UNIVERSIDADE FEDERAL DO RIO DE JANEIRO

FELIPE SOBREIRA ABRAHÃO

DEMONSTRANDO A CONSISTÊNCIA DA ARITMÉTICA

Rio de Janeiro

2011

Felipe Sobreira Abrahão

DEMONSTRANDO A CONSISTÊNCIA DA ARITMÉTICA

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em História das Ciências e das Técnicas e Epistemologia, Universidade Federal do Rio de Janeiro, como requisito para obtenção do título de Mestre em Ciências, em História das Ciências e das Técnicas e Epistemologia.

Orientador: Prof. Dr. Francisco Antonio de Moraes Accioli Doria

Rio de Janeiro

2011

Abrahão, Felipe Sobreira.

Demonstrando a Consistência da Aritmética/ Felipe Sobreira Abrahão. - Rio de Janeiro: UFRJ/ HCTE, 2011.

viii, 40 p., 29,7 cm.

Orientador: Francisco Antonio de Moraes Accioli Doria

Dissertação (Mestrado em História das Ciências e das Técnicas e Epistemologia) – Coppe/IQ/IM, Universidade Federal do Rio de Janeiro, HCTE, Rio de Janeiro 2011.

Referências Bibliográficas: p. 69-70.

1. Consistência da Aritmética 2. Lógica Matemática 3. Filosofia da Matemática. I. Doria, Francisco Antonio. II. Universidade Federal do Rio de Janeiro, Institutos Coppe/IQ/IM, Pós-graduação e Pesquisa em História das Ciências e das Técnicas e Epistemologia. III. Demonstrando a Consistência da Aritmética.

Felipe Sobreira Abrahão

DEMONSTRANDO A CONSISTÊNCIA DA ARITMÉTICA

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em História das Ciências e das Técnicas e Epistemologia, Universidade Federal do Rio de Janeiro, como requisito para obtenção do título de Mestre em Ciências, em História das Ciências e das Técnicas e Epistemologia.

Aprovado em 02/03/2011.

Banca Examinadora

____

Prof. Francisco Antonio de Moraes Accioli Doria, Professor Emérito, UFRJ

____

Prof. Ricardo Silva Kubrusly, Ph.D., University of Texas

____

Prof. Carlos Alberto Nunes Cosenza, TITULO, COPPE/UFRJ

DEDICATÓRIA

Dedico esse trabalho a minha namorada, Raquel Cardoso Oscar, com a qual, nos últimos anos, tenho passado os melhores momentos da minha vida.

AGRADECIMENTOS

Aos professores Francisco Antônio de Moraes Accioli Dória, Ricardo Silva Kubrusly, Lev D. Beklemishev, Jeff B. Paris e Gregory John Chaitin pelos ensinamentos e contribuições para o conteúdo desse trabalho.

Aos meus familiares pelo apoio, sem o qual a realização dessa dissertação seria extremamente difícil.

Resumo

O presente trabalho irá apresentar algumas demonstrações da consistência da aritmética clássica, que foi provada por Gödel (1931) como sendo indemonstrável dentro da própria aritmética, e irá discuti-las do ponto de vista lógico e filosófico. Primeiramente, demonstrará a consistência se baseando na prova do Schütte (1951), uma prova *a la* Gentzen, com utilização de novos conceitos, definições e teoremas. Na próxima parte, serão usados os princípios de reflexão e o princípio combinatorial de Paris-Harrington para mostrar que a consistência pode ser obtida por extensões recursivas e verdadeiras, no sentido lógico-matemático levando em conta métodos além da axiomática de Peano (Teoria dos Conjuntos). Por último, discorrerá sobre problemas e questões que ainda permanecem sobre a fundamentação tanto lógica matemática quanto filosófica dos temas abordados. Se provamos realmente a consistência da aritmética, sobre quais bases se deram essas provas? Não estaríamos nos baseando em outros pressupostos, escondidos ou não, para chegar a esses resultados? Seríamos capazes de provar um indecidível, no sentido godeliano?

Palavras-chaves: Consistência da aritmética. Princípios de reflexão. Regra infinitária. Computabilidade da matemática.

Abstract

This paper will present some demonstrations of the consistency of classical arithmetic, which was proven by Gödel (1931) as being unprovable inside the arithmetic and will discuss them in logical and philosophical terms. First, will demonstrate consistency based on the Schütte´s proof (1951), an a la Gentzen proof, using new concepts, definitions and theorems. In the next part, we will use the reflection principles and the Paris-Harrington combinatorial principle to show that consistency can be obtained by recursive extensions and that it is a true extension in the logical-mathematical sense using methods beyond the Peano axiomatic (Set theory). Finally, will discuss problems and issues that still remain on the mathematical logic and philosophical foundations of the addressed subjects. If we really prove the arithmetic´s consistency, upon which bases we give that? We would not be based on other assumptions, hidden or not, to achieve such results? Would we be able to prove an undecidable in the godelian sense?

Keywords: Consistency of Peano arithmetic. Reflection principles. Infinitary rule. Computability and Axiomatic theories.

SUMÁRIO

Introdução

Houve um fervilhar de ideias e concepções sobre o que deveria fundar a matemática, principalmente, na virada do século XIX para o XX. Dentre as principais escolas de pensamento vigoravam a Logicista, a Intuicionista e a Formalista[1].

A prerrogativa logicista era de traduzir toda a matemática já feita para expressões lógicas, ou seja, reduzir a matemática à lógica. Acreditava-se que a matemática nada a mais seria do que lógica "disfarçada". Já o intuicionismo tentava eliminar as provas não construtivas, isto é, aquelas em que se prova a existência de algo por redução ao absurdo, da matemática e da lógica. Pois, se baseando na premissa de que o conhecimento matemático verdadeiro era somente aquele que vem por meio de construções mentais, todas as provas deveriam ser feitas por um processo construtivo. Pelo qual, objetos matemáticos mais elaborados têm sua existência provada somente a partir de objetos elementares – no caso, os números naturais - por meio de processos finitos.

David Hilbert (1862 –1943), um dos mais influentes matemáticos alemães da época, concordou com os intuicionistas que o finitismo proveniente dos números naturais era a base da matemática. Porém, diferentemente, dizia que eles eram apenas símbolos e não construções mentais, o que abre a possibilidade de os mesmos serem representados também por entidades físicas. O intuicionismo de Brouwer era visto com limitações por Hilbert que, inclusive, o acusava de mutilar a matemática por jogar fora tudo aquilo que parecesse problemático. Com isso, iniciou o projeto de axiomatizar toda a matemática por meio da lógica. Uma proposta muito mais radical que a logicista, justamente, por extirpar a semântica do discurso matemático. Seria uma pura manipulação de símbolos, um *sistema simbólico formal*. Daí, seu desígnio de Formalismo.

Muitos teoremas dentro do vasto universo matemático são provados usando uma matemática dita de nível mais alto, que não se calca na Aritmética de Peano (PA), por exemplo, os teoremas de análise e de teoria dos conjuntos. Além disso, esta "alta matemática" era usada frequentemente para provar coisas sobre a matemática básica, a

---

[1] Talvez, uma quarta escola, o Predicativismo, também seja importante.

teoria dos números naturais. Hilbert era ciente disso e, iniciando seu Programa de Conservação, dizia que tudo aquilo que puder ser provado com o uso de atalhos pela alta matemática, também pode ser derivado diretamente, por passos finitos, dos axiomas de Peano. Para isso, era, no mínimo, necessário mostrar que os axiomas desses sistemas simbólicos superiores eram consistentes. Ele afirmava que se fosse provado que um sistema axiomático não levasse a contradições, então este seria verdadeiro (um sistema *Sound*). E, curiosamente, tal problemática é retomada, por outro caminho, pelo estudo de extensões da aritmética capazes de "garantir" que ela seja *Sound*, como será visto no capítulo 2. Em outras palavras, provar a consistência de um conjunto de axiomas seria provar que os objetos definidos por tais axiomas existem. O que, de fato, é um teorema que pôde ser formalizado pela teoria dos modelos.

Obviamente, sendo coerente com sua proposta formalista, tudo isso deveria ser provado dentro da parte da matemática mais "segura", aquela que fosse sua base, ou seja, a própria aritmética. Esse foi o chamado *Programa de Consistência de Hilbert.*

Infelizmente ou não, demonstradas por Kurt Gödel em 1931, a incompletude da Aritmética de Peano (*Peano Arithmetic* (PA), *teoria formal dos números* ou *aritmética*) e a indecidibilidade da consistência nos diz, respectivamente, que não é possível sempre demonstrar dentro de PA que uma fórmula é verdadeira ou que é falsa (isto é, A ou que $\neg A$, onde A é uma fórmula na linguagem de PA), nem que a própria teoria é consistente. O primeiro é o Primeiro Teorema da Incompletude e o seguinte, o Segundo Teorema da Incompletude. É importante lembrar que esses dois teoremas partem da hipótese de que PA seja consistente. Então, por exemplo, o segundo teorema da incompletude assevera que se a aritmética for consistente, então ela não consegue demonstrar que ela mesma é consistente. O sistema axiomático usado por Gödel para os números se baseia em regras de inferência dedutivas, das quais é possível definir a própria demonstrabilidade de uma expressão dentro da teoria formal dos números, ou seja, é possível construir uma sentença na linguagem de PA – chamemos de $Pr_T[\varphi]$ - que diz (representa) que uma fórmula φ é demonstrável pela teoria T. Logo, para qualquer fórmula φ demonstrável em PA, PA também demonstra $Pr_{PA}[\varphi]$. Portanto, Gödel partiu das mesmas bases propostas pelo Programa de Hilbert chegando ao resultado de que este era fadado ao fracasso.

Gerhard Gentzen, em 1936, construindo um sistema lógico – vamos chamá-lo de PA_∞ – para a aritmética mais poderoso que a teoria formal dos números, consegue demonstrar, não só que PA_∞ é consistente e completo, como também, que PA é consistente. No livro *Introduction to Mathematical Logic*, escrito por Elliott Mendelson, no qual se baseia o primeiro capítulo desta dissertação, pode-se encontrar tal demonstração na versão do *Kurt Schütte* (1951). Ambas as demonstrações se dão por indução transfinita sobre os ordinais.

Mostraremos, no primeiro capítulo, a versão do Schütte (1951) sobre a demonstração do Gentzen (1936) da consistência da aritmética. Tanto PA quanto PA_∞ são sistemas axiomáticos numa lógica de primeira ordem, porém, possuindo regras de inferência e axiomas distintos.

A diferença central de PA_∞ para PA está na infinite induction rule, uma regra de inferência infinitária que nos permite obter uma conclusão a partir de infinitas premissas. Com ela, tornamos tal novo sistema lógico para a aritmética não dedutivo, ou seja, que não pode ser reduzido às regras dedutivas clássicas.

No segundo capítulo, será exposta a construção de uma extensão de PA capaz de demonstrar a consistência da aritmética. Vem de uma ideia de garantir a consistência por meio dos princípios de reflexão. Que são, informalmente, expressões que, adicionadas a PA, asseveram a corretude da teoria formal dos números – isto é, que "aquilo que é provado por PA é verdadeiro".

Terminaremos, no último capítulo, nos voltando para as sessões anteriores e para outros resultados da lógica matemática em busca de novas problemáticas e apontamentos sobre fundamentação. Se provamos realmente a consistência da aritmética, sobre quais bases se deram essas provas? Não estaríamos nos baseando em outros pressupostos, escondidos ou não, para chegar a esses resultados? Seríamos capazes de provar um indecidível, no sentido godeliano?

Alguma familiaridade com as noções e definições de lógica de primeira ordem e de matemática talvez seja necessária para o leitor do presente trabalho.

Capítulo 1: Uma prova

Nesse capítulo nos basearemos na versão do Schütte (1951) sobre a demonstração do Gentzen (1936) da consistência da aritmética.[1] Ela não estará somente transcrita, na verdade, esse capítulo contém a adição de alguns conceitos e teoremas novos. Vamos nos referir ao sistema axiomático clássico da teoria dos números (Aritmética de Peano), sobre o qual os dois teoremas de Gödel se fundamentam, por S e ao novo, introduzido por Gentzen, por S_∞, do qual provaremos a consistência de S. Ambos são sistemas axiomáticos, porém possuem regras de inferência e axiomas distintos.

Como S, S_∞ é definido sobre uma linguagem de primeira ordem – e, inclusive, importando todas as definições sobre a lógica de primeira ordem - com:

(i) símbolos Funcionais $+$, $\times$, $'$ (soma, produto e sucessor);

(ii) símbolo Predicativo $=$ (igual);

(iii) símbolo Constante 0 (elemento neutro aditivo);

(iv) quantificador $\forall$ (para todo);[2]

Os conectivos passam a ser $\vee$ e $\neg$, diferentemente de S que possui $\rightarrow$ e $\neg$. Qualquer fórmula construída sobre $\rightarrow$ e $\neg$ pode ser transformada, mantendo as condições de verdade – configurando uma tautologia -, para uma construída sobre $\vee$ e $\neg$.[3] Por exemplo, $A \rightarrow B$ passa a ser $\neg A \vee B$.

Uma fundamental diferença está nos seus axiomas. Estes são compostos por todas as fórmulas atômicas fechadas corretas e a negação de todas as fórmulas atômicas fechadas incorretas (as definições de tais termos serão explicadas a seguir). O que nos leva a um sistema com infinitos, em particular, enumeráveis, axiomas. Outro ponto importante, apesar de não necessário para a construção de S_∞, é que se parte do pressuposto de que a

---

[1] MENDELSON, E. **Introduction to Mathematical Logic**. 2ª. ed. Princeton, New Jersey: D. Van Nostrand Company, INC., 1964.

[2] Não há necessidade do quantificador existencial $\exists$, pois $\exists x A \equiv \neg\forall x \neg A$.

[3] ENDERTON, H. **A mathematical introduction to logic.** 2ª. ed. Boston, MA: Academic Press, 2001. Cap. 1. ISBN 978-0-12-238452-3.

verificação de uma fórmula atômica fechada como correta ou incorreta é sempre possível e definida, por hipótese. De fato, o sistema S, por exemplo, sempre pode decidir por processos recursivos se uma fórmula atômica fechada é correta ou incorreta (assim como, também pode ser decidido por um computador). Mas, como já dito, tal consideração não é necessária para a construção de S_∞ e dos seus axiomas, pois basta apenas tomar infinitos axiomas por princípio, independente de ter alguém os verificando ou não. A não ser que isto seja impossível para nós.[4]

Os principais resultados são o Lema A-4 e a Proposição A-8, que nos dão a consistência de S no corolário B-2. Todos os teoremas de indexação A-(algum número) podem ser encontrados no texto de referência[5] com poucas diferenças, apesar de estarem num modo de escrever diferente do que vamos apresentar aqui. Os de índice começando pela letra B são próprios dessa dissertação.

Enunciaremos as definições tendo em vista que algumas delas são importadas da lógica de primeira ordem usual ou da teoria formal dos números e que, por isso, iremos nos abster de maiores explicações. Antes disso, vamos começar expondo as regras de inferência de S_∞.

1.1 Regras de Inferência

1.1.1 Regras Fracas:

1.1.1.1 Exchange: $\frac{C \vee A \vee B \vee D}{C \vee B \vee A \vee D}$

1.1.1.2 Consolidation: $\frac{A \vee A \vee D}{A \vee D}$

1.1.2 Regras Fortes:

---

[4] Maiores discussões sobre isto poderão ser vistas no item 3.1.
[5] MENDELSON, op. cit.

1.1.2.1 Dilution: $\frac{D}{A \vee D}$, onde A é uma fórmula fechada.

1.1.2.2 DeMorgan: $\frac{\neg A \vee D \quad \neg B \vee D}{\neg(A \vee B) \vee D}$

1.1.2.3 Negation: $\frac{A \vee D}{\neg\neg A \vee D}$

1.1.2.4 Quantification: $\frac{\neg A(t) \vee D}{\neg \forall x A(x) \vee D}$, onde t é um termo fechado.

1.1.2.5 Infinite Induction: $\frac{A(n) \vee D\text{, } para\ todo\ n\ natural}{\forall x A(x) \vee D}$

1.1.3 **Cut:** $\frac{\boldsymbol{C} \vee \boldsymbol{A} \quad \neg \boldsymbol{A} \vee \boldsymbol{D}}{\boldsymbol{C} \vee \boldsymbol{D}}$

1.2 Definições

(i) Dizemos que uma fórmula (ou um termo) é fechada se ela não possui variáveis livres. Por exemplo, $\forall x \neg A(x, y)$ não é uma fórmula fechada, pois a variável y está livre. Tanto S quanto S_∞ somente possuem constantes sobre os números naturais, estão, por isso, numa linguagem enumerável.

(ii) Dizemos que uma fórmula A é atômica se ela é bem formada (well-formed formula) e composta somente pelos símbolos $+,\ \times,\ '$, $=$. Isto é, A é da forma $s = t$.

(iii) Dizemos que uma fórmula atômica fechada $s = t$ é correta se ela pode ser avaliada por um processo recursivo, definido sobre as operações de soma (onde a operação sucessor já está incluída) e produto, tal que ele conclua que o valor de s (um número natural) é o mesmo que o de t (um número natural também). Do contrário, dizemos que $s = t$ é incorreta. Analogamente fazemos o mesmo para $s \neq t$.

(iv) Dada uma regra de inferência da forma $\frac{A_1\ A_2\ \dots\ A_n \dots}{B}$, onde A_i e B são fórmulas, para todo $i \in \mathbb{N}$, dizemos que as fórmulas $A_1, A_2, \dots, A_n, \dots$ são premissas e B a conclusão.

(v) Denominamos por fórmulas laterais as fórmulas nas premissas ou na conclusão que não são afetadas pela regra de inferência em questão - elas são simbolizadas por C ou D na parte 1.1 desse capítulo. Qualquer outra fórmula numa regra que não seja uma fórmula lateral será denominada de fórmula principal – simbolizadas por A ou B.

(vi) Qualquer fórmula lateral pode ser omitida em uma regra a não ser na Dilution e na Cut, nesta, obrigatoriamente, uma das duas fórmulas laterais deve estar presente, pelo menos.

(vii) A fórmula principal na regra Cut é chamada de fórmula de corte e a soma do número de conectivos e quantificadores em $\neg A$ é o grau de um corte (não confundir com o grau de uma prova).

(viii) Uma árvore é um grafo não direcionado em que seus vértices, ou pontos, estão distribuídos em níveis horizontais – vamos chamá-los de levels. Não existem arestas ligando pontos de mesmo level. A estes níveis indexamos uma escala de levels ascendente à medida que os níveis horizontais sobem. O nível horizontal mais baixo (sobre o qual definiremos que contém somente um ponto: o ponto terminal) é chamado de level 0. O pontos ligados a este estão, obrigatoriamente, no level 1 e assim por diante. Ou seja, os pontos ligados a um determinado ponto P de level i só podem estar no level $i-1$ ou no level $i+1$.

(ix) Um ponto no level i só pode estar ligado a, no máximo, um ponto de level $i-1$ e a nenhum, um, dois ou a infinitos enumeráveis pontos de level $i+1$.

(x) Uma árvore ou prova de A é definida como sendo um grafo onde o ponto terminal é a fórmula A.

(xi) Um ponto em uma árvore é a representação de uma fórmula em S_∞. O único ponto de level 0 da árvore é chamado de ponto terminal. Os pontos que não se ligam a nenhum outro ponto de level mais alto são chamados de pontos iniciais.

(xii) Cada conjunto de arestas ligando um ponto P de level i a um, dois ou infinitos pontos de level $i+1$ representa uma regra de inferência, onde o ponto P representa a conclusão e os pontos no level $i+1$ representam as premissas. Também chamamos estes pontos de level $i+1$ de predecessores do ponto P.

(xiii) Os pontos iniciais são axiomas de S_∞.

(xiv) Dizemos que uma fórmula A é um teorema de S_∞ se ele é obtido por meio de uma árvore de A.

(xv) O número total de Cuts em uma árvore de A é definido como sendo o grau de uma árvore, prova ou de A.

Ordenam-se os Cuts contando-os pelas fórmulas que são conclusões dos respectivos Cuts. Podemos começar contando do level mais alto em que eles aparecem e da esquerda para direita, passando para o próximo level, contando da esquerda para a direita e assim por diante até chegar ao level zero.

Por exemplo, se uma árvore de A vai até o level n, então, o level mais alto que pode conter algum Cut é o level $n-2$. Pois, não é possível formar algum Cut a partir dos axiomas de S_∞ .

Dessa forma, é possível estabelecer uma ordem mesmo se a quantidade de Cuts for infinita, atribuindo números ordinais como sendo os graus das árvores.

(xvi) A cada ponto P, representando uma fórmula A, indexamos um número ordinal, e dizemos que a ordinalidade de A (ou da árvore de A) é tal número, onde:

a) os axiomas, ou pontos iniciais, tem ordinalidade zero;
b) se P é conclusão de uma regra fraca, então o ordinal de P é o mesmo de sua premissa;
c) se P é conclusão de uma regra forte ou de um Cut, então o ordinal de P é maior que o ordinal de qualquer premissa sua. Ou seja, o ordinal de P é $\max(\alpha_1, \alpha_2, \dots, \alpha_n, \dots) + 1$, onde $\alpha_1, \alpha_2, \dots, \alpha_n, \dots$ são os ordinais das premissas de P e $+$ é a soma ordinal (que, numa árvore, equivale a soma de números naturais. Ver item 1.3.(i));

(xvii) Dada uma fórmula B contida na fórmula A, definimos a história de B em A pelo conjunto de pontos na árvore de A tais que a fórmula B está contida em cada um deles e tais que existe um caminho, com pontos dentro deste conjunto, ligando qualquer um deles a A. Cada ponto desse conjunto que não se liga a nenhum ponto de level mais alto ou que B não está contido em nenhum ponto de level mais alto que se liga a ele é um ponto onde a fórmula B surgiu na história de B em A.

(xviii) Uma prova de A somente contém um número finito de levels.

1.3 Considerações Iniciais

(i) Como, por 1.2.(xviii), o número de levels em uma árvore é finito, é fácil ver que a ordinalidade de qualquer teorema de S_∞ é sempre finita. Assim como, é possível que uma árvore de A tenha grau infinito, se houver, pelo menos, uma Infinite Induction na prova. Daí a necessidade de atribuição de ordinais, como no item 1.2.(xv), aos graus das árvores.

(ii) Como, por construção, S_∞ somente tem fórmulas atômicas fechadas como axiomas e como as regras de inferência somente levam fórmulas fechadas em fórmulas fechadas, qualquer teorema de S_∞ será uma fórmula fechada.

1.4 Lema A-1

Seja A uma fórmula fechada com n conectivos e quantificadores.

Então, existe uma prova para $\neg A \vee A$ com ordinalidade $\leq 2n+1$, na qual nenhum Cut foi utilizado.

- Demonstração: (por Indução sobre n, partindo de 0 e dividindo entre os casos $\vee, \neg, \forall$.)

a) Caso $n = 0$:

A será uma fórmula atômica correta ou incorreta. Logo, $\neg A$ ou A será um axioma.

Aplica-se uma Dilution e temos a prova com ordinalidade 1.

b) Caso válido para qualquer $k < n$:

(i) Caso $A = A_1 \vee A_2$:

Pela hipótese indutiva, temos que é válido para A_1 e A_2. Ou seja, temos uma prova para $\neg A_1 \vee A_1$ e uma para $\neg A_2 \vee A_2$. Ambas, com ordinalidade $\leq 2(n-1)+1$.

Por Dilution, teremos $A_2 \vee \neg A_1 \vee A_1$ e $A_1 \vee \neg A_2 \vee A_2$. Cada uma com ordinalidade $\leq 2n$.

Por Exchange e DeMorgan, obtemos $\neg(A_1 \vee A_2) \vee A_1 \vee A_2$ com ordinalidade $\leq 2n+1$

(ii) Caso $A = \neg B$:

Pela Hipótese Indutiva, temos que é válido para B. Ou seja, temos uma prova para $\neg B \vee B$ com ordinalidade $\leq 2(n-1)+1$.

Aplica-se uma Exchange e Negation e temos uma prova de $\neg\neg B \vee \neg B$ com ordinalidade $\leq 2n$.

(iii) Caso $A = \forall x B(x)$:

Pela hipótese indutiva, é válido para $B(t)$, para qualquer termo fechado t. Ou seja, temos uma prova para $\neg B(t) \vee B(t)$ com ordinalidade $\leq 2(n-1)+1$, para qualquer termo fechado t.

Aplica-se uma Quantification, Exchange, Infinite Induction e Exchange e termos uma prova para $\neg \forall x B(x) \vee \forall x B(x)$ com ordinalidade $\leq 2n+1$. ∎

Obs.: Um método análogo pode ser usado para provar a completude de S_∞.

1.5 Lema A-2

Para qualquer termo t ou s que não for uma variável (isto é, que for um termo fechado) e para qualquer fórmula $A(x)$, onde somente x é variável livre, existe uma prova em S_∞ para $s \neq t \vee \neg A(s) \vee A(t)$, onde nenhum Cut foi usado.

- Demonstração:

Separamos em dois casos: $s = t$ é correto ou incorreto.

a) se $s = t$ for incorreto:

Logo, $\neg(s = t)$ é axioma.

Usando Dilution e Exchange duas vezes cada, obtemos a prova.

b) se $s = t$ for correto:

Pelo Lema A-1, temos que existe uma prova para $\neg A(n) \vee A(n)$, onde n é um número natural.

Tome a História de $A(n)$ em $\neg A(n) \vee A(n)$. Logo, $A(n)$ surgiu de uma fórmula do tipo $A(n) \vee B$, a menos de uma Exchange.

Teremos que n surgiu numa fórmula que surgiu por Dilution ou numa fórmula que surgiu de um Ponto Inicial (axioma).

(i) No caso de Dilution, é fácil ver que sempre se pode substituir n por t nessa fórmula.

(ii) No caso de um Axioma, se substituirmos n por t na fórmula ela ainda continuará a ser um axioma.

Substituindo na história de $A(n)$ qualquer fórmula em função de n pela mesma em função de t, teremos, então, uma demonstração para $A(t) \vee B$.

Substituindo $A(n)$ por $A(t)$ na história de $A(n)$ em $\neg A(n) \vee A(n)$ a partir de $A(n) \vee B$, demonstramos $\neg A(n) \vee A(t)$.

Analogamente para $\neg A(n)$ em $\neg A(n) \vee A(t)$, demonstramos $\neg A(s) \vee A(t)$.

Por Dilution, teremos a prova desejada. ■

1.6 Lema A-3

Toda wff fechada que for um teorema de S também é teorema de S_∞.

- Demonstração: (por indução matemática sobre os ordinais)

É possível definir uma ordinalidade para uma Árvore de prova em S, tomando seus axiomas com ordinalidade zero e o Modus Ponens e a Generalization como Regras Fortes.

Seja A uma fórmula em S qualquer de ordinalidade α, isto é, que a ordinalidade de $\vdash_S A$ seja α.

a) Caso $\alpha = 0$:

Basta tomarmos os Axiomas Lógicos (de (i) até (v)) e os Axiomas Próprios (de (vi) até (xiv)) e provar que são válidos em S_∞.

(i) A é da forma $B \to (C \to B)$, i.e., $\neg B \vee (\neg C \vee B)$:

Pelo Lema A-1, temos uma prova para $\neg B \vee B$. Logo, por Dilution e Exchange, teremos uma prova para $\neg B \vee \neg C \vee B$.

(ii) A é da forma $(B \to (C \to D)) \to ((B \to C) \to (B \to D))$, i.e., $\neg(\neg B \vee \neg C \vee D) \vee \neg(\neg B \vee C) \vee (\neg B \vee D)$:

Pelo Lema A-1, temos uma prova para $\neg(\neg B \vee \neg C \vee D) \vee \neg B \vee \neg C \vee D$ e uma para $\neg(\neg B \vee C) \vee \neg B \vee C$.

Aplicando uma Cut, com C sendo a fórmula de corte, obtemos o desejado.

(iii) A é da forma $(\neg B \to \neg A) \to ((\neg B \to A) \to B))$, i.e., $\neg(\neg\neg B \vee \neg A) \vee \neg(\neg\neg B \vee A) \vee B$:

Pelo Lema A-1, temos uma prova para $\neg B \vee B$ e para $\neg A \vee A$.

Por Negation, temos $\neg\neg\neg B \vee B$ e, com uma Exchange, $\neg\neg A \vee \neg A$.

Por Dilution e Exchange, teremos $\neg\neg\neg B \vee \neg(\neg\neg B \vee A) \vee B$, $\neg\neg\neg B \vee B \vee \neg\neg A$ e $\neg A \vee B \vee \neg\neg A$.

Por DeMorgan e Exchange usando $\neg\neg\neg B \vee B \vee \neg\neg A$ e $\neg A \vee B \vee \neg\neg A$, teremos $\neg\neg A \vee \neg(\neg\neg B \vee A) \vee B$.

E, novamente, por DeMorgan usando $\neg\neg\neg B \vee \neg(\neg\neg B \vee A) \vee B$, obtemos o desejado.

(iv) A é da forma $\forall x B(x) \to B(t)$, i.e., $\neg\forall x B(x) \vee B(t)$, onde t é um termo fechado:

Pelo Lema A-1, temos $\neg B(t) \vee B(t)$, para qualquer termo fechado t.

Logo, por Quantification, obtemos o desejado.

(v) A é da forma $\forall x(B \to C) \to (B \to \forall x C)$, i.e., $\neg\forall x(\neg B \vee C) \vee \neg B \vee \forall x C$, onde x não ocorre livre em B:

Pelo Lema A-1, temos uma prova para $\neg C(n) \vee C(n)$, para qualquer n natural e uma para $\neg B \vee B$.

Logo, por Dilution e Exchange, temos $\neg C(n) \vee \neg B \vee C(n)$ e, por Dilution, Exchange e Negation, $\neg\neg B \vee \neg B \vee C(n)$, para qualquer n natural.

Por DeMorgan, então, $\neg(\neg B \vee C(n)) \vee \neg B \vee C(n)$, para qualquer n natural.

Logo, por Quantification, Exchange e Infinite Induction, obtemos $\neg\forall x(\neg B \vee C \vee \neg B \vee \forall x C$.

(vi) A é da forma $t_1 = t_2 \to (t_1 = t_3 \to t_2 = t_3)$, i.e., $t_1 \neq t_2 \vee t_1 \neq t_3 \vee t_2 = t_3$:

Pelo Lema A-2, temos uma prova para $s \neq t \vee s \neq t_3 \vee t = t_3$. Tome s como t_1 e t como t_2 e teremos uma prova para $t_1 \neq t_2 \vee t_1 \neq t_3 \vee t_2 = t_3$.

(vii) A é da forma $t_1 = t_2 \to t'_1 = t'_2$, i.e., $t_1 \neq t_2 \vee t'_1 = t'_2$:

I. Caso $t_1 = t_2$:

Então, $t'_1 = t'_2$ será uma fórmula atômica correta e, portanto, um axioma.

Logo, por Dilution, teremos $t_1 \neq t_2 \vee t'_1 = t'_2$.

II. Caso $t_1 \neq t_2$:

Então, $t_1 \neq t_2$ será uma fórmula correta e, portanto, um axioma.

Por Dilution e Exchange, teremos $t_1 \neq t_2 \vee t'_1 = t'_2$.

(viii) A é da forma $0 \neq t'$:

$0 \neq t'$ sempre será uma fórmula correta para qualquer termo fechado t.

Logo, $0 \neq t'$ é um axioma.

(ix) A é da forma $t'_1 = t'_2 \rightarrow t_1 = t_2$, i.e., $t'_1 \neq t'_2 \vee t_1 = t_2$:

I. Caso $t_1 \neq t_2$:

Então, $t'_1 \neq t'_2$ será uma fórmula atômica correta e, portanto, um axioma.

Logo, por Dilution e Exchange, teremos $t'_1 \neq t'_2 \vee t_1 = t_2$.

II. Caso $t_1 = t_2$:

Então, $t_1 = t_2$ será uma fórmula correta e, portanto, um axioma.

Por Dilution, teremos $t'_1 \neq t'_2 \vee t_1 = t_2$.

(x) A é da forma $t + 0 = t$:

$t + 0 = t$ será sempre uma fórmula correta para qualquer termo fechado t, logo, $t + 0 = t$ é um axioma.

(xi) A é da forma $t_1 + t'_2 = (t_1 + t_2)'$:

$t_1 + t'_2 = (t_1 + t_2)'$ será sempre uma fórmula correta para quaisquer termos fechados t_1 e t_2, logo, $t_1 + t'_2 = (t_1 + t_2)'$ é um axioma.

(xii) A é da forma $t \times 0 = 0$:

$t \times 0 = 0$ será sempre uma fórmula correta para qualquer termo fechado t, logo, $t \times 0 = 0$ é um axioma.

(xiii) A é da forma $t_1 \times t'_2 = (t_1 \times t_2) + t_2$:

$t_1 \times t'_2 = (t_1 \times t_2) + t_2$ será sempre uma fórmula correta para quaisquer termos fechados t_1 e t_2, logo, $t_1 \times t'_2 = (t_1 \times t_2) + t_2$ é um axioma.

(xiv) A é da forma $B(0) \rightarrow (\forall x\big(B(x) \rightarrow B(x')\big) \rightarrow \forall x B(x))$, i.e., $\neg B(0) \vee \neg\forall x\big(\neg B(x) \vee B(x')\big) \vee \forall x B(x)$:

Temos, pelo Lema A-1, Exchange e Dilution, que

$$\neg B(0) \vee \neg\forall x\big(\neg B(x) \vee B(x')\big) \vee B(0) \qquad (1)$$

Vamos provar, por indução, que $\neg B(0) \vee \ldots \vee \neg\big(\neg B(n) \vee B(n')\big) \vee B(n')$, para todo n natural.

I. Caso $n = 0$:

Pelo Lema A-1 teremos, por Dilution, $\neg B(0) \vee \neg B(1) \vee B(1)$ e, por Dilution, Negation e Exchange, $\neg B(0) \vee \neg\neg B(0) \vee B(1)$.

Por Exchange e DeMorgan, teremos $\neg B(0) \vee \neg(\neg B(0) \vee B(1)) \vee B(1)$.

II. Caso $(\neg B(0) \vee \neg(\neg B(0) \vee B(1)) \vee \ldots \vee \neg\big(\neg B(k) \vee B(k')\big) \vee B(k'))$, para todo $k < n$:

Por Dilution e Exchange, como $k + 1 = k'$, teremos que $\neg B(0) \vee \neg\big(\neg B(0) \vee B(1)\big) \vee \ldots \vee \neg\big(\neg B(k) \vee B(k')\big) \vee B\big((k+1)\big) \vee B((k+1)')$.

Então, por Negation e Exchange, $\neg B(0) \vee \neg\big(\neg B(0) \vee B(1)\big) \vee \ldots \vee \neg\big(\neg B(k) \vee B(k')\big) \vee \neg\neg B\big((k+1)\big) \vee B((k+1)')$.

Temos, pelo Lema A-1 e por Dilution, que $\neg B(0) \vee \neg\big(\neg B(0) \vee B(1)\big) \vee \ldots \vee \neg\big(\neg B(k) \vee B(k')\big) \vee \neg B((k+1)') \vee B((k+1)')$.

Logo, por DeMorgan, $\neg B(0) \vee \neg\big(\neg B(0) \vee B(1)\big) \vee \ldots \vee \neg\big(\neg B(k) \vee$ $Bk' \vee \neg(\neg Bk{+}1 \vee Bk{+}1') \vee B(k{+}1)'$.

Logo, por indução, $\forall n \in \mathbb{N}(\neg B(0) \vee \ldots \vee \neg\big(\neg B(n) \vee B(n')\big) \vee B(n'))$.

Então, por Quantification $n+1$ vezes, teremos $\forall n \in \mathbb{N}\ (\neg B(0) \vee \neg\forall x\big(\neg B(x) \vee B(x')\big) \vee B(n')$, para todo n natural.

Logo, usando a fórmula (1), teremos, por Infinite Induction e Exchange, que $\neg B(0) \vee \neg\forall x\big(\neg B(x) \vee B(x')\big) \vee \forall x B(x)$.

b) Caso $\forall A \forall \beta < \alpha(\vdash_S A \rightarrow \ \vdash_{S_\infty} A)$, se $\vdash_S A$ tiver ordinalidade β:

Basta provar que o Modus Ponens e a Generalization são válidos em S_∞.

Suponha que $\vdash_S C$ tenha ordinalidade α.

(i) Caso C tenha surgido por Modus Ponens:

Temos que existe fórmula B tal que $\vdash_S B$ e $\vdash_S (B \rightarrow C)$

Pela hipótese indutiva, teremos que $\vdash_{S_\infty} (\neg B \vee C)$ e $\vdash_{S_\infty} B$, pois tanto $\vdash_S B$ quanto $\vdash_S (B \rightarrow C)$ têm ordinalidade menor que α.

Por Cut, teremos, então, que $\vdash_{S_\infty} C$.

(ii) Caso C tenha surgido por Generalization:

Temos que existe fórmula B tal que $\vdash_S B$, onde C é da forma $\forall x B$.

Pela hipótese indutiva, temos que $\vdash_{S_\infty} B$.

I. Caso x não ocorra em B:

Temos que $\vdash_{S_\infty} B$, $\vdash_{S_\infty} B$, ..., $\vdash_{S_\infty} B$,..., para todo n natural.

Logo, por Infinite Induction, $\vdash_{S_\infty} \forall x B$.

II. Caso x não ocorra livre em B:

Temos que $\vdash_{S_\infty} B$, $\vdash_{S_\infty} B$, ..., $\vdash_{S_\infty} B$,..., para todo n natural.

Logo, por Infinite Induction, $\vdash_{S_\infty} \forall x B$.

III. Caso x ocorra livre em B:

Temos que $\vdash_S B(n)$ com ordinalidade $\alpha - 1$, para todo n natural. Pois, se $\vdash_S B(x)$, como os axiomas de S são fechados e como não existe axioma de S que leve fórmulas fechadas em variáveis livres, então $\vdash_S \forall x B(x)$ com ordinalidade $\leq \alpha - 2$.

Logo, por Infinite Induction, $\vdash_{S_\infty} \forall x B(x)$.

Então, $\vdash_{S_\infty} C$.

Por indução, demonstramos que todo teorema de S também é teorema de S_∞. ■

1.7 Lema A-4

Se S_∞ é consistente, então S é consistente.

- Demonstração: (por contradição)

Suponha S inconsistente.

Teremos que $\vdash_S A$ e $\vdash_S \neg A$. Daqui, pelo Lema A-3, já se conclui que, para toda fórmula fechada B, $\vdash_{S_\infty} B$ e $\vdash_{S_\infty} \neg B$,pois teremos que $\vdash_S B$, para toda fórmula fechada B.

Em particular, $0 \neq 0$ é teorema de S.

Pelo Lema A-3, então $0 \neq 0$ é teorema de S_∞.

Por Dilution, para qualquer fórmula fechada A, $A \vee (0 \neq 0)$ é teorema de S_∞.

Como $0 = 0$ é teorema de S_∞, teremos que, por Exchange e Cut, A é teorema de S_∞.

Logo, para toda fórmula fechada B, $\vdash_{S_\infty} B$ e $\vdash_{S_\infty} \neg B$.

Então, S_∞ é inconsistente.

Logo, por redução ao absurdo, provamos o que queríamos. ■

1.8 Lema A-5

As regras de inferência DeMorgan, Negation e Infinite Induction são invertíveis, onde o grau e a ordinalidade são menores ou iguais.

- Demonstração:

a) DeMorgan:

Temos que $\vdash_{S_\infty} \neg(B \vee C) \vee D$.

Pelas regras de inferência de S_∞, $\neg(B \vee C)$ só pode ter surgido por Dilution ou DeMorgan numa fórmula da forma $\neg(B \vee C) \vee E$.

(i) Se $\neg(B \vee C) \vee E$ é conclusão de uma Dilution:

Podemos substituir livremente, como $\neg B$ é sempre uma fórmula fechada, $\neg(B \vee C)$ por $\neg B$ na história de $\neg(B \vee C)$ em $\neg(B \vee C) \vee D$.

Logo, $\vdash_{S_\infty} \neg B \vee D$.

Analogamente, teremos $\vdash_{S_\infty} \neg C \vee D$.

Nos dois casos, mantemos a mesma ordinalidade de $\neg(B \vee C) \vee D$.

(ii) Se $\neg(B \vee C) \vee E$ é conclusão de uma DeMorgan:

Então, $\vdash_{S_\infty} \neg B \vee E$ e $\vdash_{S_\infty} \neg C \vee E$, pois $\neg B \vee E$ e $\neg C \vee E$ são as premissas de $\neg(B \vee C) \vee E$.

Substituindo $\neg(B \vee C)$ por $\neg B$ na história de $\neg(B \vee C)$ em $\neg(B \vee C) \vee D$ a partir de $\neg(B \vee C) \vee E$ e colando a árvore de $\neg B \vee E$ no lugar da árvore de $\neg(B \vee C \vee E$, obtemos uma prova para $\neg B \vee D$.

Analogamente, teremos $\vdash_{S_\infty} \neg C \vee D$.

Em ambos os casos, diminuímos a ordinalidade em um (justamente a regra DeMorgan que foi eliminada).

b) Negation:

Temos que $\vdash_{S_\infty} \neg\neg B \vee D$.

De forma análoga ao item a), $\neg\neg B$ só pode ter surgido por Negation ou por Dilution numa fórmula da forma $\neg\neg B \vee E$.

(i) Se $\neg\neg B \vee E$ é conclusão de uma Dilution:

Analogamente ao caso (i) no item a), teremos $\vdash_{S_\infty} B \vee D$, com mesma ordinalidade de $\neg\neg B \vee D$.

(ii) Se $\neg\neg B \vee E$ é conclusão de uma Negation:

Analogamente ao caso (ii) no item a), teremos $\vdash_{S_\infty} B \vee D$, com a ordinalidade diminuída de um.

c) Infinite Induction:

Temos que $\vdash_{S_\infty} \forall x B(x) \vee D$.

De forma análoga ao item a), $\forall x B(x)$ só pode ter surgido por Infinite Induction ou por Dilution numa fórmula da forma $\forall x B(x) \vee E$.

(i) Se $\forall x B(x) \vee E$ é conclusão de uma Dilution:

Analogamente ao caso (i) no item a), teremos $\vdash_{S_\infty} B(n) \vee D$, para um número natural n qualquer, com mesma ordinalidade de $\forall x B(x) \vee D$.

(ii) Se $\neg\neg B \vee E$ é conclusão de uma Infinite Induction:

Analogamente ao caso (ii) no item a), teremos $\vdash_{S_\infty} B(n) \vee D$, para um número natural n qualquer, com a ordinalidade diminuída de um. ■

1.9 Lema B-1

Dada qualquer wff A com grau $m \geq 0$ e um número finito de quantificadores e conectivos tal que $\vdash_{S_\infty} A$, podemos obter uma árvore de A com grau zero e mesma ordinalidade.

- Demonstração:

Seja A uma wff de grau m, onde m é um número ordinal, e ordinalidade α.

- Caso $m = 0$: Nada temos a fazer.

- Caso $m = 1$:

Seja $\frac{C \vee B \quad \neg B \vee D}{C \vee D}$ tal Cut, onde $C \vee B$, $\neg B \vee D$ e $C \vee D$ têm ordinalidade α_1, $\alpha_2\, e\, \alpha_3$, respectivamente. (1)

(I) Caso B seja atômico:

Temos que todas as fórmulas na Árvore de A são fechadas.

Logo: B for correto $\Longrightarrow$ B é um axioma $\Longrightarrow$ B surgiu de um Ponto Inicial ou por Dilution. Se B for incorreto, então B surgiu por Dilution, pois não é axioma e não pode ser Ponto Inicial.

Logo, de qualquer forma, B surgiu por um Ponto Inicial ou por Dilution.

Temos que: B surgiu por um Ponto Inicial $\Longrightarrow$ $\neg B$ não é axioma $\Longrightarrow$ $\neg B$ surgiu por Dilution.

(i) B surgiu por Dilution:

Tome a História de B na Árvore de $C \vee B$.

Como B surgiu por Dilution, podemos substituir B por D na História de B e obter, da mesma forma, $C \vee D$ com grau zero e com ordinalidade $\alpha_1 < \alpha$.

(ii) B surgiu de um Ponto Inicial:

Então, $\neg B$ surgiu por Dilution.

Analogamente a (i), obteremos uma prova de $C \vee D$ com ordinalidade $\alpha_2 < \alpha$ e grau zero.

(II) Caso $B = \neg E$:

Temos, então, que $\neg B = \neg\neg E$.

Tome a História de $\neg\neg E$ na Árvore de $\neg\neg E \vee D$. Logo, $\neg\neg E$ surgiu por Dilution ou por Negation.

(i) $\neg\neg E$ surgiu por Dilution:

Analogamente a (I)(i), teremos uma prova para $C \vee D$ com grau zero e ordinalidade α_2.

(ii) $\neg\neg E$ surgiu por Negation:

Temos que $\neg\neg E$ surgiu da Regra $\frac{E \vee D_1}{\neg\neg E \vee D_1}$ na Árvore de $\neg\neg E \vee D$, que tem ordinalidade α_2.

Teremos, pelo Lema A-5, que existe uma prova para $E \vee D$, com ordinalidade $\leq \alpha_2$.

Logo, a menos de 3 regras Exchange, teremos uma prova para $C \vee D$, com ordinalidade α_3, derivada do Cut $\frac{D \vee E \quad \neg E \vee C}{D \vee C}$. Então, voltamos ao caso $m = 1$.

(III) Caso $B = E \vee F$:

Temos que o Cut será da forma $\frac{C \vee E \vee F \quad \neg(E \vee F) \vee D}{C \vee D}$.

Teremos que $\neg(E \vee F)$ surgiu por Dilution ou por DeMorgan.

(i) Por Dilution:

Analogamente a (I)(i), substitua $\neg(E \vee F)$ por C e teremos uma prova para $C \vee D$ com grau zero e ordinalidade α_2.

(ii) Por DeMorgan:

Temos que $\neg(E \vee F)$ surgiu da Regra $\frac{\neg E \vee D_1 \quad \neg F \vee D_1}{\neg(E \vee F) \vee D_1}$. Excluindo essa regra e substituindo $\neg E$ e $\neg F$ na História de $\neg(E \vee F)$ a partir de $\neg(E \vee F) \vee D_1$, obtemos uma prova para $\neg E \vee D$ e $\neg F \vee D$, respectivamente, e com ordinalidades α_2 (apesar de termos diminuído 1 ao retirarmos a regra DeMorgan podemos compensá-la aplicando uma Dilution e, depois, uma Consolidation).

(a) Obtemos, então, uma prova de $C \vee E \vee D$ através do Cut $\frac{C \vee E \vee F \quad \neg F \vee D}{C \vee E \vee D}$, com grau 1 e ordinalidade α_3. Então, voltamos ao caso $m = 1$.

(b) Resolvido (a), obtemos, então, uma prova de $C \vee D$, com grau 1 e ordinalidade $\alpha_4 = \alpha_3{}' +_o 1$, onde $\alpha_3{}'$ é a ordinalidade de $C \vee E \vee D$ nessa nova Árvore de grau zero, através do Cut $\frac{C \vee D \vee E \quad \neg E \vee D}{C \vee D \vee D}$, a menos de uma Exchange e uma Consolidation. Então, novamente, voltamos ao caso $m = 1$. (obs.: o caso (b) só entra quando (a) for resolvido, ou seja, antes de (b) sempre teve um caso (a) no qual foi possível obter um prova de $C \vee E \vee D$ com grau zero e ordinalidade α_3).

(IV) Caso $B = \forall x E(x)$:

Temos que $\forall x E(x)$ surgiu por Dilution ou por Infinite Induction, já que não pode ser um axioma. Da mesma forma, $\neg \forall x E(x)$ surgiu por Dilution ou por Quantification Rule.

(i) $\forall x E(x)$ surgiu por Dilution:

Analogamente a (I)(i), teremos uma prova para $C \vee D$ com grau zero e ordinalidade $\alpha_1 < \alpha$.

(ii) $\forall x E(x)$ surgiu por Infinite Induction:

Temos, pelo Lema A-5, que existe uma prova para $C \vee E(t_i)$, para toda constante t_i, a menos de uma Exchange, com ordinalidade α_1.

(a) Se $\neg \forall x E(x)$ surgiu por Dilution:

Analogamente a (I)(i), obtemos uma prova para $C \vee D$ com grau zero e ordinalidade α_2.

(b) Se $\neg \forall x E(x)$ surgiu por Quantification Rule:

Temos que $\neg \forall x E(x)$ surgiu da regra $\frac{\neg E(t_{i_0}) \vee D_1}{\neg \forall x E(x) \vee D_1}$, para alguma constante t_{i_0}.

Retirando essa regra e substituindo $\neg\forall x E(x)$ por $\neg E(t_{i_0})$ na História de $\neg\forall x E(x)$ em $\neg\forall x E(x) \vee D$, obtemos uma prova para $\neg E(t_{i_0}) \vee D$ com grau zero e ordinalidade α_2 (compensando a Quantification Rule excluída por uma Dilution e Consolidation).

Teremos, então, uma prova para $C \vee D$ pelo Cut $\frac{C \vee E(t_{i_0}) \quad \neg E(t_{i_0}) \vee D}{C \vee D}$, com grau 1 e ordinalidade α_3. Então, voltamos ao caso $m = 1$.

Exaurido todos os casos, podemos continuar a prova.

Temos que qualquer fórmula possui finitos quantificadores e conectivos.

Suponha que caímos numa sequência infinita com os casos (II)(ii), (III)(ii)(a), (III)(ii)(b) ou (IV)(ii)(b). Ou seja, por exemplo, se em (III)(ii)(a) caímos em (II)(ii), em (II)(ii) caímos em (IV)(ii)(b), em (IV)(ii)(b) caímos em (II)(ii) e assim por diante.

Então teremos que $C \vee D$ possui infinitos quantificadores e conectivos.

Mas, por hipótese, chegamos a uma contradição.

Logo, essa sequência só pode ser finita.

Como todos os casos estão contemplados em (I), (II), (III) e (IV), qualquer sequência de casos começando por (II)(ii), (III)(ii)(a) ou (IV)(ii)(b) terminará em algum outro caso diferente destes ou de (III)(ii)(b).

Para qualquer caso <u>diferente</u> de (II)(ii), (III)(ii)(a), (III)(ii)(b) ou (IV)(ii)(b) podemos obter uma prova para $C \vee D$ com grau zero e com ordinalidade α_2 ou α_1.

Então, como essa sequência só pode ser finita e todos os casos estão contemplados, teremos que sempre poderemos obter uma prova para $C \vee D$ com grau zero e com ordinalidade α_2 ou α_1.

Para qualquer prova de $C \vee D$ com ordinalidade $\beta < \alpha_3$, podemos aplicar Dilution e Consolidation um número finito de vezes e obter a mesma wff $C \vee D$ com ordinalidade α_3.

Então, sempre poderemos obter uma prova para $C \vee D$ com grau zero e com ordinalidade α_3.

Por fim, substituindo a primeira Árvore de $C \vee D$ pela nova de grau zero e mesma ordinalidade na Árvore de A, podemos obter uma prova para A com grau zero e ordinalidade α.

- Caso válido para qualquer prova com grau $< m$:

Note que m pode ser um ordinal limite ou um ordinal sucessor.

Tome a Árvore de A com grau m.

Substitua nela qualquer Árvore de grau $m_i < m$ que termine em um Cut por uma com grau zero e mesma ordinalidade e que prove o mesmo teorema de sua correlata com grau m_i. Note que a quantidade de m_i´s pode ser infinita, sendo que, mesmo assim, a substituição é sempre possível pela hipótese indutiva.

Se m for um ordinal sucessor, é fácil ver que podemos obter uma nova Árvore para A com grau 1 e com ordinalidade α.

Se m for um ordinal limite, fazendo todas as substituições possíveis, pela hipótese indutiva, ainda restará somente um Cut na Árvore de A. Tal Cut é, justamente, aquele em que o grau de qualquer premissa sua é m_i e que a soma ordinal de todos os graus de cada premissa e de todas as árvores à esquerda da conclusão é m.

Em ambos os casos, pela hipótese indutiva, podemos obter uma prova para A com grau zero e ordinalidade α.

- Logo, por indução transfinita, podemos obter uma prova para A com grau zero e ordinalidade α. ■

1.10 Proposição A-8

S_∞ é Consistente.

- Demonstração:

Temos que se S_∞ for inconsistente, então S_∞ demonstra qualquer fórmula.

Suponha que $S_\infty \vdash 0 \neq 0$.

Pelo Lema B-1, tome a árvore de $0 \neq 0$ de grau zero e mesma ordinalidade.

Volte ao item 1.1 e olhe as regras de inferência de S_∞.

Suponha que $0 \neq 0$ não surgiu de um ponto inicial.

Então, $0 \neq 0$ só pode ter surgido de um Cut.

Mas a demonstração tem grau zero.

Chega-se a uma contradição.

Logo, $0 \neq 0$ surgiu de um ponto inicial. Ou seja, é um axioma.

Mas $0 \neq 0$ não é uma fórmula correta, logo, não é um axioma de S_∞.

Então, por redução ao absurdo, $S_\infty \nvdash 0 \neq 0$ e, por isso, S_∞ é consistente. ■

1.11 Corolário B-2

S é consistente.

- Demonstração:

Diretamente do Lema A-4 e A-8. ■

Capítulo 2: A consistência por extensões da aritmética

Nesse capítulo discutiremos outra forma de provar a consistência da aritmética (PA). Tal ideia surge das questões abertas por Gödel com seus teoremas de incompletude. Aparentemente, a primeira formalização dos *princípios de reflexão* foi feita em 1937 por John Barkley Rosser.[1] A partir deles constrói-se uma extensão de PA que prova que PA é consistente. Além disso, uma classe de sentenças indemonstráveis em PA torna-se demonstrável nesses novos sistemas.

A sentença básica sobre a qual vamos nos basear é da forma "Se a fórmula φ é demonstrável na teoria T, então a fórmula φ é verdadeira" – a rigor, este é o *princípio de reflexão local*. Ela pode ser representada formalmente na linguagem de PA, expressando a própria Corretude. Vale lembrar que, de forma geral, um sistema é correto se tudo que for demonstrável nele for verdadeiro se seus axiomas forem verdadeiros - e o cálculo dedutivo é provadamente correto na lógica de primeira ordem. O propósito inicial do programa de Hilbert já se calcava por sobre a equivalência entre Corretude e Consistência. De fato, essa equivalência é verdadeira na teoria dos modelos.[2] Portanto, é de se esperar que adicionando a Corretude à aritmética se pudesse provar, a partir de então, sua Consistência.

Sabe-se, por corolários dos teoremas de incompletude, que para diversas fórmulas φ essa sentença não é demonstrável em PA. Logo, adicionando-as, teremos um ganho significativo em relação ao sistema anterior. E é basicamente isto que os princípios de reflexão fazem.

Serão apresentados alguns resultados básicos sobre os princípios de reflexão e como provamos a consistência de PA a partir deles. Enunciaremos também dois resultados

---

[1] BEKLEMISHEV, L. D. Reflection principles and provability. **Russian Mathematical Surveys**, v. 60:2, p. 197–268, 11 janeiro 2005.
[2] ENDERTON, H. **A mathematical introduction to logic**. 2ª. ed. Boston, MA: Academic Press, 2001. ISBN 978-0-12-238452-3. p. 124.

sobre o *princípio combinatorial de Paris-Harrington* para mostrar um caso de uma sentença verdadeira e indemonstrável em PA da qual se consegue a consistência e que implica num caso restrito do princípio de reflexão uniforme. Usarei a notação e resultados apresentados no *Handbook of Mathematical Logic*.[3] Mas um embasamento maior pode ser obtido no *Introduction to Mathematical Logic*.[4] Algumas demonstrações aqui contidas estão um pouco diferentes e outras estão omitidas no texto originário. Para certos teoremas, como poderão constatar, as demonstrações só estão indicadas, pois para uma prova formal seriam necessários muito mais definições e teoremas paralelos. E, no presente texto, queremos mostrar apenas como se pode chegar à consistência por extensões de PA.

Vamos considerar S, a teoria formal dos números, e a teoria T como sendo consistentes, pois é fácil ver que um sistema inconsistente demonstra qualquer fórmula. Dado o capítulo anterior, essa hipótese não é infundada[5]. Somente os resultados – e o leitor é convidado a verificá-los - a seguir que utilizam o segundo teorema de incompletude de Gödel em suas demonstrações necessitam dessa hipótese para serem válidos, por isso, tomaremos por conveniência omiti-la a partir daqui.

2.1 Definições

2.1.1 Seja S a teoria formal dos números (PA).[6]

S é a teoria na linguagem com as operações usuais de soma, sucessor e produto e quantificador $\forall$. Neste trabalho, usaremos, além dos conectivos $\neg$ e $\rightarrow$, como é definido na literatura indicada, o $\wedge$ e $\vee$. Note que esses quatro podem ser reduzidos aos dois primeiros sem perda de generalidade. Assim como, vale a pena lembrar que o quantificador $\exists$ também pode ser obtido a partir do $\forall$ (vide capítulo 1).

[3] BARWISE, J. (Ed.). **Handbook of Mathematical Logic**. Amsterdam: Elsivier Science Publisher B.V., 1977. ISBN 0444863885.
[4] MENDELSON, E. **Introduction to Mathematical Logic**. 2ª. ed. Princeton, New Jersey: D. VAN NOSTRAND COMPANY, INC., 1964.
[5] Para mais questões sobre esse pressuposto ver capítulo 3.
[6] MENDELSON, op. cit., p. 102.

2.1.2 Seja T uma teoria finitamente axiomatizável na mesma linguagem de S tal que os axiomas de S estão contidos nos de T.[7]

2.1.3 Dizemos que uma função f é primitiva recursiva se ela for gerada por uma composição das seguintes funções:

(i) Zero: $f(x) = 0$;
(ii) Sucessor: $f(x) = x + 1$;
(iii) Projeção: $f(x_1, x_2, \dots, x_n) = x_i$, onde n é um número finito e $1 \leq i \leq n$;
(iv) Composição: $f(\boldsymbol{x}) = g(h_1(\boldsymbol{x}), h_2(\boldsymbol{x}), \dots, h_n(\boldsymbol{x}))$, onde n é um número finito;
(v) Recursão: $\begin{cases} f(0, \boldsymbol{x}) = g(x) \\ f(y + 1, \boldsymbol{x}) = h(f(y, \boldsymbol{x}), y, \boldsymbol{x}) \end{cases}$;

A letra x em negrito simboliza um vetor de tamanho $n \geq 1$ da forma $(x_1, x_2, \dots, x_n)$.

Se, além dessas funções, também usarmos a função $f(\boldsymbol{x}) = y, se\ g(\boldsymbol{x}, y) = 0 \wedge \forall z < y(g(\boldsymbol{x}, z) \neq 0)$, simbolizada comumente na literatura por $f(\boldsymbol{x}) = \mu y(g(\boldsymbol{x}, y) = 0)$, para compor uma função podemos gerar qualquer função recursiva. Essa função de mínimo é chamada de Operador μ e é ela que diferencia as funções primitivas recursivas das recursivas.[8]

2.1.4 Um conjunto finito H é dito *relativamente grande* se, e somente se, $card(H) \geq \min(H)$ (ou seja, se o tamanho do conjunto H é maior que seu elemento mínimo).

É justamente essa parte que tornará o princípio combinatorial de Paris-Harrington indemonstrável dentro de S.

2.1.5 $Pr_T[A] \coloneqq \exists n Prov_T(n, [A])$, onde A é uma wff (fórmula bem formada), T é uma teoria e $[A]$ é o número de Gödel da fórmula A.[9]

Podemos dizer que $Prov_T(x, y)$ representa, na linguagem de S, a função primitiva recursiva que leva o número de Gödel, representado por x, de uma prova – aqui prova tem o

---

[7] BARWISE, op. cit., p.830.
[8] MENDELSON, op. cit., p.120.
[9] MENDELSON, op. cit., p. 141 e BARWISE, op. cit. p. 826.

sentido clássico que estamos acostumados, isto é, pelo cálculo dedutivo - de uma wff φ na linguagem de T a partir dos axiomas de T, no número representado por y, onde y é o número de Gödel da fórmula φ. Portanto, $Pr_T[\varphi]$ quer dizer, formalmente (dentro da linguagem de S), que φ é demonstrável dedutivamente a partir dos axiomas de T.

2.1.6 $Prov_T(n, [\varphi(\dot{x})]) := \forall y(\varphi_s([\varphi], x, y) \rightarrow Prov_T(n, y))$, onde φ é uma wff e $\varphi_s([\varphi], x, y)$ representa, na linguagem de S, a função primitiva recursiva que:[10]

(i) Calcula o número de Gödel da fórmula φ;

(ii) Calcula o número de Gödel y da fórmula $\varphi(v_1)_x^{v_1}$, isto é, o número de Gödel de φ quando x estiver no lugar da primeira variável livre v_1 de φ. Se φ não tiver variável livre alguma, então $y = [\varphi]$;

Logo, $Prov_T(n, [\varphi(\dot{x})])$ é uma wff que tem x e n como variáveis livres, já que $[\varphi]$ é uma constante para cada fórmula φ.

Analogamente, teremos que $Pr_T[\varphi(\dot{x})] \coloneqq \exists n Prov_T(n, [\varphi(\dot{x})])$.

2.1.7 $Con(T) := \neg Pr_T[\neg(\varphi \rightarrow \varphi)]$, onde φ pode ser qualquer fórmula.

Esta é a expressão na linguagem de S que representa a consistência da teoria T. Com o item 2.3.(iii) é possível mostrar que, para qualquer φ, essas sentenças são equivalentes. Portanto, não perdemos rigor ao representarmos a consistência apenas por $Con(T)$, visto que ela não está em função de nenhuma fórmula φ em particular.

2.2 Notação

Sejam e, k, r e M números naturais.

Denotamos que, para toda partição $P: [M]^e \rightarrow r$, existe um conjunto relativamente grande $H \subseteq M$ Homogêneo por P e de cardinalidade, no mínimo, k, por $M \underset{*}{\rightarrow} (k)_r^e$.

---

[10] BARWISE, J. op. cit., p. 837.

É possível mostrar que $M \underset{*}{\rightarrow} (k)_r^e$ pode ser representado por uma fórmula (primitiva recursiva) na linguagem de S. Nesse caso, denotaremos por "$\mathrm{M} \underset{*}{\rightarrow} (\mathrm{k})_{\mathrm{r}}^{\mathrm{e}}$".

2.3 Teorema (Condições de Derivabilidade de Löb)

Sejam A e B quaisquer wff na linguagem de T.
Então:

(i) $T \vdash A \Rightarrow T \vdash Pr_T[A]$;
(ii) $S \vdash Pr_T[A] \rightarrow Pr_T[Pr_T[A]]$;
(iii) $S \vdash Pr_T[A] \wedge Pr_T[A \rightarrow B] \rightarrow Pr_T[B]$;

2.3.1 Demonstração:

A demonstração detalhada pode ser encontrada no *Handbook of Mathematical Logic*[11] nas páginas 826 até a 840. A condição (iii) pode ser demonstrada pela definição de $Prov_T(x, y)$. A (i) do fato de que o cálculo dedutivo se dá sempre em passos finitos. E a (ii) se baseia em demonstrar que a fórmula $Prov_T(x, y)$ representa uma função primitiva recursiva e que, por isso, $S \vdash Prov_T(x, y) \rightarrow Pr_T[Prov_T(\dot{x}, \dot{y})]$. Para, então, juntamente com a condição (iii), chegarmos ao resultado de que $S \vdash Pr_T[A] \rightarrow Pr_T[Pr_T[A]]$.

2.4 Teorema (O teorema de Löb)

Seja φ uma sentença na linguagem de T.

---

[11] BARWISE, J. (Ed.). **Handbook of Mathematical Logic**. Amsterdam: Elsivier Science Publisher B.V., 1977. ISBN 0444863885.

Então, $T \vdash Pr_T[\varphi] \rightarrow \varphi$ se, e somente se, $T \vdash \varphi$.

2.4.1 Demonstração:

a) Caso $T \vdash \varphi \Rightarrow T \vdash Pr_T[\varphi] \rightarrow \varphi$:

Por tautologia é fácil verificar que $T \vdash \varphi \rightarrow (Pr_T[\varphi] \rightarrow \varphi)$.

b) Caso $T \vdash Pr_T[\varphi] \rightarrow \varphi \Rightarrow T \vdash \varphi$:

Por hipótese, teremos que $T \vdash \neg\varphi \rightarrow \neg Pr_T[\varphi]$.

Temos que $T + \neg\varphi \vdash \neg Pr_T[\varphi] \wedge (Pr_T[\neg\varphi \rightarrow \neg(\varphi \rightarrow \varphi)] \rightarrow Pr_T[\varphi])$, por 2.3.(iii). Observe que a última parte da sentença anterior é justamente a formalização na linguagem de S do *reductio ad absurdum*.

Então, $T + \neg\varphi \vdash \neg Pr_T[\varphi] \rightarrow \neg Pr_T[\neg\varphi \rightarrow \neg(\varphi \rightarrow \varphi)]$.

Logo, como $T \vdash \neg\varphi \rightarrow \neg Pr_T[\varphi]$, então $T + \neg\varphi \vdash \neg Pr_T[\neg\varphi \rightarrow \neg(\varphi \rightarrow \varphi)]$. Ou ainda, $T + \neg\varphi \vdash Con(T + \neg\varphi)$.[12]

Suponha que $T \nvdash \varphi$.

Então, $T + \neg\varphi$ será consistente, pois T é consistente por suposição.

Pelo segundo teorema de incompletude de Gödel, teremos que, como $T + \neg\varphi$ é consistente, $T + \neg\varphi \nvdash Con(T + \neg\varphi)$.[13]

E, com isso, chegamos a um absurdo.

Logo, $T \vdash \varphi$. ■

2.4.2 Discussão:

Pelo primeiro teorema de incompletude (na verdade, por um corolário facilmente obtido) podemos notar que para enumeráveis sentenças φ_i teremos que $T \nvdash Pr_T[\varphi_i] \rightarrow \varphi_i$. E que estas são justamente as fórmulas que T não demonstra. Portanto, adicionar sentenças da forma $Pr_T[\varphi] \rightarrow \varphi$ a T tem uma relação com adicionar sentenças φ a T. Veremos adiante que é exatamente isso que o princípio de reflexão faz.

---

[12] BARWISE, J. op. cit., p. 828.
[13] Idem, p. 828.

2.5 Os princípios de reflexão

2.5.1 O princípio de reflexão local:

$Rfn(T) := Pr_T[\varphi] \rightarrow \varphi$, onde φ é uma sentença.

2.5.2 O princípio de reflexão uniforme:

$RFN(T) := \forall x Pr_T[\varphi(\dot{x})] \rightarrow \forall x \varphi(x)$, onde φ tem somente x como variável livre.

2.5.3 Discussão:

Tanto $Rfn(T)$ quanto $RFN(T)$ são esquemas de fórmulas (ou seja, conjuntos de fórmulas com uma regra de formação particular). Isto é, simbolizam uma quantidade enumerável de fórmulas da forma como descrita nos itens 2.5.1 e 2.5.2. Por exemplo:

$$
\begin{array}{ll}
RFN(T): & \forall x Pr_T[0 = 0 \wedge \dot{x} = \dot{x}] \rightarrow \forall x(0 = 0 \wedge x = x) \\
 & \forall x Pr_T[0 \neq 0 \wedge \dot{x} = \dot{x}] \rightarrow \forall x(0 \neq 0 \wedge x = x) \\
 & \forall x Pr_T[\exists y(\dot{x} = y + 1)] \rightarrow \forall x(\exists y(x = y + 1)) \\
 & \vdots
\end{array}
$$

Por isso, faz sentido denotarmos uma teoria por $T + RFN(T)$, constituída da teoria T mais todas as fórmulas no esquema $RFN(T)$. Como mencionado no item 2.4.2, $T + RFN(T)$ é uma teoria mais poderosa que T.

2.6 Teorema

$S \vdash RFN(T) \rightarrow Rfn(T)$.

2.6.1 Demonstração:

Seja φ uma sentença qualquer.

Suponha que $S \vdash Pr_T[\varphi]$.

Por 2.3.(iii), teremos que $S \vdash Pr_T[\varphi] \rightarrow Pr_T[\forall x(\varphi \wedge x = x)]$, onde x é uma variável que não ocorre em φ.

Por 2.1.6, $S \vdash Pr_T[\forall x(\varphi \wedge x = x)] \rightarrow \forall x Pr_T[(\varphi \wedge \dot{x} = \dot{x})]$.[14] Basta lembrar que S consegue decidir sempre se uma fórmula é um axioma lógico ou não.

Por $RFN(T)$, chegamos a $S \vdash \forall x Pr_T[(\varphi \wedge \dot{x} = \dot{x})] \rightarrow \forall x(\varphi \wedge x = x)$.

Como $S \vdash \forall x(\varphi \wedge x = x) \leftrightarrow \varphi$, então $S \vdash Pr_T[\varphi] \rightarrow \varphi$. ∎

2.7 Hierarquia Aritmética

Dizemos que uma fórmula que representa uma função primitiva recursiva na linguagem de S é uma fórmula primitiva recursiva, ou ainda, uma fórmula PR.

2.7.1 Definição:[15]

Dizemos que uma fórmula φ é $\Sigma_\mathrm{n}(\Pi_\mathrm{n})$ se φ é da forma $Q_1 x_1 \ldots Q_n x_n \psi$, onde ψ é uma fórmula primitiva recursiva e $Q_i = \begin{cases} \exists(\forall), \text{se } i \text{ for ímpar} \\ \forall(\exists), se\ i\ for\ par \end{cases}$.

2.7.2 Definição:

$RFN_{\Sigma_\mathrm{n}}(T) := \forall x Pr_T[\varphi(\dot{x})] \rightarrow \forall x \varphi(x)$, onde φ tem somente x como variável livre e φ é uma fórmula Σ_n.

Analogamente, podemos definir $RFN_{\Pi_\mathrm{n}}(T)$, $Rfn_{\Sigma_\mathrm{n}}(T)$ ou $Rfn_{\Pi_\mathrm{n}}(T)$.

2.8 Teorema

---

[14]BEKLEMISHEV, L. D. Reflection principles and provability. **Russian Mathematical Surveys**, v. 60:2, p. 197–268, 11 Janeiro 2005. p. 205 ou BARWISE, J., op. cit., p. 849.
[15] BARWISE, op. cit. p. 843.

$$S \vdash RFN_{\Sigma_1}(T) \rightarrow Rfn_{\Sigma_1}(T).$$

2.8.1 Demonstração:

A demonstração é análoga à do teorema 2.5.

Seja φ uma sentença Σ_1 da forma $\exists y \psi(y)$, onde ψ representa uma função primitiva recursiva.

Suponha que $S \vdash Pr_T[\varphi]$.

Por 2.3.(iii), teremos que $S \vdash Pr_T[\varphi] \rightarrow Pr_T[\forall x \varphi]$, onde x é uma variável que não ocorre em φ.

Por 2.1.6, $S \vdash Pr_T[\forall x(\varphi)] \rightarrow \forall x Pr_T[\varphi(\dot{x})]$.

Por $RFN_{\Sigma_1}(T)$, chegamos a $S \vdash \forall x Pr_T[\varphi(\dot{x})] \rightarrow \forall x(\varphi)$.

Como $S \vdash \forall x(\varphi) \leftrightarrow \varphi$, então $S \vdash Pr_T[\varphi] \rightarrow \varphi$. ■

2.9 Teorema

$$S \vdash Rfn(T) \rightarrow Rfn_{\Sigma_1}(T).$$

2.9.1 A demonstração é direta e, por isso, será omitida.

2.10 Teorema

$$S \vdash Rfn_{\Sigma_1}(T) \rightarrow Con(T).$$

2.10.1 Demonstração:

Seja φ uma sentença Σ_1 da forma $\exists y\psi(y)$, onde ψ representa a função primitiva recursiva $y = y + 1$.

Temos que $S + Rfn_{\Sigma_1}(T) \vdash Pr_T[\exists y(y = y + 1)] \to \exists y(y = y + 1)$.

Temos, também, que $S \vdash \neg\exists y(y = y + 1)$.

Logo, $S + Rfn_{\Sigma_1}(T) \vdash \neg Pr_T[\exists y(y = y + 1)]$.

Como, por 2.3.(iii), $S + Rfn_{\Sigma_1}(T) \vdash \neg Con(T) \to Pr_T[\neg(\exists y(y = y + 1) \to \exists y(y = y + 1))]$ e $S \vdash Pr_T[\neg(\exists y(y = y + 1) \to \exists y(y = y + 1))] \to Pr_T[\exists y(y = y + 1)]$, então $S + Rfn_{\Sigma_1}(T) \vdash Con(T)$. ■

2.11 Corolários

(i) $S \vdash RFN_{\Sigma_1}(T) \to Con(T)$.

(ii) $S \vdash RFN(T) \to Con(T)$.

2.11.1 Demonstração:

a) Caso (i):
Direta dos teoremas 2.8 e 2.10.

b) Caso (ii):
Direta dos teoremas 2.6, 2.9 e 2.10.

2.11.2 Discussão:

Podemos perceber que apenas uma forma restrita (às fórmulas Σ_1) do princípio de reflexão uniforme já é suficiente para provar a consistência. Na verdade, apenas a adição de uma única fórmula do tipo $Pr_T[\varphi] \to \varphi$, onde φ seja refutável (isto é, que $S \vdash \neg\varphi$), à teoria T é suficiente para que obtenhamos a consistência. Além disso, $S \vdash Con(\mathrm{T}) \leftrightarrow (Pr_T[\varphi] \to \varphi)$ para qualquer φ refutável (isto é, que $S \vdash \neg\varphi$).[16]

[16] BARWISE, J. op. cit., p. 846.

A próxima pergunta natural é se $S \vdash Con(T) \rightarrow RFN(T)$. E a resposta é negativa,[17] como veremos a seguir. Apesar de que $S \vdash Con(T) \leftrightarrow RFN_{\Pi_1}(T)$.[18]

2.12 Teorema

Seja φ uma sentença Π_k tal que $k \leq n$. Então:

(i) $T + \varphi + Rfn_{\Sigma_n}(T) \vdash Rfn_{\Sigma_n}(T + \varphi)$;

(ii) $T + \varphi + RFN_{\Sigma_n}(T) \vdash RFN_{\Sigma_n}(T + \varphi)$;

2.12.1 Demonstração:

a) Caso (i):

Seja A uma sentença Σ_n.

Suponha $Pr_{T+\varphi}[A]$.

Temos que $S \vdash Pr_{T+\varphi}[A] \leftrightarrow Pr_T[\varphi \rightarrow A]$.

Note que $\varphi \rightarrow A$ será uma fórmula Σ_n.[19]

Então, por $Rfn_{\Sigma_n}(T)$, $T + \varphi + Rfn_{\Sigma_n}(T) \vdash Pr_{T+\varphi}[A] \rightarrow (\varphi \rightarrow A)$.

E, por *Modus Ponens,* $T + \varphi + Rfn_{\Sigma_n}(T) \vdash Pr_{T+\varphi}[A] \rightarrow A.$

Logo, $T + \varphi + Rfn_{\Sigma_n}(T) \vdash Rfn_{\Sigma_n}(T + \varphi)$.

b) Caso (ii):

Análogo ao item a). ■

2.13 Corolário

[17] Idem, p. 850.
[18] Idem, p. 846.
[19] Idem, p. 840.

$$T \nvdash Con(T) \rightarrow RFN_{\Sigma_1}(T).$$

2.13.1 Demonstração:

Da definição 2.1.6 e como $Prov_T(x,y)$ é primitivo recursivo, teremos que $Con(T)$ é uma fórmula Π_1.

Logo, pelo teorema 2.12.(ii), $T + Con(T) + RFN_{\Sigma_1}(T) \vdash RFN_{\Sigma_1}(T + Con(T))$.

Então, pelo corolário 2.11.(i), $T + Con(T) + RFN_{\Sigma_1}(T) \vdash Con(T + Con(T))$.

Suponha que $T \vdash Con(T) \rightarrow RFN_{\Sigma_1}(T)$.

Logo, $T + Con(T) \vdash Con(T + Con(T))$.

Que é um absurdo pelo segundo teorema de incompletude.[20]

Logo, por *reductio ad absurdum*, $T \nvdash Con(T) \rightarrow RFN_{\Sigma_1}(T)$. ■

2.14 Corolário

$$S \nvdash Con(T) \rightarrow RFN(T).$$

2.14.1 Demonstração:

Suponha $S \vdash Con(T) \rightarrow RFN(T)$.

Então, pela definição 2.1.2, $T \vdash Con(T) \rightarrow RFN(T)$.

Temos que, por uma demonstração direta análoga a do item 2.9, que $T \vdash Con(T) \rightarrow RFN_{\Sigma_1}(T)$.

E chegamos num absurdo com o corolário 2.13.

Logo, por *reductio ad absurdum*, $S \nvdash Con(T) \rightarrow RFN(T)$. ■

2.15 Teorema (Princípio Combinatorial de Paris-Harrington)

---

[20] BARWISE, J., op. cit., p. 828.

Para todos os números naturais e, r e k existe um número natural M tal que $M \underset{*}{\rightarrow} (k)_r^e$.

2.15.1 Discussão:

Para demonstrarmos essa proposição precisamos primeiro demonstrar o teorema de Ramsey infinito que nos garante que $\omega_0 \rightarrow (\omega_0)_\mathrm{r}^\mathrm{e}$, onde e e r são números finitos e ω_0 é o primeiro ordinal enumerável infinito. Note que é necessário o axioma do infinito para tal demonstração e, por isso, tornando-a inviável dentro de S. A outra parte da demonstração pode ser encontrada no *Handbook of Mathematical Logic*.[21] No final, temos de volta uma sentença sobre números naturais que pode ser expressa em S. Daí a significância do princípio combinatorial de Paris-Harrington ao se provar que uma sentença de S é demonstravelmente verdadeira num sistema mais poderoso (por exemplo, Zermelo-Fraenkel) que S.

Diferentemente, o teorema de Ramsey finito pode ser obtido em S a partir de uma prova por indução sobre os números naturais. Usualmente pode ser encontrado na literatura na notação $\forall e, r, k \exists M (\mathrm{M} \rightarrow (\mathrm{k})_\mathrm{r}^\mathrm{e})$. Portanto, o asterisco simboliza justamente o “relativamente grande” na notação 2.2.

2.15.2 Notação:

Iremos simbolizar essa assertiva na linguagem de S por $\forall e, r, k \exists M (\text{" } \mathrm{M} \underset{*}{\rightarrow} (\mathrm{k})_\mathrm{r}^\mathrm{e} \text{ "})$.

2.16 Lema

$S \vdash \forall e, r, k \exists M (\text{" } \mathrm{M} \underset{*}{\rightarrow} (\mathrm{k})_\mathrm{r}^\mathrm{e} \text{ "}) \rightarrow Con(T)$.

---

[21] BARWISE, J., op. cit., p. 1135.

2.16.1 Discussão:

A demonstração desse teorema será omitida, pois um detalhamento satisfatório de suas passagens fugiria do escopo do presente texto. Ela pode ser encontrada em maiores detalhes no **Handbook of Mathematical Logic** [22]. Constitui-se, basicamente, de tomar uma teoria U de forma que $S \vdash Con(U) \rightarrow Con(T)$ e $S \vdash \forall e, r, k \exists M(" \mathrm{M} \underset{*}{\rightarrow} (\mathrm{k})_{\mathrm{r}}^{\mathrm{e}} ") \rightarrow Con(U)$. É necessário um bom conhecimento da demonstração dos teoremas de Ramsey infinito e finito e de aritmetização de provas em teorias do conjunto (é imprescindível ao leitor notar que S é equivalente aos axiomas de Zermelo-Fraenkel sem o axioma do infinito, no caso de provas que envolvam somente números naturais[23]).

Como corolário, pelo segundo teorema de incompletude de Gödel, teremos que $\forall e, r, k \exists M(" \mathrm{M} \underset{*}{\rightarrow} (\mathrm{k})_{\mathrm{r}}^{\mathrm{e}} ")$ é indemonstrável dentro de S. Portanto, o princípio combinatorial de Paris-Harrington é outro exemplo de sentença verdadeira (num modelo standard de S) e independente de S além daquela formulada no primeiro teorema de incompletude.

2.17 Teorema

$$S \vdash RFN_{\Sigma_1}(T) \leftrightarrow \forall e, r, k \exists M(" \mathrm{M} \underset{*}{\rightarrow} (\mathrm{k})_{\mathrm{r}}^{\mathrm{e}} ").$$

2.17.1 Demonstração:

a) Caso →:

Pode ser visto que para cada valor fixo e, r ou k, $S \vdash \exists M(" \mathrm{M} \underset{*}{\rightarrow} (\mathrm{k})_{\mathrm{r}}^{\mathrm{e}} ")$. Pois basta um computador ir pegando cada M e ir testando para verificar se ele satisfaz a sentença que,

[22] BARWISE, J., op. cit., p. 1136
[23] Idem, p. 1135.

em alguma hora, ele vai retornar algum número natural. Além disso, é possível demonstrar que $S \vdash \forall \mathrm{e}\, Pr_S\left[\forall \mathrm{r}, \mathrm{k} \exists M(\text{" } \mathrm{M} \underset{*}{\rightarrow} (\dot{k})^{\dot{e}}_{\dot{r}} \text{ "})\right]$.[24] Também ficará a cargo do leitor verificar que a fórmula " $\mathrm{M} \underset{*}{\rightarrow} (\mathrm{k})^{\mathrm{e}}_{\mathrm{r}}$ " é primitiva recursiva.

Logo, uma aplicação direta do *Modus Ponens* nos dá que $S + RFN_{\Sigma_1}(T) \vdash \forall e, r, k \exists M(\text{" } \mathrm{M} \underset{*}{\rightarrow} (\mathrm{k})^{\mathrm{e}}_{\mathrm{r}} \text{ "})$.

b) Caso ←:

Seja $\psi(x)$ uma fórmula Σ_1 arbitrária.

Suponha $\forall x Pr_T[\psi(\dot{x})]$.

Suponha, por absurdo, que $\exists x \neg\psi(x)$.

Seja $\neg\psi(x)$, onde x é arbitrário.

Temos que $S + \forall e, r, k \exists M\left(\mathrm{M} \underset{*}{\rightarrow} (\mathrm{k})^{\mathrm{e}}_{\mathrm{r}} \right) \vdash \neg\psi(x) \to Con(T + \neg\psi(\dot{x}))$. Essa passagem pode ser inferida da demonstração do Lema 2.16.[25]

Logo, pela definição 2.1.7, $S + \forall e, r, k \exists M\left(\mathrm{M} \underset{*}{\rightarrow} (\mathrm{k})^{\mathrm{e}}_{\mathrm{r}} \right) \vdash \neg\psi(x) \to \neg Pr_{T+\neg\psi(\dot{x})}[\neg(\psi(\dot{x}) \to \psi(\dot{x}))]$.

Ou ainda, $S + \forall e, r, k \exists M\left(\mathrm{M} \underset{*}{\rightarrow} (\mathrm{k})^{\mathrm{e}}_{\mathrm{r}} \right) \vdash \neg\psi(x) \to \neg Pr_T[\neg\psi(\dot{x}) \to \psi(\dot{x})]$.

Mas, como $\forall x Pr_T[\psi(\dot{x})]$, temos, por 2.3.(iii), que $S + \forall e, r, k \exists M\left(\mathrm{M} \underset{*}{\rightarrow} (\mathrm{k})^{\mathrm{e}}_{\mathrm{r}} \right) \vdash \forall x Pr_T[\psi(\dot{x})] \to Pr_T[\neg\psi(\dot{x}) \to \psi(\dot{x})]$.

Logo, $S + \forall e, r, k \exists M\left(\mathrm{M} \underset{*}{\rightarrow} (\mathrm{k})^{\mathrm{e}}_{\mathrm{r}} \right) \vdash \forall x Pr_T[\psi(\dot{x})] \to \psi(x)$.

Então, chegamos a um absurdo.

Logo, como x era arbitrário, $\forall x \psi(x)$.

Então, $\forall x Pr_T[\psi(\dot{x})] \to \forall x \psi(x)$.

Como $\psi(x)$ era uma fórmula Σ_1 arbitrária, obtemos $RFN_{\Sigma_1}(T)$. ■

2.17.2 Discussão:

---

[24] BARWISE, J. (Ed.). **Handbook of Mathematical Logic**. Amsterdam: Elsivier Science Publisher B.V., 1977. ISBN 0444863885. p. 1141.

[25] Ibidem, p. 1136.

Note que basta uma teoria U que prove $\neg\varphi(x) \rightarrow Con(T + \neg\varphi(\dot{x}))$, para qualquer fórmula Σ_1 φ, para conseguirmos $RFN_{\Sigma_1}(T)$. Analogamente, a mesma coisa vale para $RFN_{\Sigma_n}(T)$ e $RFN_{\Pi_n}(T)$, onde n seja um número natural. Em particular, o princípio combinatorial de Paris-Harrington também pôde ser provado a partir de $RFN_{\Sigma_1}(T)$, tornando os dois equivalentes. A pergunta se o lema 2.16 é necessário para provar o item 2.17.1.b) deve ser provocativa e, se o conseguirmos por outro caminho, voltamos a provar o lema 2.16 de outra forma.

O mesmo resultado do teorema 2.15 pode ser obtido pelo item 2.17.1.a). Para isso, começamos provando que $S \vdash \forall \mathrm{e}, \mathrm{r}, \mathrm{k}\, Pr_S\left[\exists M(\text{"}\, \mathrm{M} \underset{*}{\rightarrow} (\dot{k})^{\dot{e}}_{\dot{r}}\, \text{"})\right]$ e que $\mathrm{M} \underset{*}{\rightarrow} (\dot{k})^{\dot{e}}_{\dot{r}}$ é primitivo recursivo, da onde se pode tirar que $S \vdash RFN_{\Sigma_1}(T) \rightarrow \forall e, r, k \exists M(\text{"}\, \mathrm{M} \underset{*}{\rightarrow} (\mathrm{k})^{\mathrm{e}}_{\mathrm{r}}\, \text{"})$. Basta agora provar que $RFN_{\Sigma_1}(T)$ é verdadeiro no modelo standard da aritmética (o mesmo modelo que usamos, por meio da teoria dos conjuntos, para provar o item 2.15.1). Lembremos que o modelo standard da teoria dos números é aquele composto pelo conjunto $\{0, 1, 2, \dots\}$, que são os números naturais que todos estamos habituados. Aqui vou me abster de uma formalização do que seja um modelo e de satisfatibilidade de uma fórmula em um modelo, pois fugiria do foco do argumento[26]. Se supusermos que $\forall x Pr_T[\varphi(\dot{x})]$ seja verdadeiro num modelo standard, onde φ é uma fórmula Σ_1, teremos que para cada número natural n (número standard da aritmética) podemos provar dedutivamente (isto é, em passos finitos) a partir de S a sentença $\varphi(n)$ – esta última oração é justamente a interpretação ou tradução da sentença $\forall x Pr_T[\varphi(\dot{x})]$ para tal modelo. E, pelo teorema de Corretude da lógica de primeira ordem,[27] $\varphi(n)$ será verdadeiro no modelo standard para todo n natural. Como o modelo standard só contém números naturais usuais, então $\forall x \varphi(x)$ é verdadeiro nesse modelo. Logo, a implicação $\forall x Pr_T[\varphi(\dot{x})] \rightarrow \forall x \varphi(x)$ é verdadeira no modelo standard da teoria dos números. Mas, talvez, esse caminho seja mais complicado ou extenso.

---

[26] ENDERTON, H., op. cit., p. 79.
[27] Idem, p. 124.

Capítulo 3: A consistência da consistência

No presente capítulo, começaremos analisando criticamente as provas de consistências dos capítulos anteriores. Não em busca de erros técnicos - no sentido de erros matemáticos, de sintaxe, de formalismo ou de lógica -, mas sim tentando permear as bases das argumentações apresentadas em busca de fatores de validade, universalidade, fundamentação e de relação com outros resultados, não apresentados neste trabalho. O objetivo é uma discussão mais filosófica, apesar de haver também discurso lógico-matemático, não existindo, propositalmente, intuito de demarcar de forma precisa a fronteira entre esses dois tipos de raciocínios. Não só isso é proposital como também a ironia formada pela diferença entre o discurso apresentado nos outros capítulos - o discurso matemático - com o discurso desse capítulo – discursivo -, aquele no qual será questionada a fundamentação – isto é, o nível de "certeza matemática" dos anteriores. Questões serão levantadas e algumas possíveis soluções também.

Quando tratamos de provas matemáticas e, ainda mais, de lógica é corrente a opinião na literatura e no senso comum de que nenhuma discussão precisa ser feita sobre elas. De fato, quando corretas (a palavra correta não está aqui por acaso) elas se calcam sobre as bases rígidas da lógica, preservando a verdade ao longo das inferências feitas. Não nos ateremos a prolongar essa problemática. Apesar de não ser impossível – e, inclusive, é pertinente - uma discussão, por exemplo, sobre o *Modus Ponens*, tal gama de questionamentos não faz parte da pretensão desse capítulo.

Não há como fugir dos termos filosóficos (na verdade, são bem-vindos). Problemas sobre a natureza cognitiva e epistemológica também serão encontrados, mas iremos nos abster de uma completa explicitação e fundamentação dos termos e conceitos envolvidos. De bom grado, pretende-se que o leitor possa compreender o texto à frente sem profundo conhecimento sobre os temas, obviamente, contanto que ele tenha entendido os capítulos anteriores. Todavia, é aconselhável e interessante um estudo prévio sobre tais assuntos, principalmente, sobre Filosofia da Mente.

O que queríamos com essas demonstrações? O resultado, realmente, nos levou a tal lugar? Que tipo de argumentação lógica matemática foi feita? São exemplos de perguntas que, pelo menos, serão tangenciadas a seguir.

3.1 Provamos a consistência ou a supomos?

Vamos lembrar que, no capítulo 1, é tomada como base da prova do Schütte, uma versão da prova do Gentzen, infinitos axiomas, os quais são sentenças específicas – arbitradas ou não. Toda fórmula fechada e atômica, na linguagem de S, que for correta e a negação de toda fórmula fechada e atômica que for incorreta formam tais axiomas. O leitor atento deve ter notado no início do capítulo 1 a menção à axiomática de S_∞ de que a verificabilidade de fórmulas atômicas fechadas é sempre possível. No próprio texto de referência[1] é dito que se pode efetivamente verificar se uma fórmula correta ou é incorreta. O conjunto de fórmulas atômicas fechadas corretas é recursivo. Isto pode ser entendido como alguém, ou um computador, sempre decidindo se uma fórmula atômica fechada de S_∞ é correta ou não. Um computador sempre pára, caso a fórmula seja correta ou caso seja incorreta. Sim, são desses pontos que nascem as discussões adiante.

Mas o que define tal conjunto de axiomas? Por que podemos construí-lo? Se caminharmos em direção à abordagem puramente aritmético-formal, cairemos numa espécie de raciocínio circular: nossa hipótese sendo a nossa tese. Comecemos por esse caminho.

Tal conjunto poderia ser definido por S ou por um computador, justamente, pela demonstrabilidade dedutiva que pode ser feita sempre: x pertence aos axiomas de S_∞ se

$$x \in \{x \mid (x\ \text{é}\ uma\ fórmula\ atômica\ fechada\ na\ linguagem\ de\ S \lor x\ \text{é}\ a\ negação\ de\ uma\ fórmula\ atômica\ fechada) \land S \vdash x\}.$$

Esse é um conjunto recursivamente enumerável, pois, apesar das duas primeiras condições serem decidíveis, se S for consistente, S não saberá se uma fórmula falsa x não é demonstrável (sabê-lo seria provar a consistência, o que sabemos não ser possível). Portanto, S pode enumerar os axiomas de S_∞ e, dessa forma, defini-los.

[1] MENDELSON, E. **Introduction to Mathematical Logic**. 2ª. ed. Princeton, New Jersey: D. VAN NOSTRAND COMPANY, INC., 1964. p. 258

É fácil provar que se x for incorreto, então $S \vdash \neg x$. Então, se $1 = 0$ pertencer a S, isto é, se S for inconsistente[2], tanto $1 = 0$ quanto $1 \neq 0$ pertencerão aos axiomas de S_∞. O importante aqui é que S está construindo a axiomática de S_∞. Logo, para não haver a fórmula $0 \neq 0$ dentro de seus axiomas é porque $0 \neq 0$ não pertencia à S antes. Mas isso é a própria consistência de S. Portanto, o último teorema do capítulo 1 apenas nos traz de volta da onde partimos.

Porém, não estamos presos à aritmética para poder definir tal conjunto. Pelo menos, não diretamente.[3] Caminhemos diferente então. Tanto a abordagem pela teoria dos números quanto pela teoria dos conjuntos são tidas como formais e usuais. Por isso, ainda nos resta poder usar a teoria dos conjuntos sem recorrer a S. Com certeza, é uma argumentação muito mais delicada que a anterior, pois andaremos sempre à beira de estarmos usando S de forma implícita. A verificabilidade – no sentido formal-dedutivo - não pode ser usada para estabelecermos as condições de formação de tal conjunto de axiomas. Por exemplo, tente defini-lo por:

$$\{x| \ (x \text{ é } uma\ fórmula\ atômica\ fechada\ na\ linguagem\ de\ S \vee x \text{ é } a\ negação\ de\ uma\ fórmula\ atômica\ fechada) \wedge x \text{ é } verdadeiro\}.$$

Toda a sutileza se encontra em como sabemos – nós matemáticos humanos - que a fórmula x é verdadeira.[4] Qualquer método que usemos para provar que x é verdadeiro e que se baseie em passos finitos e finitamente axiomatizáveis irá nos esconder S por trás[5] e o segundo teorema de incompletude. Ou seja, será um processo representável em S, retornando à circularidade primeira.[6] Mas se garantirmos a existência de um processo formal e não dedutivo para tal, poderemos fugir de S. Um exemplo disso seria usando a regra infinitária do capítulo 1 (Infinite Induction Rule). Contudo, aqui também andamos numa corda bamba.[7] E ficamos na dúvida se algum de nossos processos cognitivos pode ser

[2] Ao se demonstrar $1 = 0$ se demonstra qualquer fórmula, pois S também demonstra que $1 \neq 0$.
[3] Vide o item 3.2.
[4] Não há muito problema em notar que o resto das condições de tal conjunto sempre pode ser definido em S.
[5] ENDERTON, H. **A mathematical introduction to logic**. 2 ed. Boston, MA: Academic Press, 2001. Cap. 1.3. ISBN 978-0-12-238452-3. p. 199.
[6] Ver último parágrafo do item 3.1.
[7] Vide item 3.2.

realmente infinitário.[8] Seríamos obrigados, então, a abandonar a formalidade matemática para poder definir tal conjunto?[9]

Ao invés de recorrermos a uma regra infinitária vamos nos voltar para a teoria dos conjuntos e perceber que ela ainda poderia nos dar alternativa[10]. Para aqueles não familiarizados com os axiomas da teoria do conjunto de Zermelo-Fraenkel, existe um axioma que garante a existência de um conjunto infinito. Também podemos garantir a existência do conjunto vazio. Com eles, podemos definir os números ordinais até ω_0 e definir o que seriam as operações de soma e produto entre esses números na linguagem de ZF.[11] Note que vamos fazer a argumentação no sentido inverso: primeiro obter o conjunto e depois tirar dele as propriedades equivalentes aos axiomas de S. Provamos, então, que esse conjunto satisfaz todas as sentenças contidas nos axiomas de S_∞, justamente porque nos foi dado que ele existe e porque construímos suas propriedades para assim fazê-lo. Também convido o leitor a notar que toda a prova do capítulo 1 pode ser carregada em ZF.[12] Assim, fundamentamos a prova do Schütte sem recorrer a S. Foi-nos dada por ZF, outro presente da teoria dos conjuntos como o princípio combinatorial de Paris-Harrington[13], que, até agora, já nos consegue dois caminhos diferentes para a prova de consistência de PA.[14] Perceba que existe uma interpretação[15] da teoria S em ZF e, dada a devida tradução, o lema 2.16 também será um teorema de ZF.

Porém, apenas estamos passando a responsabilidade para ZF. Seus axiomas realmente correspondem às propriedades que entendemos serem universais para o que concebemos e intuímos ser um conjunto?[16]

Poderíamos nos perguntar também se ZF é consistente – e, por isso, se existe um modelo para ZF -, mas antes de discutir isso precisamos ainda passar por uma questão. Toda essa argumentação nos dando os axiomas de S_∞ por ZF não se baseia em construir

---

[8] Ver item 3.3.
[9] O que será tangenciado a seguir pela possibilidade de construção de um modelo mental.
[10] O que será questionado no final do item 3.1.
[11] KUNEN, K. **A Ramsey Theorem in Boyer-Moore Logic**. Madison, Wisconsin: Computer Sciences Department, University of Wisconsin, 1995.
[12] Ver item 3.2.
[13] Vide capítulo 2.
[14] Um deles pela prova do capítulo 1 e o outro pela do Paris-Harrington.
[15] ENDERTON, H. **A mathematical introduction to logic**. 2ª. ed. Boston, MA: Academic Press, 2001. Cap. 1.3. ISBN 978-0-12-238452-3. p. 156.
[16] O que remete ao mesmo problema de haver um modelo mental para os números naturais.

um modelo para S? Pela definição de modelo[17], esse conjunto ω_0 corresponde exatamente a um deles. Na verdade, isso já estava contido na frase "Provamos, então, que esse conjunto satisfaz todas as sentenças contidas nos axiomas de S_∞, justamente porque nos foi dado que ele existe e porque construímos suas propriedades para assim fazê-lo." Os axiomas de S ao invés de ser o princípio, agora são apenas propriedades provadamente universais desse conjunto, o que torna redundante a pergunta se PA é satisfatível por esse modelo. Lembremos, agora, o resultado conhecido na literatura pela teoria dos modelos de que uma teoria é satisfatível se, e somente se, ela for consistente.[18] Logo, por esse caminho, partimos de um resultado que já sabíamos que íamos chegar ao final do capítulo 1: de um modelo para S construímos os axiomas de S_∞ que, justamente, por S ser satisfatível por esse modelo já sabíamos que S era consistente, para, ao final do capítulo 1, provar que S é consistente.[19]

Antes de questionar a redundância ou não dessas provas de consistência, talvez, o mais interessante e imprescindível seja buscar por que é tão natural passarmos pelos axiomas de S_∞. Geralmente, proposições incansavelmente autoevidentes à nossa mente, o que se pode dizer que é a prancheta final onde um matemático trabalha, nos dão essa impressão. Portanto, o conjunto dos números naturais seria autoevidente? É claro que antes precisaríamos entender o que é e como se forma o conceito de conjunto, ou pelo menos, o que ele representa em nossa mente – se é que representamos algo. O fato da teoria dos modelos matematizar a ideia de metalíngua para fundamentar o que seria uma fórmula semanticamente verdadeira corrobora imensamente para se basear na hipótese representacional da mente[20]. Talvez, ela realmente estivesse por trás das concepções dos criadores da teoria dos modelos. Tanto que, inclusive, uma teoria dos conceitos e do significado já foi pensada nos termos quase explícitos da teoria dos modelos – e o próprio autor diz que se calca na hipótese representacional da mente.[21]

---

[17] ENDERTON, H. **A mathematical introduction to logic**. 2ª. ed. Boston, MA: Academic Press, 2001. Cap. 1.3. ISBN 978-0-12-238452-3. p. 79.
[18] ENDERTON, op. cit., p. 128.
[19] De qualquer forma, há um ganho nessa prova ao provarmos que S_∞ também é consistente.
[20] PITT, D. Mental Representation. **The Stanford Encyclopedia of Philosophy**, 2008. Disponivel em: <http://plato.stanford.edu/archives/fall2008/entries/mental-representation/>. Acesso em: 17 Fevereiro 2011.
[21] JOHNSON-LAIRD, P. N. **Mental Models**. 6 ed. Cambridge: Harvard University Press, 1995.

Por esse caminho, vamos nos ater ao exemplo a seguir. Tome alguém que experienciou durante a vida a operação de soma e produto.[22] Isso incluiria somar e multiplicar maçãs, celulares ou qualquer coisa. Não só isso, mas também aprendeu aritmética podendo realizar operações mentais correspondentes à soma e ao produto e concebendo cada número natural e o que seja o conjunto desses números. Visto isso, é de se esperar que o necessário para a formação do conceito, pelo menos, de um conjunto capaz de servir de modelo para S seja alcançado. Ainda faltaria salientar vários problemas – possivelmente mais complicados – envolvidos nesse exemplo. A representação de objetos mediante uma faculdade mental em que tais objetos aparecem como fenômenos visuais não oculares é bem estabelecida: a clássica imaginação. Ninguém acreditaria em alguém, dito normal, que diga que não pode imaginar duas maçãs, por exemplo, em sua "cabeça". No âmbito das operações mentais é onde começam as maiores dificuldades. Isso se alongaria desde como desenvolvemos a capacidade de operar com conceitos ou objetos abstratos até se há ou não representação mental dessas operações enquanto um sujeito pratica a aritmética, por exemplo. Contudo, apenas pretende-se, aqui, uma boa base de concordância para creditar que esse alguém do exemplo é capaz de conceber, mesmo que não haja representação mental para esse conceito, o conjunto dos números naturais. O ponto crucial é que ele pôde "ter em suas mãos" o conjunto, que servirá de modelo, antes de obter os axiomas S. Lembre que, historicamente, se fazia aritmética muito antes dos axiomas de Peano.

Voltemos, então, para esses axiomas. Há de se considerar a imensa possibilidade de que eles não foram arbitrados a esmo. Pelo contrário, houve muito estudo para poder estabelecê-los para satisfazer o que antes já se tinha em mente como aritmética. Logo, eles não foram o ponto de partida e sim propriedades universais, formalizadas pela lógica de primeira ordem numa linguagem bem definida, que provamos – ou que sempre persistem a parecer absolutamente verdadeiras – dar base para o queremos por aritmética. E, nesse processo, pouco importa se tais axiomas nos levarão ou não a contradições pelo cálculo dedutivo[23], o que é relevante é que eles simplesmente parecem sentenças verdadeiras, isto é, propriedades universais, como já mencionado. Isso pode ser evidenciado pelo próprio

---

[22] A exponenciação pode ser obtida através dessas duas. Mas não conseguimos tirar a produto através da soma (ENDERTON, op. cit. p. 193).

[23] Apesar de que até chegar aos axiomas de Peano, alguns candidatos a axiomas de S provaram-se inconsistentes.

Programa de Consistência de Hilbert que pretendia demonstrar a consistência daquilo que já se entendia como sendo os axiomas da aritmética.

Aqui está a quase redundância. Se os axiomas foram criados a partir de um modelo, mental ou não, então, pela teoria dos modelos, eles já são consistentes. O que nos devolve uma definição formal para os axiomas de S_∞.

Ademais, talvez, essa seja a única opção que temos para “provar” a consistência da aritmética: partir de uma explicação informal, pela formação de um conceito de um conjunto dos números naturais na mente, e usar o formalismo da teoria dos modelos para, pressupondo que existe um conjunto que é modelo para os números naturais, provar que S é consistente - seja pela forma do capítulo 1, pela do capítulo 2 ou pela teoria dos modelos, como descrito anteriormente. E note que, mesmo que ZF seja de fato inconsistente, esse tipo de demonstração é válida, pois os resultados da teoria dos modelos se mantêm os mesmos. Se demonstramos algo num sistema sem usar contradição, não é porque ele é inconsistente que tal demonstração deixou de ser válida dentro do cálculo dedutivo. Obviamente, sendo inconsistente, o que se pode afirmar é que de alguma outra forma, posteriormente, surgirá a negação daquilo que tinha sido provado.[24]

Mas ZF não nos prova que existe o conjunto ω_0, equivalente aos números naturais? Sim, porém, voltando às questões deixadas para trás nos parágrafos anteriores, ZF pode ser inconsistente. Pelo segundo teorema de Gödel, inclusive, ZF ou S não podem demonstrar a consistência de ZF.[25] Ou seja, tanto $\text{“}S \text{ é consistente”}$ quanto $\neg\text{“}S \text{ é consistente”}$ ou tanto $"x \text{ é } o\ número\ de\ Gödel\ de\ um\ axioma\ de\ S_\infty"$ quanto $\neg"x \text{ é } o\ número\ de\ Gödel\ de\ um\ axioma\ de\ S_\infty"$ podem ser teoremas de ZF. $\text{“}S \text{ é consistente”}$ ou $"x \text{ é } o\ número\ de\ Gödel\ de\ um\ axioma\ de\ S_\infty"$ serão obtidos dedutivamente sem usar nenhuma contradição, só que, uma hora, de alguma outra forma, ZF também pode nos provar – agora podendo partir de alguma contradição[26] – que $\neg\text{“}S \text{ é consistente”}$ ou que $\neg"x \text{ é } o\ número\ de\ Gödel\ de\ um\ axioma\ de\ S_\infty"$.

---

[24] Um outro exemplo disso será dado no próximo parágrafo.
[25] Existe uma interpretação de S em ZF. Logo, se S demonstrar, ZF também demonstra.
[26] Como $A \wedge \neg A \rightarrow B$, para qualquer fórmula A e B, é uma tautologia, se ZF demonstra A e $\neg A$, então toda fórmula B será um teorema de ZF.

Indiretamente, o mesmo vale para S. Se $ZF \vdash "S \text{ é } consistente"$, então $S \vdash Pr_{ZFC}[\text{“}S \text{ é consistente”}]$ e, analogamente, se S for inconsistente, então de alguma outra forma[27] $S \vdash Pr_{ZFC}[\neg\text{“}S \text{ é consistente”}]$. Portanto, se não abrirmos mão de uma perspectiva dedutiva pura, o máximo que podemos atingir é que $S \vdash Pr_{ZFC}[\text{“}S \text{ é consistente”}]$ ou que $ZF \vdash "S \text{ é } consistente"$, sem que nenhuma contradição tenha sido usada pelo caminho. Para que estes resultados tenham conteúdo semântico, isto é, "$S \text{ é } consistente$" seja satisfatível por algum modelo de ZF, é porque ZF já era consistente previamente. Em outras palavras, já confiávamos nos axiomas de ZF para poder, a partir deles, provar que S é consistente. O que apenas nos transfere todos os problemas para ZF, ao invés de S. E, como ZF herda a mesma incapacidade de demonstrar sua própria consistência, podemos recair nas mesmas questões. Além disso, se considerarmos que qualquer demonstração, dita formal, de que um sistema é consistente parte de um número finito de argumentos, ela pode ser definida por S. E, por isso, o que nos garantiria que S não prova[28], num momento futuro e sem usar contradições, que esses argumentos demonstram que ZF é inconsistente? Somente se S for consistente, voltando ao círculo vicioso, e se o sistema usado para provar a consistência de ZF for consistente, o que nos levará a uma regressão infinita[29].

3.2 Um computador pode realizar a prova do capítulo 1?

Aqui lembramos o argumento usado no segundo teorema de incompletude de Gödel [30] que diz que toda a prova do primeiro teorema de incompletude pode ser carregada dentro de ZFC (Zermelo-Fraenkel-Choice).[31] ZFC é uma teoria dos conjuntos - considerada a mais usual – composta pelos axiomas de ZF mais o axioma da escolha.[32] Logo, traduzindo o segundo teorema de incompletude para a linguagem natural, a sentença “Se S

---

[27] Um sistema inconsistente demonstra qualquer fórmula.
[28] Pois se S prova que outro sistema demonstra que “ZFC é inconsistente”, então podemos conseguir esta mesma sentença a partir dos argumentos finitos anteriores, que definem esse sistema.
[29] Se baseando na premissa de que qualquer demonstração de que um sistema qualquer é consistente parta de um número finito de argumentos.
[30] ENDERTON, op. cit., p. 244.
[31] ENDERTON, op. cit. p. 244.
[32] KUNEN, K. **A Ramsey Theorem in Boyer-Moore Logic**. Madison, Wisconsin: Computer Sciences Department, University of Wisconsin, 1995.

for consistente, então S não prova sua própria consistência" será um teorema de ZFC - em particular, o axioma da escolha não é necessário.[33]

Sabe-se que toda teoria sobre grafos também pode ser carregada dentro de ZFC, por isso, usando o mesmo argumento mencionado no início do parágrafo anterior, fica mais fácil ver que toda a prova de consistência da aritmética em S_∞ pode ser carregada dentro de ZFC - e, como discutido no item 3.1, os axiomas de S_∞ também podem ser definidos em ZFC.[34] Teremos, então, que a sentença "S é consistente" também será um teorema de ZFC. É possível construir uma fórmula em PA que represente a demonstrabilidade em ZFC - por exemplo, $Pr_{ZFC}[\varphi]$ -, pois ZFC está numa lógica de primeira ordem, numa linguagem razoável[35], com um número finito de axiomas e com regras de inferência dedutivas clássicas.

Chegamos, então, ao resultado de que $Pr_{ZFC}\left[\begin{matrix}\text{“Se } S \text{ for consistente, então } S \text{ não} \\ \text{não prova sua própria consistência”}\end{matrix}\right]$ e $Pr_{ZFC}[\text{“}S \text{ é consistente”}]$ são teoremas de S. Não há contradição evidente entre eles e nem com os teoremas de incompletude. E, de fato, como se quer mostrar a consistência do nosso sistema axiomático (S) o resultado de Gentzen não pode ser considerado com menos crédito, pois sua prova é feita sobre os mesmos argumentos dos teoremas de Gödel (ambas podem ser feitas dentro de ZFC). E vice-versa. Ademais, se S for realmente consistente, todos esses resultados não entrarão em contradição nunca.

Podemos chegar ao mesmo lugar usando os argumentos no item 3.1. Temos que a existência de um modelo (standard) para S é garantida pelo axioma do infinito. A própria demonstração que fazemos de que esse conjunto é um modelo de S pode ser rodada em ZFC.[36] Inclusive, é um quase senso comum entre os matemáticos que toda a matemática pode ser carregada em ZFC. Logo, rodando a teoria dos modelos em ZFC,[37] teremos, também, que "S é consistente" é um teorema de ZFC. E, por isso, $Pr_{ZFC}[\text{“}S \text{ é consistente”}]$ um de S. Também poderíamos obter o mesmo resultado através da prova do capítulo 2 - dos

[33] Essa sentença também pode ser um teorema de PA.
[34] Em particular, o axioma da escolha não é necessário. Por isso, o mesmo vale para ZF.
[35] ENDERTON, op, cit., p. 137.
[36] Basta lembrar que os símbolos predicativos e funcionais de S foram definidos a partir do conjunto ω_0, que já tinham sido definidos, previamente, em ZFC (KUNEN, 1995).
[37] Nesse ponto, se abre toda uma gama de interessantes propriedades ao se usar ZFC para carregar a teoria dos modelos sendo que a teoria a ser modelada pode ser a própria ZFC.

pressupostos contidos nesse capítulo juntamente com os citados no item 3.1, se espera que o leitor possa verificar tal procedimento.

Voltando ao título do item 3.2, é bem estabelecido na literatura, pela tese de Church-Turing[38], que qualquer demonstração feita por S pode ser feita por um computador. Vamos entender um computador como algo equivalente a uma máquina de Turing[39]. Poderíamos nos alongar em discutir as bases dessa tese, mas visamos não fazê-lo. A tese nos diz que uma função é computável [40] por uma máquina de Turing se, e somente se, ela for recursiva[41]. A definição de função recursiva é formalmente dada pela representação dessa função em S. As questões, digamos, não formais estão envolvidas na definição de função computável, pois ela se baseia no entendimento do que seja um *processo efetivo*. E, talvez, não coincidentemente, aqui se encontre a interface do que concebemos por uma operação efetiva pela nossa mente com o que está realmente envolvido por trás dessa operação mental. De forma crua, um processo efetivo seria aquele em que podemos encontrar o resultado a partir de passos sucessivos e finitos seguindo regras finitas e determinísticas.[42] Por isso, diz-se que a tese de Church-Turing não pode ser provada ou refutada (no sentido formal). O mais interessante é que ela persiste em nos tentar a acreditar nela. Até hoje toda demonstração feita em S pôde ser feita por uma máquina de Turing. Seria um grande desafio, imerso numa grande possibilidade de ser considerado um mentiroso ou um esquizofrênico, alguém atestar que consegue realizar um processo efetivo em sua mente que não pode ser passado para um computador.[43] Portanto, somos inclinados a dizer sim para a pergunta: um computador pode realizar a prova do capítulo 1? $Pr_{ZFC}[\text{“}S \text{ é consistente”}]$ pode ser obtido por meio de processos computáveis.

Note que as demonstrações desta dissertação possuem propositalmente uma aparência que lembra um pouco a dedução natural (encadeamento de suposições, etc) para ajudar a convencer o leitor de que elas poderiam ser feitas por um computador, já que a dedução natural é uma operação sabidamente computável.

---

[38] ENDERTON, op. cit., p. 199.
[39] LEWIS, H. R.; PAPADIMITRIOU, C. H. **Elementos de Teoria da Computação**. 2ª. ed. Porto Alegre: Bookman, 2000.
[40] ENDERTON, op. cit. p. 200.
[41] ENDERTON, op. cit. p. 199.
[42] ENDERTON, op. cit. p. 60.
[43] Eu, o autor, estou tentando há muito tempo.

Vale ressaltar que não estamos discutindo o aspecto semântico da prova ou das fórmulas envolvidas nela. Não é problema ver que a versão computadorizada está escrita com simbologia diferente (strings sucessivas de zeros e uns) da matemática (em lógica de primeira ordem na linguagem de ZFC[44]). Mas, como já mencionado antes, espera-se que toda prova matemática possa ser traduzida para ZFC. Para simplificar, então, tome apenas o caso de um computador realizando uma operação que quando traduzida para a linguagem de ZFC equivale[45] a aqui presente no capítulo 1. Pois, espera-se que aos nossos olhos, independentemente da simbologia, as duas provas possuam conteúdo semântico logicamente igual.

3.3 Alguma regra infinitária foi usada?

É uma pergunta aparentemente impertinente e incompleta. Qualquer leitor do capítulo 1 deve ter notado que a Infinite Induction Rule (IIR) é usada. Uma regra infinitária é uma regra de inferência que parte de infinitas premissas para chegar a uma conclusão. Na simbologia de dedução natural elas seriam da forma:

$$\frac{A_1 \quad A_2 \quad \ldots \quad A_n \quad \ldots}{B}$$

Portanto, a IIR é um exemplo de regra infinitária. Logo, para manter a boa razoabilidade desse texto só resta apelar para como ela foi usada nessa dissertação (especificamente, no capítulo 1, apesar de haver relação com o princípio de reflexão apresentado no capítulo 2). E é precisamente nesse sentido da palavra "como" que pretendemos nos ater. O ponto central está em diferenciar se a regra infinitária foi representada ou não quando rodamos a prova do capítulo 1 em ZFC.

Primeiro, vamos para a opção mais óbvia. Não operamos com ela nesse texto. Porque, simplesmente, em nenhuma prova ou em nenhum discurso foram usadas infinitas

[44] No capítulo 1 boa parte das demonstrações está em linguagem natural, mas isso está apenas como simplificação, pois elas poderiam ser traduzidas para linguagem matemática sem problemas.
[45] Essa equivalência pode ser definida mediante a presença de um sujeito interpretante. Por exemplo, nós, que lemos a prova.

sentenças, palavras ou frases. Aliás, a grande maioria dos cientistas concordaria que uma demonstração usando regra infinitária não pode ser feita em nenhum aparato, seja natural ou feito pelo homem. Experimente colocá-la num papel, num gravador ou mesmo num computador. Mas poderíamos tê-la representado ou operado com ela fora do texto de alguma forma. Talvez, em nossas mentes. Essa é, possivelmente, uma das opções mais controversas. Porém, antes de a discutirmos um pouco mais, voltemos a um outro ponto de vista.

Considere, por enquanto, somente a demonstração do capítulo 1. Uma regra infinitária está definida lá. Agora, volte ao item 3.2. Toda sua demonstração pode ser formalizada por ZFC e, não só isso, cada passo que demos também pode ser programado em um computador. Põe-se um computador para rodar ZFC e uma hora vai aparecer exatamente a demonstração do capítulo 1. Isso nos revela, e confirma nossa aparente intuição, de que usamos **apenas regras recursivamente definidas** em um número finito de passos, um processo efetivo[46]. Se uma regra infinitária tivesse sido usada nessa prova, a parte em negrito da frase anterior não estaria correta.[47] Por exemplo, tome um computador qualquer e o programe para rodar as demonstrações a partir dos axiomas de ZFC pelo cálculo dedutivo clássico – é dessa forma que, usualmente, fazemos um computador rodar ZFC, como mencionado no item 3.2. A cada output, ele vai nos dando uma fórmula correspondente a uma fórmula de ZFC a partir, sempre, de um número finito de operações. Para a Infinite Induction Rule ser emulada[48] ou ele precisaria gerar um número infinito de fórmulas como output ou ele precisaria gerar um output a partir de um número infinito de operações. Entendendo um computador como equivalente a uma máquina de Turing, como é feito usualmente, fica claro que nenhuma dessas duas opções é válida.

Contudo, a IIR está ali. Uma regra com infinitas premissas pôde ser representada em ZFC – e, por isso, teve que ser representada por um número finito de símbolos – para que S a represente na fórmula $Pr_{ZFC}[Pr_{S_\infty}[\varphi]]$[49], onde φ é uma fórmula na linguagem de S_∞, $Pr_{S_\infty}[\varphi]$ está na linguagem de ZFC e $[Pr_{S_\infty}[\varphi]]$ é o número de Gödel da sentença $Pr_{S_\infty}[\varphi]$?

---

[46] Vide item 3.2.
[47] Atentar para a palavra “apenas”.
[48] É um termo herdado da computação. Basicamente, quer dizer a ação de um programa ao simular outro. Ou seja, dado os mesmos inputs, um sistema sempre gera os mesmos outputs do outro. Por exemplo, quando um jogo de vídeogame está sendo rodado por um computador, dizemos que o computador está emulando tal vídeogame.
[49] Vide item 2.1.5.

Pretendemos indicar como de forma informal, porém, facilmente verificável para alguém familiarizado com ZFC e as demonstrações envolvidas no capítulo 1.

Temos que a sentença $Pr_S[\varphi]$ representa que "Existe x tal que (para todo i, se $\mathrm{d_i}$ é o i-ézimo número da sequência x, então (i) ou (ii) ou (iii)) e $[\varphi]$ é o último número da sequência representada por x", onde:

(i) $\mathrm{d_i}$ é o número de Gödel de um axioma de S;

(ii) $\mathrm{d_i}$ é o número de Gödel de um axioma lógico;

(iii) $\exists j, k < i(\mathrm{d_j}$ é um número da sequência representada por x e é o número de Gödel da fórmula $(\mathrm{A} \rightarrow \mathrm{B})$ e $\mathrm{d_k}$ é um número da sequência representada por x e é o número de Gödel da fórmula A e $\mathrm{d_i}$ é o número de Gödel da fórmula B);

Essa definição pode ser completamente formalizada na linguagem de S, como é feito no primeiro teorema de incompletude.[50]

Vamos fazer algo análogo só que na linguagem da teoria dos conjuntos e para a as árvores de prova de S_∞. Seja $Axiom(x)$ a fórmula de ZFC que define se x é ou não o número de Gödel de um axioma de S_∞.[51] Volte ao item 1.2 para relembrar a definição de level e de árvore. Logo, $Pr_{S_\infty}[\varphi]$ representa a fórmula na linguagem de ZFC que diz "Existe uma árvore tal que (a), (b) e (c)", onde:

(a) $[\varphi]$ é o número de Gödel da sentença φ e que está na linguagem de S_∞;

(b) $[\varphi]$ é o ponto terminal da árvore;

(c) $\forall x(x$ é o número de Gödel de uma fórmula que é um ponto inicial da árvore se, e somente se, $Axiom(x))$;

As maiores dificuldades serão em construir fórmulas que representem o que é uma árvore como no item 1.2. Mas, como já mencionado, são perfeitamente definíveis em ZFC. Por isso, é deixado implícito na fórmula $Pr_{S_\infty}[\varphi]$ uma quarta condição (d) definindo todas as propriedades do item 1.2 pela teoria dos conjuntos. O uso da Infinite Induction Rule está

[50] ENDERTON, op. cit., p. 225.
[51] Vide item 3.1.

dentro dessa condição. Por exemplo, o conjunto L_{i+1} de pontos de level $i+1$ está ligado a um ponto x_{L_i} de level i por uma Infinite Induction Rule se, e somente se,

$$("x_{L_i} \text{ é o número de Gödel da fórmula } \forall x A(x) \vee D") \wedge \forall x(x \in L_{i+1} \rightarrow \exists n(n \in \omega_0 \wedge ("x \text{ é o número de Gödel da fórmula } A(n) \vee D")).$$

Não é do escopo deste trabalho esmiuçar todas essas passagens, traduzindo-as para a linguagem de ZFC. Como já dito antes, basta ter em mente que toda demonstração matemática é tida como traduzível para ZFC.[52] Talvez, isso seja um critério, inconsciente ou não, de validação de uma prova formal pela comunidade matemática atual. Em particular, a teoria dos grafos é mais fácil de ver que pode ser definida por ZFC. Seria suficiente mostrar, então, que, no capítulo 1, não usamos nenhum número infinito de condições para definir o que seja uma árvore, uma Cut, uma Infinite Induction, um level, um grau, etc. O que se acredita que o leitor possa verificar – por exemplo, note que o capítulo 1 possui apenas um número finito de palavras, frases, etc.

Uma coisa é falar que uma pessoa deu infinitos passos, outra é dar infinitos passos como essa pessoa. Por mais simples que pareça, essa alusão cotidiana – nem tão cotidiana assim, pois ninguém que eu conheça é capaz de tal proeza - simboliza bem a problemática que queremos chegar.

Podemos tentar ser mais formais. Um bom exemplo é a própria consistência de S. Tivemos que $S \vdash Pr_{ZFC}[\text{“}S \text{ é consistente”}]$. Porém, S não demonstra sua própria consistência. Contudo, há uma representação do que ZFC é capaz de fazer dentro da linguagem de S[53]. Em particular, desconsiderando o axioma da escolha, o que a teoria dos conjuntos ganha em relação à dos números é o axioma do infinito, como já mencionado no item 2.16.1. Imagine uma teoria T composta pelos axiomas de S mais alguma sentença independente de S[54]. É fácil ver que ela provará tudo que S prova e mais algumas coisas. Isto é uma boa analogia para o que acontece entre ZF e S, dadas as devidas interpretações e restrições de linguagem. Além disso, existe uma fórmula que representa uma demonstração para qualquer extensão finita de S – denotamos por $Pr_T[\varphi]$, onde φ é uma fórmula qualquer na

---

[52] O que por si só, já é uma questão muito interessante.
[53] Justamente, é a sentença $Pr_{ZFC}[\varphi]$, onde φ é uma fórmula qualquer na linguagem da teoria dos conjuntos.
[54] $Con(S)$ é um exemplo.

linguagem da teoria T, que é uma extensão finita de S - mesmo que esta seja mais poderosa que S. De qualquer forma, o que queremos salientar é que um sistema provar que outro prova alguma coisa não é a mesma coisa que esse primeiro sistema provar aquilo que o outro prova. Esta seria a questão na base do que acontece entre o capítulo 1, o item 3.1 e o 3.2.

Continuando por outro caminho, tome qualquer regra de inferência como uma operação, dada as premissas uma máquina abstrata[55] nos devolve a conclusão. Portanto, uma regra infinitária também seria um operador. Usamos a notação

$$\frac{A(0) \vee D \quad A(1) \vee D \quad \ldots \quad A(n) \vee D \quad \ldots}{\forall x A(x) \vee D}$$

para simbolizar a IIR. Mas perceba que é um aglomerado finito de símbolos. Obviamente, as reticências estão simbolizando, conforme seu próprio sentido denotativo, uma suspensão de pensamento ou discurso, omitindo as infinitas fórmulas que deveriam estar ali. Mas isso estaria relacionado com a semântica que essa notação possui, estando relacionado com processos cognitivos, no mínimo.

Nós não precisamos escrever no papel todas as possíveis fórmulas da forma $A(n) \vee D$ e escrever $\forall x A(x) \vee D$ embaixo delas, respectivamente. Porém, ainda resta a possibilidade de termos feito isso mentalmente por meio de processos cognitivos não conscientes de juízo – se o fizéssemos por algum processo consciente, tomaríamos ciência dele, o que não é o caso[56] -, que pode ser uma interpretação daquilo que chamamos de intuição. Veja que não é simples alguém provar que existe tal processo cognitivo, justamente, porque ele não é consciente. É claro que se uma pessoa aparecesse dizendo que consegue conscientemente seria, provavelmente, desacreditado, apesar de que seria muito mais fácil de ser verificado, pelo menos pela própria pessoa.

---

[55] Tanto faz ser um processo cognitivo como um processo físico ou metafísico.

[56] Essa possibilidade não é descartada, mas parece existir um senso comum e científico de que ninguém foi capaz disso até hoje. Um exemplo seria alguém imaginar infinitas bolas ao mesmo tempo, ser capaz de montar uma proposição de tamanho infinito, saber o número de todas as casas do número π de uma vez, etc.

No caso inconsciente[57], o resultado da operação (isto é, da regra de inferência infinitária) seria sempre uma sentença finita. Ou seja, seríamos sempre privados de tomar ciência de qualquer processo cognitivo infinitário, apesar de seu resultado ser "mostrado" a nós. Ocorreria por trás da consciência e a conclusão dessa inferência infinitária seria como qualquer proposição que estamos acostumados a fazer – uma proposição declarativamente finita. Portanto, só nos restaria, para provar que alguma regra infinitária foi "usada", conseguirmos obter uma proposição ou uma representação de um objeto que só possa ser obtida por meio de infinitas operações. Por exemplo, saber a última casa de um número incomputável[58]. Mas note que não é apenas recitar um número ou tomar ciência do conceito de um número, seria preciso comprovar que ele foi obtido por meio de um processo mental equivalente a uma máquina de Turing que pode andar infinitas vezes ou mais. E aqui reside a grande dificuldade. Mesmo que um sujeito vivencie um estado de crença absoluta de que essa proposição, que veio a sua mente, está correta (isto é, de acordo com as regras de inferência infinitária ou dedutivas) em seu pensamento, sua mente ainda o pode estar enganando. Infelizmente, discutir se há parâmetros biológicos e físicos para a averiguação dessa hipótese fugiria completamente do escopo do presente trabalho.

O peculiar e provocante é que, até agora, toda sentença matemática, tida como provadamente verdadeira, pôde ser obtida dedutivamente a partir de ZFC.[59] O que decorre das regras de uma demonstração aceitável, que são consideradas corretas, serem definíveis em ZFC. Mas e se fizéssemos uma demonstração na linguagem de ZFC de que ZFC é consistente, por exemplo? Não entraria em contradição com o segundo teorema de Gödel? Crendo que ZFC seja consistente, na verdade, essa seria uma prova de que a partir de certos pressupostos ZFC é consistente ou de que outro sistema prova a consistência de ZFC ou que o modelo que ZFC está provando que existe para ZFC, ainda não é o dele mesmo (pelo teorema da indefinibilidade de Tarski, não pode existir fórmula em ZFC que defina o que seja uma fórmula verdadeira no modelo do próprio ZFC[60]).

---

[57] Entenda como não consciente. A palavra "inconsciente" geralmente é atrelada aos conceitos da psicanálise, o que não é nossa intenção.

[58] CONTRIBUTORS, W. Chaitin's constant. **Wikipedia, The Free Encyclopedia**, 2011. ISSN 413788003. Disponivel em: <http://en.wikipedia.org/w/index.php?title=Chaitin%27s_constant&oldid=413788003>. Acesso em: 17 Fevereiro 2011.

[59] Obviamente, ainda existem conjecturas que não puderam ser provadas. Mas estas não são tidas como verdadeiras por todos os matemáticos. Muitos ainda duvidam. E, quando a prova delas for feita e aceita pela comunidade matemática, alegamos que ela poderá ser feita em ZFC.

[60] ENDERTON, op. cit., p. 228.

Voltemos ao capítulo 2 e ao princípio de reflexão uniforme: $\forall x Pr_T[\varphi(\dot{x})] \rightarrow \forall x \varphi(x)$, onde φ é uma fórmula qualquer na linguagem de T e tem somente x como variável livre. Interpretando-o pela teoria dos modelos[61], num modelo standard $\mathfrak{N}$, ele ficaria da forma:

$$\left(\neg \forall x(\vDash_{\mathfrak{N}} Pr_T[\varphi(\dot{x})])\right) \vee (\vDash_{\mathfrak{N}} \forall x \varphi(x))$$

Assumindo que um modelo standard satisfazer a fórmula $Pr_T[\varphi(\dot{x})]$ corresponde exatamente à nossa noção de demonstração pelo cálculo dedutivo, o que é bastante aceitável, então poderemos reescrevê-lo por:[62]

$$\left(\exists n \in \mathbb{N}\left(T \nvdash \varphi(\overline{n})\right)\right) \vee (\vDash_{\mathfrak{N}} \forall x \varphi(x))$$

ou seja,

$$\left(\forall n \in \mathbb{N}\left(T \vdash \varphi(\overline{n})\right)\right) \Rightarrow (\vDash_{\mathfrak{N}} \forall x \varphi(x))$$

Neste ponto parece começar a ficar mais claro que tipo de intenção está por trás do princípio de reflexão. Seria criar uma extensão capaz de demonstrar aquelas sentenças verdadeiras num modelo standard e que não eram demonstráveis. Apesar de que, para isso, seria necessário que $T \vdash \forall x Pr_T[\varphi(\dot{x})]$ para qualquer φ tal que $\vDash_{\mathfrak{N}} \forall x \varphi(x)$. Portanto, o ganho principal[63] de $T + RFN(T)$ em relação a T são nas fórmulas φ tais que $T \vdash \forall x Pr_T[\varphi(\dot{x})]$ e $T \nvdash \forall x \varphi(x)$. Dada essa nova forma de entender tal princípio, se torna mais fácil tentar transformá-lo numa regra de inferência. Por exemplo:

$$\frac{Pr_T[\varphi(0)] \quad Pr_T[\varphi(1)] \ \ldots \ Pr_T[\varphi(n)] \ \ldots}{\forall x \varphi(x)} \text{, onde } n \in \mathbb{N}.$$

Querendo dizer exatamente que se $T \vdash \varphi(0)$, $T \vdash \varphi(1)$, ..., $T \vdash \varphi(n)$, ..., então $\forall x \varphi(x)$. Aonde chegamos numa semelhança com a Infinite Induction Rule. Mas vale atentar para as diferenças. Ao contrário da Infinite Induction Rule, suas premissas estão presas a serem provadas somente por T, sem a IIR ter sido usada nenhuma vez. Pois, no caso de S_∞, suas

---

[61] ENDERTON, op. cit., p.82.

[62] A notação $\overline{n}$ representa um símbolo constante qualquer e, como estamos lidando com uma linguagem enumerável num modelo standard, $\overline{n}$ representa algum número natural qualquer.

[63] Pois podem existir casos em que $T \nvdash \forall x Pr_T[\varphi(\dot{x})]$, mas $T + RFN(T) \vdash \forall x Pr_T[\varphi(\dot{x})]$.

premissas podem ser obtidas usando quantas Infinite Induction Rule forem necessárias anteriormente. Portanto, nessa mesma linha de raciocínio, para representarmos essa regra numa extensão de S seria preciso adicionar tanto $\forall x Pr_T[\varphi(\dot{x})] \rightarrow \forall x \varphi(x)$ quanto $\forall x Pr_{T+\forall x Pr_T[\varphi(\dot{x})]\rightarrow \forall x\varphi(x)}[\varphi(\dot{x})] \rightarrow \forall x \varphi(x)$ e assim por diante. Isto é, seria uma extensão do tipo:[64]

$$S + RFN(S) + RFN\big(S + RFN(S)\big) + RFN\Big(S + RFN(S) + RFN\big(S + RFN(S)\big)\Big) + \cdots$$ [65]

Levando-nos a questionar se é possível uma extensão finita de S – vamos denotá-la por S_{RFN} - tal que:

$$S_{RFN} \vdash S + RFN(S) + RFN\big(S + RFN(S)\big) + RFN\Big(S + RFN(S) + RFN\big(S + RFN(S)\big)\Big) + \cdots$$

Se tivesse, o que é relevante é o fato de que não seria uma representação da regra infinitária:

$$\frac{\varphi(0) \quad \varphi(1),\ \ldots,\ \varphi(n),\ \ldots}{\forall x \varphi(x)}$$

Para provar isso basta usar o segundo teorema de Gödel: se S_{RFN} for consistente, então:

$$S_{RFN} \nvdash Con(S_{RFN})$$

e

$$S_{RFN} + \frac{\neg Prov_{S_{RFN}}(0, [0 \neq 0]) \quad \neg Prov_{S_{RFN}}(1, [0 \neq 0]),\ \ldots,\ \neg Prov_{S_{RFN}}(n, [0 \neq 0]),\ \ldots}{\forall x \neg Prov_{S_{RFN}}(x, [0 \neq 0])}$$
$$\vdash Con(S_{RFN})$$

---

[64] Tem uma espécie de recursão parecida com aquela ocorrida quando se monta os números ordinais, por exemplo. Essa semelhança não é puro acaso.

[65] As reticências aqui desempenham um papel crucial no poder que essa extensão terá. A quantidade de iterações determina se essa extensão será recursiva ou não. Para mais detalhes ver FRANZÉN, T. Transfinite Progressions: a second look at completness. **The Bulletin of Symbolic Logic**, v. 10:2, Setembro 2004.

Contudo, pode ser provado, com o auxílio do teorema 2.8, que $T' \nvdash RFN(T)$, onde T' é qualquer extensão finita de T.[66] Logo, $S_{RFN} \nvdash RFN(S)$, e não será possível que exista tal S_{RFN}.

Assim, podemos ver que o princípio de reflexão uniforme tem uma aparência que lembra a IIR. Na verdade, foi pensado já com a intenção de tornar o sistema anterior *Sound*, ou seja, que aquilo que foi provado por ele seja verdadeiro num modelo standard. O que é conseguido também pela IIR.

Porém, tal princípio não pode chegar a ser uma representação de uma regra infinitária. Por exemplo, se tentarmos usar o mesmo processo de atribuição de números de Gödel às demonstrações de S_∞ - isto quer dizer, definir uma fórmula representando a demonstrabilidade em S_∞ -, precisaremos indexar cada ponto da árvore a um número natural de forma a construir uma sequência de números que corresponda biunivocamente à árvore. Mas isto nos levará, em certos casos, à construção de uma sequência infinita de números naturais. Tomando também as propriedades de S_∞ já descritas aqui nesta dissertação, não poderemos construir uma fórmula na linguagem de S_∞ que represente uma demonstração em S_∞. Isto nos leva à impossibilidade de fazer uma demonstração análoga a do primeiro teorema de incompletude de Gödel. Em certos sistemas com regras de inferência infinitárias não "vale Gödel". E, como a linguagem de S_∞ é a mesma de S num modelo standard, a menos de uma transformação de conectivos[67], não será possível construir uma sentença do tipo $Pr_{S_\infty}[\varphi]$ que represente uma demonstração em S_∞ na linguagem de S. Apesar de que foi possível fazê-lo na linguagem de ZFC. Espera-se que fique mais fácil visualizar, por esse exemplo, que qualquer sistema que use regras infinitárias não será representável em S. Pois, se fosse seria possível construir uma demonstração de incompletude *a la* Gödel para S_∞, o que é falso.

Ainda temos que qualquer teoria Y, dedutiva e com finitos axiomas, pode ser emulada por S – pela sentença $Pr_Y[\varphi]$. Portanto, se algum processo efetivo pudesse emular uma regra infinitária, S poderia. O que é falso, pois teríamos uma fórmula representando-a em S.

---

[66] BARWISE, op. cit., p. 848.
[67] Vide capítulo 1.

Mas ZFC é uma teoria dedutiva e com finitos axiomas e ela pôde representar a regra infinitária. É esse o cerne da questão. Apesar de $Pr_{S_\infty}[\varphi]$ representar em ZFC o que seja uma árvore de φ em S_∞, ainda existirão fórmulas φ' que são teoremas de S_∞ tais que $ZFC \nvdash Pr_{S_\infty}[\varphi']$. Pois, senão, $S \vdash Pr_{ZFC}[Pr_{S_\infty}[\varphi']]$ e $Pr_{ZFC}[Pr_{S_\infty}[\varphi]]$ representaria uma demonstração em S_∞ na linguagem de S, o que levaria a um teorema de incompletude, como já dito.

Portanto, essa "representação" em ZFC não é completa e, por isso, não é uma representação verdadeira. Porque ZFC não é capaz de emular S_∞. Isso se traduziria por: ZFC diz o que S_∞ faz, mas não tudo o que S_∞ pode fazer. Voltando à alusão cotidiana já mencionada.

Assim, fica ainda mais forte a hipótese de que não foram atingidos por nós, em qualquer capítulo deste trabalho, resultados através de regras infinitárias. Pois, todas as provas aqui contidas se dão num sistema recursivo de regras. Porém, pode chegar o dia em que constataremos algo matematicamente verdadeiro e que só pode ser demonstrado usando regras infinitárias. Essa seria uma evidência da não-computabilidade da mente, que, talvez, seja uma hipótese para sempre em aberto.

Conclusão

Percorremos algumas demonstrações que envolvem a consistência da aritmética. Somente por se discutir algo que é considerado indemonstrável já se revelam inquietações sobre como demonstrar o que não pode ser demonstrado. É desta propriedade perturbadora que a consistência nos leva a dúvidas sobre sua demonstrabilidade e sobre a nossa própria capacidade de entendê-la. Como algo indemonstrável pode ser demonstrado por nós? Apesar de ser uma pergunta que esconde vários ludos com os significados da palavra "demonstração", ela nos instiga por seu significado mais raso, aquele em que aparece um possível paradoxo, nos restando apenas dissolvê-lo.

Primeiramente tentamos nos descolar daquilo que é incapaz de demonstrar o que queremos – o verbo querer, talvez, já nos prenda ao fardo de conseguir demonstrá-lo. No capítulo 1 apelamos para um sistema formal mais poderoso que a comum dedução. Não se quer perder a teoria formal dos números e, por isso, o sistema S_∞ é construído para englobá-la. Englobando de uma forma em que se almeja a perfeição: um sistema consistente e completo.

Contudo, vimos no capítulo 3 que não é assim tão simples a resposta aos nossos anseios. Calcamo-nos na matemática usual, entendida, mais precisamente, pela teoria dos grafos e dos números para representar uma regra de inferência aparentemente intangível, uma regra infinitária. A matemática usual tem uma estrita ligação com o que entendemos pela teoria dos conjuntos de Zermelo-Fraenkel (ZF) e, por ela, conseguimos, dedutivamente, os mesmos resultados apresentados pela prova *a la* Gentzen mostrada aqui.[1]

Até que ponto tal demonstração de que S, a teoria formal dos números (PA), é de fato consistente realmente nos prova que S seja consistente? O que pudemos provar, se confiarmos em todas essas demonstrações, é que S é um sistema suficientemente forte para provar que outro sistema prova que S é consistente.[2] Mas podemos provar a mesma coisa, passo a passo e com igual validade, se S for realmente inconsistente. Em outras

[1] Do capítulo 1.
[2] Analogamente, o mesmo vale para os teoremas de Gödel.

palavras, todos esses resultados se mantêm provados da mesma forma se S vier a chegar numa contradição um dia.[3]

Poderíamos ter apenas usado uma extensão finita da aritmética como $S + Con(S)$ ou $S + \forall e, r, k \exists M(\text{"}\, M \underset{*}{\rightarrow} (k)_r^e \,\text{"})$,[4] conseguindo o mesmo resultado. Adicionalmente, mesmo que ZF corresponda a algo mais poderoso que uma mera extensão finita de S, todas as questões de indemonstrabilidade se desdobram, da mesma forma, sobre a teoria dos conjuntos pelo conhecido segundo teorema de Gödel. Não só isso, também nos levando a questionar a fundamentação formal de provas de consistência: seríamos obrigados a cair num círculo vicioso, quando nos prendemos ao sistema axiomático, nesse caso?[5]

O que induz, por um caminho ou por outro, a nos depararmos com a própria evidência intuitiva de tais resultados. Por mais estranho e inquietante, há a possibilidade de que a consistência seja algo mentalmente autoevidente, usando a própria matemática usual[6]: um sistema consistente A criando um sistema B que corresponda ao primeiro só poderia nos guiar à consistência de B. Uma redundância bem-vinda de nós por nós mesmos.[7]

Concomitantemente, corremos ao lado do desejo ou da dúvida sobre a capacidade escondida de nossas mentes realizarem operações que não podem ser feitas por um computador, partindo do princípio de que um computador consegue provar tudo que a teoria formal dos números consegue. Sendo que, nesse ponto, possibilidades também ficam em aberto. Tudo feito nesse trabalho poderia ser obtido sem prescindir de um sistema poderoso o suficiente para conter uma regra infinitária, apesar de termos tratado, formalmente, sobre provas num sistema infinitário.[8] O qual pôde ser representado num sistema dedutivo (no caso, ZF) e que deu inspiração para construções de extensões de S (pelos princípios de reflexão) que buscassem emulá-la[9]: um sistema falando o que outro sistema mais poderoso que o primeiro consegue, mas ainda se mantendo mais fraco. Que é, no fundo, um

[3] Caso análogo a ZF ser inconsistente descrito no item 3.1.
[4] Que é o princípio combinatorial de Paris-Harrington do capítulo 2.
[5] Vide item 3.1.
[6] Teoria dos Modelos
[7] Vide item 3.1.
[8] Vide item 3.2.
[9] Vide item 3.3.

problema de linguagem sobre referentes, mesmo estando preso às rígidas formalidades da lógica matemática.

Novamente, vem à superfície a computabilidade da matemática. Porém, sem negar a possibilidade de que, algum dia, algo verdadeiro para nós só possa ser obtido por meio de um sistema não dedutivo (ou seja, dedutivo adicionado de uma regra infinitária). Apesar de que nada apresentado aqui possui essa exclusividade. Ademais, todas as demonstrações de consistência não estão presentes nessa dissertação, mas espera-se que tais outras partam dos mesmos fundamentos, ou sejam feitas de forma análoga, que as aqui mencionadas ou descritas: por uma extensão finita de S (como por $S + Con(S)$ ou $S + \forall e, r, k \exists M(\text{"} \mathrm{M} \underset{*}{\rightarrow} (\mathrm{k})_{\mathrm{r}}^{\mathrm{e}} \text{"})$); por uma extensão recursiva de S (como pelo princípio de reflexão); por uma extensão não recursiva (usando regras infinitárias, por exemplo); por um sistema numa linguagem mais poderosa (em ZF, por exemplo).

Mas se toda a matemática feita por nós pode ser computável, mais interessante ainda é perceber que essa impossibilidade de demonstrarmos, em última instância, que a aritmética é realmente consistente sem recorrer a pressupostos arbitrários (outros sistemas axiomáticos) ou argumentos não matemáticos corrobora com que a aritmética seja, realmente, consistente, pelo segundo teorema de Gödel. Uma ironia godeliana.

Pretende-se, como o ponto de maior concordância sobre esta dissertação, que fiquem bem estabelecidas as provas de consistência, principalmente a do capítulo 1 - já que no cap. 2 omitimos muitos teoremas em relação ao princípio combinatorial de Paris-Harrington - do ponto de vista lógico matemático e dentro de um consenso sobre o que seja um discurso matemático válido, inclusive porque já são resultados conhecidos na literatura. Mesmo considerando uma possível falta de fundamentação formal para que eles sejam absolutamente verdadeiros, como defendido nessa dissertação.[10] E que, por fim, por esses dois motivos, justamente, configura-se, talvez, a ironia, mencionada no parágrafo anterior, de algo intuitivamente óbvio não poder ser formalmente atestado sem recorrer, em última instância, à nossa própria intuição (um argumento não matemático), ao mesmo tempo em que outros sistemas formais, inclusive dedutivos, possam demonstrá-lo. Este “algo” é, aqui, a consistência da aritmética.

---

[10] Vide item 3.1.

Referências

BARWISE, J. (Ed.). **Handbook of Mathematical Logic**. Amsterdam: Elsivier Science Publisher B.V., 1977. ISBN 0444863885.

BEKLEMISHEV, L. D. Reflection principles and provability. **Russian Mathematical Surveys**, v. 60:2, p. 197–268, 11 Janeiro 2005.

CONTRIBUTORS, W. Philosophy of mind. **Wikipedia, The Free Encyclopedia**, 2009. ISSN 308403498. Disponivel em:<http://en.wikipedia.org/w/index.php?title=Philosophy_of_mind&oldid=308403498>. Acesso em: 17 Fevereiro 2011.

CONTRIBUTORS, W. Chaitin's constant. **Wikipedia, The Free Encyclopedia**, 2011. ISSN 413788003. Disponivel em: <http://en.wikipedia.org/w/index.php?title=Chaitin%27s_constant&oldid=413788003>. Acesso em: 17 Fevereiro 2011.

DORIA, F. A.; CARNIELLI, W. A. Are the Foundations of Computer Science Logic–Dependent? **Dialogues, Logics and Other Strange Things**, 20 Outubro 2008.

ENDERTON, H. **A mathematical introduction to logic**. 2 ed. Boston, MA: Academic Press, 2001. Cap. 1.3. ISBN 978-0-12-238452-3.

FRANZÉN, T. Transfinite Progressions: a second look at completness. **The Bulletin of Symbolic Logic**, v. 10:2, Setembro 2004.

HORSTEN, L. Philosophy of Mathematics. **The Stanford Encyclopedia of Philosophy**, 29 Agosto 2008. Disponivel em: <http://plato.stanford.edu/archives/fall2008/entries/philosophy-mathematics/>. Acesso em: 17 fev. 2011.

JOHNSON-LAIRD, P. N. **Mental Models**. 6 ed. Cambridge: Harvard University Press, 1995.

KUNEN, K. **A Ramsey Theorem in Boyer-Moore Logic**. Madison, Wisconsin: Computer Sciences Department, University of Wisconsin, 1995.

LEWIS, H. R.; PAPADIMITRIOU, C. H. **Elementos de Teoria da Computação**. 2 ed. Porto Alegre: Bookman, 2000.

MENDELSON, E. **Introduction to Mathematical Logic**. 2ª. ed. Princeton, New Jersey: D. Van Nostrand Company, Inc., 1964.

PITT, D. Mental Representation. **The Stanford Encyclopedia of Philosophy**, 2008. Disponivel em: <http://plato.stanford.edu/archives/fall2008/entries/mental-representation/>. Acesso em: 17 Fevereiro 2011.