Sobre Esquemas de Indução

Jorge Petrúcio Viana

Tese submetida ao corpo docente da Coordenação dos programas de Pós-graduação em Engenharia da Universidade Federal do Rio de Janeiro como parte dos requisitos necessários para obtenção do grau de Mestre em Ciências em Engenharia de Sistemas e Computação.

Aprovada por :

Sheila Regina Murgel Veloso

Prof$^{\underline{a}}$ Sheila Regina Murgel Veloso, D.Sc.
(Presidente)

Prof. Paulo Augusto Silva Veloso, Ph.D.

Prof$^{\underline{a}}$ Sueli Bandeira Mendes, Ph.D.

Prof. Edward Hermann Haeusler, D.Sc.

Rio de Janeiro, RJ – Brasil

Abril de 1994

VIANA, JORGE PETRÚCIO

Sobre Esquemas de Indução. [Rio de Janeiro] 1994.

VI, 78 p., 29,7cm (COPPE/UFRJ, M.Sc., Engenharia de Sistemas e Computação, 1994)
Tese – Universidade Federal do Rio de Janeiro, COPPE.

1 - Aritmética elementar 2 - Esquemas de axiomas

3 - Esquemas de indução 4 - Especificações

5 - Teorias

I. COPPE/UFRJ II. Título (série).

Resumo da Tese apresentada à COPPE/UFRJ como parte dos requisitos necessários para a obtenção do grau de Mestre em Ciências (M.Sc.)

Sobre Esquemas de Indução

Jorge Petrúcio Viana

Abril de 1994

Orientadores : Sheila Regina Murgel Veloso e Paulo Augusto Silva Veloso
Programa : Engenharia de Sistemas e Computação

Existem duas maneiras usuais de se definir um esquema de axiomas em uma linguagem de primeira ordem $\mathcal{L}$: uma devida a Frege e a outra devida a Von Neumann. No sentido de Von Neumann, um esquema de axiomas é um conjunto de sentenças de $\mathcal{L}$ que possuem a mesma forma. No sentido de Frege, um esquema é uma expressão bem formada em uma extensão (não elementar) de $\mathcal{L}$. Neste trabalho, apresentamos uma formalização onde os esquemas, em ambos os sentidos, podem ser definidos e comparados. Caracterizamos os esquemas no sentido de Frege, de modo que esquemas no sentido de Von Neumann possam ser obtidos por aplicação de esquemas no sentido de Frege a extensões (elementares) de $\mathcal{L}$. Alguns resultados sobre o papel de esquemas de axiomas na especificação de subteorias da aritmética elementar são também apresentados.

Abstract of Thesis presented to COPPE/UFRJ as partial fulfillment of the requirements for the degree of Master of Science (M.Sc.)

On Induction Squemata

Jorge Petrúcio Viana

April, 1994

Thesis Supervisors : Sheila Regina Murgel Veloso and Paulo Augusto Silva Veloso
Department : Computing and Systems Engineering

Usually there are two approaches to define axiom schemata in a first order language $\mathcal{L}$: one due to Frege and the other due to Von Neumann. The Von Neumann approach considers an axiom schem as a set of sentences of $\mathcal{L}$ which has a common form, while in the approach due to Frege a schem is a well formed formula in a (non elementary) extension of $\mathcal{L}$. In this work we present a formalization to represent both schemata so that they can be compared. We characterize Frege's approach so that schemata in the Von Neumann sense can be obtained by application of Frege schemata to (elementar) extensions of $\mathcal{L}$. Some results on the role of axiom schemata on the specification of subtheories of number theory are also presented.

Sumário

Capítulo 1

Introdução

O objetivo deste trabalho é apresentar, de maneira sistemática, alguns conceitos e resultados referentes ao uso de esquemas de axiomas na definição de teorias axiomáticas.

Nossa motivação é decorrente do estudo de alguns trabalhos, sobre o papel desempenhado por esquemas de axiomas esquemas de indução, em subteorias da aritmética elementar [4, 13].

Inicialmente, fazemos uma distinção formal entre o *princípio de indução*, o *axioma de indução*, ou seja a expressão do princípio de indução em uma linguagem de segunda ordem e o *esquema de axiomas de indução*, ou seja, a expressão de parte do conteúdo de princípio de indução em uma linguagem de primeira ordem.

Em seguida, discutimos as duas maneiras usuais de se considerar a noção de esquema de axiomas.

A primeira maneira, introduzida por Frege em 1879, apresenta o esquema de axiomas através da noção de *teoria esquemática.*

Um exemplo de teoria esquemática que pode ser utilizado em estudos sobre aritmética formal, contém entre seus axiomas os usuais para 0, S, $+$ e $\cdot$ e em sua linguagem, $\mathcal{L}(\mathcal{V}_{os+\cdot})$, além dos símbolos usuais da aritmética uma *variável esquemática* X. Nesta teoria o esquema de indução matemática pode ser definido como a expressão

$$EIM.\ X[o] \wedge \forall x\ (X[x] \rightarrow X[sx]) \rightarrow \forall x\ X[x],$$

Associando a X uma noção de substituição de variáveis esquemáticas por fórmulas da linguagem da aritmética, o esquema de axiomas é, então, *aplicado* a $\mathcal{L}(\mathcal{V}_{os+\cdot})$, definindo um conjunto de sentenças da forma

$$A[o] \wedge \forall x\ (A[x] \rightarrow A[sx]) \rightarrow \forall x\ A[x],$$

obtidas pela substituição de X em EIM por fórmulas $A[x]$ sobre $\mathcal{L}(\mathcal{V}_{os+\cdot})$, cuja única variável livre é x.

A segunda maneira, introduzida por Von Neumann em 1927, difere da primeira quanto a metodologia, mas não ao conteúdo. O esquema de axiomas é, simplesmente, definido como o conjunto de sentenças da linguagem, que possuem a *forma* de EIM.

A distinção entre os dois modos de se considerar o esquema de axiomas é que, para o primeiro, existe uma noção *formal* de aplicação do esquema a qualquer linguagem $\mathcal{L}$ que possua entre seus símbolos a ocorrência dos símbolos primitivos que ocorrem no esquema. Como veremos, isto acarreta uma distinção no poder de prova de teorias obtidas por extensão da teoria original.

Neste trabalho, apresentamos uma formalização dos conceitos envolvidos na discussão acima e fazemos uma comparação entre as duas maneiras usuais de se considerar o conceito de esquema de axiomas e, em particular, o de esquema de axiomas de indução.

Este trabalho está organizado em sete capítulos.

No capítulo 1, que é esta introdução, apresentamos os objetivos gerais e uma lista das principais definições, resultados e notações pressupostos para a leitura dos capítulos seguintes.

No capítulo 2, apresentamos as noções de *estrutura indutiva* e *princípio de indução.* Nosso objetivo é mostrar a correspondência que existe entre estes dois conceitos.

No capítulo 3, discutimos, através de um exemplo particular, o problema de expressarmos princípios de indução em linguagens formais.

O exemplo apresentado é a *aritmética dos números naturais* e sua escolha se deve aos seguintes motivos: Em primeiro lugar, é bem conhecido o papel do axioma de indução e de diversos esquemas de axiomas de indução, nesta teoria [6, 8, 9, 12, 13]. Em segundo, existem diversos problemas em Teoria da Computação que se relacionam a questões referentes ao uso de esquemas de axiomas de indução em subteorias da aritmética formal [8], motivando assim um estudo detalhado dos conceitos subjacentes ao tratamento destes esquemas. Em último lugar, as questões tratadas neste capítulo podem ser estendidas para o caso de princípios de indução, em geral [6].

Apresentamos uma noção de *esquema de axiomas* e salientamos uma distinção importante quanto a seu uso na definição de teorias axiomáticas.

No capítulo 4, apresentamos as noções de *linguagem esquemática* e *teoria esquemática*. Mostramos como podemos, utilizando tais linguagens, formalizar as duas maneiras usuais de se considerar a noção de esquema de axiomas. Provamos alguns resultados que justificam o uso das linguagens esquemáticas na definição de teorias axiomáticas e, em particular, uma relação existente entre as duas maneiras de se considerar o conceito de esquemas de axiomas.

Nos capítulos 5 e 6, iniciamos o estudo do papel de alguns esquemas de indução na especificação de subteorias da aritmética elementar. Tratamos da teoria $Th(\mathbb{N}, 0, S)$, onde $\mathbb{N}$, 0 e S são usuais. Esta é uma teoria bastante simples e nosso interesse em estudá-la é que os resultados obtidos podem ser aplicados no estudo de teorias mais complexas.

Finalmente, no capítulo 7, concluímos com propostas para futuras pesquisas.

Apresentamos agora uma lista das principais definições, conceitos e notações pressupostas para a leitura dos capítulos seguintes.

Uma *estrutura* consistirá de um conjunto não vazio N, chamado *domínio*, de algumas relações e operações em N e de alguns elementos distinguidos de N.

Estruturas serão denotadas pelas letras $\mathcal{N}$ e $\mathcal{M}$, indexadas ou não e seus respectivos domínios pelas letras N ou M, seguidas do mesmo índice associado as letras caligráficas.

Dado N, relações e operações em N serão, respectivamente, denotadas por P_N ou f_N, indexadas ou não.

Se $\mathcal{N}$ for uma estrutura, N o domínio de $\mathcal{N}$, $P_N^1, \ldots, P_N^i$, as relações de $\mathcal{N}$, $f_N^1, \ldots, f_N^j$, as operações de $\mathcal{N}$ e $c_N^1, \ldots, c_N^k$, os elementos distinguidos de $\mathcal{N}$, então $\mathcal{N}$ será denotada $\langle N, P_N^1, \ldots, P_N^i, f_N^1, \ldots, f_N^j, c_N^1, \ldots, c_N^k \rangle$.

Um *vocabulário* será um conjunto de *símbolos* particionado em *predicadores, funtores* e *constantes individuais.*

Predicadores, funtores e constantes individuais serão denotados, respectivamente, pelas letras P, f ou c, indexadas ou não. Associado a cada predicador P (ou funtor f) existirá um número natural não nulo, chamado o *peso* de P (ou f). Um predicador (ou funtor) *m-ário* será um predicador (ou funtor) de peso m.

Vocabulários serão denotados pela letra $\mathcal{V}$, indexada ou não. Um vocabulário finito, $\mathcal{V} = \{P_1, \ldots, P_i, f_1, \ldots, f_j, c_1, \ldots, c_k\}$, será também denotado $\mathcal{V}_{P_1,\ldots,P_i,f_1,\ldots,f_j,c_1,\ldots,c_k}$.

Dados $\mathcal{N}$ uma estrutura e $\mathcal{V}$ um vocabulário, $\mathcal{V}$ será *adequado* para $\mathcal{N}$ se pudermos associar a cada predicador m-ário P de $\mathcal{V}$ uma relação m-ária P_N de $\mathcal{N}$, a cada funtor m-ário f de $\mathcal{V}$ uma operação m-ária f_N de $\mathcal{N}$ e a cada constante individual c de $\mathcal{V}$ um elemento distinguido c_N de $\mathcal{N}$. $\mathcal{N}$ será *adequada* para $\mathcal{V}$ se $\mathcal{V}$ for adequado para $\mathcal{N}$.

Dado um vocabulário $\mathcal{V}$, a *linguagem de primeira ordem* (com igualdade) sobre $\mathcal{V}$, denotada $\mathcal{L}(\mathcal{V})$, e a *linguagem de segunda ordem* (com igualdade) sobre $\mathcal{V}$, denotada $\mathcal{L}^2(\mathcal{V})$, serão definidas de maneira usual, considerando-se os elementos de $\mathcal{V}$ como os *símbolos não lógicos.*

Admitiremos como conhecidos os conceitos básicos referentes a sintaxe e a semântica destas linguagens, tais como são apresentados, por exemplo, em [2].

Uma estrutura será *adequada* para uma linguagem se for adequada para seu vocabulário.

Seja $\mathcal{L}$ uma linguagem de primeira ordem, $\mathcal{N}$ uma estrutura adequada para $\mathcal{L}$, t um *termo* de $\mathcal{L}$ e A uma *fórmula* de $\mathcal{L}$. Denotaremos por $Vl(A)$ o *conjunto das variáveis livres* de A. Por $A[x_1, \ldots, x_m]$ uma fórmula, tal que $Vl(A) = \{x_1, \ldots, x_m\}$. A será uma *sentença* se $Vl(A) = \emptyset$. Se A for uma sentença, $\models_{\mathcal{N}} A$ significará que A é *verdadeira* em $\mathcal{N}$. Neste caso, diremos também que $\mathcal{N}$ é um *modelo* de A. Se Σ for um conjunto de sentenças de $\mathcal{L}$, um *modelo* de Σ será um modelo de cada um dos elementos de Σ. A será uma *conseqüência semântica* de Σ, denotado $\Sigma \models A$, se toda estrutura adequada para $\mathcal{L}$ que for um modelo de Σ, também for um modelo de A. A será *válida*, denotado $\models A$, se $\emptyset \models A$.

Uma noção de *demonstração* a partir de um conjunto de hipóteses, tal como é apresentada, por exemplo, em [2], é admitida. Uma sentença A será uma *conseqüência sintática* de um conjunto de sentenças Σ, denotado $\Sigma \vdash A$, se existir uma demonstração de A a partir de Σ. A será um *teorema*, denotado $\vdash A$, se $\emptyset \vdash A$.

O resultado seguinte expressa a equivalência entre os conceitos de conseqüência semântica e sintática:

Teorema 1.1 (da completude) *Se $\mathcal{L}$ for uma linguagem de primeira ordem, A uma sentença de $\mathcal{L}$ e Σ um conjunto de sentenças de $\mathcal{L}$, então as seguintes condições serão equivalentes:*

a) $\Sigma \models A$;

b) $\Sigma \vdash A$.

Assim, usaremos indistintamente os símbolos $\models$ e $\vdash$, sempre que acharmos conveniente. Diremos simplesmente A é conseqüência de Σ e denotaremos $A \in Cn(\Sigma)$.

Uma *teoria* (elementar) sobre uma linguagem de primeira ordem $\mathcal{L}$ será um conjunto de sentenças de $\mathcal{L}$, fechado para a relação de conseqüência. Existem duas maneiras usuais de se definir uma teoria sobre uma linguagem $\mathcal{L}$: *semântica* e *sintaticamente*.

Semânticamente, uma teoria é definida como o conjunto de todas as sentenças de $\mathcal{L}$ que são verdadeiras em uma classe $\mathcal{K}$ de estruturas adequadas para $\mathcal{L}$. A teoria definida a partir de $\mathcal{K}$ será chamada a teoria de $\mathcal{K}$ e denotada $Th(\mathcal{K})$. Se $\mathcal{K} = \{\mathcal{N}\}$, então a teoria de $\mathcal{K}$ será denotada simplesmente $Th(\mathcal{N})$. Se $\mathcal{N} = \langle N, P_N^1, \ldots, P_N^i, f_N^1, \ldots, f_N^j, c_N^1, \ldots, c_N^k \rangle$, então $Th(\mathcal{N})$ será denotada $Th(N, P_N^1, \ldots, P_N^i, f_N^1, \ldots, f_N^j, c_N^1, \ldots, c_N^k)$.

Sintaticamente, uma teoria é definida do seguinte modo:

(1) Fixamos um determinado conjunto recursivo $\mathcal{A}x$ de sentenças de $\mathcal{L}$;

(2) Definimos a teoria como o conjunto de todas as sentenças de $\mathcal{L}$ que são conseqüência dos elementos de $\mathcal{A}x$.

$\mathcal{A}x$ será chamado um *conjunto de axiomas* para a teoria. Uma teoria $\mathcal{T}$ será *axiomatizável* se existir um conjunto $\mathcal{A}x$ de axiomas para T. Será *finitamente axiomatizável* se for axiomatizável e $\mathcal{A}x$ for finito. (Podemos dizer que este trabalho, consiste do estudo de duas maneiras distintas de se definir um conjunto de axiomas para uma teoria axiomatizável.)

Uma teoria $\mathcal{T}$ será *completa* se para qualquer sentença A de sua linguagem, $\mathcal{T} \vdash A$ ou $\mathcal{T} \vdash \neg A$. Será *consistente* se para nenhuma sentença A de sua linguagem, $\mathcal{T} \vdash A$ e $\mathcal{T} \vdash \neg A$.

Capítulo 2

Princípios de Indução

Neste capítulo, descrevemos uma construção algébrica que pode ser efetuada em uma dada estrutura $\mathcal{N}$, dados $B \subseteq N$ e $\mathcal{R}$ e $\mathcal{F}$, respectivamente, conjuntos de relações e operações de $\mathcal{N}$. O resultado desta construção será uma subestrutura de $\mathcal{N}$, chamada a *estrutura gerada* em $\mathcal{N}$, a partir de B, por $\mathcal{R}$ e $\mathcal{F}$. Em particular, nosso objetivo é mostrar que a toda estrutura definida por este processo corresponde um enunciado, chamado o *princípio de indução* associado a B, $\mathcal{R}$ e $\mathcal{F}$. Reciprocamente, veremos que a todo princípio de indução associado a B, $\mathcal{R}$ e $\mathcal{F}$ corresponde uma estrutura gerada a partir de B por $\mathcal{R}$ e $\mathcal{F}$.

Os resultados deste capítulo são bem conhecidos e encontram-se reunidos, por exemplo, em [2].

2.1 Alguns exemplos da aritmética

Seja $\mathcal{N}$ uma estrutura, $B \subseteq N$, $\mathcal{R}$ e $\mathcal{F}$, respectivamente, conjuntos de relações e operações de $\mathcal{N}$. O domínio C da subestrutura de $\mathcal{N}$ que queremos construir, deverá conter:

1) todos os elementos de B;

2) todos os elementos $b \in N$ para os quais existem $b_1, \ldots, b_m \in C$ e $P_N \in \mathcal{R}$, $(m+1)$-ária, de modo que $P_N(b_1, \ldots, b_m, b)$;

3) todos os elementos $b \in N$ para os quais existem $b_1, \ldots, b_m \in C$ e $f_N \in \mathcal{F}$, m-ária, de modo que $b = f_N(b_1, \ldots, b_m)$.

A idéia é que são dados em 1) certos elementos iniciais, com os quais podemos iniciar a construção de C. Em 2) e 3) certos modos de se combinar estes elementos, obtendo novos elementos de C. De uma maneira geral, os elementos obtidos por aplicações dos passos 2) e 3) não são, necessariamente, distintos. Mas o que queremos é que C contenha exatamente todos os elementos que somos habilitados a construir.

EXEMPLO Considerando a estrutura $Z = \langle \mathbb{Z}, S, <, +, \cdot \rangle$, onde $\mathbb{Z}$, S, $<$, $+$ e $\cdot$ são usuais, podemos construir $\mathbb{N} \subset \mathbb{Z}$ de quatro maneiras distintas:
a) Tomando como elementos inicial o número 0 e aplicando sucessivamente a operação unária S. Os elementos de $\mathbb{N}$ serão os números inteiros 0, $S(0) = 1$, $S(S(0)) = 2$, $S(S(S(0))) = 3$, ... Neste caso, $B = \{0\}$, $\mathcal{R} = \emptyset$ e $\mathcal{F} = \{S\}$;
b) Tomando como elementos inicial o número 0 e utilizando a relação $<$ para "selecionar" os números naturais dentre os números inteiros. Os elementos de $\mathbb{N}$ serão os números inteiros não negativos $0 < 1 < 2 < 3 < \ldots$. Neste caso, $B = \{0\}$ $\mathcal{R} = \{<\}$ e $\mathcal{F} = \emptyset$;
c) Tomando como elementos iniciais os números 0 e 1 e aplicando sucessivamente a operação binária $+$. Os elementos de $\mathbb{N}$ serão os números inteiros 0, 1, $1+1 = 2$, $1+1+1 = 3$, ... Neste caso, $B = \{0, 1\}$, $\mathcal{R} = \emptyset$ e $\mathcal{F} = \{+\}$;
d) Tomando como elementos iniciais o número 0, o número 1, todos os números primos positivos e aplicando sucessivamente a operação binária $\cdot$. Os elementos de $\mathbb{N}$ serão 0, 1 e os números inteiros que podem ser decompostos em um produto de números primos positivos. Denotando o conjunto dos números primos por Π, neste caso, teremos $B = \{0, 1\} \cup \Pi$, $\mathcal{R} = \emptyset$ e $\mathcal{F} = \{\cdot\}$.

Dados $\mathcal{N}$, B, $\mathcal{R}$ e $\mathcal{F}$, para definir C de maneira formal, podemos escolher entre duas opções: o método *Top-down* e o método *Bottom-up*. Passaremos agora a examinar cada um destes métodos.

2.2 Top-down

No método *top-down* definimos C como o menor subconjunto de N que contenha B e que tenha como elementos cada um dos elementos de N que pode ser obtido a partir de elementos que já estejam em C, por aplicação das relações e operacões "construtoras". Teremos, então as seguintes definições:

Definição Seja $\mathcal{N}$ uma estrutura, $X \subseteq N$, P_N uma relação $(m+1)$-ária de $\mathcal{N}$ e f_N uma operação m-ária de $\mathcal{N}$.

i) X será *fechado* para P_N se para todos $b_1, \ldots, b_m, b \in N$, tivemos que $b_1, \ldots, b_m \in X$ e $P_N(b_1, \ldots, b_m, b)$ acarretam $b \in X$;

ii) X será *fechado* para f_N se para todos $b_1, \ldots, b_m \in N$, tivermos que $b_1, \ldots, b_m \in X$ e $f_N(b_1, \ldots, b_m) = b$ acarretam $b \in X$.

Assim, X será fechado para uma relação ou operação se não pudermos "sair" de X por aplicações sucessivas desta relação ou operação a elementos de X.

Definição Seja $\mathcal{N}$ uma estrutura, $B \subseteq N$, $\mathcal{R}$ um conjunto de relações de $\mathcal{N}$ e $\mathcal{F}$ um conjunto de operações de $\mathcal{N}$. Um subconjunto X de N será *estável* com relação a B, $\mathcal{R}$ e $\mathcal{F}$ se satisfizer as seguintes condições:

i) $B \subseteq X$;

ii) X é fechado para cada uma das relações de $\mathcal{R}$;

iii) X é fechado para cada uma das operações de $\mathcal{F}$.

A proposição seguinte é imediata das definições:

Proposição 2.1 *Se $\mathcal{N}$, B, $\mathcal{R}$ e $\mathcal{F}$, forem como na definição anterior, então N será estável com relação a B, $\mathcal{R}$ e $\mathcal{F}$.*

Prova:

Obviamente, $B \subseteq N$ e N é fechado para cada elemento de $\mathcal{R} \cup \mathcal{F}$. ∎

Assim, a família dos subconjuntos estáveis com relação a B, $\mathcal{R}$ e $\mathcal{F}$, de uma dada estrutura $\mathcal{N}$, é não vazia.

Isto motiva a seguinte definição:

Definição Seja $\mathcal{N}$, B, $\mathcal{R}$ e $\mathcal{F}$ como nas definições anteriores. O *conjunto gerado* a partir de B pelas relações de $\mathcal{R}$ e operações de $\mathcal{F}$, denotado $C^*_{B,\mathcal{R},\mathcal{F}}$, será definido pela seguinte igualdade:

$C^*_{B,\mathcal{R},\mathcal{F}} = \bigcap_{X \subseteq N}\{X : X$ é estável em $\mathcal{N}$ com relação a $B, \mathcal{R}$ e $\mathcal{F}\}$.

Os resultados seguintes mostram que $C^*_{B,\mathcal{R},\mathcal{F}}$ é, na verdade, o subconjunto C que estamos procurando.

Proposição 2.2 *Se $\mathcal{N}$, B, $\mathcal{R}$ e $\mathcal{F}$ forem como nas definições anteriores, então $C^*_{B,\mathcal{R},\mathcal{F}}$ será estável.*

Prova:

i) Se $x \in B$ e $X \subseteq N$ for estável, então como $B \subseteq X$, teremos $x \in X$. Assim, para todo $X \subseteq N$, estável, $x \in X$, ou seja $x \in C^*_{B,\mathcal{F},\mathcal{R}}$;

ii) Seja P_N uma relação $(m+1)$-ária de $\mathcal{R}$ e $b_1, \ldots, b_m, b \in N$, tais que $b_1, \ldots, b_m \in C^*_{B,\mathcal{R},\mathcal{F}}$ e $P_N(b_1, \ldots, b_m, b)$.

Se $X \subseteq N$ for estável, então $b_1, \ldots, b_m \in X$ e $P_N(b_1, \ldots, b_m, b)$. Daí, $b \in X$. Assim, para todo $X \subseteq N$, estável, $b \in X$, ou seja, $b \in C^*_{B,\mathcal{R},\mathcal{F}}$;

iii) Seja f_N uma operação m-ária de $\mathcal{F}$ e $b_1, \ldots, b_m, b \in N$, de modo que $b_1, \ldots, b_m \in C^*_{B,\mathcal{R},\mathcal{F}}$ e $f_N(b_1, \ldots, b_m) = b$.

Se $X \subseteq N$ for estável, então $b_1, \ldots, b_m \in X$ e $f_N(b_1, \ldots, b_m) = b$. Daí, $b \in X$. Assim, para todo $X \in N$, estável, $b \in X$, ou seja $b \in C^*_B$. ■

A proposição acima garante que $C^*_{B,\mathcal{R},\mathcal{F}}$ é um subconjunto estável de $\mathcal{N}$, com relação a B, $\mathcal{R}$ e $\mathcal{F}$.

Proposição 2.3 *Se $\mathcal{N}$, B, $\mathcal{R}$ e $\mathcal{F}$ forem como nas definições anteriores e $X \subseteq N$ for estável com relação a B, $\mathcal{R}$ e $\mathcal{F}$, então $C^*_{B,\mathcal{R},\mathcal{F}} \subseteq X$.*

Prova:

$C^*_{B,\mathcal{R},\mathcal{F}} = \bigcap_{X \subseteq N}\{X : X$ é estável com relação a B, $\mathcal{R}$ e $\mathcal{F}\} \subseteq X$. ■

A proposição acima garante que $C^*_{B,\mathcal{R},\mathcal{F}}$ é o menor subconjunto estável de $\mathcal{N}$, com relação a B, $\mathcal{R}$ e $\mathcal{F}$.

2.3 Bottom-up

No método *bottom-up* definimos C como o subconjunto de N que contenha B e que tenha como elementos todos os elementos de N que podem ser alcançados a partir dos elementos de B, por um número finito de aplicações das operações construtoras. Temos, então, as seguintes definições:

Definição Seja $\mathcal{N}$ uma estrutura, $B \subseteq N$, $\mathcal{R}$ um conjunto de relações de $\mathcal{N}$ e $\mathcal{F}$ um cojunto de operações de $\mathcal{N}$. Uma seqüência finita $\langle a_1, \ldots, a_m \rangle$ de elementos de N será uma *seqüência de construção* em relação a B, $\mathcal{R}$ e $\mathcal{F}$ se para cada índice i, $1 \leq i \leq m$, tivermos ao menos uma das seguintes condições:

i) $a_i \in B$;

ii) existem $a_{i1}, \ldots, a_{ik}$, anteriores a a_i na seqüência e R_N uma relação $(k+1)$-ária de $\mathcal{R}$, tais que $R_N(a_{i1}, \ldots, a_{ik}, a_i)$;

iii) existem $a_1, \ldots, a_k$, anteriores a a_i na seqüência e f_N uma operação k-ária em $\mathcal{F}$, tal que $f_N(a_{i1}, \ldots, a_{ik}) = a_i$.

Uma seqüência de construção descreve como podemos gerar um elemento de C a partir dos elementos de B, por aplicação das operações construtoras.

Definição Seja $\mathcal{N}$, B, $\mathcal{R}$ e $\mathcal{F}$ como na definição anterior e $a \in N$.

i) Uma *seqüência de construção de a* em relação a B, $\mathcal{R}$ e $\mathcal{F}$ será uma seqüência de construção em relação a B, $\mathcal{R}$ e $\mathcal{F}$ que termina em a;

ii) O *conjunto gerado* a partir de B pelas relações de $\mathcal{R}$ e operações de $\mathcal{F}$, denotado $C_*^{B,\mathcal{R},\mathcal{F}}$, será definido pela seguinte igualdade:

$C_*^{B,\mathcal{R},\mathcal{F}} = \{a \in N :$ existe uma seqüência de construção de a em relação a B, $\mathcal{R}$ e $\mathcal{F}\}$.

Denotamos por $C_m^{B,\mathcal{R},\mathcal{F}}$ ao conjunto dos elementos de N para os quais existe uma seqüência de construção de comprimento m.

Os resultados seguintes mostram que $C_*^{B,\mathcal{R},\mathcal{F}}$ é, na verdade, o subconjunto C que estamos procurando.

Proposição 2.4 $C_1^{B,\mathcal{R},\mathcal{F}} = B$.

Prova:

Para cada elemento $b \in B$, $\langle b \rangle$ é uma seqüência de construção de b em relação a B, $\mathcal{R}$, $\mathcal{F}$. ■

Proposição 2.5 *Se m for um número natural não nulo, então* $C_m^{B,\mathcal{R},\mathcal{F}} \subseteq C_{m+1}^{B,\mathcal{R},\mathcal{F}}$.

Prova:

Se $a \in C_m^{B,\mathcal{R},\mathcal{F}}$, então existirá $\langle a_1, \ldots a_m \rangle$ uma seqüência de construção de a em relação a B, $\mathcal{R}$ e $\mathcal{F}$, de comprimento m. É fácil verificar que $\langle a_1, \ldots, a_m, a \rangle$ será uma seqüência de construção para a em relação a B, $\mathcal{R}$ e $\mathcal{F}$, de comprimento $m+1$. ∎

Proposição 2.6 $C_*^{B,\mathcal{R},\mathcal{F}} = \bigcup_{m \in \mathbb{N}^*} C_m^{B,\mathcal{R},\mathcal{F}}$.

Prova:

($\Rightarrow$) Se $a \in C_*^{B,\mathcal{R},\mathcal{F}}$, então existirá uma seqüência de construção para a em relação a B, $\mathcal{R}$ e $\mathcal{F}$. Como toda seqüência de construção é finita, $a \in C_m^{B,\mathcal{R},\mathcal{F}}$, para algum número natural não nulo m.

($\Leftarrow$) Se existir um número natural não nulo m, tal que $a \in C_m^{B,\mathcal{R},\mathcal{F}}$, então existirá uma seqüência de construção de a em relação a B, $\mathcal{R}$ e $\mathcal{F}$, de comprimento m. Assim, $a \in C_*^{B,\mathcal{R},\mathcal{F}}$. ∎

2.4 Conjuntos gerados finitamente

Agora que temos duas maneiras distintas de construir o subconjunto C, resta-nos provar o seguinte resultado:

Proposição 2.7 *Se $\mathcal{N}$ for uma estrutura, $B \subseteq N$, $\mathcal{R}$ um conjunto de relações de $\mathcal{N}$ e $\mathcal{F}$ um conjunto de operações de $\mathcal{N}$, então $C^*_{B,\mathcal{R},\mathcal{F}} = C_*^{B,\mathcal{R},\mathcal{F}}$.*

Prova:

($\Rightarrow$) Para provar que $C^*_{B,\mathcal{R},\mathcal{F}} \subseteq C_*^{B,\mathcal{R},\mathcal{F}}$ basta mostrar que $C_*^{B,\mathcal{R},\mathcal{F}}$ é indutivo. Isto é, que $B \subseteq C_*^{B,\mathcal{R},\mathcal{F}}$ e que $C_*^{B,\mathcal{R},\mathcal{F}}$ é fechado para todas as relações de $\mathcal{R}$ e operações de $\mathcal{F}$.

i) $B = C_1 \subseteq C_*^{B,\mathcal{R},\mathcal{F}}$.

ii) Se $b_1, \ldots, b_m, b \in N$ e $R_N(b_1, \ldots, b_m, b)$, então existirá uma seqüência de construção de b em relação a B, $\mathcal{R}$ e $\mathcal{F}$.

Agora, se $b_1, \ldots, b_m \in C_*^{B,\mathcal{R},\mathcal{F}}$, existirão, $\langle b_{11}, \ldots, b_{1m_1} \rangle$, $\langle b_{21}, \ldots, b_{2m_2} \rangle$, ..., $\langle b_{m1}, \ldots, b_{mm_k} \rangle$ seqüências de construção de $b_1, \ldots, b_m$ em relação a B,

$\mathcal{R}$ e $\mathcal{F}$. É fácil verificar que $\langle b_{11}, \ldots, b_{1m_1}, b_{21}, \ldots, b_{2m_2}, \ldots, b_{m1}, \ldots, b_{mm_k}\rangle$ é uma seqüência de construção de b em relação a B, $\mathcal{R}$ e $\mathcal{F}$.

($\Leftarrow$) Se $a \in C_*^{B,\mathcal{R},\mathcal{F}}$, existirá uma seqüência de construção $\langle a_1, \ldots, a_m\rangle$ de a, em relação a B, $\mathcal{R}$ e $\mathcal{F}$. Vamos provar por indução em m que cada um dos a_i, $1 \leq i \leq m$, é um elemento de $C^*_{B,\mathcal{R},\mathcal{F}}$.

Base: Se $m = 1$, teremos $a = a_1 \in B \subseteq C^*_{B,\mathcal{R},\mathcal{F}}$.

Hipótese: Suponhamos que para cada i, $1 \leq i \leq k$ $a_i \in C^*_{B,\mathcal{R},\mathcal{F}}$.

Passo: Como $\langle a_1, \ldots, a_m\rangle$ é uma seqüência de construção, teremos dois casos:

1º caso: Existem $a_{m1}, \ldots, a_{mk}$, anteriores a a_k na seqüência e R_N uma relação $(m_k + 1)$-ária em $\mathcal{R}$, tais que $R_N(a_{m1}, \ldots, a_{mk}, a_k)$.

2º caso: Existem $a_{m1}, \ldots, a_{mk}$, anteriores a a_k na seqüência e f_N uma operação m_k-ária em $\mathcal{F}$, tais que $f_N(a_{m1}, \ldots, a_{mk}) = a_k$.

Agora, pela hipótese de indução, $a_{m1}, \ldots, a_{mk} \in C^*_{B,\mathcal{R},\mathcal{F}}$ e como $C^*_{B,\mathcal{R},\mathcal{F}}$ é indutivo, em ambos os casos teremos $a_k \in C^*_{B,\mathcal{R},\mathcal{F}}$. ■

Assim, dada uma estrutura $\mathcal{N}$, $B \subseteq N$, $\mathcal{R}$ um conjunto de relações de $\mathcal{N}$ e $\mathcal{F}$ um conjunto de operações de $\mathcal{N}$, o resultado acima pode ser sumarizado nas seguintes igualdades:

$$\bigcap_{X \subseteq N} \{X : X \text{ é indutivo em relação a } B, \mathcal{R} \text{ e } \mathcal{F}\} = C^*_{B,\mathcal{R},\mathcal{F}} = C_*^{B,\mathcal{R},\mathcal{F}} = \bigcup_{n \in \mathbb{N}^*} C_n.$$

Temos, finalmente, a seguinte definição:

Definição Seja $\mathcal{N}$ for uma estrutura, $B \subseteq N$, $\mathcal{R}$ um conjunto de relações de $\mathcal{N}$ e $\mathcal{F}$ um conjunto de operações de $\mathcal{N}$. O *conjunto gerado* em N a partir de B, pelas relações de $\mathcal{R}$ e operações de $\mathcal{F}$, denotado $C(B, \mathcal{R}, \mathcal{F})$, será definido pela seguintes igualdades:

$$C(B, \mathcal{R}, \mathcal{F}) = C^*_{B,\mathcal{R},\mathcal{F}} = C_*^{B,\mathcal{R},\mathcal{F}}.$$

2.5 Princípios de indução

Dada uma estrutura $\mathcal{N}$, $B \subseteq N$, $\mathcal{R}$ um conjunto de relações de $\mathcal{N}$ e $\mathcal{F}$ um conjunto de operações de $\mathcal{N}$, podemos utilizar o conjunto $C(B, \mathcal{R}, \mathcal{F})$ para definir uma subestrutura de $\mathcal{N}$.

Definição Seja $\mathcal{N}$ uma estrutura, $B \subseteq N$, $\mathcal{R}$ um conjunto de relações de $\mathcal{N}$ e $\mathcal{F}$ um conjunto de operações de $\mathcal{N}$. A *subestrutura indutiva* de $\mathcal{N}$ com relação a B, $\mathcal{R}$ e $\mathcal{F}$, será a estrutura $\mathcal{M}$, definida do seguinte modo:

i) **Domínio:** $M = C(B, \mathcal{R}, \mathcal{F})$;

ii) **Relações distinguidas:** Para cada $R_N \in \mathcal{R}$, a restrição de R_N a $C(B, \mathcal{R}, \mathcal{F})$;

iii) **Operações distinguidas:** Para cada $f_N \in \mathcal{F}$, a restrição de f_N a $C(B, \mathcal{R}, \mathcal{F})$;

iv) **Elementos distinguidos:** Os elementos de B.

Definição Sejam $\mathcal{N}$, B, $\mathcal{R}$ e $\mathcal{F}$ como na definição anterior e $\mathcal{M} \subseteq \mathcal{N}$. O *princípio de indução* associado a $\mathcal{M}$ com relação a B, $\mathcal{R}$ e $\mathcal{F}$, denotado $I(\mathcal{M})$, será o seguinte enunciado: *Se X for um subconjunto indutivo de M com relação a B, $\mathcal{R}$ e $\mathcal{F}$, então $X = M$.*

Temos, então, o seguinte resultado:

Proposição 2.8 *Se $\mathcal{N}$, $\mathcal{M}$, B, $\mathcal{R}$ e $\mathcal{F}$ forem como nas definições anteriores, e B, $\mathcal{R}$ e $\mathcal{F}$ forem, respectivamente, os conjuntos de elementos, relações e operações distinguidas de $\mathcal{M}$, então as seguintes condições serão equivalentes:*

a) $\mathcal{M}$ é indutiva com relação a B, $\mathcal{R}$ e $\mathcal{F}$;

b) $\mathcal{M}$ satisfaz a $I(\mathcal{M})$.

Prova:

($\Rightarrow$) Se $\mathcal{M}$ for indutiva com relação a B, $\mathcal{R}$ e $\mathcal{F}$, e X for um subconjunto indutivo de M com relação a B, $\mathcal{R}$ e $\mathcal{F}$, teremos $M = C(B, \mathcal{R}, \mathcal{F}) \subseteq X$. Como $X \subseteq M$, teremos $X = M$, ou seja, $\mathcal{M}$ satisfaz a $I(\mathcal{M})$.

($\Leftarrow$) Como $C(B, \mathcal{R}, \mathcal{F})$ é indutivo com relação a B, $\mathcal{R}$ e $\mathcal{F}$ se $\mathcal{M}$ satisfizer a $I(\mathcal{M})$, então $C(B, \mathcal{R}, \mathcal{F}) = M$. Daí, $\mathcal{M}$ será indutiva com relação a B, $\mathcal{R}$ e $\mathcal{F}$. ∎

EXEMPLO Considerando $Z = \langle \mathbb{Z}, S, <, +, \cdot \rangle$, onde $\mathbb{Z}, S, <, +$ e $\cdot$ são usuais, temos:

a) $\langle \mathbb{N}, 0, S \rangle$ é indutiva em Z com relação a $\{0\}$ e $\{S\}$;

b) $\langle I\!N, 0, <\rangle$ também é indutiva em Z mas com relação a $\{0\}$ e $\{<\}$;

c) $\langle I\!N, 0, 1, +\rangle$ é indutiva em Z com relação a $\{0, 1\}$ e $\{+\}$;

d) $\langle I\!N, \{0, 1\} \cup \Pi, \cdot\rangle$ é indutiva em Z com relação a $\{0, 1\} \cup \Pi$ e $\{\cdot\}$.

Assim, associado a cada uma destas estruturas temos um princípio de indução:

a) No caso de $\langle I\!N, 0, S\rangle$, temos o conhecido *princípio de indução matemática*, $I(I\!N, 0, S)$, que pode ser enunciando do seguinte modo: *Se $X \subseteq N$ for tal que $0 \in X$ e $S(x) \in X$ sempre que $x \in X$, então $X = I\!N$*;

b) No caso de $\langle I\!N, 0, <\rangle$, temos o *princípio de indução completa*, ou *por curso de valores*, $I(I\!N, 0, <)$, que pode ser enunciando do seguinte modo: *Se $X \subseteq N$ for tal que $0 \in X$ e $y \in X$ sempre que $x \in X$ e $x < y$, então $X = I\!N$*;

c) No caso da estrutura $\langle I\!N, 0, 1, +\rangle$, temos o *princípio de indução para a adição*, $I(I\!N, 0, 1, +)$, que pode ser enunciando do seguinte modo: *Se $X \subseteq N$ for tal que $0, 1 \in X$ e $x + y \in X$ sempre que $x, y \in X$, então $X = I\!N$*;

d) Finalmente, no caso da estrutura $\langle I\!N, \{0, 1\} \cup \Pi, \cdot\rangle$, temos o *princípio de indução para a multiplicação*, $I(I\!N, \{0, 1\} \cup \Pi, \cdot)$, que pode ser enunciando do seguinte modo: *Se $X \subseteq N$ for tal que $0, 1 \in X$, $p \in X$ sempre que p for primo e $x \cdot y \in X$ sempre que $x, y \in X$, então $X = I\!N$.*

Capítulo 3

Aritmética Elementar dos Números Naturais e Esquemas de Indução

Como vimos no capítulo anterior, a toda estrutura indutiva está associado um princípio de indução e a todo princípio de indução corresponde uma estrutura indutiva. Em outras palavras, podemos considerar um princípio de indução como um enunciado informal de que uma dada estrutura pode ser obtida como o resultado de uma determinada construção algébrica. A saber, se $\mathcal{N}$ for uma estrutura e $\mathcal{M} \subseteq \mathcal{N}$ for uma subestrutura com relação a $\mathcal{R}$ e $\mathcal{F}$, então o princípio de indução $I(\mathcal{M})$ afirma que $\mathcal{M}$ é a subestrutura indutiva de $\mathcal{N}$, com relação a B, $\mathcal{R}$ e $\mathcal{F}$.

Neste capítulo, pelo estudo de um exemplo particular, consideramos o problema de expressar o conteúdo de um princípio de indução em uma linguagem formal.

3.1 Axiomas de Peano

Na axiomatização da *aritmética dos números naturais*, usualmente, consideramos os chamados *axiomas de Peano.* Estes axiomas dizem respeito aos conceitos primitivos *número natural*, *zero* e *sucessão*, e em termos informais, podem ser enunciados do seguinte modo:

P_1. Zero é um número natural;

P_2. Sucessão é uma operação que efetuada sobre um número natural x, fornece como resultado um número natural, chamado o *sucessor* de x;

S_1. Zero não é sucessor de nenhum número natural;

S_2. Números naturais distintos possuem sucessores distintos;

IM. Qualquer subconjunto do conjunto dos números naturais, que contenha o zero e que contenha o sucessor de cada um de seus elementos, conterá todos os números naturais.

Intuitivamente, os axiomas P_1 e P_2 afirmam que ao menos zero, o sucessor de zero, o sucessor do sucessor de zero, etc., são números naturais. Os axiomas S_1 e S_2 afirmam que todos os números naturais obtidos acima são distintos. E o axioma IM, na verdade o princípio de indução associado a estrutura indutiva $\langle \mathbb{N}, 0, S\rangle$, afirma que estes são os únicos números naturais.

Formalmente, prescindimos dos axiomas P_1 e P_2. Em seu lugar, podemos considerar o vocabulário $\mathcal{V}_{os} = \{o, s\}$ pois uma estrutura adequada para $\mathcal{L}(\mathcal{V}_{os})$ deverá conter em seu domínio N um elemento distinguido 0 e, definida em N, uma operação unária S.

Na linguagem $\mathcal{L}(\mathcal{V}_{os})$, S_1 e S_2 podem ser enunciados do seguinte modo:

S_1. $\forall x\ sx \neq o$;

S_2. $\forall x \forall y\ (sx = sy \rightarrow x = y)$.

De fato, dada uma estrutura $\mathcal{N} = \langle N, 0, S\rangle$, onde $N \neq \emptyset$, $0 \in N$ e $S : N \rightarrow N$ é uma operação, podemos interpretar os axiomas S_1 e S_2, do seguinte modo:

S_1. Afirma que 0 não está na imagem de S, isto é, 0 não é sucessor de nenhum número natural;

S_2. Afirma que a operação S é injetiva.

Assim, ao efetuarmos esta operação sobre um número natural, obtemos como resultado um número natural que ainda não foi gerado e, em particular, aplicando S sucessivamente a partir do zero, obtemos uma seqüência infinita de números naturais distintos.

O axioma IM, chamado *axioma de indução matemática*, é um enunciado sobre subconjuntos arbitrários de N e pode ser formalizado na linguagem $\mathcal{L}^2(\mathcal{V}_{os})$, onde quantificamos variáveis cujos valores são subconjuntos do domínio de interpretação:

IM. $\forall X\ (X[o]\ \wedge \forall x\ (X[x] \to X[sx]) \to \forall x\ X[x])$.

Assim, teremos as seguintes definições:

Definição Chamamos *aritmética de Peano*, denotada P, a teoria de segunda ordem definida do seguinte modo:

i) **Vocabulário:** $\mathcal{V}_{os}$;

ii) **Sentenças:** Todas as conseqüências dos seguintes axiomas:

S_1. $\forall x\ sx \neq o$;

S_2. $\forall x \forall y\ (sx = sy \to x = y)$;

IM. $\forall X\ (X[o] \wedge \forall x\ (X[x] \to X[sx]) \to \forall x\ X[x])$.

Um *modelo de Peano* será uma estrutura $\mathcal{N} = \langle N, 0, S\rangle$, onde $N \neq \emptyset$, $0 \in N$ e $S : N \to N$ é uma operação, que satisfaça aos axiomas S_1, S_2 e IM.

Investigamos a seguir alguns resultados fundamentais que serão utilizados na escolha de axiomas para subteorias elementares da aritmética de Peano.

O teorema do homomorfismo

O principal resultado decorrente dos axiomas de Peano fornece uma caracterização dos modelos de Peano, na classe das estruturas *do tipo* de $\langle \mathbb{N}, 0, S\rangle$, isto é, estruturas $\mathcal{N} = \langle N, 0, S\rangle$ onde $N \neq \emptyset$, $0 \in N$ e $S : N \to N$ é uma operação.

Teorema 3.1 (do homomorfismo) *Se $\mathcal{N} = \langle N, 0, S\rangle$ for uma estrutura do tipo de $\langle \mathbb{N}, 0, S\rangle$, então as seguintes condições serão equivalentes:*

a) $\mathcal{N}$ é um modelo de Peano;

b) Para toda estrutura $\mathcal{N}' = \langle N', 0', S'\rangle$ do tipo de $\langle \mathbb{N}, 0, S\rangle$, existe um único homomorfismo de $\mathcal{N}$ em $\mathcal{N}'$, isto é, existe uma única função $\Phi : N \to N'$, satisfazendo as seguintes condições:

i) $\Phi(0) = 0'$

ii) para todo $x \in N$, $\Phi(S(x)) = S'(\Phi(x))$.

Prova:

$(\Rightarrow)$*Existência:* Há, basicamente, duas maneiras de se provar a existência da função Φ.

• *Bottom-up:* Definimos um *segmento de* $\mathcal{N}$ como um subconjunto X de N, que satisfaça as seguintes condições: $0 \in X$ e para todo $x \in N$, se $S(x) \in X$, então $x \in X$. Definimos uma *função parcial* como uma função $f : X \rightarrow N'$, que satisfaça as seguintes condições: X é um segmento de $\mathcal{N}$, $f(0) = 0'$ e para todo $x \in N$, tal que $S(x) \in X$, $f(S(x)) = S'(f(x))$.

Usando os axiomas S_1, S_2 e IM, que são verdadeiros em $\mathcal{N}$, podemos provar que para toda função parcial f, $f(0) = 0'$, que todo elemento $x \in N$ está no domínio de alguma função parcial e que se f_1 e f_2 forem funções parciais e $x \in Dom(f_1) \cap Dom(f_2)$, então $f(x_1) = f(x_2)$.

Combinando estes resultados, podemos provar que para todo $x \in N$, existe um único $y \in N'$, tal que $f(x) = y$, para alguma função parcial f. Assim, definimos $\Phi : N \rightarrow N'$, tal que para cada $x \in N$, $\Phi(x)$ é o único $y \in N'$ que satisfaz a condição anterior. É imediato provar que Φ satisfaz às condições *i)* e *ii)*.

• *Top-down:* Definimos um conjunto *regular* de $\mathcal{N}$ como um subconjunto X de $N \times N$ que satisfaça as seguintes definições: $(0, 0') \in X$ e para todo $(x, y) \in N \times N'$, se $(x, y) \in X$, então $(S(x), S'(y) \in X$. Existem conjuntos regulares pois, por exemplo, $N \times N'$ é regular. É imediato que X^*, a interseção de todos os conjuntos regulares é regular e que é o menor (com relação a inclusão) dos conjuntos regulares.

Usando os axiomas S_1, S_2 e IM que são verdadeiros em $\mathcal{N}$, podemos provar que para todo $x \in N$, existe um único $y \in N'$, tal que $(x, y) \in X^*$. Assim, definimos $\Phi : N \rightarrow N'$, tal que para todo $x \in N$, $\Phi(x)$ é o único $y \in N'$ que satisfaz a condição anterior. Usando a fato que X^* é regular é imediato provar que Φ satisfaz as condições *i)* e *ii)*.

Unicidade: A prova de unicidade de Φ não apresenta dificuldades.

($\Leftarrow$) Se $\mathcal{N} = \langle N, 0, S \rangle$ satisfizer a condição *b)* do teorema, vamos mostrar que $\mathcal{N}$ satisfará também a S_1, S_2 e IM.

IM: Seja $X \subseteq N$, tal que $0 \in X$ e para todo $x \in N$, se $x \in X$, então $S(x) \in X$. Se $X \neq N$, ou seja, se $Y = N \setminus X \neq \emptyset$, então poderíamos escolher de maneira adequada um conjunto M de mesma cardinalidade que Y e disjunto de N, de modo a definir uma bijeção $f : Y \rightarrow M$. Tomando, agora, $N' = M \cup N$, poderíamos definir $S' : N' \rightarrow N'$, do seguinte modo, para todo $x \in N'$:

$$S'(x) = \begin{cases} S(x) & \text{se } x \in N \\ f(S(y)) & \text{se } x = f(y),\, y \in Y \text{ e } S(y) \in Y \\ S(y) & \text{se } x = f(y),\, y \in Y \text{ e } S(y) \in X. \end{cases}$$

Definindo, agora, $\mathcal{N}' = \langle N', 0, S' \rangle$, do mesmo tipo que $\langle I\!N, 0, S \rangle$; $\Phi_1 : N \longrightarrow N'$ tal que, para todo $x \in N$, $\Phi_1(x) = x$ e $\Phi_2 : N \longrightarrow N'$ tal que, para todo $x \in N$,

$$\Phi_2(x) = \begin{cases} x & \text{se } x \in X \\ S'(x) & \text{se } x \in Y, \end{cases}$$

poderíamos mostrar que Φ_1 e Φ_2 são homomorfismos distintos de $\mathcal{N}$ em $\mathcal{N}'$. Assim, $X = N$.

S_1 e S_2: Utilizando o fato que $\mathcal{N}$ satisfaz a IM podemos mostrar que existe um homomorfismo $\Phi_1 : I\!N \longrightarrow N$. Por outro lado, a condição *b)* assegura que existe um homomorfismo $\Phi_2 : N \longrightarrow I\!N$. É um raciocínio padrão [6] mostrar que $\Phi_1 \circ \Phi_2$ é um homomorfismo bijetor de $I\!N$ em $I\!N$ e que daí, Φ_1 é um isomorfismo de $I\!N$ em N. ∎

Categoricidade da aritmética de Peano

A noção de categoricidade está relacionada com o poder de expressão de uma teoria.

Definição Uma teoria será *categórica* se quaisquer dois de seus modelos forem isomorfos.

O resultado seguinte expressa uma importante relação entre os conceitos de completude e categoricidade:

Proposição 3.1 *Se $\mathcal{T}$ for uma teoria categórica, então $\mathcal{T}$ será completa.*

Como um corolário do teorema do homomorfismo, temos o seguinte resultado:

Teorema 3.2 (de Dedekind) *Quaisquer dois modelos de Peano são isomorfos.*

Prova:

Se $\mathcal{N}$ e $\mathcal{N}'$ forem modelos de Peano, então existirão Φ e Φ' homomorfismos de $\mathcal{N}$ em $\mathcal{N}'$ e de $\mathcal{N}'$ em $\mathcal{N}$, respectivamente. Provando que $\Phi \circ \Phi'$ é um homomorfismo bijetor de $\mathcal{N}$ em $\mathcal{N}$ concluímos que Φ é um isomorfismo. ∎

O Teorema de Dedekind, no contexto de linguagens de segunda ordem, é um resultado positivo, pois estabelece a completude de P, a partir de sua categoricidade. A principal conseqüência metamatemática do Teorema de Dedekind é que para um conjunto relativamente grande de sentenças, de uma linguagem cujo vocabulário é $\mathcal{V}_{os}$, qualquer sentença que seja verdadeira em um modelo de Peano, será também verdadeira em todos os outros modelos de Peano. Assim, se uma dada sentença for verdadeira em um modelo de Peano particular, tal como o modelo $\langle I\!N, 0, S\rangle$ dos números naturais, será também uma conseqüência lógica dos axiomas de Peano. Em particular, isto se aplica a uma quantidade expressiva de sentenças reconhecidamente verdadeiras sobre números naturais.

No nosso caso, entretanto, o Teorema de Dedekind afirma que o axioma de indução matemática não encontra equivalente em linguagens de primeira ordem, uma vez que, devido ao teorema LST nenhuma teoria elementar que possua somente modelos infinitos será categórica. De fato, o próximo resultado afirma que, para linguagens de primeira ordem, a noção de categoricidade é trivial.

Proposição 3.2 *Se $\mathcal{T}$ for uma teoria consistente, então as seguintes condições serão equivalentes:*

a) $\mathcal{T}$ é categórica;

b) existe um número natural m tal que todo modelo de $\mathcal{T}$ tem cardinalidade m.

Prova:
($\Rightarrow$) Se $\mathcal{T}$ for categórica, como quaisquer dois modelos de $\mathcal{T}$ serão isomorfos, eles terão a mesma cardinalidade c. Se $c \geq \aleph_0$, como $\mathcal{T}$ é consistente, $\mathcal{T}$ possuiria um modelo $\mathcal{N}$ que, de acordo com o teorema LST, teria uma extensão elementar de cardinalidade maior que c e que também seria um modelo de $\mathcal{T}$.
($\Leftarrow$) Imediata. ∎

Definições por recursão primitiva em modelos de Peano

Outra conseqüência fundamental do Teorema do Homomorfismo que pode ser usada na escolha de axiomas para subteorias elementares da aeritmética de Peano é o fato de que, por seu intermédio, podemos definir, em modelos de Peano, operações por recursão primitiva.

Definição Seja $\mathcal{N} = \langle N, 0, S\rangle$ uma estrutura do tipo de $\langle I\!N, 0, S\rangle$, $g : N^{n-1} \to N$, $f : N^n \to N$ e $h : N^{n+1} \to N$ operações em N. f será *definida por recursão primitiva* a partir de g e h se satisfizer as seguintes condições, para todos $x_1, x_2, \ldots, x_n \in N$:

i) $f(x_1, \ldots, x_{n-1}, 0) = g(x_1, \ldots, x_{n-1})$;

ii) $f(x_1, \ldots, x_{n-1}, S(x_n)) = h(x_1, \ldots, x_n, f(x_1, x_2, \ldots, x_n))$.

Teremos, então o seguinte resultado:

Proposição 3.3 *Se $\mathcal{N} = \langle N, 0, S\rangle$ for um modelo de Peano, $g : N^{n-1} \to N$ e $h : N^{n+1} \to N$ operações em N, então existirá uma única operação $f : N^n \to N$, que é definida por recursão primitiva a partir de g e h.*

Como principais corolários da proposição acima, temos as definições de adição, multiplicação e exponenciação, em modelos de Peano.

Definição Seja $\mathcal{N} = \langle N, 0, S\rangle$ uma estrutura do tipo de $\langle I\!N, 0, S\rangle$ e $f : N^2 \to N$ uma operação binária em N:

i) f será uma *adição* em $\mathcal{N}$ se satisfizer as seguintes condições, para todos $x, y \in N$:

$A_1)$ $f(x, 0) = x$;

$A_2)$ $f(x, S(y)) = S(f(x, y))$.

ii) f será uma *multiplicação* em $\mathcal{N}$ se satisfizer as seguintes condições, para todos $x, y \in N$:

$M_1)$ $f(x, 0) = 0$;

$M_2)$ $f(x, S(y)) = g(f(x, y), y)$, onde g é uma adição em $\mathcal{N}$.

iii) f será uma *exponenciação* em $\mathcal{N}$ se satisfizer as seguintes condições, para todos $x, y \in N$:

$E_1)$ $f(x, 0) = S(0)$;

E_2) $f(x, S(y)) = g(f(x, y), y)$, onde g é uma multiplicação em $\mathcal{N}$.

Proposição 3.4 *Se $\mathcal{N} = \langle N, 0, S\rangle$ for um modelo de Peano, então existirá uma única adição, uma única multiplicação e uma única exponenciação em $\mathcal{N}$.*

As operações obtidas no teorema acima são, usualmente, denotadas $+_{\mathcal{N}}$, $\cdot_{\mathcal{N}}$ e $E_{\mathcal{N}}$ e sempre que não houver ambigüidade, simplesmente, $+$, $\cdot$ e E.

A regra de indução matemática

Uma outra propriedade importante de P é que, por intermédio de IM, podemos introduzir uma regra derivada que nos permite provar propriedades que sejam verdadeiras, para todos os números naturais. De fato, teremos:

Regra de indução matemática: Para provar que todos os números naturais possuem uma determinada propriedade $X(x)$, é suficiente provar o seguinte:

i) *Base* de indução: 0 possui a propriedade, ou seja, $X(0)$;

ii) *Passo* de indução: Para todo número natural x, $X(x)$ acarreta $X(sx)$.

Para ilustrar uma distinção importante, podemos agora, utilizando a regra acima, provar algumas propriedades referentes a modelos de Peano.

EXEMPLO 1 Um passo fundamental na prova do Teorema do Homomorfismo é mostrar que se $\mathcal{N} = \langle N, 0, S\rangle$ for um modelo de Peano, então todo elemento de N estará no domínio de alguma função parcial. Isto pode ser feito do seguinte modo, utilizando a regra de indução matemática:

Se $X(x)$ for a propriedade "existe $f : N \longrightarrow N$, tal que f é parcial e $x \in Dom(f)$", teremos:

Base: $X(0)$ é verdadeira, pois $0 \in \{0\}$ e $f : \{0\} \longrightarrow N$, tal que $f(0) = 0$ é parcial.

Passo: Supondo que $X(x)$, ou seja, que existe $f : N \longrightarrow N$, tal que f é parcial e $x \in Dom(f)$, podemos definir $f' : X \cup \{S(x)\} \longrightarrow N$, tal que para todo $y \in X \cup \{S(x)\}$,

$$f'(y) = \begin{cases} f(x) & \text{se } y \in x \\ S(f(y)) & \text{se } y = S(x) \end{cases}$$

e provar, facilmente, que f' é parcial. Assim, teremos $X(S(x))$.

Aplicando, agora, a regra de indução matemática, temos que todo número natural possui a propriedade $X(x)$. ■

EXEMPLO 2 Numa construção sistemática da aritmética a partir dos axiomas de Peano, usualmente definimos a relação de ordem e provamos suas principais propriedades, a partir das principais propriedades da adição:

Definição $\forall x \forall y\ (x < y \leftrightarrow \exists z\ (x + S(z) = y)$.

Podemos agora provar, por exemplo, que se $\mathcal{N} = \langle N, 0, S\rangle$ for um modelo de Peano e $a, b \in N$, ao menos uma das seguintes condições será verdadeira: $a < b$ ou $a = b$ ou $b < a$. Isto pode ser feito do seguinte modo, utilizando a regra de indução matemática:

Se $X(x)$ for a propriedade "para todo y, $x < y$ ou $x = y$ ou $y < x$", teremos:

Base: $X(0)$ é verdadeiro pois, dado y, teremos dois casos:

1º caso: Se $0 = y$, então obviamente, $0 < y$ ou $0 = y$ ou $y < 0$;

2º caso: Se $0 \neq y$, então $0 + y = y$ e $y = S(z)$ para algum z. Assim, $0 < y$ ou $0 = y$ ou $y < 0$.

Passo: Supondo que $X(x)$, ou seja, que para todo y, $x < y$ ou $x = y$ ou $y < x$, teremos três casos a considerar:

1º caso: Se $x < y$, então existirá z, tal que $x + S(z) = y$. Daí, $S(x) + z = y$ e teremos dois subcasos:

a) Se $z = 0$, então $S(x) = y$; *b)* Se $z \neq 0$, então $z = S(w)$, para algum w, o que acarretará $S(x) + S(w) = y$, ou seja, $S(x) < y$.

2º caso: Se $x = y$, então $S(x) = S(y) = y + 1$. Assim, $y + S(0) = S(x)$ e daí, $y < S(x)$.

3º caso: Se $y < x$, então exisistirá z, tal que $y + S(z) = x$. Daí, $S(y + S(z)) = S(x)$ e $y + S(S(z)) = s(x)$, o que acarreta $y < S(x)$.

Em todos os casos, $S(x) < y$ ou $S(x) = y$ ou $y < S(x)$. Assim $X(x)$ acarreta $X(sx)$.

Aplicando, agora, a regra de indução matemática, temos que todo número natural possui a propriedade $X(x)$. ■

Os exemplos acima ilustram diferenças importantes entre as propriedades que podem ser provadas por meio da regra de indução matemática.

Em primeiro lugar, a propriedade $X(x)$ do exemplo 1, a saber, "todo elemento está no domínio de alguma função parcial" é uma propriedade de segunda ordem. Por outro lado, a propriedade $X(x)$ do exemplo 2, a saber, "para quaisquer x e y, ao menos uma das condições $x < y$ ou $x = y$ ou $y < x$ é verdadeira e, claramente, de primeira ordem.

Em segundo lugar, utilizando os fatos anteriores, podemos mostrar que a prova de que todo elemento de N possui a propriedade $X(x)$ do exemplo 2, pode ser inteiramente formalizada no cálculo quantificacional clássico, ao passo que a prova de que todo elemento de N possui a propriedade $X(x)$ do exemplo 1, não pode ser assim formalizada.

Em terceiro e último lugar, enquanto a propriedade provada no exemplo 2 é uma propriedade aritmética usual, a propriedade provada no exemplo 1 é uma propriedade algébrica dos modelos de Peano, necessária para a prova do Teorema do Homomorfismo.

Assim, concluímos que existem vários contextos distintos em que a regra de indução matemática pode ser utilizada para a prova de propriedades da aritmética dos números naturais.

3.2 Aritmética elementar

A *aritmética elementar*, também chamada *aritmética de primeira ordem*, é a parte da *aritmética dos números naturais* que pode ser formalizada em uma linguagem de primeira ordem apropriada. Para caracterizar esta teoria de maneira precisa, consideramos a estrutura $\langle I\!N, 0, S, <, +, \cdot \rangle$, onde $I\!N$, 0, S, $<$, $+$ e $\cdot$ são usuais, definimos uma linguagem de primeira ordem apropriada para esta estrutura e estipulamos que a aritmética elementar consiste de todas as sentenças da linguagem que são verdadeiras em $\langle I\!N, 0, S, <, +, \cdot \rangle$. Assim, temos a seguinte definição:

Definição Chamamos *aritmética elementar*, denotada $Th(\mathbb{N}, 0, S, <, +, \cdot)$, a teoria definida do seguinte modo:

i) **Vocabulário:** $V_{os<+\cdot} = \{o, s, <, +, \cdot\}$, onde o é uma constante individual, s é um funtor de peso 1, $<$ é um predicador de peso 2 e $+$ e $\cdot$ são funtores de peso 2;

ii) **Sentenças:** todas as sentenças da linguagem $\mathcal{L}(\mathcal{V}_{os<+\cdot})$ que são verdadeiras na estrutura $\mathcal{N} = \langle \mathbb{N}, 0, S, <, +, \cdot \rangle$.

A teoria $Th(\mathbb{N}, 0, S, <, +, \cdot)$ é consistente e completa, pois é o conjunto das sentenças de $\mathcal{L}(\mathcal{V}_{os<+\cdot})$ que são verdadeiras em uma única estrutura.

Outras metapropriedades importantes da teoria $Th(\mathbb{N}, 0, S, <, +, \cdot)$ são as seguintes: $Th(\mathbb{N}, 0, S, <, +, \cdot)$ não é axiomatizável [5], representa todas as funções recursivas [5], é indecidível [1] (na verdade, essencialmente indecidível) e possui modelos não padrão de todas as cardinalidades infinitas [14].

Diante dos resultados negativos acima, uma questão natural que se coloca é a de estudar subteorias axiomatizáveis de $Th(\mathbb{N}, 0, S, <, +, \cdot)$ que sejam relevantes como teorias sobre aritmética elementar, ou seja, que provem uma quantidade razoável de teoremas expressivos da aritmética. Uma fonte inspiradora para a definição de tais teorias são os conceitos e resultados apresentados na seção anterior, relativos aos axiomas de Peano.

3.3 Aritmética elementar de Peano

O teorema de Dedekind e a regra de indução matemática, isto é, o fato de que IM não pode ser expresso em linguagens de primeira ordem e o de que IM introduz um método útil para a prova de propriedades referentes a números naturais, nos remetem, naturalmente, à questão de considerar o quanto de IM poderia ser expresso em linguagens elementares e que métodos de prova associados, poderíamos introduzir, na teoria considerada.

A abordagem tomada, no estudo da teoria que é usualmente conhecida como *aritmética elementar de Peano*, decorre da observação que uma grande quantidade de resultados relevantes da aritmética dos números naturais, eventualmente obtidos pelo uso da regra de indução matemática, podem ser expressos em linguagens de primeira ordem. Também é digno de nota que uma quantidade relevante de problemas em aberto, na aritmética dos números naturais, tais como, por exemplo, a Conjectura de Goldbach, podem ser expressos em linguagens elementares. Assim, uma restrição de P somente a enunciados de primeira ordem conteria uma quantidade relevante de resultados (e quem sabe até alguns problemas em aberto) e seria digna de ser estudada como uma subteoria da aritmética elementar. Assim, uma resposta interessante para a questão acima seria restringir o axioma de indução de modo que apliquemos a regra de indução matemática somente a propriedades de $\mathbb{N}$ que possam ser definidas, de uma maneira concreta, por fórmulas de $\mathcal{L}(\mathcal{V}_{os<+\cdot})$. Teremos, então a seguinte definição:

Definição Chamaremos *aritmética elementar de Peano*, denotada PA, a teoria definida do seguinte modo:

i) **Vocabulário:** $\mathcal{V}_{os+\cdot}$;

ii) **Axiomas:** Todas as conseqüências dos seguintes axiomas:

S_1. $\forall x\ sx \neq o$;

S_2. $\forall x \forall y\ (sx = sy \rightarrow x = y)$;

A_1. $\forall x\ x + o = x$;

A_2. $\forall x \forall y\ x + sy = s(x + y)$;

M_1. $\forall x\ x \cdot o = o$;

M_2. $\forall x\ x \cdot sy = x \cdot y + y$;

EIM. Todas as sentenças da forma

$$A[o] \wedge \forall x\ (A[x] \rightarrow A[sx]) \rightarrow \forall x\ A[x],$$

onde $A[x]$ é uma fórmula de $\mathcal{L}(\mathcal{V}_{os<+\cdot})$.

PA é, então, a teoria de primeira ordem que obtemos quando acrescentamos a S_1 e S_2 as definições recursivas de $+$ e $\cdot$ e tanto quanto do axioma de indução seja possível, de modo a permanecer na linguagem $\mathcal{L}(\mathcal{V}_{os+\cdot})$ e no escopo da lógica de primeira ordem.

Esta teoria é consistente pois possui um modelo. Outras metapropriedades importantes de PA são as seguintes: PA é incompleta [5], não é finitamente axiomatizável [12], representa todas as funções recursivas, é indecidível [1] e, na verdade, essencialmente indecidível.

O esquema de axiomas EIM, acima, é chamado o *esquema de axiomas de indução* e dada uma fórmula $A[x]$ em $\mathcal{L}(\mathcal{V}_{os+\cdot})$, a sentença $A[o] \wedge \forall x\ (A[x] \rightarrow A[sx]) \rightarrow \forall x\ A[x]$ é chamada o *axioma de indução associado a* $A[x]$. Em relação ao axioma de indução associado, $A[x]$ será a *fórmula de indução* e x a *variável de indução*.

De acordo com o teorema LST, PA é mais fraca que P e não caracteriza a estrutura $\langle I\!N, 0, S, <, +, \cdot\rangle$, uma vez que possui modelos não padrão de todas as cardinalidades infinitas.

Existem, agora, duas observações importantes a serem feitas. A primeira é que enquanto o axioma de indução IM é dado por uma única sentença de segunda ordem, EIM é dado por um *esquema de axiomas*, ou seja, um conjunto de fórmulas da linguagem de primeira ordem $\mathcal{L}(\mathcal{V}_{os+\cdot})$, que possuem a mesma forma. Assim, PA é recursivamente axiomatizável, isto é, existe um procedimento recursivo para decidir se uma dada sentença A é, ou não, um axioma de PA. A segundo observação é que a presença do esquema de axiomas de indução em PA nos permite introduzir uma regra derivada semelhante aquela introduzida pela presença do axioma de indução em P.

Definição Chamaremos *regra elementar de indução matemática* à regra:

$$\frac{A[o],\ \forall x\ (A[x] \rightarrow A[sx])}{\forall x\ A[x]},$$

onde $A[x]$ é uma fórmula de $\mathcal{L}(\mathcal{V}_{os+\cdot})$.

Utilizando a regra acima, podemos provar em PA quase toda a extensão do que é hoje conhecido como *teoria elementar dos números* e *combinatória finita* [8, 9].

3.4 Esquemas de axiomas

Nesta seção, investigamos mais detalhadamente a expressão dos princípios de indução em linguagens de primeira ordem.

Usualmente, expressamos parte do conteúdo de um princípio de indução em uma linguagem elementar, de uma maneira construtiva, restringindo a aplicação do princípio somente a propriedades que possam ser expressas na linguagem considerada.

EXEMPLO Na aritmética elementar de Peano, PA, a expressão do princípio de indução matemática, $I(I\!N, 0, S)$ em $\mathcal{L}(\mathcal{V}_{os+\cdot})$ é o esquema de axiomas de indução matemática, EIM, definido como o conjunto de todas as sentenças de $\mathcal{L}(\mathcal{V}_{os+\cdot})$ da seguinte forma:

$$A[o] \wedge \forall x\ (A[x] \to A[sx]) \to \forall x\ A[x],$$

onde $A[x]$ é uma fórmula de $\mathcal{L}(\mathcal{V}_{os<+})$.

Assim, o esquema de axiomas de indução matemática, é introduzido como o conjunto recursivo das sentenças de $\mathcal{L}(\mathcal{V}_{os+\cdot})$ que possuem a *forma* do princípio em questão.

Neste caso, definimos o esquema de axiomas, mediante os seguintes passos:

(1) Selecionamos um determinado conjunto recursivo Γ de fórmulas da linguagem $\mathcal{L}(\mathcal{V}_{os+\cdot})$;

(2) Associamos a cada fórmula A de Γ, uma sentença $I(A)$;

(3) Tomamos $I(\Gamma) = \{I(A) : A \text{ é uma fórmula de } \Gamma\}$.

EXEMPLO Especificamente, EIM é definido tomando-se Γ como o conjunto das fórmulas de $\mathcal{L}(\mathcal{V}_{os+\cdot})$ que possuem a ocorrência de exatamente uma variável livre e associando-se a cada fórmula $A(x)$ de Γ a sentença de $\mathcal{L}(\mathcal{V}_{os+\cdot})$ que possui a seguinte forma:

$$A(o) \wedge \forall x\ (A(x) \to A(sx)) \to \forall x\ A(x).$$

Observamos ainda que, no exemplo acima, consideramos o esquema de axiomas como o próprio conjunto $I(\Gamma)$. Mas existem situações em que é conveniente considerarmos o esquema de uma forma um pouco mais geral.

Seja $\mathcal{L}(\mathcal{V}_{os})$ a sublinguagem de $\mathcal{L}(\mathcal{V}_{os+\cdot})$ cujo vocabulário consiste apenas de o e s. Seja $\mathcal{T}_{os}$ a teoria sobre $\mathcal{L}(\mathcal{V}_{os})$, definida pelos seguintes axiomas:

S_1. $\forall x\ sx \neq o$;

S_2. $\forall x \forall y\ (sx = sy \to x = y)$;

$EIM(\mathcal{V}_{os})$. Todas as sentenças de $\mathcal{L}(\mathcal{V}_{os})$ da seguinte forma:

$$A[o] \wedge \forall x\ (A[x] \to A[sx]) \to \forall x\ A[x].$$

$EIM(\mathcal{V}_{os})$ é o conjunto de sentenças obtido por *aplicação* de IM ao conjunto das fórmulas de $\mathcal{L}(\mathcal{V}_{os})$ que possuem a ocorrência de, exatamente, uma variável livre.

No capítulo 5, mostraremos que $\mathcal{T}_{os}$ é a teoria da estrutura $\langle \mathbb{N}, 0, S\rangle$, onde $\mathbb{N}$, 0 e S são usuais. Caracterizaremos todos os seus modelos e decorrerá daí que entre estes se encontra a estrutura $\mathcal{N} = \langle N, 0_N, S_N\rangle$, definida do seguinte modo (e é a base dos logaritmos neperianos):

i) **Domínio:** $N = \mathbb{N} \cup X$, onde $X = \{e^n : n \in \mathbb{Z}\}$;

ii) **Elemento distinguido:** $0_N = 0$;

iii) **Operação distinguida:** $S_N : \mathbb{N} \cup X \to \mathbb{N} \cup X$ é a operação definida do seguinte modo, para todo $a \in \mathbb{N} \cup X$:

$$S_N(a) = \begin{cases} a+1 & \text{se } a \in \mathbb{N} \\ e \cdot a & \text{se } a \in X. \end{cases}$$

Podemos considerar a possibilidade de estendermos $\mathcal{T}_{os}$ a uma nova teoria $\mathcal{T}_{os+}$ acrescentando a S_1, S_2 e ao esquema, os seguintes axiomas, que expressam a definição recursiva da adição, a partir de o e s:

A_1. $\forall x\ x + o = x$;

A_2. $\forall x \forall y\ x + sy = s(x+y)$.

Teremos então, a seguinte questão: que propriedades usuais (associatividade, regularidade, existência do elemento neutro, comutatividade, etc.) da operação de adição, poderiam ser provadas na teoria $\mathcal{T}_{os+}$? Como veremos, existem duas respostas a esta pergunta, dependendo do modo como consideramos o esquema de axiomas.

Se consideramos o esquema apenas como o conjunto das sentenças de $\mathcal{L}(\mathcal{V}_{os})$ que possuem a forma de $I(\mathbb{N}, 0, S)$, nenhum dos seus exemplares, quando considerado como um axioma de $\mathcal{T}_{os+}$, possuirá ocorrência do símbolo $+$. Decorrerá daí que as propriedades usuais acima não estão asseguradas.

Exemplo É fácil verificar que a estrutura $\mathcal{N}' = \langle N', 0_{N'}, S_{N'}, +_{N'}\rangle$, definida abaixo é um modelo de $\mathcal{T}_{os+}$ e que $+_{N'}$ não é associativa.

i) $N', 0_{N'}, S_{N'}$ são como em $\mathcal{N}$;

ii) $+_{N'}$ é a operação binária em N', definida do seguinte modo, para $a, b \in N$:

$$a +_{N'} b = \begin{cases} a & \text{se } b = 0 \\ a + b & \text{se } a, b \in I\!N \\ e^a & \text{se } a \in I\!N \text{ e } b \in X \\ e^b & \text{se } a \in X \text{ e } b \in I\!N \\ |\ln a + \ln b| & \text{se } a, b \in X. \end{cases}$$

Por outro lado, quando passamos de $\mathcal{T}_{os}$ a $\mathcal{T}_{os+}$, é usual considerarmos a extensão dos axiomas não somente pelo acréscimo de A_1 e A_2 a S_1, S_2 e $EIM(\mathcal{V}_{os})$, mas também pelo acréscimo de todas as sentenças de $\mathcal{L}(\mathcal{V}_{os+})$ da forma de $I(I\!N, 0, S)$ que possuem a ocorrência do símbolo $+$. Neste caso, a teoria $\mathcal{T}_{os+}$ é definida pelos seguintes axiomas:

S_1. $\forall x \; sx \neq o$;

S_2. $\forall x \forall y \; (sx = sy \to x = y)$;

A_1. $\forall x \; x + o = x$;

A_2. $\forall x \forall y \; x + sy = s(x + y)$;

$EIM(\mathcal{V}_{os+})$. Todas as sentenças de $\mathcal{L}(\mathcal{V}_{os+})$ da seguinte forma:

$$A[o] \wedge \forall x \; (A[x] \to A[sx]) \to \forall x \; A[x].$$

É fácil verificar que a teoria acima prova todas as propriedades usuais da adição [9].

Assim, podemos considerar um esquema de axiomas de duas maneiras distintas:

(1) Como um conjunto $I(\Gamma)$ de sentenças de uma linguagem de primeira ordem $\mathcal{L}$, obtido pela aplicação de uma função I a um conjunto recursivo de fórmulas de $\mathcal{L}$;

(2) Como uma função I que nos permite, dada uma linguagem de primeira ordem $\mathcal{L}$ (satisfazendo a determinadas condições) e um conjunto Γ de fórmulas de $\mathcal{L}$ (satisfazendo uma determinada condição recursiva), construir um conjunto de sentenças de $\mathcal{L}$.

No primeiro caso, temos a noção de esquema devida a Von Neumann, onde o axioma é definido como o conjunto das fórmulas da linguagem que possuem uma dada *forma*.

No segundo caso, temos uma noção mais geral de esquema que incorpora, como a de Frege, o conceito de aplicação do esquema a extensões da linguagem que contém os símbolos elementares que ocorrem no esquema.

Capítulo 4

Linguagens Esquemáticas e Especificação de Teorias

Como vimos nos capítulos anteriores, a toda estrutura indutiva está associado um princípio de indução e a todo princípio de indução corresponde uma estrutura indutiva. Um axioma de indução é a expressão de um princípio de indução em uma linguagem formal. Dada uma estrutura indutiva $\mathcal{N}$, sua teoria $Th(\mathcal{N})$ e o princípio de indução $I(\mathcal{N})$ associado, devido às limitações inerentes ao poder de expressão das linguagens de primeira ordem, só podemos expressar em $Th(\mathcal{N})$ parte do conteúdo de $I(\mathcal{N})$. Com o objetivo de expressar parte do conteúdo do princípio de indução em $Th(\mathcal{N})$, introduzimos a noção de esquema de axiomas de indução como o conjunto das sentenças de $\mathcal{L}(\mathcal{N})$ que possuem a forma do princípio considerado, ou ainda, as sentenças obtidas por aplicação de $I(\mathcal{N})$ somente a propriedades que possam ser espressas em $\mathcal{L}(\mathcal{N})$. No capítulo anterior, exemplificamos duas maneiras distintas em que podemos considerar um esquema de axiomas. Neste capítulo, estudamos as duas maneiras usuais de se expressar parte do conteúdo dos princípios de indução em linguagens de primeira ordem: os *esquemas de axiomas* e as *fórmulas esquemáticas.*

Os principais conceitos e resultados aqui apresentados encontram-se dispersos na literatura e seu tratamento sistemático foi uma de nossas principais motivações. Foi somente no decorrer de nossos estudos, quando já havíamos elaborado este capítulo, que tomamos contato com [3], onde, pelas informações que pudemos angariar, tais conceitos e resultados encontram-se pela primeira vez reunidos.

4.1 Linguagens esquemáticas

Nesta seção, apresentamos o conceito de as *linguagem esquemática*. Linguagens esquemáticas serão extensões das linguagens de primeira ordem que possuem entre as suas ebfs fórmulas especiais, chamadas *fórmulas esquemáticas*. Dentre as fórmulas esquemáticas destacam-se as *sentenças esquemáticas* que desempenharão um papel fundamental na definição e na aplicação de esquemas de axiomas e, em particular, dos esquemas de axiomas de indução.

Definição Uma *linguagem esquemática* associada a uma linguagem de primeira ordem $\mathcal{L}$, denotada $\mathcal{L}E$, consistirá do seguinte:

i) **Símbolos**: Os símbolos de $\mathcal{L}E$ são:

a) Os símbolos de $\mathcal{L}$;

b) As *variáveis esquemáticas*: Uma quantidade não nula, de símbolos distintos dos símbolos de $\mathcal{L}$.

Variáveis esquemáticas serão denotadas pelas letras X, Y ou Z, indexadas ou não. Associado a cada variável esquemática X existirá um número natural chamado o *peso* ou *aridade* de X. Uma variável esquemática será n-*ária* se for de peso n.

c) Os *sinais de pontuação*: [(*abre colchetes*) e] (*fecha colchetes*).

ii) **Expressões bem formadas**: As expressões bem formadas (ebfs) de $\mathcal{L}E$ são:

a) As ebfs de $\mathcal{L}$;

b) As expressões sobre o alfabeto de $\mathcal{L}E$, dadas pela seguinte definição indutiva:

Rf_1) Se α for uma variável esquemática de peso n e $t_1, \ldots, t_n$ forem termos de $\mathcal{L}$, então $\alpha[t_1, \ldots, t_n]$ será uma ebf de $\mathcal{L}E$;

Rf_2) Se α for uma ebf de $\mathcal{L}E$, então $(\neg\alpha)$ será uma ebf de $\mathcal{L}E$;

Rf_3) Se α e β forem ebfs de $\mathcal{L}E$, então $(\alpha \to \beta)$ será uma ebf de $\mathcal{L}E$;

Rf_4) Se α for uma ebf de $\mathcal{L}E$ e x for uma variável individual de $\mathcal{L}$, então $\forall x\alpha$ será uma ebf de $\mathcal{L}E$.

As ebfs de $\mathcal{LE}$ serão também chamadas *fórmulas esquemáticas.* Fórmulas esquemáticas serão denotadas pelas letras α, β ou δ, indexadas, ou não.

Definição Uma fórmula esquemática será:

i) *atômica* se for obtida por aplicação da regra Rf_1;

ii) uma *negação esquemática* se for obtida por aplicação da regra Rf_2;

iii) uma *implicação esquemática* se for obtida por aplicação da regra Rf_3;

iv) uma *generalização esquemática* se for obtida por aplicação da regra Rf_4;

v) *estrita* se possuir ao menos uma ocorrência de variável esquemática.

Analogamente as linguagens de primeira ordem, teremos as seguintes abreviações:

Definição Seja $\mathcal{LE}$ un a linguagem esquemática, x uma variável de $\mathcal{L}$ e α, β fórmulas esquemáticas de $\mathcal{LE}$:

i) $(\alpha \wedge \beta) =_{def} \neg(\alpha \rightarrow \neg\beta)$;

ii) $(\alpha \vee \beta) =_{def} (\neg\alpha \rightarrow \beta)$;

iii) $\exists x\ \alpha =_{def} \neg\forall x\ \neg\alpha$.

Definimos também as noções de ocorrências livres e ligadas de variáveis individuais de $\mathcal{L}$ em fórmulas esquemáticas de $\mathcal{LE}$:

Definição Seja $\mathcal{LE}$ uma linguagem esquemática e α uma fórmula esquemática de $\mathcal{LE}$. O *conjunto das variáveis livres* de α, denotado $Vl(\alpha)$, será definido pelas seguintes regras:

Vl_1) Se α for uma fórmula A de $\mathcal{L}$, então $Vl(\alpha) = Vl(A)$;

Vl_2) Se α for $X[t_1, \ldots, t_n]$, onde X é uma variável esquemática de peso n, então $Vl(\alpha) = Vl(t_1) \cup \ldots \cup Vl(t_n)$;

Vl_3) Se α for $(\neg\beta)$, então $Vl(\alpha) = Vl(\beta)$;

Vl_4) Se α for $(\beta \rightarrow \delta)$, então $Vl(\alpha) = Vl(\beta) \cup Vl(\delta)$;

Vl_5) Se α for $\forall x\ \beta$, então $Vl(\alpha) = Vl(\beta) \setminus \{x\}$.

Finalmente, temos a seguinte definição:

Definição Seja $\mathcal{LE}$ uma linguagem esquemática, x uma variável de $\mathcal{L}$

e α uma fórmula esquemática de $\mathcal{L}E$.

i) x ocorrerá livre em α se $x \in Vl(\alpha)$;

ii) x ocorrerá ligada em α se x ocorrer em α e $x \notin Vl(\alpha)$.

iii) α será uma *sentença esquemática* se não possuir ocorrências livres de variáveis individuais.

EXEMPLO Algumas linguagens esquemáticas sobre $\mathcal{L}(\mathcal{V}_{os})$ são as seguintes:

a) $\mathcal{L}(\mathcal{V}_{os})E$, definida do seguinte modo:

i) **Vocabulário:** $\mathcal{V}_{os}$;

ii) **Variável esquemática:** X, de peso 1;

Exemplos de sentenças esquemáticas sobre $\mathcal{L}(\mathcal{V}_{os})E$ são os seguintes:

α_1. $X[o] \wedge \forall x\ (X[x] \rightarrow X[sx]) \rightarrow \forall x\ X[x]$;

α_2. $X[o] \wedge \forall x\ X[sx]) \rightarrow \forall x\ X[x]$;

α_1. $X[o] \wedge \forall x\ (X[x] \leftrightarrow X[sx]) \rightarrow \forall x\ X[x]$

b) $\mathcal{L}(\mathcal{V}_{os})E'$, definida do seguinte modo:

i) **Vocabulário:** $\mathcal{V}_{os}$;

ii) **Variável esquemática:** Y, de peso 2.

Exemplos de sentenças esquemáticas sobre $\mathcal{L}(\mathcal{V}_{os})E'$ são os seguintes:

β_1. $Y[o,o] \wedge \forall x \forall y\ (Y[x,y] \rightarrow Y[sx,y] \wedge Y[x,sy]) \rightarrow \forall x \forall y\ Y[x,y]$.

β_2. $\forall x\ Y[x,o] \wedge \forall y\ Y[o,y] \wedge \forall x \forall y\ (Y[x,y] \rightarrow Y[sx,sy]) \rightarrow \forall x \forall y Y[x,y]$.

4.2 Substituição

Dada uma linguagem esquemática $\mathcal{L}E$, podemos definir uma noção de substituição de variáveis esquemáticas por fórmulas esquemáticas, obtendo como resultado fórmulas esquemáticas de $\mathcal{L}E$.

Inicialmente, faremos as seguintes convenções:

- Denotaremos por $\alpha[x_1, \ldots, x_m]$ uma fórmula de $\mathcal{L}E$, tal que $Vl(\alpha) = \{x_1, \ldots, x_m\}$.

- Denotaremos por $\alpha(X_1, \ldots, X_m)$, uma fórmula esquemática de $\mathcal{L}E$, que possua, no máximo, ocorrências das variáveis esquemáticas $X_1, \ldots, X_m$.

- Denotaremos por $\alpha[t_1, \ldots, t_m]$ a fórmula esquemática de $\mathcal{LE}$, obtida por substituição simultânea de $x_1, \ldots, x_m$ por $t_1, \ldots, t_m$, respectivamente, em $\alpha[x_1, \ldots, x_m]$.

Definição Seja $\mathcal{LE}$ uma linguagem esquemática, X uma variável esquemática de peso m de $\mathcal{LE}$, $\alpha(X)$ e $\beta(x_1, \ldots, x_m)$ fórmulas esquemáticas de $\mathcal{LE}$. A *substituição adequada* de X por β em α, denotada $(\beta/X)\alpha$ e lida "β no lugar de X em α", é dada pela seguinte definição recursiva:

Rs_1) Se α for $Y(t_1, \ldots, t_m)$, então $(\beta/X)\alpha$ será $\beta(t_1, \ldots, t_m)$, se $X = Y$ ou $Y(t_1, \ldots, t_m)$, se $X \neq Y$;

Rs_2) Se α for $(\neg\gamma)$, então $(\beta/X)\alpha$ será $(\neg(\beta/X)\gamma)$;

Rs_3) Se α for $(\gamma \to \delta)$, então $(\beta/X)\alpha$ será $((\beta/X)\gamma \to (\beta/X)\delta)$;

Rs_4) Se α for $\forall x\gamma$, então $(\beta/X)\alpha$ será $\forall y(((y/x)\beta)/X)((y/x)\gamma)$, onde y é a primeira variável individual de $\mathcal{L}$ que não ocorre livre em β.

A substituição de x por y em RS_4 é feita de modo a evitar a colisão de variáveis. Na definição acima, X será chamada a *variável de substituição*, α a *fórmula substituída*, β a *fórmula subtituta* e $(\beta/X)\alpha$ o *resultado da substituição* de β no lugar de X em α.

A noção acima pode ser facilmente generalizada para a substituição simultânea de variáveis esquemáticas por fórmulas esquemáticas de $\mathcal{LE}$. Assim, faremos também a seguinte convenção:

- Denotaremos por $\alpha(\beta_1, \ldots, \beta_n)$ a fórmula obtida por substituição simultânea das variáveis esquemáticas $X_1, \ldots, X_n$ por $\beta_1, \ldots, \beta_n$, respectivamente, em $\alpha(X_1, \ldots, X_n)$.

4.3 Esquemas de fórmulas

Intuitivamente, um *esquema de fórmulas*, de uma linguagem de primeira ordem $\mathcal{L}$, é um conjunto de fórmulas de $\mathcal{L}$, que possuem a mesma forma.

Se $\mathcal{LE}$ for uma linguagem esquemática, poderemos definir de maneira formal esquemas de $\mathcal{L}$, utilizando fórmulas esquemáticas de $\mathcal{LE}$. Agora que temos uma noção de substituição de variáveis esquemáticas por fórmulas esquemáticas, isto pode ser feito se restringirmos a noção de substituição somente a fórmulas de $\mathcal{L}$, obtendo como resultados fórmulas de $\mathcal{L}$.

Definição Seja $\mathcal{L}$ uma linguagem de primeira ordem, $\mathcal{L}E$ uma linguagem esquemática associada a $\mathcal{L}$ e $\alpha(X_1, ..., X_m)$ uma fórmula esquemática de $\mathcal{L}E$.

i) O *esquema de fórmulas* de $\mathcal{L}$, gerado por $\alpha(X_1, ..., X_m)$, denotado $\mathcal{E}_\alpha$, será o conjunto de todas as fórmulas de $\mathcal{L}$, obtidas por substituição adequada de variáveis esquemáticas de $\alpha(X_1, ..., X_m)$ por fórmulas de $\mathcal{L}$.

ii) Um elemento de um esquema $\mathcal{E}$ será chamado uma *instância* de $\mathcal{E}$.

Assim, o esquema de fórmulas gerado por α é o conjunto de todas as instâncias que podem ser obtidas por substituição adequada das variáveis esquemáticas de α por fórmulas de $\mathcal{L}$, ou seja, é o conjunto de todas as fórmulas de $\mathcal{L}$ que possuem a forma determinada por α. Obviamente, se $\mathcal{E}$ for um esquema de fórmulas, então $\mathcal{E}$ será decidível.

Definição Um esquema de fórmulas será *implicativo* se for gerado por uma implicação esquemática.

4.4 Regras de inferência

Seja m um número natural e $\mathcal{L}$ uma linguagem de primeira ordem. Uma *regra de inferência* em $\mathcal{L}$ é uma relação $(m+1)$-ária entre fórmulas de $\mathcal{L}$. Como é usual, se $A_1, \ldots, A_m, B$ forem fórmulas de $\mathcal{L}$, escrevemos

$$\frac{A_1, \ldots, A_m}{B} R \quad \text{ou} \quad A_1, \ldots, A_m \overset{R}{\Longrightarrow} B$$

ao invés de $(A_1, \ldots, A_m, B) \in R$. Neste caso, diremos que B é *conseqüência* de $\{A_1, \ldots, A_m\}$ por R.

Se $\mathcal{L}E$ for uma linguagem esquemática, analogamente aos esquemas de axiomas, poderemos definir de maneira formal regras em $\mathcal{L}$, utilizando seqüências de fórmulas esquemáticas de $\mathcal{L}E$.

Definição Seja $\mathcal{L}$ uma linguagem de primeira ordem, $\mathcal{L}E$ uma linguagem esquemática associada a $\mathcal{L}$ e $R = \langle \alpha_1, \ldots, \alpha_m, \beta \rangle$ uma $(m+1)$-upla de fórmulas esquemáticas de $\mathcal{L}E$. A *regra de inferência* em $\mathcal{L}$ gerada por R será o conjunto de todas as $(m+1)$-uplas de fórmulas de $\mathcal{L}$, obtidas por substituição adequada das variáveis esquemáticas de $\alpha_1, \ldots, \alpha_m$, β por fórmulas de $\mathcal{L}$.

De maneira análoga a anterior, se $\alpha_1, \ldots, \alpha_m, \beta$ forem esquemas de fórmulas, definiremos uma regra pelas expressões

$$\frac{\alpha_1, \ldots, \alpha_m}{\beta}R \quad \text{ou} \quad \alpha_1, \ldots, \alpha_m \stackrel{R}{\Longrightarrow} \beta.$$

EXEMPLO Se $\mathcal{L}$ for uma linguagem de primeira ordem qualquer e se em $\mathcal{L}E$ ocorrerem ao menos as variáveis esquemáticas X e Y, ambas de peso 0, exemplos básicos de regras de inferência que podem ser definidas utilizando-se fórmulas esquemáticas de $\mathcal{L}E$, são a *Modus Ponens (MP)* e a *Generalização (GEN)*, definidas respectivamente por:

$$\frac{X, X \to Y}{Y}MP \quad \text{e} \quad \frac{X}{\forall x X}GEN$$

Definição Uma regra será *válida* se preservar a validade de fórmulas, isto é, se para todas as fórmulas $A_1, \ldots, A_m, B$ de $\mathcal{L}, \models A_1, \ldots, \models A_m$ e $A_1, \ldots, A_m \stackrel{R}{\Longrightarrow} B$ implicar em $\models B$. Uma regra será *não lógica* se não for válida.

EXEMPLO Modus ponens e generalização são exemplos de regras válidas. Um exemplo simples de regra não lógica é a *Eliminação do* $\vee$ $(E\vee)$:

$$\frac{X \vee Y}{X}E\vee$$

Devemos ainda observar que associada, de modo natural, a cada implicação esquemática cujo antecedente é uma conjunção, existe uma regra de inferência. A saber, se α for $(\alpha_1 \wedge \ldots \wedge \alpha_m \to \beta)$, então a regra associada a α será:

$$\frac{\alpha_1, \ldots, \alpha_m}{\beta}R_\alpha$$

Decorre daí que associada a cada esquema de fórmulas implicativo, existe uma regra. A saber, se $\mathcal{E}$ for um esquema de axiomas gerado pela fórmula esquemática $(\alpha_1 \wedge \ldots \wedge \alpha_m \to \beta)$, então $R_{(\alpha_1 \wedge \ldots \wedge \alpha_m \to \beta)}$ será a *regra associada* a $\mathcal{E}$.

A recíproca também acontece, ou seja, associada a cada regra de inferência, gerada por uma seqüência de fórmulas esquemáticas existe uma implicação esquemática e daí, um esquema de fórmulas. A saber, se R for

$$\frac{\alpha_1, \ldots, \alpha_m}{\beta} R$$

então a fórmula esquemática associada a R será $(\alpha_1 \wedge \ldots \wedge \alpha_m \rightarrow \beta)$ e o esquema de fórmulas associado a R, será $\mathcal{E}_{(\alpha_1 \wedge \ldots \wedge \alpha_m \rightarrow \beta)}$.

4.5 Especificação de teorias

Nesta seção, mostramos como podemos, dada uma linguagem de primeira ordem $\mathcal{L}$, utilizar linguagens esquemáticas, definidas sobre $\mathcal{L}$, para definir teorias de primeira ordem, sobre $\mathcal{L}$.

Uma teoria de primeira ordem sobre $\mathcal{L}$ é um conjunto de fórmulas de $\mathcal{L}$, fechado para a relação de conseqüência lógica. Existem duas maneiras usuais de se definir teorias sobre $\mathcal{L}$: *semântica* ou *sintaticamente*.

Uma teoria é definida semanticamente como o conjunto das fórmulas de $\mathcal{L}$ que são verdadeiras em uma classe de estruturas. Sintaticamente, uma teoria é definida como o conjunto de todas as fórmulas de $\mathcal{L}$ que são conseqüência de um determinado conjunto recursivo $\mathcal{A}x$, de fórmulas de $\mathcal{L}$.

No segundo caso, dizemos que $\mathcal{A}x$ *especifica* a teoria $\mathcal{T}$ ou que $\mathcal{A}x$ é um *conjunto de axiomas* para $\mathcal{T}$. Dependendo do modo como o conjunto $\mathcal{A}x$ pode ser definido, teremos duas maneiras de, dada uma linguagem de primeira ordem $\mathcal{L}$, especificar uma teoria sobre $\mathcal{L}$.

Definição Uma *especificação usual* Spc será um par ordenado $\langle \mathcal{L}, \mathcal{A}x \rangle$, onde:

i) $\mathcal{L}$ é uma linguagem de primeira ordem;

ii) $\mathcal{A}x$ é um conjunto recursivo (possivelmente vazio) de sentenças de $\mathcal{L}$.

Especificações usuais podem ser consideradas como o primeiro modo de definirmos teorias sobre $\mathcal{L}$.

Definição Seja $\mathcal{L}$ uma linguagem de primeira ordem e $\mathcal{A}x$ um conjunto recursivo de fórmulas de $\mathcal{L}$.

i) A *teoria* definida pela especificação usual $Spc = \langle \mathcal{L}, \mathcal{A}x \rangle$ será o conjunto $Cn(\mathcal{A}x)$.

ii) Um elemento de $\mathcal{A}x$ será chamado um *axioma extra lógico* de $Cn(\mathcal{A}x)$.

iii) Uma teoria $\mathcal{T}$, sobre $\mathcal{L}$, será *axiomatizável* (no sentido usual) se existir uma especificação usual, $Spc = \langle \mathcal{L}, \mathcal{A}x \rangle$, tal que $Cn(\mathcal{A}x) = \mathcal{T}$.

iv) Uma teoria $\mathcal{T}$ será *finitamente axiomatizável* (no sentido usual) se for axiomatizável por um conjunto finito.

EXEMPLO Denotaremos por $Th(\mathbb{N}, 0, S)$ a teoria definida do seguinte modo:

i) **Linguagem:** $\mathcal{L}_{os}$;

ii) **Sentenças:** Todas as sentenças de $\mathcal{L}_{os}$ que são verdadeiras na estrutura $\langle \mathbb{N}, 0, S \rangle$.

Denotamos por Spc_{os} a especificação usual definida do seguinte modo:

i) **Linguagem:** $\mathcal{L}_{os}$;

ii) **Axiomas:** $\mathcal{A}x_{os} = \{S_1, S_2, S_3, S_{4.1}, S_{4.2}, \ldots, S_{4.n}, \ldots\}$, onde:

S_1. $\forall x \; sx \neq o$;

S_2. $\forall x \forall y \; (sx = sy \rightarrow x = y)$;

S_3. $\forall x \; (x \neq o \rightarrow \exists y \; sy = x)$;

$S_{4.1}$. $\forall x \; sx \neq x$;

$S_{4.2}$. $\forall x \; ssx \neq x$;

$\vdots$

$S_{4.n}$. $\forall x \; ss \ldots sx \neq x$;

$\vdots$

No capítulo 5, mostramos que Spc_{os} é uma especificação usual para a teoria da estrutura $\langle \mathbb{N}, 0, S \rangle$. Em outras palavras, mostramos que $Cn(\mathcal{A}x_{os}) = Th(\mathbb{N}, 0, S)$.

Definição Uma *especificação esquemática* $SpcE$ será um terno ordenado $\langle \mathcal{L}E, \mathcal{A}x, \mathcal{R} \rangle$, onde:

i) $\mathcal{L}E$ é uma linguagem esquemática;

ii) $\mathcal{A}x$ é um conjunto recursivo (possivelmente vazio) de fórmulas esquemáticas de $\mathcal{L}E$;

iii) $\mathcal{R}$ é um conjunto recursivo (possivelmente vazio) de seqüências finitas de fórmulas esquemáticas estritas de $\mathcal{L}E$.

Para que possamos considerar uma especificação esquemática como a definição de uma teoria sobre $\mathcal{L}$ devemos, em primeiro lugar, munir $\mathcal{L}E$ de uma relação de conseqüência lógica.

Definição Seja $\mathcal{L}E$ uma linguagem esquemática, x, y variáveis de $\mathcal{L}$ e α, β, δ fórmulas esquemáticas de $\mathcal{L}E$. Um *axioma lógico* de $\mathcal{L}E$ será uma fórmula esquemática, obtida por aplicação de uma das seguintes regras:

Ra_1. $\alpha \to (\beta \to \alpha)$ é um axioma lógico de $\mathcal{L}E$;

Ra_2. $\alpha \to (\beta \to \delta) \to ((\alpha \to \beta) \to (\alpha \to \delta))$ é um axioma lógico de $\mathcal{L}E$;

Ra_3. $(\neg\alpha \to \neg\beta) \to (\beta \to \alpha)$ é um axioma lógico de $\mathcal{L}E$;

Ra_4. Se x for substituível por t em α, então $\forall x\ \alpha \to (t/x)\alpha$ será um axioma lógico de $\mathcal{L}E$;

Ra_5. $\forall x\ (\alpha \to \beta) \to (\forall x\ \alpha \to \forall x\ \beta)$ é um axioma lógico de $\mathcal{L}E$;

Ra_6. Se $x \notin Vl(\alpha)$, então $\alpha \to \forall x\ \alpha$ será um axioma lógico de $\mathcal{L}E$;

Ra_7. $x = x$ é um axioma lógico de $\mathcal{L}E$;

Ra_8. Se α for atômica e α' for obtida a partir de α pela troca de x por y em uma ou mais ocorrências de x em α, então $x = y \to (\alpha \to \alpha')$ será um axioma lógico de $\mathcal{L}E$;

Ra_9. Se α for um axioma lógico de $\mathcal{L}E$, então $\forall x\ \alpha$ será um axioma lógico de $\mathcal{L}E$.

Definição Seja $SpcE = \langle \mathcal{L}E, \mathcal{A}x, \mathcal{R} \rangle$ uma especificação esquemática. Uma *derivação* em $SpcE$ será uma seqüência finita $d = \langle \alpha_1, \ldots, \alpha_m \rangle$ de fórmulas esquemáticas de $\mathcal{L}E$, tal que para todo índice i, $1 \leq i \leq m$, ao menos uma das seguintes condições seja satisfeita:

i) α_i é um axioma lógico de $\mathcal{L}E$;

ii) existem α_j e α_k, anteriores a α_i na seqüência, tais que $\alpha_j, \alpha_k \overset{MP}{\Longrightarrow} \alpha_i$;

iii) $\alpha_i \in \mathcal{A}x$;

iv) existem $\alpha_{i1}, \ldots, \alpha_{in}$, anteriores a α_i na seqüência e $R \in \mathcal{R}$, de aridade $n+1$, tais que $R = \langle \alpha_{i1}, \ldots, \alpha_{in}, \alpha_i \rangle$;

v) existe α_j, anterior a α_i na seqüência, tal que α_i é obtida a partir de α_j por substituição adequada, o que será denotado $\alpha_j \overset{SUB}{\Longrightarrow} \alpha_i$,

Definição Se α for uma fórmula esquemática de $\mathcal{L}E$, uma *derivação de*

α em $SpcE$ será uma derivação em $SpcE$, tal que α_m seja α.

Assim, especificações esquemáticas podem ser consideradas como definições de teorias em $\mathcal{L}E$.

Definição Seja $\mathcal{L}E$ uma linguagem esquemática, $\mathcal{A}x$ um conjunto recursivo de fórmulas esquemáticas de $\mathcal{L}E$ e $\mathcal{R}$ um conjunto recursivo de seqüências finitas de fórmulas esquemáticas de $\mathcal{L}E$.

i) A *teoria esquemática* definida pela especificação esquemática $SpcE = \langle \mathcal{L}E, \mathcal{A}x, \mathcal{R} \rangle$ será o conjunto $Cn(SpcE) = \{\alpha /$ existe uma derivação de α em $SpcE\}$, sobre $\mathcal{L}E$;

ii) Um *axioma não lógico* de $SpcE$ será um elemento de $\mathcal{A}x$;

iii) Uma *regra não lógica* de $SpcE$ será um elemento de $\mathcal{R}$;

iv) Um *esquema de axiomas* de $SpcE$ será uma fórmula esquemática de $\mathcal{A}x$ que possua ocorrência de ao menos uma variável esquemática de $\mathcal{L}E$;

v) Um *esquema de regras* de $SpcE$ será um elemento de $\mathcal{R}$ que possua ocorrência de ao menos uma variável esquemática de $\mathcal{L}E$.

EXEMPLO 1 Denotamos por Spc_{osIM} a especificação esquemática definida do seguinte modo:

i) **Linguagem esquemática:** $\mathcal{L}_{os}E$, obtida pela extensão de $\mathcal{L}_{os}$ pela variável esquemática X, de peso 1;

ii) **Axiomas:** $\mathcal{A}x_{osIM} = \{S_1, S_2, EIM\}$,

onde:

S_1. $\forall x\ sx \neq o$;

S_2. $\forall x \forall y\ (sx = sy \rightarrow x = y)$;

EIM. $X(o) \wedge \forall x\ (X(x) \rightarrow X(sx)) \rightarrow \forall x\ X(x)$;

iii) **Regras:** Nenhuma.

Por definição, Spc_{osIM} é a especificação de uma teoria sobre $\mathcal{L}_{os}E$.

EXEMPLO 2 Denotamos por Spc_{osRIM} a especificação esquemática definida do seguinte modo:

i) **Linguagem esquemática:** $\mathcal{L}_{os}E$;

ii) **Axiomas:** $\mathcal{A}x_{osRIM} = \{S_1, S_2\}$;

iii) **Regras:** RIM, definida do seguinte modo:

$$\frac{X(o), \forall x\ (X(x) \to X(sx))}{\forall x\ X(x)}.$$

Por definição, Spc_{osRIM} é a especificação de uma teoria sobre $\mathcal{L}_{os}E$.

4.6 Comparação de especificações

Como vimos anteriormente, dado um esquema implicativo cujo antecedente seja uma conjunção, poderemos tanto definir uma axioma esquema, quanto uma regra de inferência em $\mathcal{L}$. Assim, dado α deste tipo e $\mathcal{A}x$ um conjunto recursivo de sentenças de $\mathcal{L}$, podemos definir as seguintes especificações:

- $\langle \mathcal{L}, \mathcal{E}_\alpha \cup \mathcal{A}x \rangle$;
- $\langle \mathcal{L}E, \{\alpha\} \cup \mathcal{A}x \rangle$;
- $\langle \mathcal{L}E, \mathcal{A}x, \{R_\alpha\} \rangle$.

Em particular, estamos interessados em comparar as teorias sobre $\mathcal{L}$ que cada uma delas define.

Definição Seja $SpcE$ uma especificação esquemática.
i) $SpcE$ será de *primeiro tipo* se $\mathcal{R} = \emptyset$;
ii) $SpcE$ será de *segundo tipo* se $\mathcal{R} \neq \emptyset$.

Assim, especificações esquemáticas de primeiro tipo podem ser identificadas com o par $\langle \mathcal{L}E, \mathcal{A}x \rangle$.

Como nosso principal objetivo é utilizar especificações esquemáticas para definir especificações usuais sobre extensões de $\mathcal{L}$, temos a seguinte definição:

Definição Seja $SpcE = \langle \mathcal{L}E, \mathcal{A}x \rangle$ uma especificação esquemática de primeiro tipo e $\mathcal{L}' \supseteq \mathcal{L}$. A *aplicação* de $SpcE$ a $\mathcal{L}'$, será a especificação usual $SpcE(\mathcal{L}') = \langle \mathcal{L}_1, \mathcal{A}x_1 \rangle$, definida do seguinte modo:

i) $\mathcal{L}_1 = \mathcal{L}'$;

ii) $Ax_1 = \{\alpha(A_1, \ldots, A_m) : \alpha(X_1, \ldots, X_m) \in \mathcal{A}x$ e $A_1, \ldots, A_m$ são fórmulas de $\mathcal{L}\}$.

Assim, especificações esquemáticas de primeiro tipo podem ser consideradas como funções de linguagens em especificações usuais. A aplicação de uma especificação esquemática sobre $\mathcal{L}E$ a uma linguagem $\mathcal{L}' \supseteq \mathcal{L}$ é a especificação usual obtida tomando-se como axiomas todas as sentenças de $\mathcal{L}$ que forem axiomas de $\mathcal{L}E$ e todas as sentenças de $\mathcal{L}$ que possuam a mesma *forma* dos esquemas de axiomas de $\mathcal{L}E$.

Os resultados seguintes justificam o uso de especificações esquemáticas de primeiro tipo como definições de especificações usuais.

Proposição 4.1 *Se $SpcE = \langle \mathcal{L}E, \mathcal{A}x \rangle$ for uma especificação esquemática de primeiro tipo e $\mathcal{L}' \supseteq \mathcal{L}$, então para cada fórmula esquemática $\alpha(X_1, \ldots, X_m)$ de $\mathcal{L}E$ e $A_1, \ldots, A_m$ de $\mathcal{L}'$, teremos:*

Se $SpcE \vdash \alpha(X_1 \ldots, X_m)$, então $SpcE(\mathcal{L}') \vdash \alpha(A_1, \ldots, A_m)$.

Prova:

Seja $d = \langle \alpha_1(X_1, \ldots, X_m), \ldots, \alpha_n(X_1, \ldots, X_m) \rangle$, uma derivação de α em $SpcE$. Vamos provar por indução em teoremas de $SpcE$ que para cada índice i, $1 \leq i \leq m$, $SpcE(\mathcal{L}') \vdash \alpha_i(A_1, \ldots, A_m)$.

Base: Se $i = 1$, então $\alpha_i(X_1, \ldots, X_m)$ será um axioma de $SpcE$ e daí, pela definição, $\alpha_i(A_1, \ldots, A_m)$ será um axioma de $SpcE(\mathcal{L}')$.

Hipótese: Suponhamos que para cada índice j, $1 \leq j < i$, o resultado seja verdadeiro.

Passo: Teremos dois casos a considerar:

1º caso: Se existirem α_j e α_k, $1 \leq j, k < i$, tais que $\alpha_j, \alpha_k \stackrel{MP}{\Longrightarrow} \alpha_i$, então teremos: α_k é $(\alpha_j \rightarrow \alpha_i)$. Pela hipótese de indução, $SpcE(\mathcal{L}') \vdash \alpha_j(A_1, \ldots, A_m)$ e $SpcE(\mathcal{L}') \vdash \alpha_j(A_1, \ldots, A_m) \rightarrow \alpha_i(A_1, \ldots, A_m)$. Assim, por MP em $SpcE(\mathcal{L}')$, teremos $SpcE(\mathcal{L}') \vdash \alpha_i(A_1, \ldots, A_m)$.

2º caso: Se existir j, $1 \leq j < i$, tal que $\alpha_j \stackrel{SUB}{\Longrightarrow} \alpha_i$, então teremos: Existem $\beta_1, \ldots, \beta_m$, fórmulas esquemáticas de $\mathcal{L}E$, tais que α_i é $\alpha_j(\beta_1, \ldots, \beta_m)$. Pela hipótese de indução e pela composição de substituições, $SpcE(\mathcal{L}') \vdash \alpha_j(\beta_1(A_1, \ldots, A_m)), \ldots, (\beta_m(A_1, \ldots, A_m))$. Assim, teremos finalmente que $SpcE(\mathcal{L}') \vdash \alpha_i(A_1, \ldots, A_m)$. ∎

Proposição 4.2 *Se* $SpcE = \langle \mathcal{L}E, \mathcal{A}x \rangle$ *for uma especificação esquemática de primeiro tipo e* $\mathcal{T} = Cn(SpcE(\mathcal{L}))$*, então* $SpcE$ *será uma extensão conservativa de* $\mathcal{T}$*.*

Prova:

Já sabemos que $\mathcal{T} \subseteq SpcE$. Agora, se A for uma fórmula de $\mathcal{L}$, tal que $SpcE \vdash A$, então de acordo com a proposição anterior $SpcE(\mathcal{L}) \vdash A$. ∎

Proposição 4.3 *Se* $SpcE = \langle \mathcal{L}E, \mathcal{A}x \rangle$ *for uma especificação esquemática de primeiro tipo e* $\mathcal{L}' \supseteq \mathcal{L}$*, então* $SpcE(\mathcal{L}')$ *será uma extensão conservativa de* $SpcE(\mathcal{L})$*.*

Prova:

Se existisse uma fórmula A de $\mathcal{L}$, tal que $SpcE(\mathcal{L}') \vdash A$ e $SpcE(\mathcal{L}) \nvdash A$, teríamos $SpcE \vdash A$ e $SpcE(\mathcal{L}) \nvdash A$, uma contradição. ∎

Definição Seja $SpcE$ uma especificação esquemática de primeiro tipo, com esquema implicativo α. A *regralização* de $SpcE$ por α, será a especificação esquemática de segundo tipo $SpcE_R(\alpha) = \langle \mathcal{L}E, \mathcal{A}x \setminus \{\alpha\}, \{\mathcal{R}_\alpha\} \rangle$.

Definição Seja $SpcE$ uma especificação esquemática de segundo tipo, com regra inválida R_α. A *esquematização* de $SpcE$ por R_α será a especificação esquemática de primeiro tipo $SpcE_{\mathcal{E}}(R_\alpha) = \langle \mathcal{L}E, \mathcal{A}x \cup \{\alpha\} \rangle$.

Proposição 4.4 *Se* $SpcE = \langle \mathcal{L}, \mathcal{A}x \rangle$ *for uma especificação esquemática de primeiro tipo com esquema implicativo* α*, então* $Cn(SpcE_R(\alpha)) \subseteq Cn(SpcE)$*.*

Prova:

Seja $\beta \in Cn(SpcE_R(\alpha))$ e $d = \langle \beta_1, \ldots, \beta_n \rangle$ uma derivação de β em $SpcE_R(\alpha)$. Vamos provar, por indução em teoremas de $SpcE_R(\alpha)$, que para cada índice i, $1 \leq i \leq n$, $SpcE \vdash \beta_i$.

Base: Se $i = 1$, então $\beta_1 \in \mathcal{A}x \setminus \{\alpha\}$ e assim, será uma axiona de $SpcE$.

Hipótese: Suponhamos que para cada índice j, $1 \leq j < i$, o resultado seja verdadeiro.

Passo: Teremos dois casos a considerar:

1º caso: Se β_i for obtido de anteriores na seqüência por uma aplicação de MP ou SUB, nada há a demonstrar, pois estas regras também atuam em $SpcE$.

2º caso: Se existirem $\beta_{i1}, \ldots, \beta_{in}$ anteriores a β_i na seqüência, tais que $\beta_{i1}, \ldots, \beta_{in} \stackrel{R_\alpha}{\Longrightarrow} \beta_1$, então pela hipótese de indução, teremos que $SpcE \vdash \beta_{i1}, \ldots, SpcE \vdash \beta_{in}$. Daí, $SpcE \vdash \beta_{i1} \wedge \ldots \wedge \beta_{in}$ e como, $\beta_{i1} \wedge \ldots \wedge \beta_{in} \rightarrow \beta$ é um exemplar de α, por MP em $SpcE$, teremos $SpcE \vdash \beta_i$. ∎

Capítulo 5

Aritmética Elementar com Zero e Sucessão

5.1 Introdução

Neste capítulo, estudamos algumas metapropriedades da teoria da estrutura $\langle I\!N, 0, S\rangle$, denotada $Th(I\!N, 0, S)$. Em particular, caracterizamos todos os seus modelos, provamos que é axiomatizável e que não é finitamente axiomatizável. Nosso objetivo é utilizar estes resultados para estudar o papel de alguns esquemas de axiomas de indução na especificação de $Th(I\!N, 0, S)$.

Excetuando-se as relações de independência entre os axiomas que especificam $Th(I\!N, 0, S)$, um esboço de todos os resultados deste capítulo encontram-se em [2].

5.2 As teorias $Th(I\!N, 0, S)$ e $Cn(\mathcal{A}x_{os})$

A *aritmética elementar com zero e sucessão* é a parte da aritmética dos números naturais que pode ser formalizada numa linguagem de primeira ordem adequada, cujo vocabulário consiste de o, e s. Para definir esta teoria de maneira precisa, consideramos a estrutura $\mathcal{N} = \langle I\!N, 0, S\rangle$, onde $I\!N$, 0 e S são usuais e estipulamos que a aritmética elementar com zero e sucessão consiste de todas as sentenças de $\mathcal{L}(\mathcal{V}_{os})$ que são verdadeiras em $\mathcal{N}$.

Definição Chamaremos *aritmética elementar com zero e sucessão*, denotada $Th(I\!N, 0, S)$, a teoria definida do seguinte modo:

i) **Vocabulário:** $\mathcal{V}_{os}$;

ii) **Sentenças:** todas as sentenças da linguagem $\mathcal{L}(\mathcal{V}_{os})$ que são verdadeiras na estrutura $\mathcal{N} = \langle I\!N, 0, S \rangle$.

$Th(I\!N, 0, S)$ é consistente e completa, pois é o conjunto de todas as sentenças de $\mathcal{L}(\mathcal{V}_{os})$ que são verdadeiras em uma única estrutura. Vamos agora mostrar que é axiomatizável. Para isto, definiremos axiomaticamente uma subteoria de $Th(I\!N, 0, S)$ e mostraremos que, na verdade, ambas as teorias são iguais. Adotaremos ainda, a seguinte abreviação:

Definição Se m for um número natural, s^m será $s \dots s$ a seqüência constituída de m ocorrências do funtor unário s. Admitiremos também o caso limite em que $m = 0$.

Assim, temos a seguinte definição:

Definição Chamaremos Spc_{os} a seguinte especificação usual:
i) **Vocabulário:** $\mathcal{V}_{os}$;
ii) **Axiomas:** $\mathcal{A}x_{os} = \{S_1, S_2, S_3\} \cup ES_4$, onde:
S_1. $\forall x \; sx \neq o$;
S_2. $\forall x \forall y \; (sx = sy \rightarrow x = y)$;
S_3. $\forall x \; (x \neq o \rightarrow \exists y \; sy = x)$;
ES_4. Todas as sentenças da forma $\forall x \; s^n x \neq x$, onde n é um número natural não nulo.

Denotamos por $\mathcal{A}x_{os}$ ao conjunto consistindo de todos os axiomas especificados acima. Deste modo, a teoria definida por Spc_{os} será também denotada $Cn(\mathcal{A}x_{os})$.

O resultado seguinte é imediato das definições:

Proposição 5.1 $Cn(\mathcal{A}x_{os}) \subseteq Th(I\!N, 0, S)$.

Prova:

Todos os elementos de $\mathcal{A}x_{os}$ são verdadeiros em $\langle I\!N, 0, S \rangle$. ∎

5.3 Modelos de $Cn(\mathcal{A}x_{os})$

Para provar que a recíproca da inclusão acima também é verdadeira, ou seja, que $\mathcal{A}x_{os}$ é um conjunto de axiomas para $Th(I\!N, 0, S)$, vamos descrever o comportamento algébrico dos modelos de $Cn(\mathcal{A}x_{os})$.

Definição Seja $\mathcal{N} = \langle N, 0_N, S_N\rangle$ uma estrutura adequada para $\mathcal{L}(\mathcal{V}_{os})$ e a, $b \in N$.

i) b será o *sucessor* de a em $\mathcal{N}$ se $S_N(a) = b$;

ii) a será o *antecessor* de b em $\mathcal{N}$ se b for o sucessor de a em $\mathcal{N}$.

Assim, se $\mathcal{N} = \langle N, 0_N, S_N\rangle$ for um modelo de $\mathcal{A}x_{os}$, podemos interpretar os elementos de $\mathcal{A}x_{os}$ em $\mathcal{N}$, do seguinte modo:

S_1. Afirma que 0_N não está na imagem de S_N, isto é, que 0_N não possui antecessor em $\mathcal{N}$.

S_2. Afirma que S_N é uma função injetiva em N, isto é, elementos distintos de N possuem sucessores distintos em $\mathcal{N}$.

S_3. Afirma que S_N é uma função sobrejetiva de N em $N \setminus \{0_N\}$, isto é, que todo elementos não nulo de N possui um antecessor em $\mathcal{N}$.

Decorre de S_2 e S_3 que o antecessor de todo elemento $a \in N$, distinto de 0_N, existe e é único.

Proposição 5.2 $S_2, S_3 \vdash \forall x\ (x \neq o \to \exists! y\ sy = x)$.

Prova:
Existência: (axioma S_3).
Unicidade: (axioma S_2). ∎

Para interpretarmos o esquema de axiomas ES_4, necessitamos da seguinte definição:

Definição Seja $\mathcal{N} = \langle N, 0_N, S_N\rangle$ uma estrutura adequada para $\mathcal{L}(\mathcal{V}_{os})$, m um número natural não nulo.

i) Um *m-ciclo* de $\mathcal{N}$ será uma seqüência $\langle a_1, a_2, \ldots, a_m\rangle$ de elementos distintos de N, tal que $S(a_m) = a_1$ e para todo i, $1 \leq i \leq m-1$, $S(a_i) = a_{i+1}$;

ii) Um *ciclo* de $\mathcal{N}$ será uma seqüência de elementos de N que seja um

m-ciclo, para algum número natural m.

Assim, se $\mathcal{N} = \langle N, 0_N, S_N \rangle$ for um modelo de $\mathcal{A}x_{os}$, teremos:

ES_4. Afirma que nenhuma restrição de S a um subconjunto de N será um ciclo.

É um fato bem conhecido [10] que existe uma estreita relação entre teorias que possuem axiomas como S_1, S_2 e S_3 e a estrutura que pode, naturalmente, ser associada ao conjunto de termos de sua linguagem. Vejamos esta relação mais detalhadamente no caso de $Cn(\mathcal{A}x_{os})$, para introduzir alguns conceitos básicos.

Números naturais padrão

Os termos de $\mathcal{L}(\mathcal{V}_{os})$ são de quatro tipos:

i) a constante individual o;

ii) as variáveis individuais da linguagem;

iii) $s^m o$ ou $s^m x$, onde x é uma variável individual.

Os termos da forma $s^m o$, serão chamados *numerais*. O m-ésimo numeral pode ser definido recursivamente do seguinte modo:

Definição Seja t um termo de $\mathcal{L}(\mathcal{V}_{os})$.

i) t será o 0-ésimo numeral se t for o;

ii) Se t for o m-ésimo numeral, então st será o $(m+1)$-ésimo numeral.

iii) t será um *numeral* se existir um número natural m, tal que t seja o m-ésimo numeral.

Obviamente, para cada natural m, o m-ésimo numeral é único e é denotado $s^m o$. Todo numeral é livre de variáveis, assim, se $\mathcal{N} = \langle N, 0_N, S_N \rangle$ for um modelo de $Cn(\mathcal{A}x_{os})$ e m um número natural, o numeral $s^m o$ denotará um elemento $S_N^m(0_N)$ específico de N. O resultado seguinte nos diz que isto se dá de maneira única.

Proposição 5.3 *Se m e n forem números naturais, então as seguintes condições serão equivalentes:*

a) $m = n$*;*

b) $S_1, S_2 \vdash s^m o = s^n o$*.*

Prova:

($\Rightarrow$) Imediata.

($\Leftarrow$) (axiomas S_1 e S_2). ■

A proposição 5.3 motiva a seguinte definição:

Definição A *álgebra dos numerais, com zero e sucessão* será a estrutura $\mathcal{N}_{os} = \langle N, 0_N, S_N \rangle$, definida do seguinte modo:

i) $N = \{o, so, s^2o, s^3o, \ldots\}$;

ii) $0_N = o$;

iii) $S_N : N \to N$

$$t \to st$$

O resultado seguinte é imediato.

Proposição 5.4

i) *$\mathcal{N}_{os}$ é um modelo de $Cn(\mathcal{A}x_{os})$.*

ii) $\mathcal{N}_{os} \cong \langle I\!N, 0, S \rangle$.

Assim, se $\mathcal{N} = \langle N, 0_N, S_N \rangle$ for um modelo de $Cn(\mathcal{A}x_{os})$, os numerais de $\mathcal{L}(\mathcal{V}_{os})$ definirão em $\mathcal{N}$ um subconjunto N' de elementos de N, que será o domínio de uma subestrutura de $\mathcal{N}$, isomorfa à estrutura padrão dos números naturais com zero e sucessão. Os elementos de N' serão exatamente os elementos de N que são denotados por algum (e exatamente um) numeral de $\mathcal{L}(\mathcal{V}_{os})$, Ou seja, 0_N, $S_N(0_N)$, $S_N^2(0_N)$, etc, ou ainda, aqueles que podem ser alcançados a partir de 0_N por um número finito de aplicações da operação S_N.

Definição Seja $\mathcal{N} = \langle N, 0_N, S_N \rangle$ um modelo de $Cn(\mathcal{A}_{os})$ e $a \in N$.

i) a será um *número natural padrão* de $\mathcal{N}$ se existir um número natural m, tal que $S_N^m(0_N)$ seja a.

ii) A *parte padrão* de $\mathcal{N}$ será a estrutura $\mathcal{N}padrão = \langle N', 0'_N, S'_N \rangle$, definida do seguinte modo:

1) $N' = \{a \in N : a$ é um número natural padrão$\}$;

2) $0'_N = 0_N$;

3) $S' = N' \to N'$

$$a \to S_N(a).$$

Os seguintes resultados são imediatos.

Proposição 5.5 *Se* $\mathcal{N} = \langle N, 0_N, S_N\rangle$ *for um modelo de* $Cn(\mathcal{A}x_{os})$*, então* $\mathcal{N}padrão \cong \mathcal{N}_{os}$.

Proposição 5.6 $\mathcal{N}_{os}$ *é um modelo minimal de* $Cn(\mathcal{A}x_{os})$.

Proposição 5.7 *Todo modelo de* $Cn(\mathcal{A}x_{os})$ *é infinito.*

Números naturais infinitos

Os resultados acima são um primeiro passo na descrição do comportamento algébrico dos modelos de $Cn(\mathcal{A}x_{os})$. Em conjunto, nos dizem que todo modelo de $Cn(\mathcal{A}x_{os})$ possui uma parte padrão, isomorfa a estrutura $\langle \mathbb{N}, 0, S\rangle$, dos números naturais com zero e sucessão. Em alguns casos esta será a única parte que estes modelos possuem. Mas, de acordo com os teoremas limitadores do formalismo, sabemos que a maior parte dos modelos de $Cn(\mathcal{A}x_{os})$ possuirá também outros "números naturais", além dos números naturais padrão. Nosso objetivo, daqui por diante, será descrever o comportamento destes outros "números naturais", de modo a determinar como são os modelos de $Cn(\mathcal{A}x_{os})$.

Definição Seja $\mathcal{N} = \langle N, 0_N, S_N\rangle$ um modelo de $Cn(\mathcal{A}x_{os})$ e $a \in N$. a será um *número natural infinito* de $\mathcal{N}$ se não for um número natural padrão de $\mathcal{N}$.

Assim, dado um modelo $\mathcal{N}$ de $Cn(\mathcal{A}x_{os})$, os números naturais infinitos de $\mathcal{N}$, se existirem, serão os elementos do domínio de $\mathcal{N}$ que não podem ser alcançados a partir de 0_N por um número finito de aplicações da operação S_N. Em particular, nenhum deles é 0_N (axioma S_1). Agora, como S_N é total, sabemos que, mesmo para um número natural infinito a de $\mathcal{N}$, existirão o sucessor de a, o sucessor do sucessor de a, etc. Todos estes elementos serão distintos de 0_N (axioma S_1) e distintos de qualquer número natural padrão (axioma S_2). Por outro lado, como todo elemento distinto de 0_N possui um *antecessor* (axioma S_3) e como este será também distinto de zero pois, caso contrário, a não seria um número natural infinito, existirão o predecessor de a, o predecessor do predecessor de a, etc. Agora, dado a, todos os elementos acima serão distintos, (esquema de axiomas ES_4) e, assim, estarão arranjados numa cadeia discreta, sem primeiro e último elementos. Obviamente, qualquer número destas cadeias é possível. Todas as cadeias serão disjuntas (axioma S_2) e todas as cadeias serão distintas da parte padrão (axioma S_2).

Se o leitor já estiver convencido de que os modelos de $Cn(\mathcal{A}x_{os})$ terão todos a forma descrita acima poderá, sem nenhum prejuízo, saltar imediatamente para o teorema 5.1, pois o que faremos daqui até aquele ponto será apenas enunciar e provar de maneira formal o que já foi dito acima.

As relações $\hookrightarrow$ e $\sim$

Considerando que os elementos de $\mathcal{N}$ se dividem em números naturais padrão e números naturais infinitos e que, para todos estes, existirão elementos que podem alcançá-los por um número finito de aplicações da operação S_N, é natural considerarmos a seguinte definição:

Definição Seja $\mathcal{N} = \langle N, 0_N, S_N \rangle$ um modelo de $Cn(\mathcal{A}x_{os})$ e a e b elementos de N. Diremos que a *alcança* b, e denotaremos $a \hookrightarrow b$, se existir um número natural n, tal que $S_N^n(a) = b$, isto é, se a função S aplicada um número finito de vezes a a fornecer b.

Proposição 5.8 *Se $\mathcal{N} = \langle N, 0_N, S_N \rangle$ for um modelo de $Cn(\mathcal{A}_{os})$ e a, b e c forem elementos de N, então teremos as seguintes propriedades:*

a) $a \hookrightarrow a$;

b) Se $a \hookrightarrow b$ e $b \hookrightarrow c$, então $a \hookrightarrow c$.

Prova:

a) Basta tomar $n = 0$;

b) Segue imediatamente do seguinte resultado, que se prova por indução (na metalinguagem) em n:

Se m e n forem números naturais, então $S_1, S_2 \vdash \forall x \forall y \forall z\ s^m(x) = y \wedge s^n(y) = z \rightarrow s^{m+n}(x) = z$. ■

A proposição acima nos diz que a relação $\hookrightarrow$, definida em N é uma relação de pré-ordem.

Definição Seja $\mathcal{N} = \langle N, 0_N, S_N \rangle$ um modelo de $Cn(\mathcal{A}x_{os})$ e a e b elementos de N. Diremos que a e b são *equivalentes*, denotado $a \sim b$, se $a \hookrightarrow b$ ou $b \hookrightarrow a$, isto é, dois elementos serão equivalentes se a partir de algum deles pudermos alcançar o outro.

Proposição 5.9 *Se $\mathcal{N} = \langle N, 0_N, S_N \rangle$ for um modelo de $Cn(\mathcal{A}x_{os})$ e a, b e c forem elementos de N, então teremos as seguintes propriedades:*

a) $a \sim a$;

b) Se $a \sim b$, então $b \sim a$;

c) Se $a \sim b$ e $b \sim c$, então $a \sim c$.

A proposição acima nos diz que a relação $\sim$, definida em N, é uma relação de equivalência. Assim, $\sim$ define uma partição $N/\sim = \{\tilde{a} : a \in N\}$ de N, em classes de equivalência. Descrevendo o comportamento algébrico de cada uma destas classes, teremos descrito o comportamento algébrico dos modelos de $Cn(\mathcal{A}x_{os})$.

$\mathbb{N}$-cópias e $\mathbb{Z}$-cadeias

Proposição 5.10 *Se $\mathcal{N} = \langle N, 0_N, S_N \rangle$ for um modelo de $Cn(\mathcal{A}x_{os})$, $N/\sim$ o conjunto quociente de N por $\sim$ e $\tilde{a}$ um elemento de $N/\sim$, então as seguintes condições serão equivalentes:*

a) $0_N \in \tilde{a}$;

b) Para todo $b \in \tilde{a}$, existe um número natural n, tal que $S_N^n(0_N) = b$.

Prova:

($\Rightarrow$) Temos dois casos:

1º caso: Se $b = 0_N$, basta tomar $n = 0$.

2º caso: Se $b \neq 0_N$ e não existisse um número natural n tal que $S_N^n(0_N) = b$, como $b \in \tilde{a}$ e $0_N \in \tilde{a}$, teríamos $b \in \tilde{0}_N$. Daí, existiria um número natural m,

tal que $S_N^m(b) = 0_N$. Agora, como $b \neq 0_N$, teríamos $m \neq 0$ e daí $m = k + 1$, o que acarretaria $S_N(S_N^k(b)) = 0_N$, uma contradição (axioma S_1).
($\Leftarrow$) Basta tomar $b = a$. ∎

O resultado acima nos diz que $\tilde{0}_N$, a classe de 0_N, é exatamente o conjunto dos números naturais padrão de $\mathcal{N}$.

Proposição 5.11 *Se $\mathcal{N} = \langle N, 0_N, S_N \rangle$ for um modelo de $Cn(\mathcal{A}x_{os})$, $N/\sim$ o conjunto quociente de N por $\sim$ e $\tilde{a}$ um elemento de $N/\sim$, então as seguintes condições serão equivalentes:*

a) $0_N \notin \tilde{a}$;

b) A relação $P_N \subseteq \tilde{a} \times \tilde{a}$, definida pela propriedade

(*) *Para todos b e c em $\tilde{a}$, $\langle b, c \rangle \in P_N$ se e somente se $S_N(c) = b$,*

é uma função.

Prova:
($\Rightarrow$) Suponhamos que $0_N \notin \tilde{a}$. Seja $P_N \subseteq \tilde{a} \times \tilde{a}$ definida pela propriedade (*) e $b \in \tilde{a}$. Temos que mostrar a existência e a unicidade de $P_N(b)$.
Existência: Como $b \neq 0_N$, existirá $c \in N$, tal que $S_N(c) = b$ (axioma S_3). Obviamente, $c \in \tilde{a}$. Daí, $P_N(b) = c$.
Unicidade: Suponhamos que existam c_1 e $c_2 \in \tilde{a}$, tais que $P_N(b) = c_1$ e $P_N(b) = c_2$. Daí, $S_N(c_1) = b$, $S_N(c_2) = b$ e $S_N(c_1) = S_N(c_2)$. Como S_N é injetiva (axioma S_2), $c_1 = c_2$.
($\Leftarrow$) Suponhamos que $P_N \subseteq \tilde{a} \times \tilde{a}$, definida pela propriedade (*) seja uma função. Se $0_N \in \tilde{a}$, teríamos a existência de $b \in \tilde{a}$, tal que $P_N(0_N) = b$. Isto acarretaria que $S_N(b) = 0_N$, uma contradição (axioma S_1). ∎

Proposição 5.12 *Se $\mathcal{N} = \langle N, 0_N, S_N \rangle$ for um modelo de $Cn(\mathcal{A}x_{os})$, $N/\sim$ o conjunto quociente de N por $\sim$ e $\tilde{a}$ um elemento de $N/\sim$, então teremos as seguintes propriedades:*

a) $0_N \in \tilde{a}$ se e somente se $(\tilde{a}, 0_N, S_N) \cong (\mathbb{N}, 0, S)$;

b) $0_N \notin \tilde{a}$ se e somente se $(\tilde{a}, S_N, P_N) \cong (\mathbb{Z}, S, S^{-1})$.

Prova:

$a)(\Rightarrow)$ Pelo Teorema da Recursão, existe um homomorfismo $\Phi : I\!N \to \tilde{a}$, definido do seguinte modo, para todo número natural x:

$$\Phi(x) = \begin{cases} 0_N & \text{se } x = 0 \\ S_N(\Phi(y)) & \text{se } S(y) = x \end{cases}$$

Vamos mostrar, por indução (na metalinguagem) que para todo número natural x, $\Phi(x) = S_N^x(0_N)$.

Base: Se $x = 0$, $\Phi(x) = 0_N = S_N^0(0_N)$.

Hipótese: Suponhamos que $\Phi(x) = S_N^x(0_N)$.

Passo: Daí, $\Phi(S(x)) = S_N(\Phi(x)) = S_N(S_N^x(0_N)) = S_N^{x+1}(0_N)$.

Podemos agora, mostrar que Φ é uma bijeção.

Injetividade: Suponhamos que $x \in Nuc(\Phi)$, ou seja $\Phi(x) = 0_N$. Se $x \neq 0$, exisitiria um número natural y, tal que $S(y) = x$. Daí, $\Phi(x) = S_N(\Phi(y))$ e isto acarretaria que $S_N(\Phi(y)) = 0_N$, uma contradição. Logo, $x = 0$.

Sobrejetividade: Seja $b \in \tilde{a}$. Se $b = 0_N$, tomando $x = 0$, teremos $\Phi(x) = y$. Se $b \neq 0_N$, existe um número natural não nulo n, tal que $S_N^n(0) = b$. Assim, tomando $x = n$, teremos: $\Phi(x) = \Phi(n) = S_N^n(0) = b$.

$(\Leftarrow)$ Imediata.

$b)(\Rightarrow)$ Se $b \in \tilde{a}$, existem números naturais m e n, tais que $S_N^m(b) = a$ ou $S_N^n(a) = b$. Agora, podemos aprimorar nossos conhecimentos em relação a este fato. Em primeiro lugar, as duas possibilidades acima são exclusivas. De fato, se existissem m e n tais que $S_N^m(b) = a$ e $S_N^n(a) = b$, teríamos $S_N^m(S_N^n(a)) = a$ e daí, $S_N^{m+n}(a) = a$, uma contradição (esquemas de axiomas ES_4). Por último, das duas possibllidades acima, a que acontece se dá de maneira única. De fato, se existissem números naturais m_1 e m_2, tais que $S_N^{m_1}(b) = a$ e $S_N^{m_2}(b) = a$, a injetividade de S_N acarretaria que $m_1 = m_2$ (axioma S_2). Analogamente, para o outro caso.

Assim, podemos definir $\Phi : \tilde{a} \to Z\!\!\!Z$ do seguinte modo, para todo $x \in \tilde{a}$:

$$\Phi(x) = \begin{cases} -m & \text{se } S_N^m(x) = a \\ m & \text{se } S_N^m(a) = x \end{cases}$$

Vamos mostrar que Φ é um homomorfismo de $(\tilde{a}, S_N, P_N)$ em $(Z\!\!\!Z, S, S^{-1})$ e que é uma bijeção.

Φ é homomorfismo: Se $x \in \tilde{a}$, teremos dois casos a considerar:

1º caso: Se $x = a$, como $\Phi(x) = 0$, teremos: $\Phi(S_N(x)) = 1 = S(0) = S(\Phi(x))$ e $\Phi(P_N(x)) = -1 = S^{-1}(0) = S^{-1}(\Phi(x))$.

2º caso: Se $x \neq a$, teremos dois subcasos:

Se $S_N^m(x) = a$, $m \neq 0$ e daí, $S_N^{m-1}(S_N(x)) = a$ e $S_N^{m+1}(P_N(x)) = a$. Logo, $\Phi(S_N(x)) = -m + 1 = S(-m) = S(\Phi(x))$ e $\Phi(P_N(x)) = -m - 1 = S^{-1}(-m) = S^{-1}(\Phi(x))$.

Se $S_N^n(a) = x$, analogamente, teremos: $\Phi(S_N(x)) = S(\Phi(x))$ e $\Phi(P_N(x)) = P(\Phi(x))$.

Φ *é injetiva:* Sejam $x, y \in \tilde{a}$, tais que $\Phi(x) = \Phi(y)$. Teremos dois casos a considerar:

1º caso: Se $\Phi(x) \geq 0$, então existem números naturais m e n, $m = n$, tais que $S_N^m(x) = a$ e $S_N^n(y) = a$. Decorre então, da injetividade de S_N, que $x = y$.

2º caso: Se $\Phi(x) \leq 0$, analogamente, teremos $x = y$.

Φ *é sobrejetiva:* Seja $z \in \mathbb{Z}$. Teremos três casos a considerar:

1º caso: Se $z = 0$, tomando $x = a$, teremos $\Phi(x) = z$.

2º caso: Se $z > 0$, tomando $x = S_N^z a$, teremos $\Phi(x) = z$.

3º caso: Se $z < 0$, tomando $x = P^{-z}(a)$, teremos $S^z(a) = x$ e daí, $\Phi(x) = -(-z) = z$.

$(\Leftarrow)$ Imediata. ∎

Definição Seja $\mathcal{N} = \langle N, 0_N, S_N \rangle$ um modelo de $Cn(\mathcal{A}x_{os})$, $N/\sim$ o conjunto quociente de N por $\sim$ e $\tilde{a}$ um elemento de $N/\sim$. Diremos que $\tilde{a}$ é uma *$\mathbb{N}$-cópia* ou *parte padrão* de $\mathcal{N}$ se $0 \in \tilde{a}$. Caso contrário, isto é, se $0 \notin \tilde{a}$, diremos que $\tilde{a}$ é uma *$\mathbb{Z}$-cadeia* ou *parte não padrão* de $\mathcal{N}$.

A proposição 5.12 afirma que um modelo qualquer de $Cn(\mathcal{A}x_{os})$ consiste de uma $\mathbb{N}$-cópia juntamente com um certo número de $\mathbb{Z}$-cadeias. O axioma S_3 nos garante que a $\mathbb{N}$-cópia é única. Verificando que cada um dos axiomas apresentados é verdadeiro em um modelo, independente do número de partes não padrão que ele possua, concluímos que o conjunto de $\mathbb{Z}$-cadeias de um modelo de $Cn(\mathcal{A}x_{os})$ pode ser de qualquer cardinalidade. Temos, assim, caracterizados todos os modelos de $Cn(\mathcal{A}x_{os})$.

Teorema 5.1 *Se* $\mathcal{N} = \langle N, 0_N, S_N \rangle$ *for uma estrutura onde* $0_N \in N$ *e* S_N *é uma operação unária em* N*, então as seguintes condições serão equivalentes:*

a) $\mathcal{N}$ *é um modelo de* $Cn(\mathcal{A}x_{os})$*;*

b) $\mathcal{N}$ *pode ser decomposto em uma* $\mathbb{N}$*-cópia e em um número de* $\mathbb{Z}$*-cadeias.*

Prova:

($\Rightarrow$) Se $\mathcal{N} = \langle N, 0_N, S_N \rangle$ for um modelo de $Cn(\mathcal{A}x_{os})$ a relação $\sim$ em N definirá uma partição de N em elementos $\tilde{0_N}, \tilde{a}_1, \tilde{a}_2, \ldots$, cuja cardinalidade depende da cardinalidade de N. Agora, segundo a proposição 5.12 o primeiro destes elementos é uma $\mathbb{N}$-cópia e os outros são $\mathbb{Z}$-cadeias.
($\Leftarrow$) Se $\mathcal{N}$ puder ser decomposto em uma $\mathbb{N}$-cópia e um número qualquer de $\mathbb{Z}$-cadeias, a simples verificação de que S_1, S_2, S_3 e ES_4 são verdadeiras em $\mathcal{N}$ mostrará que $\mathcal{N}$ é um modelo de $Cn(\mathcal{A}x_{os})$. ∎

O teorema acima fornece, então, uma caracterização algébrica dos modelos de $Cn(\mathcal{A}x_{os})$. Em outras palavras, afirma que dada um modelo $\mathcal{N}$ de $Cn(\mathcal{A}x_{os})$, existirá um conjunto de índices I, tal que $\mathcal{N}/\!\sim\; = \{\mathbb{N}_0\} \cup \bigcup_{i \in I} \mathbb{Z}_i$, onde $\mathbb{N}_0$ é a $\mathbb{N}$-cópia de $\mathcal{N}$ e para cada $i \in I$, $\mathbb{Z}_i$ é uma $\mathbb{Z}$-cadeia de $\mathcal{N}$.

5.4 Algumas metapropriedades de $Cn(\mathcal{A}x_{os})$

Nesta seção mostramos que $Cn(\mathcal{A}x_{os})$ é completa e investigamos a independência dos elementos de $\mathcal{A}x_{os}$.

Completude

A prova da completude de $Cn(\mathcal{A}x_{os})$ baseia-se no seguinte conceito:

Definição Seja $\mathcal{L}$ uma linguagem de primeira ordem, $\mathcal{T}$ uma teoria sobre $\mathcal{L}$ e c um número cardinal. $\mathcal{T}$ será *categórica em potência* c, denotada c-categórica, se todos os modelos de $\mathcal{T}$, de cardinalidade c, forem isomorfos.

A importância do conceito de c-categoricidade decorre do seguinte resultado:

Teorema 5.2 (Teste de Łós-Vaught) *Se uma teoria $\mathcal{T}$ possuir somente modelos infinitos e for categórica em alguma potência c, então $\mathcal{T}$ será completa.*

Já sabemos que $Cn(\mathcal{A}x_{os})$ possui somente modelos infinitos. Vamos agora, investigar se é categórica em alguma potência.

Proposição 5.13 *Se $\mathcal{N}$ e $\mathcal{N}'$ forem modelos de $Cn(\mathcal{A}x_{os})$ que possuem o mesmo número de $\mathbb{Z}$-cadeias, então $\mathcal{N} \cong \mathcal{N}'$.*

Prova:

Sejam $\mathcal{N} = \langle N, 0_N, S_N \rangle$ e $N' = \langle N', 0'_N, S'_N \rangle$, modelos de $Cn(\mathcal{A}x_{os})$ e $\mathcal{N}/\!\sim$, $\mathcal{N}'/\!\sim$, respectivamente, os conjuntos quocientes de $\mathcal{N}$ e $\mathcal{N}'$ por $\sim$ em N e N'. De acordo com o teorema 5.1, existirão conjuntos de índices I e J, tais que $\mathcal{N}/\!\sim = \{\mathbb{N}_0\} \cup \bigcup_{i \in I} \mathbb{Z}_i$ e $\mathcal{N}'/\!\sim = \{\mathbb{N}'_0\} \cup \bigcup_{j \in J} \mathbb{Z}_j$.

Agora, se $\mathcal{N}$ e $\mathcal{N}'$ possuirem a mesma quantidade de $\mathbb{Z}$-cadeias, existirá uma bijeção $f : I \to J$. Por outro lado, existem isomorfismos $F : \mathbb{N}_0 \to \mathbb{N}'_0$ e, para cada $i \in I$, $\Phi_i : \mathbb{Z}_i \to \mathbb{Z}_{f(i)}$.

Definiremos, então, $\Phi : N \to N'$ do seguinte modo, para todo $a \in N$:

$$\Phi(a) = \begin{cases} F(a) & \text{se } a \in \mathbb{N}_0 \\ \Phi_i(a) & \text{se } a \in \mathbb{Z}_i. \end{cases}$$

Vamos mostrar que Φ é um isomorfismo de $\mathcal{N}$ em $\mathcal{N}'$.

Injetividade: Se $a, b \in N$ forem tais que $\Phi(a) = \Phi(b)$, teremos dois casos:

1º caso: Se $a, b \in \mathbb{N}_0$, então $F(a) = F(b)$ e como F é injetiva, $a = b$.

2º caso: Se existir $i \in I$, tal que $a, b \in \mathbb{Z}_i$, então $\Phi_i(a) = \Phi_i(b)$ e como Φ_i é injetiva, $a = b$.

Todos os outros casos são excluídos pela definição de Φ.

Sobrejetividade: Se $b \in N'$, teremos dois casos:

1º caso: Se $b \in \mathbb{N}'_0$, então como F é sobrejetiva, existirá $a \in \mathbb{N}_0$, tal que $F(a) = b$, ou seja, $\Phi(a) = b$.

2º caso: Se exisitir $i \in I$, tal que $b \in \mathbb{Z}_{f(i)}$, então como Φ_i é sobrejetiva, existirá $a \in \mathbb{Z}_i$, tal que $\Phi_i(a) = b$, ou seja $\Phi(a) = b$.

Φ é homomorfismo:

a) $\Phi(0_N) = F(0_N) = 0_{N'}$.

b) Se $a \in N$ e $a \neq 0_N$, teremos dois casos:

1º caso: Se $a \in I\!N_0$, então $\Phi(S_N(a)) = F(S_N(a)) = S_{N'}(F(a))$.

2º caso: Se existir $i \in I$, tal que $a \in \mathbb{Z}_i$, então $\Phi(S_N(a)) = \Phi_i(S_N(a)) = S_{N'}(\Phi_i(a))$. ∎

Proposição 5.14 *$Cn(\mathcal{A}x_{os})$ é categórica em toda potência incontável, ou seja, se $\mathcal{N}$ e $\mathcal{N}'$ forem modelos incontáveis de $Cn(\mathcal{A}x_{os})$ de mesma cardinalidade, então $\mathcal{N} \cong \mathcal{N}'$.*

Prova:

De acordo com o teorema 5.1, se $\mathcal{N}$ e $\mathcal{N}'$ forem modelos de $Cn(\mathcal{A}x_{os})$, então existirão conjuntos de índices I e J, tais que $\mathcal{N}/\!\sim\; = \{I\!N_o\} \cup \bigcup_{i\in I} \mathbb{Z}_i$ e $\mathcal{N}'/\!\sim\; = \{I\!N'_o\} \cup \bigcup_{j\in J} \mathbb{Z}_j$. Assim, denotando a cardinalidade de um conjunto X por $\#X$, teremos $\#N = \aleph_o + \#I \cdot \aleph_o$ e $\#N' = \aleph_o + \#J \cdot \aleph_o$. Agora, como $\#N = \#N'$ e $\#N = \#N' > \aleph_o$, a aritmética cardinal acarretará $\#I = \#J$ e $\mathcal{N}$ e $\mathcal{N}'$ possuirão a mesma quantidade de $\mathbb{Z}$-cadeias. Usando a proposição 5.13, teremos $\mathcal{N} \cong \mathcal{N}'$. ∎

Teorema 5.3 *$Cn(\mathcal{A}x_{os})$ é completa.*

Prova:

$Cn(\mathcal{A}x_{os})$ possui somente modelos infinitos e é categórica na cardinalidade do contínuo. Assim, pelo Teste de Lós-Vaught, é completa. ∎

Independência

Definição Seja $\mathcal{L}$ uma linguagem de primeira ordem e Σ um conjunto de fórmulas de $\mathcal{L}$. Σ será *independente* se para toda fórmula $A \in \Sigma$, $\Sigma \backslash \{A\} \not\models A$.

Isto é, Σ é independente se nenhuma fórmula de Σ é uma conseqüência das demais.

Podemos mostrar que $\mathcal{A}x_{os}$ não é um conjunto independente de axiomas para $Cn(\mathcal{A}x_{os})$ mas como, no próximo capítulo, estaremos interesados na relação de dependência entre os conjuntos $\{S_1\}$, $\{S_2\}$, $\{S_3\}$ e ES_4, provaremos os seguintes resultados:

Proposição 5.15 $\{S_2\} \cup \{S_3\} \cup ES_4 \not\models S_1$.

Prova:

Basta considerar a estrutura $\mathcal{N} = \langle N, 0_N, S_N \rangle$, definida do seguinte modo:

i) $N = \mathbb{Z}$;

ii) $0_N = 0$;

iii) S_N é a função definida do seguinte modo, para todo $m \in \mathbb{Z}$: $S_N(m) = m + 1$.

Teremos, então:

1) $\not\models_{\mathcal{N}} S_1$, pois $S_N(-1) = 0$;

2) $\models_{\mathcal{N}} S_2$, pois S_N é injetiva;

3) $\models_{\mathcal{N}} S_3$, pois dado $m \in \mathbb{Z}^*$, $S_N(m-1) = m$;

4) $\models_{\mathcal{N}} ES_4$, pois nenhuma restrição de S_N a um subconjunto de $\mathbb{Z}$ é um ciclo. ∎

Proposição 5.16 $\{S_1\} \cup \{S_3\} \cup ES_4 \not\models S_2$.

Prova:

Basta considerar a estrutura $\mathcal{N} = \langle N, 0_N, S_N \rangle$, definida do seguinte modo:

i) $N = \mathbb{N}$;

ii) $0_N = 0$;

iii) S_N é a função definida do seguinte modo, para todo $m \in \mathbb{Z}$:.

$$S_N(m) = \begin{cases} 1 & \text{se } m = 0, 2 \text{ ou } 3 \\ m - 2 & \text{se } m \neq 0, 2 \text{ ou } 3. \end{cases}$$

Teremos, então:

1) $\models_{\mathcal{N}} S_1$, pois para todo $m \in \mathbb{N}$, $S_N(m) \neq 0$;

2) $\not\models_{\mathcal{N}} S_2$, pois $S_{\mathcal{N}}$ não é injetiva;

3) $\models_{\mathcal{N}} S_3$, pois se $m \neq 0$, teremos: $S_N(0) = m$, se $m = 1$ ou $S_N(m+2) = m$, se $m \neq 1$.

4) $\models_{\mathcal{N}} ES_4$, pois nenhuma restrição de S_N a um subconjunto de $\mathcal{N}$ é um ciclo. ∎

Proposição 5.17 $\{S_1\} \cup \{S_2\} \cup ES_4 \not\models S_3$.

Prova:

Basta considerar a estrutura $\mathcal{N} = \langle N, 0_N, S_N \rangle$, definida do seguinte modo:

i) $N = I\!N$;

ii) $0_N = 0$;

iii) S_N é a função definida do seguinte modo, para todo $m \in N$: $S_N(m) = m + 2$.

Teremos, então:

1) $\models_{\mathcal{N}} S_1$, pois para todo $m \in I\!N$, $S_N(m) = m + 2 \neq 0$;

2) $\models_{\mathcal{N}} S_2$, pois $S_{\mathcal{N}}$ é injetiva;

3) $\not\models_{\mathcal{N}} S_3$, pois para todo $m \in N$, $S_N(m) = m + 2 \neq 1$;

4) $\models_{\mathcal{N}} ES_4$, pois nenhuma restrição de S_N a um subconjunto de $I\!N$é um ciclo. ∎

Proposição 5.18 $\{S_1\} \cup \{S_2\} \cup \{S_3\} \not\models ES_4$.

Prova:

Basta considerar a estrutura $\mathcal{N} = \langle N, 0_N, S_N \rangle$, definida do seguinte modo:

i) $N = Z\!\!\!Z \cup \{\sqrt{2}\}$;

ii) $0_N = 0$;

iii) S_N é a função definida do seguinte modo, para todo $m \in Z\!\!\!Z \cup \{\sqrt{2}\}$:

$$S_N(m) = \begin{cases} \sqrt{2} & \text{se } m = \sqrt{2} \\ m + 1 & \text{se } n \neq \sqrt{2}, \end{cases}$$

Teremos, então:

1) $\models_{\mathcal{N}} S_1$, pois $\sqrt{2} \neq 0$ e para todo $m \in \mathcal{N}$, $m + 1 \neq 0$;

2) $\models_{\mathcal{N}} S_2$, pois $S_{\mathcal{N}}$ é injetiva;

3) $\models_{\mathcal{N}} S_3$, pois dado $m \in N^* \cup \{\sqrt{2}\}$, se $m = \sqrt{2}$, então $S_N(m-1) = m$;

4) $\not\models_{\mathcal{N}} ES_4$, pois a restrição de S_N a $\{\sqrt{2}\}$ é um ciclo. ∎

5.5 Algumas metapropriedades de $Th(I\!N, 0, S)$

Podemos agora provar algumas propriedades metamatemáticas importantes de $Th(I\!N, 0, S)$, a partir da completude de $Cn(\mathcal{A}x_{os})$.

Axiomatizabilidade

Neste parágrafo, mostramos que Spc_{os} é uma especificação usual para $Th(I\!N, 0, S)$, ou seja, que $\mathcal{A}x_{os}$ é um conjunto de axiomas para a aritmética dos números naturais com zero e sucessão.

Teorema 5.4 *$\mathcal{A}x_{os}$ é um conjunto de axiomas para $Th(I\!N, 0, S)$, ou seja, $Th(I\!N, 0, S)$ é axiomatizável.*

Prova:

Sabemos que $Cn(\mathcal{A}x_{os}) \subseteq Th(I\!N, 0, S)$ e que as duas teorias são completas. Daí, $Cn(\mathcal{A}x_{os}) = Th(I\!N, 0, S)$. ∎

Podemos, agora, mostrar que $Th(I\!N, 0, S)$ não é finitamente axiomatizável. De fato, isto é equivalente a provar que $Cn(\mathcal{A}x_{os})$ não é finitamente axiomatizável, o que pode ser feito mostrando-se que nenhum subconjunto finito de $\mathcal{A}x_{os}$ é suficiente para isto.

Proposição 5.19 *$Th(I\!N, 0, S)$ não é finitamente axiomatizàvel.*

Prova:

Seja, $\Sigma \subseteq \mathcal{A}x_{os}$, tal que Σ seja finito. Seja n o maior número natural tal que $\forall x\ S^n x \neq x$ ocorra em Σ. Daí, tomando a estrutura $\mathcal{N} = (N, 0_N, S_N)$ definida por

i) $N = I\!N \cup \{a_1, a_2, \ldots, a_n, a_{n+1}\}$;

ii) $0_N = 0$;

iii) $S_N : N \longrightarrow N$, tal que para todo $x \in N$,

$$S_N(x) = \begin{cases} S(x) & \text{se } x \in I\!N \\ a_{i+1} & \text{se } x = a_i, 1 \leq i \leq n \\ a_1 & \text{se } x = a_{i+1}, \end{cases}$$

teremos que $\mathcal{N}$ é um modelo de Σ mas não é um modelo de $Cn(\mathcal{A}x_{os})$, pois possui um ciclo. ∎

Decidibilidade

Neste parágrafo mostramos a existência de um algoritmo que decide a pertinência de uma sentença de $\mathcal{L}(\mathcal{V}_{os})$ a $Th(I\!N, 0, S)$.

Definição Uma teoria $\mathcal{T}$ será *decidível* se existir um algoritmo tal que, dada uma sentença A de $\mathcal{L}(\mathcal{T})$, o algoritmo responde se A pertence, ou não, a $\mathcal{T}$.

A prova que $Th(I\!N, 0, S)$ é decidível baseia-se no seguinte resultado:

Teorema 5.5 (de Janicak) *Se $\mathcal{T}$ for uma teoria consistente e completa, então as seguintes condições serão equivalentes:*

a) $\mathcal{T}$ é axiomatizável;

b) $\mathcal{T}$ é decidível.

Assim, como um corolário imediato da completude e da axiomatizabilidade de $Th(I\!N, 0, S)$, temos o seguinte resultado:

Teorema 5.6 *$Th(I\!N, 0, S)$ é decidível.*

Prova:

$Th(I\!N, 0, S)$ é consistente, é completa e é axiomatizável. ∎

Capítulo 6

Esquemas de Axiomas de Indução em $Th(\mathbb{N}, 0, S)$

Neste capítulo, estudamos o papel de alguns esquemas de axiomas de indução na especificação da aritmética elementar, cujos conceitos primitivos são *zero* e *sucessão*.

6.1 O esquema de axiomas $EIM(\mathcal{V}_{os})$

Seja $\mathcal{L}(\mathcal{V}_{os})E$, a linguagem esquemática definida sobre $\mathcal{L}(V_{os})$, pela adição de uma variável esquemática X, de peso 1. Chamaremos *esquema de indução matemática* a seguinte fórmula de $\mathcal{L}(\mathcal{V}_{os})E$:

$$EIM.\ X(o) \wedge \forall x\ (X(x) \rightarrow X(sx)) \rightarrow \forall x\ X(x).$$

Nesta seção, estudamos o papel desempenhado pelo esquema de axiomas definido pela aplicação de EIM a $\mathcal{L}(\mathcal{V}_{os})$, na especificação de $Th(\mathbb{N}, 0, S)$.

Dado um esquema de axiomas em uma linguagem esquemática qualquer, para respondermos satisfatóriamente que papel este esquema desempenha na especificação de uma teoria, devemos levar em conta, pelo menos, a consideração das seguintes questões:

- Qual o papel desempenhado pela aplicação do esquema de axiomas na especificação da teoria considerada;

- Qual o papel desempenhado pela aplicação do esquema de axiomas em especificações de extensões da teoria considerada;

- Que outros esquemas de axiomas de indução poderiam ser considerados nesta mesma linguagem;
- Qual a relação existente entre os novos esquemas e o esquema original;
- Qual o papel desempenhado pela aplicação destes novos esquemas em especificação de extensões da teoria original.

Agora que temos uma axiomática para $Th(I\!N, 0, S)$, podemos dar uma resposta para a primeira destas questões, verificando quais axiomas de $\mathcal{A}x_{os}$ podem ser suprimidos, na presença de $EIM(\mathcal{V}_{os})$. Em outras palavras, comparando Spc_{os} com a aplicação do esquema EIM a $\mathcal{L}(\mathcal{V}_{os})$.

Temos, então, o seguinte resultado:

Proposição 6.1

a) $EIM(\mathcal{V}_{os}) \not\models S_1$;

b) $EIM(\mathcal{V}_{os}) \not\models S_2$;

c) $EIM(\mathcal{V}_{os}) \vdash S_3$;

d) *Se m for um número natural não nulo, então* $S_1, S_2, EIM(\mathcal{V}_{os}) \models \forall x\ s^m x \neq x$, *ou seja,* $S_1, S_2, EIM(\mathcal{V}_{os}) \vdash ES_4$.

Prova:

a) Basta tomar a estrutura $\mathcal{N} = \langle N, 0_N, S_N \rangle$, definida do seguinte modo:

i) $N = \{0\}$;

ii) $0_N = 0$;

iii) $S_N : N \to N$ é tal que $S_N(0_N) = 0_N$.

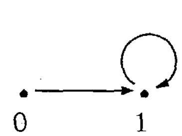
Obviamente, $\models_{\mathcal{N}} EIM(\mathcal{V}_{os})$ mas $\not\models_{\mathcal{N}} S_1$.

b) Basta tomar a estrutura $\mathcal{N} = \langle N, 0_N, S_N \rangle$, definida do seguinte modo:

i) $N = \{0, 1\}$;

ii) $0_N = 0$;

iii) S_N é a função definida pelo seguinte diagrama:



Obviamente, $\models_{\mathcal{N}} EIM(\mathcal{V}_{os})$ mas $\not\models_{\mathcal{N}} S_2$.

c) Denotando a fórmula $x \neq o \rightarrow \exists y \ sy = x$ por $A(x)$, temos:

Base: Obviamente $o \neq o \rightarrow \exists y \ sy = o$, ou seja, $A(o)$.

Passo: Também é um fato imediato que $sx \neq o \rightarrow \exists y \ sy = sx$, ou seja $A(sx)$. Daí, $A(o) \wedge \forall x \ (A(x) \rightarrow A(sx))$, acarretando $\forall x \ A(x)$.

d) Seja $m = k+1$, onde k é um número natural qualquer e $A(x)$ a fórmula $s^m x \neq x$.

Base: Temos $s^m o = s^{k+1} o = s(s^k o) \neq o$ (axioma S_1). Assim, $A(o)$.

Hipótese: Suponhamos $A(x)$.

Passo: Daí, $s^m(sx) \neq sx$ que é $A(sx)$. ∎

É um fato bem conhecido que no caso das linguagens de segunda ordem, os axiomas S_1, S_2 e EIM não são independentes. Isto acontece porque em todos os modelos do axioma de indução ao menos um dos axiomas S_1 ou S_2 é verdadeiro [6]. Os resultados anteriores nos mostram que isto não acontece, no caso de $Th(I\!N, 0, S)$.

A proposição 6.1 motiva a seguinte definição:

Definição Chamaremos $ESpc_{osEIM}$ a seguinte especificação esquemática:

i) **Vocabulário:** $\mathcal{V}_{os}$;

ii) **Variável esquemática:** X, de peso 1;

iii) **Axiomas:** S_1 e S_2;

iv) **Esquema de axiomas:** EIM.

Temos, então o seguinte resultado:

Proposição 6.2 *A aplicação $ESpc_{osEIM}(\mathcal{V}_{os})$ é uma especificação usual para a teoria $Th(I\!N, 0, S)$.*

6.2 O esquema de axiomas $EIF(\mathcal{V}_{os})$

Na seção anterior, confrontamos o esquema $EIM(\mathcal{V}_{os})$ com a axiomática anteriormente obtida e investigamos o papel da aplicação de EIM a $\mathcal{L}(\mathcal{V}_{os})$ na especificação de $Th(I\!N, 0, S)$. Nesta seção e na próxima, investigamos de maneira análoga o papel de dois outros esquemas definidos por outras duas fórmulas esquemáticas que podem ser interpretadas como formalizando formas fracas de princípios de indução, em estruturas que possuem zero e sucessão entre seus conceitos primitivos.

A introdução destes novos esquemas decorre de uma análise do método de prova introduzido pela presença de EIM na especificação de uma teoria.

Uma prova por indução matemática, numa teoria formal $\mathcal{T}$, de uma sentença $\forall x\ A(x)$ consiste, usualmente, na prova de dois lemas independentes:

Lema 6.1 (***Base*** **de indução)** *Mostrar que* $\vdash_{\mathcal{T}} A(o)$.

Lema 6.2 **(Cláusula do** ***fecho*****)** *Mostrar que* $\vdash_{\mathcal{T}} \forall x\ (A(x) \rightarrow A(sx))$.

O objetivo dos lemas 6.1 e 6.2 é provar a conjunção das sentenças $A(o)$ e $\forall x\ (A(x) \rightarrow A(sx))$, que nos permite provar $\forall x\ A(x)$, usando um exemplar de EIM e Modus Ponens.

A prova do lema 6.1 pode ser feita ou diretamente dos axiomas, pelos métodos usuais de prova ou, no caso de propriedades aritméticas aparentemente mais complexas da forma $\forall x\ B(x)$, pelo próprio método de indução matemática aplicado a x e $B(x)$, como variável e fórmula de indução, respectivamente.

A prova do lema 6.2 se faz, usualmente, efetuando-se três passos básicos:

1) *Hipótese* de indução: Supor $A(x)$;

2) *Passo* de indução: Provar que $A(x) \vdash_{\mathcal{T}} A(sx)$;

3) Concluir que $\vdash_{\mathcal{T}} A(x) \rightarrow A(sx)$, pelo Teorema da Dedução e que $\vdash_{\mathcal{T}} \forall x\ (A(x) \rightarrow A(sx))$, por Generalização.

Não é difícil mostrar que, em alguns casos particulares, a prova do lema 6.2 não necessita da execução dos três passos acima. Por exemplo, na prova de S_3 a partir de $EIM(\mathcal{V}_{os})$ provamos que $sx \neq o \rightarrow \exists y\ sy = sx$ sem usar, necessariamente, $s \neq o \rightarrow \exists y\ sy = x$.

Assim, para algumas propriedades aparentemente mais simples, podemos mostrar que $\vdash_{\mathcal{T}} \forall x\ (A(x) \rightarrow A(sx))$ provando diretamente que $\vdash_{\mathcal{T}} A(sx)$ e introduzindo $A(x)$ ou pela monotonicidade do $\vdash$ em conjunto com o Teorema da Dedução ou pela Afirmação do Conseqüente.

Parece, então, natural considerarmos um outro tipo de esquema de axiomas de indução que pode ser expresso em $\mathcal{L}(\mathcal{V}_{os})E$. A saber, aquele definido pela seguinte fórmula esquemática:

$$EIF.\ X(o) \wedge \forall x\, X(sx) \to \forall x\, X(x).$$

A fórmula acima pode ser considerada como obtida a partir de EIM por um enfraquecimento da cláusula do fecho e, analogamente a EIM, dá origem a um método de prova que, como veremos adiante, pode ser aplicado à prova de todas as propriedades decorrentes do fato de que em modelos de $Th(I\!N, 0, S)$, S é sobrejetiva em $I\!N \setminus \{0\}$. Tal fórmula será chamada *indução fraca* e o esquema de axiomas obtido pela aplicação de EIF a uma linguagem adequada $\mathcal{L}$, será chamado de *esquema fraco de indução* de $\mathcal{L}$.

Temos, então, o seguinte resultado:

Proposição 6.3

a) $EIF(\mathcal{V}_{os}) \not\models S_1$.

b) $EIF(\mathcal{V}_{os}) \not\models S_2$.

c) $EIF(\mathcal{V}_{os}) \vdash\dashv S_3$.

d) *Se n for um número natural não nulo, então $EIF \not\models \forall x\ s^n x \neq x$, ou seja, $EIF \not\vdash ES_4$.*

Prova:

a) e b) Os mesmos modelos apresentados na proposição 6.1.

c) Denotando a fórmula $x \neq o \to \exists y sy = x$, ou seja, $A(o)$, teremos:

Base: Obviamente, $o \neq o \to \exists y sy = o$, ou seja, $A(o)$;

Passo: É imediato que $sx \neq o \to \exists y sy = sy$, ou seja $A(sx)$.

Daí, $A(o) \wedge \forall x A(sx)$ e assim, $\forall x A(x)$ (esquema EIF).

d) Basta considerar a estrutura $\mathcal{N} = \langle N, 0_N, S_N \rangle$, definida do seguinte modo:

i) $N = \{a_1, a_2, \ldots, a_n\}$;

ii) $0_N = a_1$;

iii) $S_N : N \to N$ definida do seguinte modo, para todo $i, 1 \leq i \leq n$:

$$S_N(a_i) = \begin{cases} a_{i+1} & \text{se } i \leq n \\ a_1 & \text{se } i = n, \end{cases}$$

Em resumo, $\mathcal{N}$ é exatamente um n-ciclo que o axioma $\forall x\ s^n x \neq x$ exclui dos modelos de $Th(\mathbb{N}, 0, S)$.

Teremos, então:

1) $\models_{\mathcal{N}} EIF$, pois em um ciclo todos os elementos são sucessores;

2) $\not\models_{\mathcal{N}} \forall x\ s^n x \neq x$, pois, por exemplo, $s^n a_1 = a_1$. ■

O resultado acima motiva a seguinte definição:

Definição Chamaremos $ESpc_{osEIF}$ a seguinte especificação esquemática:

i) **Vocabulário:** $\mathcal{V}_{os}$;

ii) **Variável esquemática:** X, de peso 1;

iii) **Axiomas:** S_1, S_2, $S_{4.2}$, $\ldots$, $S_{4.m}$, $\ldots$;

iv) **Esquema de axiomas:** EIF.

Temos, então o seguinte resultado:

Proposição 6.4 *A aplicação $ESpc_{osEIF}(\mathcal{V}_{os})$ é uma especificação usual para a teoria $Th(\mathbb{N}, 0, S)$.*

6.3 O esquema de axiomas $EIS(\mathcal{V}_{os})$

Continuando a análise efetuada na seção anterior um pouco adiante, podemos obter um outro tipo de enfraquecimento da cláusula do fecho, considerando àquelas propriedades aritméticas para as quais, além de provarmos que $A(x) \vdash_{\mathcal{T}} A(sx)$, poderíamos também provar que $A(sx) \vdash_{\mathcal{T}} A(x)$.

Assim, podemos considerar ainda um outro tipo de axioma de indução que pode ser expresso em $\mathcal{L}(\mathcal{V}_{os})$, a saber, aquele definido pela seguinte fórmula esquemática:

$$EIS.\ X(o) \wedge \forall x\ (X(x) \leftrightarrow X(sx)) \rightarrow \forall x\ X(x).$$

Tal fórmula será chamada *indução simétrica* e o esquema de axiomas obtido por aplicação de EIS a uma linguagem adequada $\mathcal{L}$, será chamado *esquema simétrico de indução* de L.

Proposição 6.5

a) $EIS(\mathcal{V}_{os}) \not\models S_1$;

b) $EIS(\mathcal{V}_{os}) \not\models S_2$;

c) $EIS(\mathcal{V}_{os}) \not\models S_3$;

d) $S_1, S_2, EIF(\mathcal{V}_{os}) \vdash\dashv ES_4$.

Prova:

c) Sendo m um número natural não nulo, basta considerar a estrutura $\mathcal{N} = \langle \mathbb{N}, 0_N, S_N \rangle$, definida do seguinte modo:

i) $N = \mathbb{N} \cup \{\sqrt{2}\}$;

ii) $0_N = 0$;

iii) $S_N : N \to N$ definida do seguinte modo, para todo $n \in N$:

$$S_N(n) = \begin{cases} m & \text{se } n = \sqrt{2} \\ n+1 & \text{se } n \in \mathbb{N}, \end{cases}$$

Teremos, então:

a) $\not\models_{\mathcal{N}} S_3$, pois para todo $n \in \mathbb{N}$, $n + 1 \neq \sqrt{2}$, ou seja, $S_N(n) \neq \sqrt{2}$;

b) $\not\models_{\mathcal{N}} EIS(\mathcal{V}_{os})$. De fato, seja $A(x)$ uma fórmula de $\mathcal{L}(\mathcal{V}_{os})$, tal que $\models_{\mathcal{N}} A(o)$, $\models_{\mathcal{N}} \forall x\ (A(x) \leftrightarrow A(sx))$ e $\not\models_{\mathcal{N}} \tilde{\forall} x\ A(x)$. ∎

O resultado acima motiva a seguinte definição:

Definição Chamaremos $ESpc_{osEIS}$ a seguinte especificação esquemática:

i) **Vocabulário:** $\mathcal{V}_{os}$;

ii) **Variável esquemática:** X, de peso 1;

iii) **Axiomas:** S_1, S_2 e S_3;

iv) **Esquema de axiomas:** EIS.

Temos, então o seguinte resultado:

Proposição 6.6 *A aplicação $ESpc_{osEIS}(\mathcal{L}(\mathcal{V}_{os}))$ é uma especificação usual para a teoria $Th(\mathbb{N}, 0, S)$.*

6.4 A relação entre as aplicações $EIM(\mathcal{V}_{os})$, $EIF(\mathcal{V}_{os})$ e $EIS(\mathcal{V}_{os})$

Nesta seção, investigamos a relação existente entre as aplicações dos esquemas EIM, EIF e EIS a $\mathcal{L}(\mathcal{V}_{os})$.

Proposição 6.7 $S_1, S_2, EIF(\mathcal{V}_{os}), EIS(\mathcal{V}_{os}) \vdash\dashv S_1, S_2, EIM(\mathcal{V}_{os})$.

Prova:

($\Rightarrow$) Segue dos resultados anteriores que S_1, S_2, $EIF(\mathcal{V}_{os})$ e $EIS(\mathcal{V}_{os}) \vdash S_1, S_2, S_3$ e $ES4$. Agora, S_1, S_2, S_3 e $ES4 \vdash S_1, S_2$ e $EIM(\mathcal{V}_{os})$. Logo, da transitividade do $\vdash$, temos o resultado desejado.

($\Leftarrow$) Segue dos resultados anteriores que S_1, S_2 e $EIM(\mathcal{V}_{os}) \vdash S_1, S_2, S_3$ e ES_4. Agora, S_1, S_2, S_3 e $ES_4 \vdash S_1, S_2$ e $EIM(\mathcal{V}_{os})$. Logo, da transitividade do $\vdash$, temos o resultado desejado. ∎

Observe que a prova da proposição 6.7 não é feita no cálculo esquemático e depende diretamente da axiomática apresentada.

Capítulo 7

Conclusões

Este trabalho é uma introdução ao estudo dos esquemas de axiomas de indução na especificação de teorias elementares.

Existem duas motivações básicas para a introdução deste tipo de axioma na especificação de uma teoria. Em primeiro lugar, dada uma estrutura indutiva $\mathcal{N}$ e uma linguagem de primeira ordem $\mathcal{L}$, adequada para $\mathcal{N}$, podemos estar interessados em investigar o quanto do princípio de indução associado a $\mathcal{N}$, pode ser expresso em $\mathcal{L}$. Conseqüentemente, interessa determinar o quanto de $Th(\mathcal{N})$ esta porção do princípio de indução consegue assegurar.

Por outro lado, podemos introduzir o esquema como uma maneira de garantir que determinados métodos de prova estejam diponíveis para $Th(\mathcal{N})$. Conseqüentemente, interessa também investigar o quanto de $Th(\mathcal{N})$ estes métodos de prova conseguem assegurar.

A abordagem iniciada neste trabalho a ambas as questões colocadas acima nos conduzem ao problema de comparar a aplicação do esquema de axiomas associado a $I(\mathcal{N})$ com uma axiomática independente para $\mathcal{N}$. Como conseqüência, dada uma estrutura indutiva $\mathcal{N}$, somos levados a considerar as seguintes questões:

(1) De que formas podemos definir $\mathcal{N}$ indutivamente?

(2) É $Th(\mathcal{N})$ axiomatizável? Caso a resposta a esta questão seja afirmativa, encontrar uma axiomática independente para $Th(\mathcal{N})$;

(3) Investigar o papel de cada axioma na caracterização algébrica dos modelos de $\mathcal{N}$;

(4) Comparar a aplicação dos esquemas de axiomas de indução associados

aos princípios de indução encontrados no item (1) com a axiomática obtida;

(5) Com as informações obtidas acima, determinar o papel de cada esquema de axiomas na especificação de $Th(\mathcal{N})$ e comparar os esquemas entre si.

Neste trabalho, apresentamos alguns elementos necessários para a consideração destas questões. Em particular, iniciamos a execução do plano acima, para subteorias axiomatizáveis da aritmética elementar, tratando da teoria $Th(\mathbb{N}, O, S)$. Como extensão imediata, indicamos o estudo das teorias das seguintes estruturas: $\langle \mathbb{N}, < \rangle$, $\langle \mathbb{N}, + \rangle$, $\langle \mathbb{N}, \cdot \rangle$.

Bibliografia

[1] A. CHURCH, An Unsolvable Problem of Elementary Number Theory, *American Journal of Mathematics*, **58** (1936), pp. 345–363.

[2] H.B. ENDERTON, "A Mathematical Introduction to Logic", New York, Academic Press, 1972.

[3] S. FEFERMAN, Reflecting on Incompleteness, *The Journal of Symbolic Logic*, **56** (1991), pp. 1–49.

[4] I. GARRO, "Independence Proofs in Arithmetic Theories with Very Weak Induction", Doktorgrades Dissertation, Bonn, 1973.

[5] K. GÖDEL, Über Formal Unentscheidbare Sätze der Principia Mathematica und Verwandter System I, *Monatshefte für Mathematik und Physik* **38** (1931), pp. 173–197. Traduzido em: J. van Heijenoort (Editor), "From Frege to Gödel: A Source book in Mathematical Logic, 1879-1931" Cambridge, Harvard University Press, (1981).

[6] L. HENKIN, On Mathematical Induction, *The American Mathematical Monthly*, **67** (1960), pp. 323–338.

[7] A. JANICAK, A Remark Concerning Decidability of Complete Theories, *The Journal of Symbolic Logic*, **15** (1956), pp. 273–275.

[8] R. KAYE, "Models of Peano Arithmetic", Oxford, Clarendon Press, 1991.

[9] S.C. KLEENE, "Introduction to Metamathematics", Amsterdam, North-Holland, 1952.

[10] A.I. MAL'CEV, Construtive Algebras I, em: B.F. Wells, III, "The Metamathematics of Algebraic Systems", Amsterdam, North-Holland, (1971), pp. 148–214.

[11] A. MARGARIS, Sucessor Axioms for the Integers, *The American Mathematical Monthly*, **68** (1961), pp. 441–444.

[12] C. RYLL-NARDZEWSKI, The Role of the Axiom of Induction in Elementary Arithmetic, *Fundamenta Mathematicae*, **39** (1952), pp. 239–263.

[13] J.C. SHEPHERDSON, Weak and Strong Induction, *The American Mathematical Monthly*, **76** (1969), pp. 989–1004.

[14] T.A. SKOLEM, Über die Nichtcharakterisierbarkeit der Zahlenreihe mittels endlich oder abzählbar unendlich vielen Anssagen mit ausschliesslich Zahlenvariablen, *Fundamenta Mathematicae* **23** (1934), pp. 150–161. Traduzido em: "Mathematical Interpretations of Formal Systems" Amsterdam, North-Holland.