$;

c) $\forall \bar{x} \forall z \forall \bar{X} \forall W \forall \omega \preceq t_1(\bar{x}, z)\ (N_1^\Sigma(\omega, \bar{x}, \bar{X}, z, W) \longleftrightarrow N_1^\Pi(\omega, \bar{x}, \bar{X}, z, W))$;

então existem uma fórmula $\Sigma_1^{1,b}$*-estendida,* $\gamma^\Sigma(\omega, \bar{x}, \bar{X}, z)$, *uma fórmula* $\Pi_1^{1,b}$*-estendida,* $\gamma^\Pi(\omega, \bar{x}, \bar{X}, z)$, *e um termo de* $\mathcal{L}$, $q(\bar{x}, z)$, *tais que, a teoria* $\Sigma_1^{1,b}$-NIA *demonstra:*

(1) $\forall \bar{x} \forall z \forall \bar{X} \forall \omega \preceq q(\bar{x}, z)(\gamma^\Sigma(\omega, \bar{x}, \bar{X}, z) \longleftrightarrow \gamma^\Pi(\omega, \bar{x}, \bar{X}, z))$;

(2) $\forall \bar{x} \forall \bar{X} \forall \omega(\omega \preceq q(\bar{x}, \varepsilon) \wedge \gamma^\Sigma(\omega, \bar{x}, \bar{X}, \varepsilon) \longleftrightarrow \omega \preceq t(\bar{x}) \wedge \Psi^\Sigma(\omega, \bar{x}, \bar{X}))$;

(3) $\forall \bar{x} \forall z \forall \bar{X} \forall \omega(\omega \preceq q(\bar{x}, z0) \wedge \gamma^\Sigma(\omega, \bar{x}, \bar{X}, z0) \longleftrightarrow \omega \preceq t_0(\bar{x}, z) \wedge N_0^\Sigma(\omega, \bar{x}, \bar{X}, z, \{u \preceq q(\bar{x}, z) : \gamma^\Sigma(u, \bar{x}, \bar{X}, z)\}))$;

(4) $\forall\bar{x}\forall z\forall\bar{X}\forall\omega(\omega \preceq q(\bar{x}, z1)\wedge\gamma^{\Sigma}(\omega, \bar{x}, \bar{X}, z1) \longleftrightarrow \omega \preceq t_1(\bar{x}, z)\wedge N_1^{\Sigma}(\omega, \bar{x}, \bar{X}, z,$ $\{u \preceq q(\bar{x}, z) : \gamma^{\Sigma}(u, \bar{x}, \bar{X}, z)\}))$.

Observação 21 *O que pretendemos notar pela última componente na fórmula* $N_0^{\Sigma}(\omega, \bar{x}, \bar{X}, z, \{u \preceq q(\bar{x}, z) : \gamma^{\Sigma}(u, \bar{x}, \bar{X}, z)\})$ *foi explicado na observação 17 a propósito da fórmula* Θ *do teorema fundamental.*

Dem. (Esboço)

Seja $H_z = \{< \varepsilon, \omega >: \omega \preceq t(\bar{x})\wedge\ \Psi^{\Sigma}(\omega, \bar{x}, \bar{X})\} \cup \{< i, \omega >: \varepsilon \prec i \subseteq z\wedge$ $\wedge\exists v \subseteq i\ ((v0 = i \wedge \omega \preceq t_0(\bar{x}, v) \wedge N_0^{\Sigma}(\omega, \bar{x}, \bar{X}, v, \{u :< v, u >\in H_z\}))\vee\ (v1 = i\wedge$ $\wedge\omega \preceq t_1(\bar{x}, v) \wedge N_1^{\Sigma}(\omega, \bar{x}, \bar{X}, v, \{u :< v, u >\in H_z\}))))\}$.

Seja $p(\bar{x}, z) := (z \frown t(\bar{x}) \frown t_0(\bar{x}, z) \frown t_1(\bar{x}, z)1) \times 11$. Facilmente se constata que existe uma fórmula $\Sigma_1^{1,b}$-*estendida*, que notaremos por $Cond(H^p, \bar{x}, \bar{X}, z)$, que indica que H^p é constituído pelos elementos do conjunto H_z.

Definimos $\gamma^{\Sigma}(\omega, \bar{x}, \bar{X}, z)$ como sendo a seguinte fórmula $\Sigma_1^{1,b}$-*estendida* $\exists H^p(Cond(H^p, \bar{x}, \bar{X}, z) \wedge \exists b \preceq p(b =< z, \omega > \wedge b \in H^p))$; definimos $\gamma^{\Pi}(\omega, \bar{x}, \bar{X}, z)$ como sendo $\forall H^p(Cond(H^p, \bar{x}, \bar{X}, z) \rightarrow \exists b \preceq p(b =< z, \omega > \wedge b \in H^p))$ que é uma fórmula $\Pi_1^{1,b}$-*estendida* e definimos $q(\bar{x}, z)$ como sendo $p(\bar{x}, z)$.

Vejamos que

(*) $\Sigma_1^{1,b}$-$NIA \vdash \forall\bar{x}\forall\bar{X}\forall z\exists^1 H^p Cond(H^p, \bar{x}, \bar{X}, z)$.

<u>Existência:</u>

Fixemos $\bar{x}$ e $\bar{X}$ e vejamos, por indução na notação em z, que $\forall z\underbrace{\exists H^p Cond(H^p, \bar{x}, \bar{X}, z)}_{\Sigma_1^{1,b}-estendida}$.

Para $z = \varepsilon$ tomamos $H^p = \{< \varepsilon, u >: u \preceq t(\bar{x})\wedge\ \Psi^{\Sigma}(u, \bar{x}, \bar{X})\}$, o que é possível, pois como vimos no capítulo 4, proposição 10, temos compreensão para fórmulas $\Delta_1^{1,b}$-*estendidas*.

Por hipótese de indução consideremos que o resultado é válido para z, i.e. $\exists H^{p(\bar{x},z)} Cond(H^{p(\bar{x},z)}, \bar{x}, \bar{X}, z)$, e vejamos que é válido para $z0$ e $z1$.

Para $z0$ tomamos $H^{p(\bar{x},z0)} := H^{p(\bar{x},z)} \cup \{< z0, u >: u \preceq t_0(\bar{x}, z) \wedge N_0^{\Sigma}(u, \bar{x}, \bar{X}, z,$ $\{u :< z, u >\in H^{p(\bar{x},z)}\})\}$ e para $z1$ tomamos $H^{p(\bar{x},z1)} := H^{p(\bar{x},z)} \cup \{< z1, u >:$ $u \preceq t_1(\bar{x}, z) \wedge N_1^{\Sigma}(u, \bar{x}, \bar{X}, z, \{u :< z, u >\in H^{p(\bar{x},z)}\})\}$.

<u>Unicidade:</u>

Fixemos $\bar{x}$, $\bar{X}$ e z. Suponhamos que existem H_1 e H_2 tais que $Cond(H_1, \bar{x}, \bar{X}, z)$ e $Cond(H_2, \bar{x}, \bar{X}, z)$. Por indução na notação em ω pode ver-se que $\forall\omega\forall i \subseteq \omega$ $\forall u \preceq p(< i, u >\in H_1 \longleftrightarrow < i, u >\in H_2)$. Logo $H_1 = H_2$.

As condições (1), (2), (3) e (4) são imediatas por (*) e pela forma como definimos $Cond(H^p, \bar{x}, \bar{X}, z)$. ■

Observação 22 *Pelo lema anterior sabemos que se* ϕ *for um funcional definido por recursão limitada na notação*

$\phi(\bar{x}, \bar{X}, \varepsilon) = \Psi(\bar{x}, \bar{X})$

$\phi(\bar{x}, \bar{X}, z0) = \Phi_0(\bar{x}, \bar{X}, z, \phi(\bar{x}, \bar{X}, z))$

$\phi(\bar{x}, \bar{X}, z1) = \Phi_1(\bar{x}, \bar{X}, z, \phi(\bar{x}, \bar{X}, z)),$

em que as imagens são conjuntos definidos por fórmulas $\Delta_1^{1,b}$*-estendidas, limitados por determinados termos, i.e existem fórmulas* Ψ^Q, N_0^Q, N_1^Q, *com* $Q \in \{\Sigma, \Pi\}$ *e termos* t, t_0 *e* t_1 *tais que*

$\Psi(\bar{x}, \bar{X}) = \{\omega \preceq t(\bar{x}) : \Psi^Q(\omega, \bar{x}, \bar{X})\}$

$\Phi_0(\bar{x}, \bar{X}, z, W) = \{\omega \preceq t_0(\bar{x}, z) : N_0^Q(\omega, \bar{x}, \bar{X}, z, W)\}$

$\Phi_1(\bar{x}, \bar{X}, z, W) = \{\omega \preceq t_1(\bar{x}, z) : N_1^Q(\omega, \bar{x}, \bar{X}, z, W)\},$

então existe uma fórmula $\Sigma_1^{1,b}$*-estendida,* γ^Σ, *uma fórmula* $\Pi_1^{1,b}$*-estendida,* γ^Π *e um termo* $q(\bar{x}, z)$ *tais que* $\phi(\bar{x}, \bar{X}, z) = \{\omega \preceq q(\bar{x}, z) : \gamma^\Sigma(\omega, \bar{x}, \bar{X}, z)\} = \{\omega \preceq q(\bar{x}, z) : \gamma^\Pi(\omega, \bar{x}, \bar{X}, z)\}$.

O resultado continua válido se considerarmos vários funcionais a serem definidos simultaneamente por recursão limitada na notação:

$\phi_i(\bar{x}, \bar{X}, \varepsilon) = \Psi^i(\bar{x}, \bar{X})$

$\phi_i(\bar{x}, \bar{X}, z0) = \Phi_0^i(\bar{x}, \bar{X}, z, \phi_1(\bar{x}, \bar{X}, z), \phi_2(\bar{x}, \bar{X}, z), ..., \phi_n(\bar{x}, \bar{X}, z))$

$\phi_i(\bar{x}, \bar{X}, z1) = \Phi_1^i(\bar{x}, \bar{X}, z, \phi_1(\bar{x}, \bar{X}, z), \phi_2(\bar{x}, \bar{X}, z), ..., \phi_n(\bar{x}, \bar{X}, z)),$

com $1 \leq i \leq n$.

Bibliografia

[1] Balcázar J., Díaz J., Gabarró J., *Structural Complexity I*, 2^a edição, Springer-Verlag (1995).

[2] Balcázar J., Díaz J., Gabarró J., *Structural Complexity II*, Springer-Verlag (1990).

[3] Bridges D., *Computability-A Mathematical Sketchbook*, Springer-Verlag (1994).

[4] Buss S., *Bounded Arithmetic*, Bibliopolis (1986).

[5] Buss S., "An Introduction to Proof Theory", em *Handbook of Proof Theory*, organizado por Samuel Buss, volume 137, North-Holland (1998), pp.1-78.

[6] Chang C. C., Keisler H. J., *Model Theory*, 2^a edição, North-Holland (1977).

[7] Ferreira F., *Polynomial Time Computable Arithmetic and Conservative Extensions*, PH. D. Dissertation, Pennsylvania State University (1988).

[8] Ferreira F., "Polynomial Time Computable Arithmetic", em *American Mathematical Society*, Vol.106 (1990), pp.137-156.

[9] Ferreira F., "Stockmeyer Induction", em *Feasible Mathematics*, organizado por Samuel Buss e Philip Scott, Birkhäuser (1990), pp.161-179.

[10] Ferreira F., "A Feasible Theory for Analysis", em *The Journal of Symbolic Logic*, Vol.59, número 3 (1994), pp.1001-1011.

[11] Hermes H., *Enumerability-Decidability-Computability*, Springer-Verlag (1965).

[12] Krajíček J., *Bounded Arithmetic, Propositional logic and Complexity Theory*, Encyclopedia of Mathematics and its Applications 60 (1995).

[13] Malitz J., *Introduction to Mathematical Logic*, Springer-Verlag (1979).

[14] Oitavem I., *Três Assuntos de Lógica e Complexidade*, Dissertação de Mestrado, Faculdade de Ciências da Universidade de Lisboa (1994).

[15] Papadimitriou C., *Computational Complexity*, University of California-San Diego, Addison-Wesley Publishing Company (1994).

[16] Takeuti G., *Proof Theory*, 2^a edição, North-Holland (1987).