O Teorema da Completude e os Teoremas da Incompletude de Gödel

Alexssandra Thais Pereira Alves de Souza

Universidade Federal do ABC

Título: O Teorema da Completude e os Teoremas da Incompletude de Gödel

Autor: Alexssandra Thais Pereira Alves de Souza
Orientadora: Prof.ª Dr.ª Ana Carolina Boero

Trabalho de Conclusão de Curso apresentado como requisito parcial para obtenção do título de Bacharela em Matemática pela Universidade Federal do ABC.

Banca Examinadora:

Prof.ª Dr.ª Ana Carolina Boero
Universidade Federal do ABC

Prof. Dr. Jair Donadelli Júnior
Universidade Federal do ABC

Prof. Dr. Rodrigo Roque Dias
Universidade Federal do ABC

Santo André, 14 de setembro de 2023.

Sumário

"Daria um filme
Uma negra e uma criança nos braços
Solitária na floresta de concreto e aço
Veja, olha outra vez o rosto na multidão
A multidão é um monstro sem rosto e coração

Hei, São Paulo, terra de arranha-céu
A garoa rasga a carne, é a Torre de Babel
Família brasileira, dois contra o mundo
Mãe solteira de um promissor vagabundo

Luz, câmera e ação, gravando a cena vai
Um bastardo, mais um filho pardo sem pai
Hei, senhor de engenho, eu sei bem quem você é
Sozinho cê num guenta, sozinho cê num entra a pé

[...]

Eu recebi seu ticket, quer dizer kit
De esgoto a céu aberto e parede madeirite
De vergonha eu não morri, to firmão, eis-me aqui
Você não, cê não passa quando o mar vermelho abrir

Eu sou o mano, homem duro, do gueto, Brown, oba
Aquele loco que não pode errar
Aquele que você odeia amar nesse instante
Pele parda e ouço funk
E de onde vem os diamante? Da lama
Valeu mãe, negro drama"

Negro Drama - Racionais MC's

AGRADECIMENTOS

Em primeiro lugar agradeço imensamente à minha mãe, Gilda, e à minha irmã, Fernanda, que sempre me apoiaram de todas as formas possíveis e confiaram em minhas escolhas. O que quer que eu faça é por nós, por amor.

Agradeço a todos os amigos que fiz durante o Bacharelado em Ciência e Tecnologia, em especial, à Roberta e ao Gabriel por todo tempo que passamos juntos fazendo listas. Ao Victor por tudo que compartilhamos durante minha curta jornada na física e sua curta jornada na matemática. Aos amigos que o Victor me trouxe, Nati, Helo, Leo e Hugo, por todo o tempo compartilhado na sala 202.

Agradeço ao amigos que o Bacharelado em Matemática me trouxe, Borgiani, Greg, Julia, Henrique, Nathan e Willyan, por tudo que compartilhamos na matemática e na vida. E agradeço ao Daniel, que foi meu companheiro durante a graduação, por me apoiar de todas as formas em todos os momentos e em todos os aspectos da minha vida, e por acreditar, incondicionalmente, em mim.

Agradeço também a todos os professores, técnicos administrativos e servidores terceirizados da UFABC que fizeram parte, direta ou indiretamente, da minha formação acadêmica. Me sinto sortuda por ter recebido a formação e o apoio do corpo docente do Bacharelado em Matemática da UFABC. Agradeço ainda a toda a organização do I e II Encontro Brasileiro de Mulheres Matemáticas da UFABC pelo voto de confiança em uma ideia que, entre muitos resultados, fez com que criássemos laços entre nós alunas e com nossas professoras. A universidade pública é minha segunda casa.

Agradeço ao Racionais MC's por estar comigo nos momentos mais difíceis em que eu não soube me expressar pra ninguém, me fazer ter orgulho de toda a minha trajetória e me ensinar a não desistir.

Um obrigada especial ao Rodrigo, que me acompanhou praticamente desde o primeiro dia de aula na UFABC, me guiou e apoiou durante toda a graduação e me fez não desistir da matemática quando Análise Real I me atingiu. Que me apresentou à área de pesquisa na qual me encontrei e compartilhou comigo seu entusiasmo.

E claro, um agradecimento muitíssimo especial à Ana. Por todas as reuniões em que compartilhamos o entusiasmo pelos resultados que aqui apresentamos, e, para além da matemática, por ser exemplo vivo da bondade, em um sentido muito amplo. Uma vez a Ana me disse que chegamos onde estamos agora graças às oportunidades que tivemos e a bondade das pessoas ao nosso redor.

Por fim, mas não menos importante, agradeço à Alexssandra do passado por todo esforço e dedicação empenhados a este TCC e à vida acadêmica. Ela fez um ótimo trabalho! (Mas não poderia deixar de destacar aqui que tudo o que construí foi graças às oportunidades que tive acesso. Que ninguém use minha história individual para apontar uma falsa meritocracia.)

Com toda certeza esses poucos parágrafos de agradecimento deixaram de fora nomes que me ajudaram direta ou indiretamente ao longo desses 5 anos. Saibam que sou imensamente grata a todos! $\heartsuit$

Resumo

Neste trabalho de conclusão de curso estudamos o Teorema da Completude e os Teoremas da Incompletude de Gödel. O Teorema da Completude afirma, grosso modo, que, toda sentença (de primeira ordem) que é verdadeira em todos os modelos de uma dada teoria deve ser logicamente dedutível nesta teoria, e vice-versa. Os Teoremas da Incompletude afirmam, grosso modo, que se uma teoria é consistente e capaz de expressar a aritmética de Peano, então ela é incompleta e não pode provar sua própria consistência. Os teoremas de Gödel são resultados de muita importância e que geraram um grande impacto, além de serem muito bonitos e apresentarem ideias e argumentações extremamente elegantes (do ponto de vista estético de um matemático). Por fim, este trabalho foi pensado para ser uma referência para a compreensão dos resultados aqui mostrado, precisando somente de conhecimento básico de teoria de conjuntos.

Palavras-chave: Teorema da Completude de Gödel, Teoremas da Incompletude de Gödel, lógica de primeira ordem.

Abstract

In this undergraduate thesis we study Gödel's Completeness Theorem and Gödel's Incompleteness Theorems. The Completeness Theorem states, roughly speaking, that every (first-order) sentence that is true in all models of a given theory must be logically deducible in this theory, and vice versa. The Incompleteness Theorems roughly state that if a theory is consistent and able to express Peano's arithmetic, then it is incomplete and cannot prove its own consistency. Gödel's theorems are very important results that have generated a great impact, besides being very beautiful and presenting extremely elegant ideas and arguments (from the aesthetic point of view of a mathematician). Finally, this work was designed to be a reference for understanding the results shown here, requiring only basic knowledge of set theory.

Keywords: Gödel's Completeness Theorem, Gödel's Incompleteness Theorems, first order logic.

Introdução

No fim do século XIX, Georg Cantor deu início à teoria dos conjuntos ao usar bijeções para comparar o tamanho de conjuntos e mostrando que existem infinitos de tamanho diferentes, como por exemplo infinitos enumeráveis e não enumeráveis. Após este trabalho, outros matemáticos como Gottlob Frege e Bertrand Russell perceberam que era possível usar a lógica para fundamentar a matemática, e que para isto seria necessário construir uma lógica simbólica dotada de uma linguagem que fosse universal. Eles notaram que seria possível utilizar a teoria dos conjuntos desenvolvida principalmente por Cantor, mas Russell apontou algumas inconsistências desta teoria à época. Até então, um conjunto era qualquer coleção de objetos que satisfazem uma determinada propriedade. Ele então propôs que considerássemos o conjunto $S = \{X : X \notin X\}$ e poderíamos em particular perguntar se S é um elemento de S. Se $S \in S$ então pela definição de S temos que $S \notin S$, e se $S \notin S$ então pela definição de S temos que $S \in S$. Teríamos então uma contradição. Este é conhecido como o Paradoxo de Russell, que apontou a necessidade de uma noção mais precisa do que era um conjunto. Russell e Alfred Whitehead escreveram o *Principia Mathematica* com o objetivo de fundamentar as bases da matemática e para contornar o paradoxo de Russell eles desenvolveram a teoria dos tipos. Tais trabalhos foram importantes para o início do desenvolvimento da lógica simbólica e fundamentação matemática.

Em 1900, no Congresso Internacional de Matemáticos de Paris, David Hilbert expôs 23 problemas que ele acreditava que seriam relevantes para a matemática do século que se iniciava. O segundo problema tratava de demonstrar que a aritmética de Peano é consistente, isto é, não leva a contradições. Em 1921 ele iniciou o programa de Hilbert com o intuito de estabelecer um sistema para a formalização da matemática. Dois dos principais princípios para tal sistema estabeleciam que ele fosse consistente e decidível, isto é, que para toda fórmula φ expressa na linguagem do conjunto de axiomas, ou φ ou sua negação fosse consequência lógica do conjunto de axiomas. Com seu programa, Hilbert pretendia encerrar as questões da fundamentação "de uma vez por todas" [9]. A célebre frase de Hilbert, que encontra-se atualmente gravada em sua lápide, “devemos saber, saberemos”, expressava sua crença de que seria apenas uma questão de tempo para saber a resposta de qualquer problema matemático. Tal programa estimulou diversos resultados importantes, como o Teorema da Completude de Gödel, que culminou no início da teoria de modelos:

Teorema 0.1 (Teorema da Completude de Gödel) *Seja Σ um conjunto de sentenças da linguagem $\mathcal{L}$ para a lógica de primeira ordem. Então:*

1. $Con_{\models}(\Sigma)$ *se, e somente se,* $Con_{\vdash,\mathcal{L}}(\Sigma)$.

2. *Para toda sentença φ de $\mathcal{L}$, $\Sigma \models \varphi$ se, e somente se, $\Sigma \vdash_{\mathcal{L}} \varphi$.*

Escrevemos $Con_{\models}(\Sigma)$ para expressar que Σ é semanticamente consistente, ou seja, existe uma estrutura $\mathfrak{E}$ tal que para toda sentença $\varphi \in \Sigma$ tem-se que φ é verdade em $\mathfrak{E}$. Já $Con_{\vdash,\mathcal{L}}(\Sigma)$ expressa a consistência sintática de Σ, que remete ao conceito de não haver contradições deduzidas a partir Σ. Então este teorema mostra que as noções de consistência sintática e semântica são equivalentes — em outras palavras, ele diz que uma teoria é (sintaticamente) consistente se e somente se admite modelo. O Teorema da Completude foi formulado e demonstrado pela primeira vez por Kurt Gödel em 1929 e no mesmo ano Jacques Herbrand desenvolveu, de maneira independente, um método para construir um modelo para uma dada teoria usando os termos da linguagem dessa teoria. Em 1949 Leon Henkin se baseou no método de Herbrand de construção de modelos para demonstrar o Teorema da Completude, e é esta demonstração que apresentaremos neste trabalho.

Outros resultados importantes, e surpreendentes, são os Teoremas da Incompletude de Gödel, que colocaram um fim no programa de Hilbert.

Teorema 0.2 (Primeiro Teorema da Incompletude de Gödel [6]) *Seja T uma teoria na linguagem $\mathcal{L}_A$ satisfazendo as seguintes condições:*

1. *T tem um conjunto de axiomas recursivo;*

2. $\vdash_T 0 \neq \overline{1}$;

3. *toda função recursiva é representável em T.*

Então, se T é consistente, não ocorre $\vdash_T \mathcal{G}$, e se T é ω-consistente então não ocorre $\vdash_T \neg\mathcal{G}$, onde $\mathcal{G}$ é uma sentença de Gödel. Consequentemente, se T é ω-consistente então $\mathcal{G}$ é uma sentença indecidível de T.

Em outras palavras, uma teoria que satisfaz as condições do Primeiro Teorema da Incompletude de Gödel será incompleta, pois existirá uma sentença que não pode ser demonstrada nem refutada na teoria. Afirmações assim são denominadas *independentes*. John Barkley Rosser mostrou em 1936 que a hipótese "ω-consistente" poderia ser substituída por "consistente" no enunciado do teorema anterior, obtendo assim um resultado mais forte, já que ω-consistência implica consistência. Um conjunto de axiomas que surgiu à época e é atualmente amplamente aceito é ZFC (axiomas de Zermelo-Fraenkel e o Axioma da Escolha). O primeiro problema da lista de Hilbert era demonstrar a Hipótese do Contínuo (CH), que é a afirmação de que $2^{\aleph_0} = \aleph_1$, que Cantor havia passado seus últimos anos tentando provar. Após sua morte foi demonstrado por Gödel e mais recentemente por Paul Cohen que CH é independente de ZFC. Logo, seria impossível demonstrar CH ou a negação de CH a partir de ZFC. Esta é uma das primeiras afirmações independentes de ZFC, e outras mais conhecidas atualmente são o Axioma de Martin e a Hipótese de Suslin. Há ainda resultados de afirmações que são dedutíveis em ZF, mas independentes da Aritmética de Peano. Tais resultados podem ser encontrados em [2] e [7].

Outro importante resultado é o Segundo Teorema da Incompletude de Gödel:

Teorema 0.3 (Segundo Teorema da Incompletude de Gödel [6]) *Se $\mathcal{P}$ é consistente, então não ocorre $\mathcal{P} \vdash_{\mathcal{L}_{\mathcal{A}}} Cons_{\mathcal{P}}$.*

A teoria $\mathcal{P}$ no enunciado do teorema representa uma teoria capaz de expressar a aritmética dos naturais baseada nos axiomas de Peano. Em outras palavras, o teorema nos diz que se $\mathcal{P}$ é consistente então sua consistência não é um teorema de $\mathcal{P}$ — em outras palavras, que $\mathcal{P}$ não prova sua própria consistência.

Este trabalho é composto por 5 capítulos. No primeiro capítulo introduzimos a Notação Polonesa e estabelecemos um alfabeto para a lógica de primeira ordem nesta notação, com o qual definimos os termos e fórmulas desta linguagem. No segundo capítulo introduzimos noções semânticas da lógica de primeira ordem, tais como valoração para termos e fórmulas. No terceiro capítulo introduzimos a noção de prova formal e formalizamos alguns argumentos clássicos utilizados em demonstrações. No quarto capítulo provamos o Teorema da Completude e no quinto capítulo provamos os Teoremas da Incompletude.

1 Linguagem para a lógica de primeira ordem

Nosso objetivo neste capítulo é fixar uma linguagem para a lógica de primeira ordem. Na primeira seção definiremos a noção de alfabeto e veremos a regra de formação de uma expressão, em um alfabeto fixado, na Notação Polonesa. Na segunda seção veremos que uma linguagem para a lógica de primeira ordem é constituída de um alfabeto e de expressões na Notação Polonesa que obedecem a determinadas regras de formação, que chamaremos de termos e fórmulas. As principais referências bibliográficas para este capítulo são [3] e [5].

1.1 Notação Polonesa

Iniciaremos com a definição do objeto mais simples para construir nossa linguagem. Tal objeto é o alfabeto, cujos elementos são os blocos dos quais uma expressão é constituída. Fixado um alfabeto, há diversas formas de representar uma expressão. Utilizaremos aqui a representação de uma expressão na Notação Polonesa — a vantagem de tal escolha será explorada mais adiante.

Definição 1.1 *Um* ***alfabeto*** *é um par* $(\mathcal{W}, \alpha)$*, onde* $\mathcal{W}$ *é um conjunto de símbolos e* $\alpha : \mathcal{W} \to \omega$ *é uma função e* ω *denota o conjunto dos números naturais. Seja* $\mathcal{W}_n = \{s \in \mathcal{W} : \alpha(s) = n\}$*. Dizemos que os símbolos em* $\mathcal{W}_n$ *possuem* ***aridade*** n *(ou são* ***símbolos*** n***-ários****). Uma* ***expressão*** *(bem formada) de* $(\mathcal{W}, \alpha)$ *na Notação Polonesa é uma sequência construída recursivamente pela seguinte regra:*

Se $s \in \mathcal{W}_n$ *e* τ_i *é uma expressão para cada* $i < n$*, então* $s\tau_0 ... \tau_{n-1}$ *é uma expressão.*

Nesta definição, a palavra "símbolo" não possui significado específico. Poderíamos ter dito "elementos" de $\mathcal{W}$, mas escolhemos a palavra "símbolo" para se relacionar com a noção intuitiva de blocos fundamentais que, quando juntos e respeitando uma determinada regra, possuem novos significados (as expressões). A palavra "alfabeto" também explicita esta ideia, onde a junção de letras (símbolos) formam palavras (expressões). Quando a aridade de todo símbolo do conjunto $\mathcal{W}$ for clara, simplesmente escreveremos $\mathcal{W}$ ao invés de $(\mathcal{W}, \alpha)$.

Note que todo elemento de $\mathcal{W}_0$ é uma expressão de $(\mathcal{W}, \alpha)$, uma vez que não existe $i \in \omega$ satisfazendo $i < 0$. E ainda, procuramos destacar, por meio da locução "bem formada", que estamos interessados em expressões que "façam sentido". Por exemplo, a sequência $= x$ é uma sequência finita de símbolos, mas não é o que chamamos de expressão (bem formada), pois $=$ é um símbolo binário e, portanto, deve ser seguido de duas expressões, mas está seguido de apenas uma expressão.

Por exemplo, o conjunto $\mathcal{W} = \{x, y, z, +, \cdot, !\}$ e a função α que associa x, y, z ao número 0, $!$ ao número 1 e $+, \cdot$ ao número 2 formam um alfabeto. Neste caso temos $\mathcal{W}_0 = \{x, y, z\}$, $\mathcal{W}_1 = \{!\}$, $\mathcal{W}_2 = \{+, \cdot\}$ e os demais $\mathcal{W}_n$ para $n > 2$ são vazios. Assim, as seguintes sequências de símbolos são exemplos de expressões (bem formadas) de $(\mathcal{W}, \alpha)$ na Notação Polonesa: x, $!y$, $+xy$, $\cdot zy$, $+x \cdot y!z$.

A Notação Polonesa possui a desvantagem de ser mais difícil de ser lida. Por exemplo, $\cdot + x!y+!zy$ é a Notação Polonesa da expressão $(x + y!) \cdot (z! + y)$ escrita na linguagem usual. A forma usual de denotar é mais fácil de ser lida (talvez por ser a notação que estamos acostumados a usar), mas a vantagem da Notação Polonesa é a unicidade de leitura sem a necessidade do uso de parênteses ou de convenções sobre a precedência dos símbolos. Tal unicidade será de grande importância para o que faremos posteriormente.

A unicidade da expressão $\cdot + x!y+!zy$ pode ser facilmente verificada usando a definição de expressão. Por exemplo, como o primeiro símbolo da expressão $\cdot + x!y+!zy$ tem aridade 2, segue da definição de expressão que existem σ_1 e σ_2 expressões tais que $\cdot+x!y+!zy$ é escrita como $\cdot\sigma_1\sigma_2$. E note que se σ_1' e σ_2' são expressões tais que $\cdot + x!y+!zy$ é $\cdot\sigma_1'\sigma_2'$, então $\sigma_1 = \sigma_1'$ e $\sigma_2 = \sigma_2'$. Com efeito, o primeiro símbolo de σ_1 e σ_1' é o símbolo da operação binária $+$, então as duas próximas expressões devem ser alvo de atuação deste símbolo. O símbolo seguinte é x, que é um símbolo de aridade 0, portanto, x é uma expressão em si (e a primeira a ser alvo de atuação da operação $+$). O símbolo seguinte é a operação unária $!$, seguida do símbolo y de aridade 0. Portanto, os símbolos $!y$ formam a segunda expressão que sucede o símbolo $+$. Logo obtemos a expressão $+x!y$, que é a Notação Polonesa de $x + y!$. De forma análoga, a expressão seguinte deve ser $+!zy$, que é a Notação Polonesa de $z! + y$, e é a segunda expressão depois do símbolo binário $\cdot$. Logo, na notação usual obtemos a expressão $(x + y!) \cdot (z! + y)$. Assim, as expressões τ_1 e τ_1' devem ser obrigatoriamente iguais à expressão $+x!y$, e as expressões τ_2 e τ_2' devem ser obrigatoriamente iguais à expressão $+!zy$, pois estas são as duas únicas expressões que são alvo de atuação da operação $\cdot$. Em geral, essa unicidade nos é garantida pelo Teorema 1.2. Para demonstrá-lo, dada $\tau \in \mathcal{W}^{<\omega}$, ou seja, τ é uma sequência finita de símbolos de $\mathcal{W}$, denotaremos por $|\tau|$ o comprimento de τ.

Teorema 1.2 (Unicidade de representação) *Seja σ uma expressão do alfabeto $(\mathcal{W}, \alpha)$ na Notação Polonesa. Então:*

1. *Nenhum segmento inicial próprio de σ é uma expressão.*
2. *Se o primeiro símbolo de σ é o símbolo s de aridade n, então existem expressões únicas $\tau_0, ..., \tau_{n-1}$ tais que σ é a expressão $s\tau_0...\tau_{n-1}$.*

Demonstração: Seja σ uma expressão de $(\mathcal{W}, \alpha)$ na Notação Polonesa. Mostraremos tal resultado por indução em $|\sigma|$. Se $|\sigma| = 1$, como σ não possui segmentos iniciais próprios, se o primeiro símbolo de σ é s então σ é a expressão s. Logo valem 1 e 2. Suponha agora que as duas condições valem para toda expressão de comprimento menor que $|\sigma|$. Suponha também que o primeiro símbolo de σ é o símbolo s de aridade $n \geq 1$. Pela definição de expressão, temos que existem τ_0, ..., τ_{n-1} expressões tais que σ é a expressão $s\tau_0...\tau_{n-1}$.

Seja σ' uma expressão que é um segmento inicial de σ. Mostraremos que $\sigma' = \sigma$. Pela definição de expressão (e por σ' ser um segmento inicial de σ, seu primeiro símbolo é s, e s possui aridade n), existem τ'_0, ..., τ'_{n-1} expressões tais que σ' é a expressão $s\tau'_0...\tau'_{n-1}$. Dessa forma segue que $\tau_0 = \tau'_0$, pois, caso contrário, ou $s\tau_0$ é um segmento inicial próprio de $s\tau'_0$ ou $s\tau'_0$ é um segmento inicial próprio de $s\tau_0$. E consequentemente, ou τ_0 é um segmento inicial próprio de τ'_0 ou τ'_0 é um segmento inicial próprio de τ_0, o que é um absurdo, pois τ_0 e τ'_0 são expressões tais que $|\tau_0| < |\sigma|$ e $|\tau'_0| < |\sigma|$.

Mostraremos agora que $\tau_i = \tau'_i$ para todo $0 \leq i \leq n-1$, e faremos isto por indução em i. O caso base foi feito no parágrafo anterior. Suponha então que para todo $j < i$ tem-se $\tau_j = \tau'_j$. Então σ é a expressão $s\tau_0...\tau_{i-1}\tau_i\tau_{i+1}...\tau_{n-1}$ e a expressão $s\tau_0...\tau_{i-1}\tau'_i\tau'_{i+1}...\tau'_{n-1}$. Se $\tau_i \neq \tau'_i$, ou $s\tau_0...\tau_{i-1}\tau_i$ é um segmento inicial próprio de $s\tau_0...\tau_{i-1}\tau'_i$ ou vice-versa. E então ou τ_i é um segmento inicial próprio de τ'_i ou vice-versa, o que é um absurdo, pois τ_i e τ'_i são expressões tais que $|\tau_i| < |\sigma|$ e $|\tau'_i| < |\sigma|$.

Dessa forma, obtemos que $\tau_i = \tau'_i$ para todo $i < n$, e então $\sigma = \sigma'$. Assim garantimos a condição 2 e, como σ' era um segmento inicial arbitrário de σ, segue que todo segmento inicial de σ que é uma expressão é o próprio σ, e consequentemente não é um segmento inicial próprio. Logo, vale a condição 1. $\square$

Vejamos alguns conceitos importantes sobre expressões.

Definição 1.3 *Se σ é uma expressão do alfabeto $(\mathcal{W}, \alpha)$ na Notação Polonesa, definimos uma **subexpressão** de σ como uma sequência consecutiva de símbolos de σ que é também* *uma expressão.*

No caso da expressão $\cdot + x!y+!zy$ que havíamos visto, a sequência $\cdot+$ não é uma subexpressão, pois embora seja uma sequência consecutiva de símbolos de $\cdot + x!y+!zy$, não é uma expressão. A sequência $+xz$ também não é uma subexpressão de $\cdot + x!y+!zy$, pois embora seja uma expressão, não é uma sequência consecutiva de símbolos de $\cdot + x!y+!zy$. Já as sequências x, $!z$, $+!zy$ e $\cdot + x!y+!zy$ são subexpressões de $\cdot + x!y+!zy$.

Note ainda que cada símbolo em uma expressão é o início de uma subexpressão. Por exemplo, na expressão $\cdot x + yz$, $\cdot$ é o início da subexpressão $\cdot x + yz$, x é o início da subexpressão x, $+$ é o início da subexpressão $+yz$ e y e z são o início das subexpressões y e z, respectivamente. Mais geralmente, temos o seguinte resultado.

Teorema 1.4 *Se σ é uma expressão do alfabeto $(\mathcal{W}, \alpha)$ na Notação Polonesa, então em toda ocorrência de um símbolo em σ temos o início de uma única subexpressão de σ.*

Demonstração: Seja σ uma expressão de $(\mathcal{W}, \alpha)$ na Notação Polonesa. Faremos a demonstração deste resultado por indução em $|\sigma|$. Suponha que $|\sigma| = 1$. Então σ é uma expressão que contém apenas um símbolo. Dessa forma, se p é um símbolo que ocorre em σ, então σ é a expressão p. Portanto, em p temos o início de uma única subexpressão de σ — a saber, a própria σ.

Suponha que o resultado do enunciado vale para toda expressão de comprimento estritamente menor que $|\sigma|$. Seja p uma ocorrência de um símbolo em σ. Pela regra de formação de expressões, temos que existem $s \in \mathcal{W}_n$ e $\tau_0, ..., \tau_{n-1}$ expressões tais que σ é a expressão $s\tau_0...\tau_{n-1}$. Se p é o primeiro símbolo de σ, isto é, se p é o símbolo s, então segue o resultado pelo item (1) do Teorema 1.2. Suponha então que p não é o primeiro símbolo. Então p ocorre dentro de alguma expressão τ_i para $i \in \{0, ..., n-1\}$. Como τ_i é uma expressão com comprimento estritamente menor que o comprimento de σ, então pela hipótese de indução segue que em p ocorre o início de uma única subexpressão, digamos φ, de τ_i. E note que uma subexpressão de τ_i é também uma subexpressão de σ, pois é uma sequência consecutiva de símbolos de σ que também é uma expressão. Assim, pelo item (2) do Teorema 1.2 existem expressões únicas $\tilde{\tau}_0, ..., \tilde{\tau}_{k-1}$ tais que φ é a expressão $p\tilde{\tau}_0...\tilde{\tau}_{k-1}$, onde k é a aridade de p. Pelo item (1) do Teorema 1.2 nenhuma expressão ψ que se inicia em p pode ser uma subexpressão própria de $p\tilde{\tau}_0...\tilde{\tau}_{k-1}$ e nem $p\tilde{\tau}_0...\tilde{\tau}_{k-1}$ pode ser uma subexpressão própria de ψ. Desta forma, segue que $\psi = \varphi$, e então vale a unicidade de φ, portanto segue o resultado. $\square$

Pelo Teorema 1.4, podemos definir o escopo de uma ocorrência de um símbolo em uma expressão.

Definição 1.5 *Se σ é uma expressão do alfabeto $(\mathcal{W}, \alpha)$ na Notação Polonesa, então o* ***escopo*** *de uma ocorrência de um símbolo em σ é a única subexpressão de σ que se inicia em tal ocorrência.*

Por exemplo, se tomarmos a expressão σ dada por $\cdot + xy + zw$, então o escopo de $\cdot$ é a própria expressão σ, o escopo do primeiro $+$ é a expressão $+xy$, e o escopo do segundo $+$ é a expressão $+zw$. Note que escopo de todo símbolo de aridade 0 é a expressão formada pelo próprio símbolo, então os escopos de x, y, z e w são x, y, z e w, respectivamente.

1.2 Linguagem de primeira ordem

Nosso objetivo nesta seção é construir uma linguagem para a lógica de primeira ordem, ou simplesmente, uma linguagem de primeira ordem. Tal linguagem será constituída por um alfabeto e por uma coleção de expressões deste alfabeto na Notação Polonesa que obedecem a determinadas regras. Começamos fixando alguns elementos que utilizaremos recorrentemente.

Definição 1.6 *Chamamos de* ***símbolos lógicos*** *os símbolos:*

$$\wedge \quad \vee \quad \neg \quad \rightarrow \quad \leftrightarrow \quad \forall \quad \exists \quad =$$

junto com os elementos de um conjunto infinito enumerável VAR de variáveis.

Note que as variáveis são símbolos de aridade 0. Os símbolos $\forall$ e $\exists$ são comumente chamados de **quantificadores universal e existencial**, respectivamente. O símbolo $\neg$ tem aridade 1 e os demais símbolos lógicos possuem aridade 2.

Definição 1.7 *Um* ***alfabeto para a lógica de primeira ordem*** *é constituído dos símbolos lógicos e de um conjunto $\mathcal{L}$ (cujos elementos são chamados de* ***símbolos não lógicos****), particionado como $\mathcal{L} = \mathcal{F} \cup \mathcal{P}$. Os conjuntos $\mathcal{F}$ e $\mathcal{P}$, por sua vez, são particionados por aridade: $\mathcal{F} = \bigcup_{n\in\omega} \mathcal{F}_n$ e $\mathcal{P} = \bigcup_{n\in\omega} \mathcal{P}_n$. Para cada $n \in \omega$ com $n > 0$, os símbolos em $\mathcal{F}_n$ são chamados* ***símbolos de funções n-árias*** *e os símbolos em $\mathcal{P}_n$ são chamados* ***símbolos de predicados n-ários****, ou mais comumente,* ***símbolos de relações n-árias****. Já os símbolos em $\mathcal{F}_0$ são chamados de* ***símbolos de constantes*** *e os símbolos em $\mathcal{P}_0$ são chamados de* ***letras proposicionais****.*

Em muitos dos exemplos que veremos, a maior parte dos conjuntos da forma $\mathcal{F}_n$ e $\mathcal{P}_n$ são vazios. Por exemplo, para axiomatizar a teoria dos conjuntos, é suficiente considerar um alfabeto cujo único símbolo não lógico é o símbolo de relação $\in$ de aridade 2. Neste caso, $\mathcal{F}_n = \emptyset$ para todo $n \in \omega$, $\mathcal{P}_2 = \{\in\}$ e $\mathcal{P}_n = \emptyset$ para todo $n \in \omega \setminus \{2\}$.

Note que o alfabeto a ser adotado depende da maneira escolhida para apresentar a teoria em questão. Por exemplo, para axiomatizar a teoria dos grupos por meio dos seguintes axiomas (enunciaremos tais axiomas na notação usual)

1. $\forall x \forall y \forall z((x \cdot y) \cdot z = x \cdot (y \cdot z))$

2. $\exists e(\forall x(x \cdot e = e \cdot x = x) \wedge \forall x \exists y(x \cdot y = y \cdot x = e))$

basta considerar um alfabeto cujo único símbolo não lógico é o símbolo de função $\cdot$ de aridade 2. Contudo, para axiomatizar a teoria dos grupos por meio dos seguintes axiomas

1. $\forall x \forall y \forall z((x \cdot y) \cdot z = x \cdot (y \cdot z))$

2. $\forall x(x \cdot e = e \cdot x = x)$

3. $\forall x(x \cdot i(x) = i(x) \cdot x = e)$

o nosso alfabeto deve incluir, além do símbolo de função $\cdot$ de aridade 2, um símbolo de função i de aridade 1 e um símbolo de constante e.

Definiremos agora algumas expressões especiais de um alfabeto para a lógica de primeira ordem: os termos, as fórmulas atômicas e as fórmulas.

Definição 1.8 *Dado um alfabeto para a lógica de primeira ordem como na Definição 1.7, dizemos que:*

1. *os **termos** de $\mathcal{L}$ são as expressões (bem formadas) do alfabeto $\mathcal{F} \cup VAR$ na Notação Polonesa;*

2. *as **fórmulas atômicas** de $\mathcal{L}$ são as sequências de símbolos da forma $p\tau_1...\tau_n$ onde $n \geq 0$, $\tau_1, ..., \tau_n$ são termos de $\mathcal{L}$, e, ou $p \in \mathcal{P}_n$, ou $n = 2$ e p é o símbolo $=$;*

3. *as **fórmulas** de $\mathcal{L}$ são as sequências de símbolos construídas recursivamente pelas seguintes regras:*

   (a) *todas as fórmulas atômicas são fórmulas;*

   (b) *se φ é uma fórmula e $x \in VAR$, então $\forall x\varphi$ e $\exists x\varphi$ são fórmulas;*

(c) *se φ é uma fórmula, então $\neg\varphi$ também é uma fórmula;*

(d) *se φ e ψ são fórmulas, então $\wedge\varphi\psi$, $\vee\varphi\psi$, $\rightarrow\varphi\psi$ e $\leftrightarrow\varphi\psi$ também são fórmulas.*

No item 2, o caso especial de p ser o símbolo = e $n = 2$ se deve ao fato de termos definido o símbolo = como um símbolo lógico, então = não é um elemento de $\mathcal{P}_2$. Note também que, pela Definição 1.8, toda fórmula e todo termo são expressões do alfabeto $\mathcal{F} \cup \mathcal{P} \cup VAR \cup \{\wedge, \vee, \neg, \rightarrow, \leftrightarrow, \forall, \exists, =\}$ na Notação Polonesa.

Definição 1.9 *Uma* ***linguagem para a lógica de primeira ordem*** *(ou, simplesmente, uma* ***linguagem de primeira ordem****) é constituída de um alfabeto que satisfaz a Definição 1.7, bem como dos termos e fórmulas dados pela Definição 1.8.*

No que segue, $\mathcal{L}$ denotará não apenas o alfabeto, mas a própria linguagem em si. Uma caracterização dos termos de uma linguagem de primeira ordem (de certa forma, mais tratável) é dada pelo Teorema 1.10.

Teorema 1.10 *Os termos de uma linguagem de primeira ordem $\mathcal{L}$ são exatamente as sequências finitas de símbolos do alfabeto desta linguagem que obedecem as seguintes regras:*

1. *a expressão na Notação Polonesa formada por um único símbolo de variável é um termo;*

2. *a expressão na Notação Polonesa formada por um único símbolo de constante é um termo;*

3. *se $\tau_1, .., \tau_n$ são termos e $f \in \mathcal{F}_n$ é um símbolo de função n-ária, então a expressão na Notação Polonesa $f\tau_1...\tau_n$ é um termo.*

Demonstração: Se τ é uma variável ou uma constante, então valem as regras de formação 1 ou 2, respectivamente. Se $\tau \notin VAR$ e $\tau \notin \mathcal{F}_0$ então existem $f \in \mathcal{F}_n$ com $n \geq 1$ e $\tau_1, ..., \tau_n$ expressões de $\mathcal{F} \cup VAR$ na Notação Polonesa (pois τ é uma expressão de $\mathcal{F} \cup VAR$ na Notação Polonesa) tais que τ é a expressão $f\tau_1...\tau_n$. Logo $\tau_1, ..., \tau_n$ também são termos e, assim, τ obedece à regra de formação dada pelo item 3.

Reciprocamente, seja τ uma variável ou uma constante. Então τ é uma expressão de $\mathcal{F} \cup VAR$ na Notação Polonesa, logo τ é um termo. Seja, agora, $f \in \mathcal{F}_n$ para algum $n \in \omega$ e sejam $\tau_1, ..., \tau_n$ termos. Então, pela regra de formação de expressões na Notação Polonesa, $f\tau_1...\tau_n$ é uma expressão de $\mathcal{F} \cup VAR$, logo, é um termo. □

Vejamos agora um resultado que nos permitirá definir subfórmulas e subtermos.

Teorema 1.11 *Em uma fórmula φ, o escopo de qualquer ocorrência de um símbolo de $\mathcal{P} \cup \{\wedge, \vee, \neg, \rightarrow, \leftrightarrow, \forall, \exists, =\}$ é uma fórmula, e o escopo de qualquer ocorrência de um símbolo de $\mathcal{F} \cup VAR$ é um termo.*

Demonstração: Seja φ uma fórmula. Mostraremos o resultado por indução no comprimento de φ. Se $|\varphi| = 1$, então a única possibilidade é φ ser uma fórmula atômica da forma p para $p \in \mathcal{P}_0$. Neste caso, a única ocorrência de um símbolo é a de p, e como o escopo de p é a própria fórmula φ, temos o resultado, pois $p \in \mathcal{P} \cup \{\wedge, \vee, \neg, \rightarrow, \leftrightarrow, \forall, \exists, =\}$.

Suponha agora que o resultado do enunciado seja válido para toda fórmula com comprimento estritamente menor que $|\varphi| > 1$. Se φ é uma fórmula atômica, há duas possibilidades. A primeira é que φ seja da forma $= \tau_1\tau_2$, com τ_1 e τ_2 termos. Neste caso, seja p um símbolo que ocorre em φ. Se p é o símbolo $=$, então o escopo desta ocorrência é a própria fórmula φ, e o resultado vale. Suponha agora que p ocorra em τ_1 ou τ_2. Como τ_1 e τ_2 são termos (que são expressões de $\mathcal{F} \cup VAR$ na Notação Polonesa), então $p \in \mathcal{F} \cup VAR$ e o escopo de p também é uma expressão de $\mathcal{F} \cup VAR$ na Notação Polonesa, e portanto, é um termo. Logo, vale o resultado. A segunda possibilidade é φ ser da forma $s\tau_1...\tau_n$ onde $n \geq 1$ (pois $|\varphi| \geq 2$), $s \in \mathcal{P}_n$ e $\tau_1, ..., \tau_n$ são termos. Seja p uma ocorrência de um símbolo em φ. Se p é o símbolo s que ocorre no início de φ, então o escopo de p é a própria fórmula φ, e assim segue o resultado, pois $p \in \mathcal{P} \cup \{\wedge, \vee, \neg, \rightarrow, \leftrightarrow, \forall, \exists, =\}$. Se p não ocorre no início de φ, então p ocorre em algum τ_i para $i \in \{1, ..., n\}$. Como τ_i é uma expressão de $\mathcal{F} \cup VAR$ na Notação Polonesa, e como p ocorre dentro de τ_i, então o escopo de p é uma subexpressão de τ_i, logo, é uma expressão de $\mathcal{F} \cup VAR$ na Notação Polonesa. Sendo assim, o escopo de p é um termo, e então segue o resultado.

Suponha agora que φ seja uma fórmula do tipo $\forall x\psi$, onde $x \in VAR$ e ψ é uma fórmula. Seja p uma ocorrência de um símbolo em φ. Se p é o primeiro símbolo de φ, isto é, o símbolo $\forall$, então o escopo de p é a própria fórmula φ, e neste caso segue o resultado, pois $\forall \in \mathcal{P} \cup \{\wedge, \vee, \neg, \rightarrow, \leftrightarrow, \forall, \exists, =\}$. Se p é a ocorrência do segundo símbolo em φ, isto é, a variável x, então o escopo de x é o próprio x. E como x é um termo, e neste caso $p \in \mathcal{F} \cup VAR$, segue o resultado. Suponha então que p seja um símbolo que ocorre dentro da fórmula ψ. Note que o comprimento da fórmula ψ é estritamente menor que o comprimento da fórmula φ. Dessa forma, pela hipótese da indução, segue que o escopo de p é uma fórmula, caso $p \in \mathcal{P} \cup \{\wedge, \vee, \neg, \rightarrow, \leftrightarrow, \forall, \exists, =\}$, ou é um termo, caso $p \in \mathcal{F} \cup VAR$. Note que um argumento inteiramente análogo a este mostra que, se φ for uma fórmula do tipo $\exists x\psi$, onde $x \in VAR$ e ψ uma fórmula, então vale o resultado.

Suponha agora que φ seja uma fórmula do tipo $\neg\psi$, onde ψ é uma fórmula, e seja p uma ocorrência de um símbolo em φ. Se p é o primeiro símbolo de φ, isto é, se p é o símbolo $\neg$, então o escopo de p é a própria fórmula φ. Neste caso segue o resultado, pois $\neg \in \mathcal{P} \cup \{\wedge, \vee, \neg, \rightarrow, \leftrightarrow, \forall, \exists, =\}$. Se p não é o primeiro símbolo de φ, então p ocorre em ψ. Note que a fórmula ψ tem comprimento estritamente menor que a fórmula φ, então pela hipótese da indução segue que o escopo da ocorrência de p é uma fórmula, caso $p \in \mathcal{P} \cup \{\wedge, \vee, \neg, \rightarrow, \leftrightarrow, \forall, \exists, =\}$, ou é um termo, caso $p \in \mathcal{F} \cup VAR$.

Suponha agora que φ é uma fórmula do tipo $\wedge\phi\psi$, onde ϕ e ψ são fórmulas. Seja p uma ocorrência de um símbolo em φ. Se p é o primeiro símbolo de φ, isto é, se p é o símbolo $\wedge$, então o escopo de p é a fórmula φ. Neste caso, segue o resultado, pois $\wedge \in \mathcal{P} \cup \{\wedge, \vee, \neg, \rightarrow, \leftrightarrow, \forall, \exists, =\}$. Se p não é o primeiro símbolo de φ, então p ocorre em ϕ ou em ψ. Como os comprimentos de ϕ e de ψ são estritamente menores que o comprimento de φ, então pela hipótese da indução, o escopo de p é uma fórmula, caso $p \in \mathcal{P} \cup \{\wedge, \vee, \neg, \rightarrow, \leftrightarrow, \forall, \exists, =\}$, ou é um termo, caso $p \in \mathcal{F} \cup VAR$. Note que para fórmulas do tipo $\vee\phi\psi$, $\rightarrow \phi\psi$ e $\leftrightarrow \phi\psi$, o argumento é inteiramente análogo a este último caso. $\square$

Definição 1.12 *O escopo de uma ocorrência de um símbolo em uma fórmula é chamado* ***subfórmula*** *se o símbolo pertence a* $\mathcal{P} \cup \{\wedge, \vee, \neg, \rightarrow, \leftrightarrow, \forall, \exists, =\}$ *e é chamado de* ***subtermo*** *se o símbolo pertence a* $\mathcal{F} \cup VAR$.

Dois outros conceitos importantes relacionados à noção de escopo são o de variável livre e o de sentença.

Definição 1.13 *Uma ocorrência de uma variável* y *em uma fórmula* φ *é dita* ***limitada*** *se ela ocorre no escopo de um dos símbolos* $\forall$ *ou* $\exists$ *seguido pela variável* y*. Uma ocorrência é dita* ***livre*** *se não for limitada. E a fórmula* φ *é dita uma* ***sentença*** *se nenhuma variável ocorre de forma livre em* φ*. Assim, uma* ***variável livre*** *numa dada fórmula é uma variável em que ao menos uma ocorrência é livre em tal fórmula, e uma* ***variável limitada*** *numa dada fórmula é uma variável em que todas as ocorrências são limitadas em tal fórmula.*

Por exemplo, considere a fórmula na notação usual $\forall x(x+y = z)$. Nesta fórmula, as duas ocorrências da variável x são limitadas, e as ocorrências das variáveis y e z são livres. Sendo assim, tal fórmula não é uma sentença, enquanto a fórmula $\forall y \forall z \forall x(x + y = z)$ é uma sentença, uma vez que não há variáveis livres.

Por fim, definimos fecho universal de uma fórmula.

Definição 1.14 *Se φ é uma fórmula, um **fecho universal** de φ é uma sentença da forma $\forall x_1 \forall x_2 ... \forall x_n \varphi$, onde $n \geq 0$ e $x_1, ..., x_n$ são variáveis distintas.*

No exemplo anterior, a sentença $\forall y \forall z \forall x(x + y = z)$ é um fecho universal da fórmula $\forall x(x + y = z)$. Vale observar que se $\forall x_1 \forall x_2 \ldots \forall x_n \varphi$ é um fecho universal de φ, então $\forall x_n \ldots \forall x_2 \forall x_1 \varphi$ também é um fecho universal de φ e eles são, a rigor, distintos. Assim $\forall z \forall y \forall x(x + y = z)$ também é um fecho universal da fórmula $\forall x(x + y = z)$, e é distinto do primeiro fecho universal visto. Contudo, mostraremos adiante que quaisquer dois fechos universais de uma fórmula são logicamente equivalentes.

Na Seção 2.1 definiremos os conceitos de estrutura para uma linguagem de primeira ordem, e nessa definiremos os conceitos de interpretação e valoração para fórmulas, e a partir disto, definiremos quando uma estrutura é um modelo para um conjunto de sentenças. Na Seção 2.2 definiremos o conceitos de fórmulas logicamente equivalentes, que surge como uma generalização da forma como vemos que duas fórmulas possuem o mesmo valor lógico, como as fórmulas dos tipos $\forall x\varphi$ e $\neg\exists x(\neg\varphi)$. Na Seção 2.3 estudaremos os conceitos de redução e expansão de estruturas. E na Seção 2.4 retomaremos o conceito de fórmulas logicamente equivalentes para definir tautologias. As principais referências bibliográficas para este capítulo são [3] e [5].

2.1 Interpretação e valoração

Até agora, estávamos interessados em estabelecer a noção de linguagem de primeira ordem, destacando aspectos sintáticos como a construção de termos e fórmulas a partir de um alfabeto dado. Estamos agora interessados em interpretar o significado dessas expressões num dado contexto e dizer quando uma sentença é, nesse contexto, verdadeira ou falsa. Considere, por exemplo, a seguinte sentença da linguagem $\mathcal{L} = \{0, \cdot, <\}$ (escrita em notação usual, para facilitar a leitura):

$$RQ : \forall x(0 < x \rightarrow \exists y(x = y \cdot y)).$$

O que estamos tentando expressar é que todo número estritamente positivo possui uma raiz quadrada. Sabemos que RQ é uma sentença verdadeira em $\mathbb{R}$, mas é falsa em $\mathbb{Q}$.

Para estudar quando uma sentença é verdadeira em uma determinada estrutura abstrata, precisamos definir rigorosamente o conceito de estrutura e, posteriormente, o que significa dizer que uma sentença é verdadeira na estrutura em questão. É isso que faremos nesta seção.

Definição 2.1 *Dada uma linguagem* $\mathcal{L} = \mathcal{F} \cup \mathcal{P} = \bigcup_{n\in\omega} \mathcal{F}_n \cup \bigcup_{n\in\omega} \mathcal{P}_n$ *para a lógica de* *primeira ordem , uma* ***estrutura*** *para $\mathcal{L}$ (ou, ainda, uma* ***$\mathcal{L}$-estrutura****) é um par $\mathfrak{E} = (A, \mathfrak{I})$ onde A é um conjunto não vazio (denominado* ***universo*** *da estrutura) e $\mathfrak{I}$ é uma função (denominada* ***interpretação****) com domínio em $\mathcal{L}$ e que associa a cada $s \in \mathcal{L}$ um elemento $\mathfrak{I}(s) := s^{\mathfrak{E}}$ da seguinte maneira:*

- *se $f \in \mathcal{F}_n$ com $n > 0$, então $f^{\mathfrak{E}} : A^n \to A$;*
- *se $p \in \mathcal{P}_n$ com $n > 0$, então $p^{\mathfrak{E}} \subseteq A^n$;*
- *se $c \in \mathcal{F}_0$, então $c^{\mathfrak{E}} \in A$;*
- *se $p \in \mathcal{P}_0$, então $p^{\mathfrak{E}} \in \{0, 1\}$.*

Os dois primeiros casos da definição acima dizem que um símbolo de função ou relação n-ária (para $n > 0$) será interpretado como uma função ou relação, respectivamente, definida no universo A. O terceiro item nos diz que toda constante da linguagem $\mathcal{L}$ deve ter um representante $c^{\mathfrak{E}}$ no universo A. E o último item nos diz que toda letra proposicional assume valor 0 ou 1. No contexto da definição, usaremos F (lido como "falso") para denotar 0 e V (lido como "verdadeiro") para denotar 1. Note que para as letras proposicionais, a interpretação independe do universo A da estrutura, pois elas sempre assumem valores 0 ou 1.

Nosso objetivo agora é estudar quando uma fórmula é verdadeira numa dada estrutura. Já mencionamos que a sentença RQ não é verdadeira na estrutura cujo conjunto universo é $\mathbb{Q}$ e cuja interpretação de 0, $\cdot$ e $<$ é a usual. Mas note que a fórmula

$$RQ' : \exists y(x = y \cdot y)$$

pode ser verdadeira ou falsa em $\mathbb{Q}$, dependendo do valor que atribuirmos para x. Por exemplo, se $x = 1$, então ela é verdadeira: basta tomar $y = 1$; mas se $x = 2$, ela passa a ser falsa, pois não existe uma atribuição de valor para y em $\mathbb{Q}$ que a satisfaça.

Com esse exemplo, percebemos que, para analisar a veracidade de uma fórmula, precisamos atribuir valores para algumas variáveis e tais valores precisam estar no conjunto universo da estrutura. Com isso em mente, vamos definir dois conjuntos de variáveis às quais precisaremos atribuir valores do conjunto universo para que seja possível (posteriormente) definir o que chamaremos de valoração de uma fórmula.

Definição 2.2 *Sejam τ um termo e φ uma fórmula. Definimos $V(\tau)$ como o conjunto das variáveis que ocorrem em τ, e $V(\varphi)$ como o conjunto das variáveis livres em φ.*

Note que $V(\tau), V(\varphi) \subseteq VAR$. Como dissemos antes, o objetivo de definir os conjuntos $V(\tau)$ e $V(\varphi)$ é reunir neles todas as variáveis de um termo ou fórmula que impedem que esta seja avaliada (em termos de verdadeiro ou falso) até que fixemos um valor para estas variáveis. No caso dos termos, são todas as variáveis, e no caso das fórmulas, são todas as variáveis livres. Com a próxima definição conseguiremos atribuir um elemento do conjunto universo da estrutura em questão para cada uma das variáveis em $V(\tau)$ e $V(\varphi)$.

Definição 2.3 *Sejam $\mathcal{L}$ uma linguagem para a lógica de primeira ordem, $\mathfrak{E} = (A, \mathcal{I})$ uma estrutura para $\mathcal{L}$ e α um termo ou uma fórmula de $\mathcal{L}$. Uma **atribuição** para α em A*[1] *é uma função σ tal que $V(\alpha) \subseteq dom(\sigma) \subseteq VAR$ e $im(\sigma) \subseteq A$.*

Quando não especificarmos o conjunto universo A de uma estrutura $\mathfrak{E}$, diremos que σ é uma atribuição para α em $\mathfrak{E}$. Agora que já sabemos quais são as variáveis que precisam ter um elemento atribuído e que já conseguimos atribuir um elemento de A para cada uma delas, podemos definir o conceito de valoração. Começaremos com a valoração de termos.

Definição 2.4 *Se $\mathfrak{E}$ é uma estrutura para uma linguagem de primeira ordem $\mathcal{L}$ cujo universo é A, definimos $val^{\mathfrak{E}}(\tau)[\sigma] \in A$ quando τ é um termo de $\mathcal{L}$ e σ é uma atribuição para τ em A da seguinte maneira:*

1. $val^{\mathfrak{E}}(x)[\sigma] = \sigma(x)$ *se* $x \in dom(\sigma)$;

2. $val^{\mathfrak{E}}(c)[\sigma] = c^{\mathfrak{E}}$ *se* $c \in \mathcal{F}_0$;

3. $val^{\mathfrak{E}}(f\tau_1 ... \tau_n)[\sigma] = f^{\mathfrak{E}}(val^{\mathfrak{E}}(\tau_1)[\sigma], ..., val^{\mathfrak{E}}(\tau_n)[\sigma])$ *se* $f \in \mathcal{F}_n$ *com* $n > 0$ *e* $\tau_1, ..., \tau_n$ *são termos.*

*Lemos $val^{\mathfrak{E}}(\tau)[\sigma]$ como a **valoração para o termo** τ **em** $\mathfrak{E}$ **sob a atribuição** σ. E se $V(\tau) = \emptyset$, denotamos $val^{\mathfrak{E}}(\tau)[\emptyset]$ por $val^{\mathfrak{E}}(\tau)$.*

Note que a definição acima é recursiva: estamos sempre definindo uma valoração de um termo com base na valoração prévia dos termos mais simples que o compõem. A valoração para termos trata de associar a cada termo um elemento do conjunto universo A, por isso também podemos chamá-la de **interpretação para termos**. Como os termos são elementos da linguagem, a valoração mostra como podemos representá-los por elementos do conjunto universo.

[1]

Por exemplo, dados $\mathfrak{E} = \mathbb{R}$ (cometemos aqui o abuso de notação de identificar a estrutura com o conjunto universo, pois a linguagem e interpretação são as usuais e estão subentendidas) e a atribuição $\sigma = \{(x,1),(y,2),(z,3)\}$, temos $val^{\mathbb{R}}(x)[\sigma] = 1$, pois x é uma variável no domínio de σ, $val^{\mathbb{R}}(0)[\sigma] = 0$, pois 0 é uma constante da linguagem $\mathcal{L}$ e a interpretação é a usual, e $val^{\mathbb{R}}(+\cdot xyz)[\sigma] = +val^{\mathbb{R}}(\cdot xy)[\sigma]val^{\mathbb{R}}(z)[\sigma] = +\cdot val^{\mathbb{R}}(x)[\sigma]val^{\mathbb{R}}(y)[\sigma]\,3 = +\cdot 1\ 2\ 3 = 5$.

Definiremos agora valoração para uma fórmula atômica.

Definição 2.5 *Se $\mathfrak{E}$ é uma estrutura para uma linguagem de primeira ordem $\mathcal{L}$ cujo universo é A, definimos $val^{\mathfrak{E}}(\varphi)[\sigma] \in \{0,1\}$ quando φ é uma fórmula atômica de $\mathcal{L}$ e σ é uma atribuição para φ em A da seguinte maneira:*

1. *$val^{\mathfrak{E}}(p)[\sigma] = p^{\mathfrak{E}}$ se $p \in \mathcal{P}_0$;*
2. *$val^{\mathfrak{E}}(p\tau_1...\tau_n)[\sigma] = 1$ se, e somente se, $(val^{\mathfrak{E}}(\tau_1)[\sigma],...,val^{\mathfrak{E}}(\tau_n)[\sigma]) \in p^{\mathfrak{E}}$, se $p \in \mathcal{P}_n$ com $n > 0$ e $\tau_1,...,\tau_n$ são termos;*
3. *$val^{\mathfrak{E}}(=\tau_1\tau_2)[\sigma] = 1$ se, e somente se, $val^{\mathfrak{E}}(\tau_1)[\sigma] = val^{\mathfrak{E}}(\tau_2)[\sigma]$, onde τ_1 e τ_2 são termos.*

Lemos $val^{\mathfrak{E}}(\varphi)[\sigma]$ como a ***valoração para a fórmula atômica φ em $\mathfrak{E}$ sob a atribuição σ****.*

Vejamos alguns exemplos. Seja $\mathfrak{E} = \mathbb{Q}$ e as valorações $\sigma_1 = \{(x,2),(y,6),(z,3)\}$ e $\sigma_2 = \{(x,6),(y,2),(z,3)\}$. Então para a fórmula atômica $= y\cdot xz$ (isto é, $y = x\cdot z$ na notação usual) temos que $val^{\mathbb{Q}}(= y\cdot xz)[\sigma_1] = 1$ e $val^{\mathbb{Q}}(= y\cdot xz)[\sigma_2] = 0$. De fato, para a valoração σ_1, por um lado temos $val^{\mathbb{Q}}(y)[\sigma_1] = 6$ e por outro lado, $val^{\mathbb{Q}}(\cdot xz)[\sigma_1] = \cdot val^{\mathbb{Q}}(x)[\sigma_1]val^{\mathbb{Q}}(z)[\sigma_1] = \cdot\ 3\ 2$, e como em $\mathbb{Q}$ temos $6 = 2\cdot 3$, segue que $val^{\mathbb{Q}}(= y\cdot xz)[\sigma_1] = 1$. E para a valoração σ_2, por um lado $val^{\mathbb{Q}}(y)[\sigma_2] = 2$ e por outro lado, $val^{\mathbb{Q}}(\cdot xz)[\sigma_2] = \cdot val^{\mathbb{Q}}(x)[\sigma_2]val^{\mathbb{Q}}(z)[\sigma_2] = \cdot\ 6\ 3$, e como em $\mathbb{Q}$ temos $2 \neq 6\cdot 3$, segue que $val^{\mathbb{Q}}(= y\cdot xz)[\sigma_2] = 0$.

Nosso próximo objetivo é definir valoração para fórmulas em geral. Mas antes disto precisaremos definir substituição de uma variável numa atribuição σ.

Definição 2.6 *Dada uma atribuição σ, definimos $\sigma+(y/a)$ como a função $\sigma\restriction_{VAR\setminus\{y\}} \cup\{(y,a)\}$, onde $a \in A$.*

Em outras palavras, se a variável y estiver no domínio de σ, então $\sigma + (y/a)$ substitui o elemento que σ atribuía a y por a; isto é feito ao restringir σ a $VAR \setminus \{y\}$, e a substituição por a é feita ao unir $\sigma\restriction_{VAR\setminus\{y\}}$ com o conjunto $\{(y,a)\}$. E note que, mesmo que y não pertença ao domínio de σ, y pertencerá ao domínio de $\sigma + (y/a)$. Alguns exemplos: se σ for a atribuição $\{(x,4)\}$, então $\sigma + (y/2)$ será a atribuição $\{(x,1),(y,2)\}$; se σ for a atribuição $\{(x,1),(y,3),(z,5)\}$, então $\sigma + (y/2)$ será a atribuição $\{(x,1),(y,2),(z,5)\}$.

Agora sim, podemos definir valoração para fórmulas.

Definição 2.7 *Se $\mathfrak{E}$ é uma estrutura para uma linguagem de primeira ordem $\mathcal{L}$ cujo universo é A, definimos $val^{\mathfrak{E}}(\varphi)[\sigma]$ quando φ uma fórmula de $\mathcal{L}$ e σ uma atribuição para φ em A da seguinte maneira:*

1. *$val^{\mathfrak{E}}(\neg\varphi)[\sigma] = 1 - val^{\mathfrak{E}}(\varphi)[\sigma]$;*

2. *$val^{\mathfrak{E}}(\wedge\varphi\psi)[\sigma], val^{\mathfrak{E}}(\vee\varphi\psi)[\sigma], val^{\mathfrak{E}}(\rightarrow\varphi\psi)[\sigma], val^{\mathfrak{E}}(\leftrightarrow\varphi\psi)[\sigma]$ são definidas a partir de $val^{\mathfrak{E}}(\varphi)[\sigma]$ e $val^{\mathfrak{E}}(\psi)[\sigma]$ usando as tabelas-verdade[2] dos símbolos $\wedge, \vee, \rightarrow$ e $\leftrightarrow$ respectivamente;*

3. *$val^{\mathfrak{E}}(\exists y\varphi)[\sigma] = 1$ se, e somente se, $val^{\mathfrak{E}}(\varphi)[\sigma + (y/a)] = 1$ para algum $a \in A$;*

4. *$val^{\mathfrak{E}}(\forall y\varphi)[\sigma] = 1$ se, e somente se, $val^{\mathfrak{E}}(\varphi)[\sigma + (y/a)] = 1$ para todo $a \in A$.*

*Lemos $val^{\mathfrak{E}}(\varphi)[\sigma]$ como a **valoração para a fórmula φ em $\mathfrak{E}$ sob a atribuição** σ. Escrevemos, ainda, $\mathfrak{E} \vDash \varphi[\sigma]$ para denotar $val^{\mathfrak{E}}(\varphi)[\sigma] = 1$, e $\mathfrak{E} \nvDash \varphi[\sigma]$ para denotar $val^{\mathfrak{E}}(\varphi)[\sigma] = 0$. Se $V(\varphi) = \emptyset$ (isto é, se φ é uma sentença), então $val^{\mathfrak{E}}(\varphi)$ abrevia $val^{\mathfrak{E}}(\varphi)[\emptyset]$ e $\mathfrak{E} \vDash \varphi$ denota $val^{\mathfrak{E}}(\varphi) = 1$.*

Lembre-se de que adotamos a convenção de escrever 0 para falso e 1 para verdadeiro. Assim, diremos que uma fórmula φ é **verdadeira na estrutura $\mathfrak{E}$ para a atribuição** σ (ou, ainda, que $\mathfrak{E}$ **satisfaz a fórmula** φ **para a atribuição** σ) se $val^{\mathfrak{E}}(\varphi)[\sigma] = 1$, que equivale a dizer que $\mathfrak{E} \vDash \varphi[\sigma]$. E diremos que uma fórmula φ é **falsa na estrutura $\mathfrak{E}$ para a atribuição** σ (ou, ainda, que $\mathfrak{E}$ **não satisfaz a fórmula** φ **para a atribuição** σ) se $val^{\mathfrak{E}}(\varphi)[\sigma] = 0$, que equivale a dizer que $\mathfrak{E} \nvDash \varphi[\sigma]$, ou, ainda (pela definição de valoração para uma fórmula do tipo $\neg\varphi$), que $\mathfrak{E} \vDash \neg\varphi[\sigma]$.

Vejamos alguns exemplo de valoração para fórmulas. Considere $\mathfrak{E} = \mathbb{Q}$, a atribuição $\{(x,1),(y,2),(z,3)\}$ e as fórmulas φ, ψ dadas respectivamente por $= +xyz$ e $= \cdot xyz$. Pela valoração de termos e fórmulas atômicas que vimos anteriormente, temos que $val^{\mathbb{Q}}(\varphi)[\sigma] = 1$ e $val^{\mathbb{Q}}(\psi)[\sigma] = 0$. Dessa forma, temos que $val^{\mathbb{Q}}(\neg\varphi)[\sigma] = 1 - val^{\mathbb{Q}}(\varphi)[\sigma] = 1 - 1 = 0$, e analogamente, $val^{\mathbb{Q}}(\neg\psi)[\sigma] = 1$. Também temos que $val^{\mathbb{Q}}(\wedge\varphi\psi)[\sigma] = 1 \wedge 0 = 0$, de acordo com a tabela-verdade de $\wedge$. E, analogamente,

[2] Descritas no Apêndice 1.

$val^{\mathbb{Q}}(\vee\varphi\psi)[\sigma] = 1$, $val^{\mathbb{Q}}(\rightarrow \varphi\psi)[\sigma] = 0$, $val^{\mathbb{Q}}(\leftrightarrow \varphi\psi)[\sigma] = 0$, de acordo com as respectivas tabelas verdade. Para os dois últimos casos, temos as seguintes possibilidades: a fórmula $\exists w\varphi$ é tal que $val^{\mathbb{Q}}(\exists w\varphi)[\sigma] = 1$, pois $\mathbb{Q} \neq \emptyset$ e para todo $a \in \mathbb{Q}$ temos $val^{\mathbb{Q}}(\varphi)[\sigma + (w/a)] = 1$, já que w não ocorre em φ. Pelo mesmo motivo, a fórmula $\forall w\varphi$ é tal que $val^{\mathbb{Q}}(\forall w\varphi)[\sigma] = 1$. Considere agora a fórmula $\exists z\psi$.Vimos que $val^{\mathbb{Q}}(\psi)[\sigma] = 0$, mas $val^{\mathbb{Q}}(\psi)[\sigma + (z/2)] = 1$. Então temos que $val^{\mathbb{Q}}(\exists z\psi)[\sigma] = 1$. Já a fórmula $\forall z\psi$ é tal que $val^{\mathbb{Q}}(\psi)[\sigma + (z/3)] = 0$, então $val^{\mathbb{Q}}(\forall z\psi)[\sigma] = 0$.

Uma consequência (imediata) da tabela-verdade dos símbolos $\wedge, \vee, \rightarrow, \leftrightarrow$ e da notação $\vDash$ definida anteriormente é o Corolário 2.8 a seguir.

Corolário 2.8 *Sejam $\mathfrak{E}$ uma estrutura para uma linguagem de primeira ordem $\mathcal{L}$, φ e ψ fórmulas de $\mathcal{L}$ e σ uma atribuição para φ e ψ. Então vale:*

- $\mathfrak{E} \vDash (\varphi \wedge \psi)[\sigma]$ *se, e somente se,* $\mathfrak{E} \vDash \varphi[\sigma]$ *e* $\mathfrak{E} \vDash \psi[\sigma]$*;*

- $\mathfrak{E} \vDash (\varphi \vee \psi)[\sigma]$ *se, e somente se,* $\mathfrak{E} \vDash \varphi[\sigma]$ *ou* $\mathfrak{E} \vDash \psi[\sigma]$*;*

- $\mathfrak{E} \vDash (\varphi \rightarrow \psi)[\sigma]$ *se, e somente se,* $\mathfrak{E} \vDash \psi[\sigma]$ *ou* $\mathfrak{E} \nvDash \varphi[\sigma]$*.*

Note que $val^{\mathfrak{E}}(\varphi)[\sigma']$ só depende do valor atribuído por σ às variáveis livres de φ, isto é, se $\sigma' \restriction_{V(\varphi)} = \sigma \restriction_{V(\varphi)}$ então $val^{\mathfrak{E}}(\varphi)[\sigma'] = val^{\mathfrak{E}}(\varphi)[\sigma]$. Dessa forma, no caso em que φ é uma sentença, $val^{\mathfrak{E}}(\varphi)[\sigma] = val^{\mathfrak{E}}(\varphi)[\emptyset] = val^{\mathfrak{E}}(\varphi)$, pois $V(\varphi) = \emptyset$. Sendo assim, se uma sentença é verdadeira para uma atribuição, então ela é verdadeira para todas as atribuições. Isto nos dá o seguinte resultado:

Proposição 2.9 *Se $\mathfrak{E}$ é uma estrutura para uma linguagem de primeira ordem $\mathcal{L}$ e φ é uma sentença de $\mathcal{L}$, então ocorre exatamente uma dessas duas possibilidades: $\mathfrak{E} \vDash \varphi$ ou $\mathfrak{E} \vDash \neg\varphi$.*

A seguir, definiremos a satisfação de um conjunto Σ de sentenças por uma estrutura $\mathfrak{E}$. Em outras palavras, definiremos quando uma estrutura é um modelo para um conjunto de sentenças.

Definição 2.10 *Sejam $\mathfrak{E}$ uma estrutura para uma linguagem de primeira ordem $\mathcal{L}$ e Σ um conjunto de sentenças de $\mathcal{L}$. Escrevemos $\mathfrak{E} \vDash \Sigma$, e lemos "$\mathfrak{E}$ **satisfaz** Σ" ou "$\mathfrak{E}$ **é um modelo para** Σ", para indicar que $\mathfrak{E} \vDash \varphi$ para toda $\varphi \in \Sigma$.*

Por exemplo, um grupo é um modelo para o conjunto dos axiomas da teoria de grupos. Usualmente denotaremos uma estrutura genérica por $\mathfrak{E}$, e, quando uma estrutura for também um modelo para um conjunto de sentenças, a denotaremos por $\mathfrak{E}$.

Definição 2.11 *Sejam $\mathcal{L}$ uma linguagem de primeira ordem, Σ um conjunto de sentenças de $\mathcal{L}$ e φ uma sentença de $\mathcal{L}$. Escrevemos $\Sigma \vDash \varphi$ para indicar que $\mathfrak{E} \vDash \varphi$ para toda $\mathcal{L}$-estrutura $\mathfrak{E}$ tal que $\mathfrak{E} \vDash \Sigma$. Neste caso, dizemos que φ é uma* ***consequência semântica*** *ou* ***consequência lógica*** *de Σ.*

Note que, da definição acima, é trivialmente válido que $\Sigma \vDash \varphi$ para toda sentença $\varphi \in \Sigma$.

Definição 2.12 *Seja Σ um conjunto de sentenças de uma linguagem de primeira ordem $\mathcal{L}$. Dizemos que Σ é* ***semanticamente consistente****, e indicamos isso por $Con_{\vDash}(\Sigma)$, se existe alguma $\mathcal{L}$-estrutura $\mathfrak{E}$ tal que $\mathfrak{E} \vDash \Sigma$. Dizemos ainda que Σ é* ***semanticamente inconsistente*** *se Σ não é semanticamente consistente e, neste caso, indicamos isso por $\neg Con_{\vDash}(\Sigma)$.*

Neste sentido, as teorias que estamos acostumados a estudar (como as de grupos, anéis, corpos, etc.) são consistentes, pois existem modelos para os conjuntos formados por seus respectivos axiomas (por exemplo, $\mathbb{R}$ com as respectivas operações usuais e interpretação usual).

Teorema 2.13 *Sejam $\mathcal{L}$ uma linguagem de primeira ordem, Σ um conjunto de sentenças de $\mathcal{L}$ e φ uma sentença de $\mathcal{L}$. Valem os seguintes resultados:*

1. *$\Sigma \vDash \varphi$ se, e somente se, $\neg Con_{\vDash}(\Sigma \cup \{\neg\varphi\})$.*

2. *$\Sigma \vDash \neg\varphi$ se, e somente se, $\neg Con_{\vDash}(\Sigma \cup \{\varphi\})$.*

Demonstração: Vamos demonstrar primeiro o item 1. Suponha que $\Sigma \cup \{\neg\varphi\}$ é semanticamente consistente. Então existe uma $\mathcal{L}$-estrutura $\mathfrak{E}$ tal que $\mathfrak{E} \vDash \Sigma \cup \{\neg\varphi\}$. Como $\neg\varphi \in \Sigma \cup \{\neg\varphi\}$, segue que $\mathfrak{E} \vDash \neg\varphi$, ou equivalentemente, $\mathfrak{E} \nvDash \varphi$. E note que, sendo $\mathfrak{E}$ um modelo para $\Sigma \cup \{\neg\varphi\}$, então, em particular, $\mathfrak{E}$ é um modelo para Σ. Dessa forma, $\mathfrak{E}$ é um modelo para Σ que atesta que não ocorre $\Sigma \vDash \varphi$. Reciprocamente, suponha que não ocorre $\Sigma \vDash \varphi$. Então existe uma $\mathcal{L}$-estrutura $\mathfrak{E}$ tal que $\mathfrak{E} \vDash \Sigma$ e $\mathfrak{E} \nvDash \varphi$, isto é, $\mathfrak{E} \vDash \neg\varphi$. Assim, $\mathfrak{E} \vDash \Sigma \cup \{\neg\varphi\}$, pois já tínhamos que $\mathfrak{E} \vDash \psi$ para todo $\psi \in \Sigma$. Dessa forma, $\mathfrak{E}$ é um modelo para $\Sigma \cup \{\neg\varphi\}$, o que atesta que $\Sigma \cup \{\neg\varphi\}$ é semanticamente consistente.

Para verificar a validade do item 2, note antes que $\mathfrak{E} \vDash \varphi$ se, e somente se, $\mathfrak{E} \nvDash \neg\varphi$. Suponha primeiro que $\Sigma \cup \{\varphi\}$ é semanticamente consistente. Então existe uma $\mathcal{L}$-estrutura $\mathfrak{E}$ tal que $\mathfrak{E} \vDash \Sigma \cup \{\varphi\}$. Assim, em particular, $\mathfrak{E}$ é um modelo para Σ, isto é, $\mathfrak{E} \vDash \Sigma$, e também que $\mathfrak{E} \vDash \varphi$ e, consequentemente, $\mathfrak{E} \nvDash \neg\varphi$. Logo, $\mathfrak{E}$ é um modelo para Σ que atesta que não ocorre $\Sigma \vDash \neg\varphi$. Reciprocamente, suponha que não ocorre $\Sigma \vDash \neg\varphi$. Então existe uma $\mathcal{L}$-estrutura $\mathfrak{E}$ tal que $\mathfrak{E} \vDash \Sigma$ e $\mathfrak{E} \nvDash \neg\varphi$, isto é,

$\mathfrak{E} \vDash \varphi$. Logo, $\mathfrak{E}$ é um modelo para $\Sigma \cup \{\varphi\}$, o que atesta que $\Sigma \cup \{\varphi\}$ é semanticamente consistente. $\square$

2.2 Fórmulas logicamente equivalentes

Nas sessões que se seguem usaremos a notação usual para fórmulas e termos em vez da Polonesa, a fim de facilitar a leitura. Também iremos usar $f(\tau_1, \ldots, \tau_n)$ em vez de $f\tau_1 \ldots \tau_n$ e $p(\tau_1, \ldots, \tau_n)$ em vez de $p\tau_1 \ldots \tau_n$, onde f é um símbolo de função n-ário, p é um símbolo de relação n-ário e $\tau_1, \ldots, \tau_n$ são termos.

Definição 2.14 *Sejam $\mathcal{L}$ uma linguagem para a lógica de primeira ordem e φ uma fórmula de $\mathcal{L}$. Dizemos que φ é* ***logicamente válida*** *se $\mathfrak{E} \vDash \varphi[\sigma]$ para toda $\mathcal{L}$-estrutura $\mathfrak{E}$ e para toda atribuição σ para φ em $\mathfrak{E}$.*

Um exemplo de fórmula logicamente válida é dado por $x = x$, ou, ainda, pela sentença $\forall x(x = x)$. De fato, o símbolo lógico $=$ é sempre interpretado como igualdade em todos os modelos. Outra fórmula logicamente válida é $\forall x\varphi \to \neg\exists x(\neg\varphi)$. De fato, fixe uma $\mathcal{L}$-estrutura $\mathfrak{E}$ e uma atribuição σ para $\forall x\varphi \to \neg\exists x(\neg\varphi)$ em $\mathfrak{E}$. Note que $\mathfrak{E} \vDash (\forall x\varphi \to \neg\exists x(\neg\varphi))[\sigma]$ se, e somente se, $\mathfrak{E} \vDash \forall x\varphi[\sigma]$ ou $\mathfrak{E} \nvDash \neg\exists x\neg\varphi[\sigma]$. Se $\mathfrak{E} \vDash \forall x\varphi[\sigma]$ temos o resultado. Suponha, então, que $\mathfrak{E} \nvDash \forall x\varphi[\sigma]$. Disto segue que $val^{\mathfrak{E}}(\varphi)[\sigma + (y/a)] = 0$ para algum $a \in A$, e então $val^{\mathfrak{E}}(\neg\varphi)[\sigma + (y/a)] = 1$. Por sua vez, disto segue que $val^{\mathfrak{E}}(\exists x(\neg\varphi))[\sigma] = 1$, e portanto $val^{\mathfrak{E}}(\neg\exists x\neg\varphi)[\sigma] = 0$, logo, $\mathfrak{E} \nvDash \neg\exists x\neg\varphi[\sigma]$, como queríamos. De forma análoga podemos mostrar que a fórmula $\neg\exists x(\neg\varphi) \to \forall x\varphi$ também é logicamente válida.

Estes dois últimos exemplos nos remetem à ideia de fórmulas logicamente equivalentes, que definiremos a seguir.

Definição 2.15 *Sejam $\mathcal{L}$ uma linguagem para a lógica de primeira ordem e φ e ψ fórmulas de $\mathcal{L}$. Dizemos que φ e ψ são* ***logicamente equivalentes*** *se a fórmula $\varphi \leftrightarrow \psi$ é logicamente válida.*

A fórmula $\forall x\varphi \leftrightarrow \neg\exists x(\neg\varphi)$ é logicamente válida, sendo assim $\forall x\varphi$ e $\neg\exists x(\neg\varphi)$ são fórmulas logicamente equivalentes. Este exemplo mostra que reformular fórmulas com o quantificador $\exists$ em termos do quantificador $\forall$ e símbolos lógicos de forma adequada preserva a equivalência lógica. Note ainda que dizer que as fórmulas φ e ψ são logicamente equivalentes equivale a dizer que $\mathfrak{E} \vDash \varphi[\sigma]$ se, e somente se, $\mathfrak{E} \vDash \psi[\sigma]$, para toda $\mathcal{L}$-estrutura $\mathfrak{E}$ e toda atribuição σ para ϕ e ψ em $\mathfrak{E}$. Assim, um outro exemplo de fórmulas logicamente equivalentes é dado pelas fórmulas $\varphi \vee \psi$ e $\psi \vee \varphi$.

Do próximo resultado segue que todos os fechos universais de uma fórmula são logicamente equivalentes.

Teorema 2.16 *Sejam* $\mathfrak{E}$ *uma estrutura para uma linguagem de primeira ordem* $\mathcal{L}$*,* φ *uma fórmula de* $\mathcal{L}$ *e* $\forall x_1 \forall x_2 ... \forall x_n \varphi$ *um fecho universal de* φ*. Então* $\mathfrak{E} \vDash \varphi[\sigma]$ *para toda atribuição* σ *para* φ *se em* $\mathfrak{E}$ *se, e somente se,* $\mathfrak{E} \vDash \forall x_1 \forall x_2 ... \forall x_n \varphi$*.*

Demonstração: Sejam $\forall x_1 \forall x_2 ... \forall x_n \varphi$ um fecho universal de φ e A o universo de $\mathfrak{E}$. Temos que

$$\begin{aligned}
\mathfrak{E} \vDash \forall x_1 \forall x_2 \forall x_3 \ldots \forall x_n \varphi &\Leftrightarrow val^{\mathfrak{E}}(\forall x_1 \forall x_2 \forall x_3 \ldots \forall x_n \varphi)[\emptyset] = 1 \\
&\Leftrightarrow val^{\mathfrak{E}}(\forall x_2 \forall x_3 \ldots \forall x_n \varphi)[\{(x_1, a_1)\}] = 1, \forall a_1 \in A \\
&\Leftrightarrow val^{\mathfrak{E}}(\forall x_3 \ldots \forall x_n \varphi)[\{(x_1, a_1), (x_2, a_2)\}] = 1, \forall a_1, a_2 \in A \\
&\ \ \vdots \\
&\Leftrightarrow val^{\mathfrak{E}}(\varphi)[\{(x_1, a_1), (x_2, a_2), ..., (x_n, a_n)\}] = 1, \forall a_1, a_2, ..., a_n \in A
\end{aligned}$$

Pelo que comentamos após o Corolário 2.8, $val^{\mathfrak{E}}(\varphi)[\sigma]$ só depende de $\sigma \upharpoonright_{V(\sigma)}$. Como $V(\sigma) \subseteq \{x_1, ..., x_n\}$, segue que $val^{\mathfrak{E}}\varphi[\{(x_1, a_1), (x_2, a_2), ..., (x_n, a_n)\}] = 1, \forall a_1, a_2, ..., a_n \in A$ se, e somente se, $val^{\mathfrak{E}}(\varphi)[\sigma] = 1$ para toda atribuição σ de φ em $\mathfrak{E}$, e, por sua vez, isto ocorre se, e somente se, $\mathfrak{E} \vDash \varphi[\sigma]$ para toda atribuição σ de φ em $\mathfrak{E}$. □

Na definição de equivalência lógica, pedimos que $\varphi \leftrightarrow \psi$ seja logicamente válida, ou seja, pedimos que $\mathfrak{E} \vDash (\varphi \leftrightarrow \psi)[\sigma]$ para toda $\mathcal{L}$-estrutura $\mathfrak{E}$ e toda atribuição σ da fórmula $\varphi \leftrightarrow \psi$ em $\mathfrak{E}$. Na definição a seguir, pedimos uma equivalência apenas nos modelos para um conjunto de sentenças pré-estabelecido.

Definição 2.17 *Sejam* $\mathcal{L}$ *uma linguagem para a lógica de primeira ordem e* Σ *um conjunto de sentenças de* $\mathcal{L}$*.*

- *Se* φ *e* ψ *são fórmulas de* $\mathcal{L}$*, dizemos que* φ *e* ψ *são* ***equivalentes em relação a*** Σ *se um (e, portanto, todos) fecho universal da fórmula* $\varphi \leftrightarrow \psi$ *é verdadeiro em todas as* $\mathcal{L}$*-estruturas que modelam* Σ*.*

- *Se* τ_1 *e* τ_2 *são termos de* $\mathcal{L}$*, dizemos que* τ_1 *e* τ_2 *são* ***equivalentes em relação a*** Σ *se para toda* $\mathcal{L}$*-estrutura* $\mathfrak{E}$ *tal que* $\mathfrak{E} \vDash \Sigma$ *e para toda atribuição* σ *para* τ_1 *e* τ_2 *em* $\mathfrak{E}$ *tem-se que* $val^{\mathfrak{E}}(\tau_1)[\sigma] = val^{\mathfrak{E}}(\tau_2)[\sigma]$*.*

Se, por exemplo, o conjunto Σ contém a sentença $\forall x \forall y \forall z((x \cdot y) \cdot z = x \cdot (y \cdot z))$ então os termos $x \cdot (y \cdot z)$ e $(x \cdot y) \cdot z$ são equivalentes em relação a Σ. Dessa forma, em qualquer $\mathcal{L}$-estrutura que modela Σ, podemos seguramente escrever $x \cdot y \cdot z$ como uma abreviação dos termos $x \cdot (y \cdot z)$ e $(x \cdot y) \cdot z$.

Vejamos agora o conceito de substituição em termos e fórmulas.

Definição 2.18 *Sejam $\mathcal{L}$ uma linguagem para a lógica de primeira ordem, τ e β termos de $\mathcal{L}$ e x uma variável. Denotamos por $[\beta]_x^\tau$ o **termo obtido ao substituir todas as ocorrências de x em β pelo termo τ**. Equivalentemente:*

- *$[x]_x^\tau$ é o termo τ;*
- *se y é uma variável diferente de x, então $[y]_x^\tau$ é o termo y;*
- *se c é uma constante, então $[c]_x^\tau$ é o termo c;*
- *se β é da forma $f\beta_1...\beta_n$ onde $f \in \mathcal{F}_n$, $n > 0$ e $\beta_1, ..., \beta_n$ são termos de $\mathcal{L}$, então $[\beta]_x^\tau$ é o termo $f[\beta_1]_x^\tau...[\beta_n]_x^\tau$.*

Vejamos um exemplo: considere a linguagem $\mathcal{L} = \{+, \cdot, -, 0, 1\}$ da teoria de anéis e o termo $x \cdot y$. Então $[x \cdot y]_x^{x+z}$ é o termo $(x + z) \cdot y$. Note que, na verdade, apenas substituímos a variável x em $x \cdot y$ pelo termo $x + z$.

Considerando a atribuição $\sigma = \{(x, 1), (y, 2)(z, 5)\}$, note que $val^{\mathfrak{E}}([x \cdot y]_x^{x+z})[\sigma] = val^{\mathfrak{E}}((x + z) \cdot y)[\sigma] = 12$ e, por outro lado, $val^{\mathfrak{E}}(x \cdot y)[\sigma + (x/6)] = 12$. Não por acaso temos que $val^{\mathfrak{E}}(x + z)[\sigma] = 6$.

Teorema 2.19 *Sejam $\mathcal{L}$ uma linguagem para a lógica de primeira ordem, $\mathfrak{E} = (A, \mathcal{I})$ uma estrutura para $\mathcal{L}$, x uma variável, τ e β termos de $\mathcal{L}$ e σ uma atribuição para τ e β em A. Se $val^{\mathfrak{E}}(\tau)[\sigma] = a \in A$, então $val^{\mathfrak{E}}([\beta]_x^\tau)[\sigma] = val^{\mathfrak{E}}(\beta)[\sigma + (x/a)]$.*

Demonstração: Faremos a prova por indução no comprimento do termo β. Se o comprimento de β é 1, então β é uma constante ou uma variável. Se $\beta = c$ uma constante, então por um lado $val^{\mathfrak{E}}([\beta]_x^\tau)[\sigma] = val^{\mathfrak{E}}(c)[\sigma] = c^{\mathfrak{E}}$ e, por outro lado, $val^{\mathfrak{E}}(\beta)[\sigma + (x/a)] = val^{\mathfrak{E}}(c)[\sigma + (x/a)] = c^{\mathfrak{E}}$, logo, vale o resultado. Se β é uma variável, há dois casos possíveis. Se $\beta = x$, então por um lado $val^{\mathfrak{E}}([\beta]_x^\tau)[\sigma] = val^{\mathfrak{E}}([x]_x^\tau)[\sigma] = val^{\mathfrak{E}}(\tau)[\sigma]$ e, por outro lado, $val^{\mathfrak{E}}(\beta)[\sigma + (x/a)] = val^{\mathfrak{E}}(x)[\sigma + (x/a)] = a = val^{\mathfrak{E}}(\tau)[\sigma]$, logo, segue o resultado. Se $\beta = y$ onde y é uma variável distinta de x, então por um lado $val^{\mathfrak{E}}([\beta]_x^\tau)[\sigma] = val^{\mathfrak{E}}([y]_x^\tau)[\sigma] = val^{\mathfrak{E}}(y)[\sigma]$, e, por outro lado, $val^{\mathfrak{E}}(\beta)[\sigma + (x/a)] = val^{\mathfrak{E}}(y)[\sigma + (x/a)] = val^{\mathfrak{E}}(y)[\sigma]$, logo, vale a igualdade.

Suponha agora que $|\beta| = n > 1$ e que o resultado seja válido para todo termo com comprimento estritamente menor que n. Pela regra de formação de termos, existem $f \in \mathcal{F}_n$ e $\tau_1, ..., \tau_n$ termos tais que $\beta = f\tau_1...\tau_n$. Por um lado, temos que

$val^{\mathfrak{E}}([\beta]^\tau_x)[\sigma] = val^{\mathfrak{E}}([f\tau_1...\tau_n]^\tau_x)[\sigma] = val^{\mathfrak{E}}(f[\tau_1]^\tau_x...[\tau_n]^\tau_x)[\sigma]$ e, por outro lado, $val^{\mathfrak{E}}(\beta)[\sigma + (x/a)] = val^{\mathfrak{E}}(f\tau_1...\tau_n)[\sigma + (x/a)] = f^{\mathfrak{E}}(val^{\mathfrak{E}}(\tau_1)[\sigma + (x/a)],...,val^{\mathfrak{E}}(\tau_n)[\sigma + (x/a)])$. Como cada τ_i possui comprimento estritamente menor que n, então pela hipótese da indução temos que para cada $i \in \{1,...,n\}$ vale $val^{\mathfrak{E}}(\tau_i)[\sigma+(x/a)] = val^{\mathfrak{E}}([\tau_i]^\tau_x)[\sigma]$, logo, $f^{\mathfrak{E}}(val^{\mathfrak{E}}(\tau_1)[\sigma + (x/a)],...,val^{\mathfrak{E}}(\tau_n)[\sigma + (x/a)]) = f^{\mathfrak{E}}(val^{\mathfrak{E}}([\tau_1]^\tau_x)[\sigma],...,val^{\mathfrak{E}}([\tau_n]^\tau_x)[\sigma]) = val^{\mathfrak{E}}(f([\tau_1]^\tau_x,...,[\tau_n]^\tau_x))[\sigma]$ e, então, vale a igualdade. $\square$

Vejamos agora um conceito análogo para fórmulas.

Definição 2.20 *Sejam $\mathcal{L}$ uma linguagem para a lógica de primeira ordem, φ uma fórmula de $\mathcal{L}$, τ um termo de $\mathcal{L}$ e x uma variável. Denotamos por $[\varphi]^\tau_x$* ***a fórmula obtida ao substituir todas as ocorrências livres de** x **em** φ **por** τ. Equivalentemente:*

- *se φ é da forma $p\tau_1...\tau_n$ para $p \in \mathcal{P}_n$ e $\tau_1,...,\tau_n$ termos de $\mathcal{L}$, então $[\varphi]^\tau_x$ é a fórmula $p[\tau_1]^\tau_x...[\tau_n]^\tau_x$;*
- *se φ é da forma $= \tau_1\tau_2$ para τ_1 e τ_2 termos de $\mathcal{L}$, então $[\varphi]^\tau_x$ é a fórmula $= [\tau_1]^\tau_x[\tau_2]^\tau_x$;*
- *se φ é da forma $\neg\psi$ onde ψ é uma fórmula de $\mathcal{L}$, então $[\varphi]^\tau_x$ é a fórmula $\neg[\psi]^\tau_x$;*
- *se φ é da forma $\wedge\psi\phi$, $\vee\psi\phi$, $\rightarrow \psi\phi$ ou $\leftrightarrow \psi\phi$ onde ψ e ϕ são fórmulas de $\mathcal{L}$, então $[\varphi]^\tau_x$ é, respectivamente, a fórmula $\wedge[\psi]^\tau_x[\phi]^\tau_x$, $\vee[\psi]^\tau_x[\phi]^\tau_x$, $\rightarrow [\psi]^\tau_x[\phi]^\tau_x$ ou $\leftrightarrow [\psi]^\tau_x[\phi]^\tau_x$;*
- *se φ é da forma $\forall y\psi$ ou $\exists y\psi$, onde y é uma variável diferente de x, então $[\varphi]^\tau_x$ é, respectivamente, a fórmula $\forall y[\psi]^\tau_x$ ou $\exists y[\psi]^\tau_x$;*
- *se φ é da forma $\forall x\psi$ ou $\exists x\psi$, então $[\varphi]^\tau_x$ é a própria fórmula φ.*

Note que, se φ é uma sentença, então para todo termo τ e toda variável x tem-se que $[\varphi]^\tau_x$ é a própria fórmula φ, já que φ não possui variáveis livres.

Sejam $x_1,...,x_n$ variáveis, $\tau_1,...,\tau_n$ termos e φ uma fórmula. Escrevemos $\varphi(x_1,...,x_n)$ para denotar a fórmula φ onde $x_1,...,x_n$ são todas as variáveis livres de φ listadas sem repetição. E escrevemos $\varphi(\tau_1,...,\tau_n)$ para denotar $[...[[\varphi]^{\tau_1}_{x_1}]^{\tau_2}_{x_2}...]^{\tau_n}_{x_n}$, isto é, a fórmula obtida ao substituir todas as ocorrências livres de $x_1,...,x_n$ por $\tau_1,...,\tau_n$, respectivamente, na fórmula φ.

Vejamos alguns exemplos. Considere a linguagem $\mathcal{L} = \{+,\cdot,-,0,1,<\}$ da teoria dos corpos ordenados e a fórmula φ dada por $\exists y(y\cdot y = x+z)$. Então $[\varphi]^1_x$ é a fórmula $\exists y(y\cdot y = 1+z)$, enquanto $[\varphi]^1_y$ é a própria fórmula φ, pois não há nenhuma ocorrência livre da variável y na fórmula φ. Seja, agora, a fórmula ψ dada por $\exists y(x < y)$. Seu fecho universal é uma sentença verdadeira em $\mathbb{R}$. Seja τ_1 o termo $z + z$. Neste caso, temos que $[\psi]_x^{\tau_1}$ é a fórmula $\exists y(z+z<y)$ e seu fecho universal ainda é uma sentença verdadeira em $\mathbb{R}$. Mas se tomarmos o termo $\tau_2 = y+1$, então $[\psi]_x^{\tau_2}$ é a sentença $\exists y(y+1<y)$, que é falsa em $\mathbb{R}$. Isto ocorreu porque a variável y já possuía uma ocorrência limitada em ψ, e ao inserirmos o termo τ_2 no lugar da ocorrência livre de x, a variável y advinda do termo τ_2 passou a sofrer ação do $\exists y$ presente em ψ. Portanto nem sempre valerá um resultado análogo ao Teorema 2.19 para fórmulas. Para poder expressar o caso em que vale um resultado análogo, precisaremos de uma definição.

Definição 2.21 *Sejam $\mathcal{L}$ uma linguagem para a lógica de primeira ordem, τ um termo de $\mathcal{L}$, φ uma fórmula de $\mathcal{L}$ e x uma variável. Dizemos que τ **é livre para** x **em** φ se nenhuma ocorrência livre de x em φ ocorre no escopo de um quantificador $\forall y$ ou $\exists y$, onde y é uma variável que ocorre em τ.*

Note que, no exemplo anterior, o termo τ_2 não é livre para x na fórmula ψ, pois x ocorre livremente no escopo de $\exists y$, e y é uma variável que ocorre em τ_2. Quando a substituição for feita inserindo um termo livre para a variável considerada, teremos o resultado a seguir, que é análogo ao Teorema 2.19, só que para fórmulas.

Teorema 2.22 *Sejam $\mathcal{L}$ uma linguagem de primeira ordem, $\mathfrak{E} = (A, \mathcal{I})$ uma estrutura para $\mathcal{L}$, φ e τ uma fórmula e um termo, respectivamente, de $\mathcal{L}$, x uma variável e σ uma atribuição para τ e φ em A. Se $a = val^{\mathfrak{E}}(\tau)[\sigma]$ e τ é livre para x em φ, então $\mathfrak{E} \vDash [\varphi]_x^\tau[\sigma]$ se, e somente se, $\mathfrak{E} \vDash \varphi[\sigma + (x/a)]$.*

Demonstração: Faremos a demonstração por indução nos tipos de fórmula, de acordo com a Definição 1.8. Para as fórmulas atômicas basta aplicar o Teorema 2.19 e usar a Definição 2.5 de valoração para fórmulas atômicas.

Faremos o caso $\neg\varphi$ e os casos da forma $\varphi \wedge \psi$, $\varphi \vee \psi$, $\varphi \to \psi$ e $\varphi \leftrightarrow \psi$, seguirão de maneira análoga. Suponha então que vale

$$(\star)\ \mathfrak{E} \vDash [\varphi]_x^\tau[\sigma] \Leftrightarrow \mathfrak{E} \vDash \varphi[\sigma + (x/a)],$$

quando $a = val^{\mathfrak{E}}(\tau)[\sigma]$ e τ é livre para x em φ.

Supondo agora que τ é livre para x em $\neg\varphi$, queremos mostrar que vale a equivalência $\mathfrak{E} \vDash [\neg\varphi]_x^\tau[\sigma] \Leftrightarrow \mathfrak{E} \vDash \neg\varphi[\sigma + (x/a)]$. Note primeiro que $\neg\varphi$ não acrescenta nenhuma variável ou quantificador em relação à φ, então vale que τ é livre para x em φ, logo, estamos nas condições de $(\star)$. Suponha então que $\mathfrak{E} \vDash [\neg\varphi]_x^\tau[\sigma]$, ou seja, que $val^{\mathfrak{E}}([\neg\varphi]_x^\tau)[\sigma] = 1$. Como $[\neg\varphi]_x^\tau = \neg[\varphi]_x^\tau$, então de $val^{\mathfrak{E}}([\neg\varphi]_x^\tau)[\sigma] = 1$ segue que $val^{\mathfrak{E}}(\neg[\varphi]_x^\tau)[\sigma] = 1$, e pela definição de valoração para fórmulas segue que $val^{\mathfrak{E}}([\varphi]^{\tau}_{x})[\sigma] = 0$. Pela equivalência ($\star$) obtemos $val^{\mathfrak{E}}(\varphi)[\sigma + (x/a)] = 0$, logo $val^{\mathfrak{E}}(\neg\varphi)[\sigma + (x/a)] = 1$, e portanto $\mathfrak{E} \vDash \neg\varphi[\sigma + (x/a)]$, como queríamos. Reciprocamente, assumindo $\mathfrak{E} \vDash \neg\varphi[\sigma + (x/a)]$ concluímos o resultado de uma forma semelhante.

Vejamos agora o caso em que φ é da forma $\forall y\psi$ ou $\exists y\psi$. Note primeiro que se x não ocorre livremente em φ então $[\varphi]^{\tau}_{x}$ é a própria φ, e o valor atribuído por σ a x não importa. Desta forma vale imediatamente a equivalência do enunciado, pois em ambos os lados teremos $\mathfrak{E} \vDash \varphi[\sigma]$. Suponha então que x possui ao menos uma ocorrência livre em φ. Dessa forma temos que x e y são variáveis distintas (pela forma de φ) e portanto a ocorrência livre de x deve acontecer em ψ. Sendo, por hipótese, τ livre para x em φ, segue que y não pode ocorrer em τ. Disto segue que, dado $b \in A$ qualquer, obtemos que $a = val^{\mathfrak{E}}(\tau)[\sigma] = val^{\mathfrak{E}}(\tau)[\sigma + (y/b)]$. E portanto a equivalência desejada seguirá da Definição 2.7 para os casos de fórmula com quantificadores. $\square$

Temos o seguinte resultado (que é uma consequência direta do resultado anterior):

Corolário 2.23 *Sejam $\mathfrak{E}$ uma estrutura para uma linguagem de primeira ordem $\mathcal{L}$, $\varphi(x_1, ..., x_n)$ uma fórmula de $\mathcal{L}$ que possui somente as variáveis $x_1, ..., x_n$ livres e $\tau_1, ..., \tau_n$ termos de $\mathcal{L}$ sem variáveis. Se $a_i = val^{\mathfrak{E}}(\tau_i)$, então $\mathfrak{E} \vDash \varphi(\tau_1, ..., \tau_n)$ se, e somente se, $\mathfrak{E} \vDash \varphi[\sigma]$, onde σ é a atribuição para φ em $\mathfrak{E}$ dada por $\sigma(x_1) = a_1, ..., \sigma(x_n) = a_n$.*

2.3 Redução e expansão de estruturas

Vejamos agora outras definições importantes em relação à semântica. Para tal, se $\mathcal{L}_0$ e $\mathcal{L}_1$ são linguagens de primeira ordem, ao escrevermos $\mathcal{L}_0 \subseteq \mathcal{L}_1$ estamos assumindo, implicitamente, que os símbolos de $\mathcal{L}_0$ possuem, em $\mathcal{L}_1$, o mesmo tipo e a mesma aridade que possuem em $\mathcal{L}_0$.

Definição 2.24 *Sejam $\mathcal{L}_0$ e $\mathcal{L}_1$ linguagens de primeira ordem tais que $\mathcal{L}_0 \subseteq \mathcal{L}_1$. Se $\mathfrak{E} = (A, \mathcal{I})$ é uma estrutura para $\mathcal{L}_1$, então $\mathfrak{E}\restriction_{\mathcal{L}_0} = (A, \mathcal{I}\restriction_{\mathcal{L}_0})$ é denominado uma **redução** de $\mathfrak{E}$. Neste caso, $\mathfrak{E}$ é dita uma **expansão** de $\mathfrak{E}\restriction_{\mathcal{L}_0}$.*

Por exemplo, considere a linguagem da teoria dos corpos $\mathcal{L} = \{+, \cdot, -, i, 0, 1\}$, onde i indica a operação de inversão. Então $\mathfrak{E} = \mathbb{R}$ com a interpretação usual é uma estrutura para $\mathcal{L}$. Tomando determinados subconjuntos de $\mathcal{L}$ podemos ver o universo de $\mathfrak{E}$ de formas diferente, como corpo ou como grupo abeliano, por exemplo.

O teorema a seguir nos mostra que as noções de consequência semântica e consistência semântica se conservam em uma redução e em uma expansão.

Teorema 2.25 *Sejam $\mathcal{L}_0$ e $\mathcal{L}_1$ linguagens de primeira ordem tais que $\mathcal{L}_0 \subseteq \mathcal{L}_1$, Σ um conjunto de sentenças de $\mathcal{L}_0$ e φ uma sentença de $\mathcal{L}_0$. São equivalentes:*

A. *Existe uma $\mathcal{L}_0$-estrutura $\mathfrak{E}_0$ tal que $\mathfrak{E}_0 \vDash \Sigma$.*

B. *Existe uma $\mathcal{L}_1$-estrutura $\mathfrak{E}$ tal que $\mathfrak{E} \vDash \Sigma$.*

Também são equivalentes:

1. *$\mathfrak{E}_0 \vDash \varphi$ para toda $\mathcal{L}_0$-estrutura $\mathfrak{E}_0$ tal que $\mathfrak{E}_0 \vDash \Sigma$.*

2. *$\mathfrak{E}_1 \vDash \varphi$ para toda $\mathcal{L}_1$-estrutura $\mathfrak{E}$ tal que $\mathfrak{E}_1 \vDash \Sigma$.*

Demonstração: $(A \Rightarrow B)$. Seja $\mathfrak{E}_0 = (A, \mathcal{I})$ uma $\mathcal{L}_0$-estrutura tal que $\mathfrak{E}_0 \vDash \Sigma$. Podemos expandir $\mathfrak{E}_0$ para uma $\mathcal{L}_1$-estrutura $\mathfrak{E} = (A, \mathcal{J})$ da seguinte forma: para cada símbolo de $\mathcal{L}_1 \setminus \mathcal{L}_0$, a função $\mathcal{J}$ associa tal símbolo, respectivamente, à função vazia, ao conjunto vazio, a um elemento arbitrário de A e a 0, caso esse símbolo seja um símbolo de função de aridade n (com $n > 0$), relação n-ária (com $n > 0$), constante ou uma letra proposicional. Dessa forma $\mathfrak{E}$ será uma $\mathcal{L}_1$-estrutura.

Note que $\mathfrak{E} \vDash \Sigma$, pois sendo Σ um conjunto de sentenças de $\mathcal{L}_0$, a satisfação de $\psi \in \Sigma$ independe das interpretações adicionadas na expansão, e como $\mathfrak{E}_0 \vDash \psi$, então ψ também será satisfeita em $\mathfrak{E}$, já que esta mantém as interpretações dos símbolos de $\mathcal{L}_0$. Logo $\mathfrak{E} \vDash \Sigma$, como queríamos.

$(B \Rightarrow A)$. Seja $\mathfrak{E} = (A, \mathcal{J})$ uma $\mathcal{L}_1$-estrutura tal que $\mathfrak{E} \vDash \Sigma$. Note que $\mathfrak{E}_0 = (A, \mathcal{J}\upharpoonright_{\mathcal{L}_0})$ é uma $\mathcal{L}_0$-estrutura, e como Σ é um conjunto de sentenças de $\mathcal{L}_0$ e que $\mathfrak{E} \vDash \Sigma$, podemos concluir que $\mathfrak{E}_0 \vDash \Sigma$, pois a satisfação de $\psi \in \Sigma$ só dependerá das interpretações dos elementos de $\mathcal{L}_0$, e estas são mantidas por $\mathfrak{E}_0$.

$(1 \Rightarrow 2)$. Seja $\mathfrak{E}_1 = (A, \mathcal{J})$ uma $\mathcal{L}_1$-estrutura tal que $\mathfrak{E}_1 \vDash \Sigma$. Note que $\mathfrak{E}_0 = (A, \mathcal{J}\upharpoonright_{\mathcal{L}_0})$ é uma $\mathcal{L}_0$-estrutura, e como Σ é um conjunto de sentenças de $\mathcal{L}_0$ e $\mathfrak{E}_1 \vDash \Sigma$, podemos concluir que $\mathfrak{E}_0 \vDash \Sigma$. Logo, pela hipótese, $\mathfrak{E}_0 \vDash \varphi$. Como φ é uma sentença de $\mathcal{L}_0$ e $\mathcal{L}_0 \subseteq \mathcal{L}_1$ então a satisfação de φ em $\mathfrak{E}_0$ garante a satisfação de φ em $\mathfrak{E}_1$. Portanto, $\mathfrak{E}_1 \vDash \varphi$.

$(2 \Rightarrow 1)$. Seja $\mathfrak{E}_0 = (A, \mathcal{I})$ uma $\mathcal{L}_0$-estrutura tal que $\mathfrak{E}_0 \vDash \Sigma$. Podemos expandir $\mathfrak{E}_0$ para uma $\mathcal{L}_1$-estrutura $\mathfrak{E}_1 = (A, \mathcal{J})$ da mesma forma que fizemos anteriormente e teremos que $\mathfrak{E}_1 \vDash \Sigma$. Assim, por hipótese, temos que $\mathfrak{E}_1 \vDash \varphi$. E como φ é uma sentença de $\mathcal{L}_0$, então a satisfação de φ é mantida por $\mathfrak{E}_0$, já que $\mathfrak{E}_1$ coincide com $\mathfrak{E}_0$ nas interpretações dos símbolos de $\mathcal{L}_0$. Em outras palavras $\mathfrak{E}_0 \vDash \varphi$. □

Note que se permitíssemos, na definição de estrutura, que o domínio A fosse vazio, então não poderíamos obter tal resultado. De fato, se existisse ao menos um símbolo de constante em $\mathcal{L}_1 \setminus \mathcal{L}_0$ e se A fosse vazio, então não poderíamos construir uma expansão, como fizemos na demonstração, pois deve haver ao menos um elemento em A para que os símbolos de constantes de $\mathcal{L}_1 \setminus \mathcal{L}_0$ sejam levados nele.

2.4 Tautologias

Definiremos agora o conceito de tautologia. Para tal, olharemos apenas para as fórmulas que não se iniciam com nenhum conectivo proposicional.

Definição 2.26 *Uma fórmula de uma linguagem de primeira ordem é dita* ***básica*** *se sua escrita em Notação Polonesa não se inicia com nenhum símbolo do conjunto* $\{\wedge, \vee, \neg, \rightarrow, \leftrightarrow\}$.

Todas as fórmulas atômicas são básicas. Outros exemplos são as fórmulas $\forall x\varphi$ e $\exists x\varphi$. Já a fórmula $\forall x\varphi \rightarrow \exists x\varphi$ não é básica, pois sua Notação Polonesa $\rightarrow \forall x\varphi\exists x\varphi$ se inicia com o símbolo $\rightarrow$.

Definição 2.27 *Uma* ***atribuição verdade*** *para uma linguagem de primeira ordem* $\mathcal{L}$ *é uma função* v *do conjunto das fórmulas básicas de* $\mathcal{L}$ *em* $\{0, 1\}$. *Dada uma atribuição verdade* v, *definimos a função* $\overline{v}$ *que estende* v *para uma fórmula arbitrária, da seguinte maneira:*

- $\overline{v}(\neg\varphi) = 1 - \overline{v}(\varphi)$;
- $\overline{v}(\wedge\varphi\psi) = 1$ *se, e somente se,* $\overline{v}(\varphi) = 1$ *e* $\overline{v}(\psi) = 1$;
- $\overline{v}(\vee\varphi\psi) = 1$ *se, e somente se,* $\overline{v}(\varphi) = 1$ *ou* $\overline{v}(\psi) = 1$;
- $\overline{v}(\rightarrow \varphi\psi) = 1$ *se, e somente se,* $\overline{v}(\varphi) = 0$ *ou* $\overline{v}(\psi) = 1$;
- $\overline{v}(\leftrightarrow \varphi\psi) = 1$ *se, e somente se,* $\overline{v}(\varphi) = \overline{v}(\psi)$.

E dizemos que uma fórmula φ *é uma* ***tautologia proposicional*** *(ou, simplesmente, uma* ***tautologia****) se* $\overline{v}(\varphi) = 1$ *para toda atribuição verdade* v.

Assim, para verificar se uma fórmula φ é uma tautologia, devemos analisar o que ocorre com todas as possíveis atribuições de 0 ou 1 a todas as subfórmulas básicas de φ. Vejamos um exemplo. Considere φ a fórmula $\forall xp(x) \rightarrow \forall yp(y)$, onde p é um símbolo de relação unária. As subfórmulas básicas de φ são $\forall xp(x)$ e $\forall yp(y)$, assim, existem quatro possíveis atribuições verdade, v_1, v_2, v_3 e v_4, tais que: $v_1(\forall xp(x)) = 0$ e $v_1(\forall yp(y)) = 0$, $v_2(\forall xp(x)) = 0$ e $v_2(\forall yp(y)) = 1$, $v_3(\forall xp(x)) = 1$ e $v_3(\forall yp(y)) = 0$, e, $v_4(\forall xp(x)) = 1$ e $v_4(\forall yp(y)) = 1$. Pela definição acima, temos que $\overline{v_1}(\varphi) = 1$, $\overline{v_2}(\varphi) = 1$, $\overline{v_3}(\varphi) = 0$ e $\overline{v_4}(\varphi) = 1$. Assim, φ não é uma tautologia, pois $\overline{v_3}(\varphi) \neq 1$. Já a fórmula $p(x) \rightarrow p(x)$ é uma tautologia, pois há somente duas atribuições verdade possíveis: $w_1(p(x)) = 0$ e $w_2(p(x)) = 1$ e, pela definição acima, ocorre $\overline{w_i}(\psi) = 1$, para $i \in \{1, 2\}$.

Teorema 2.28 *Toda tautologia proposicional é logicamente válida.*

Demonstração: Sejam φ uma tautologia proposicional, $\mathfrak{E}$ uma $\mathcal{L}$-estrutura e σ uma atribuição para φ em $\mathfrak{E}$. Devemos mostrar que $\mathfrak{E} \vDash \varphi[\sigma]$, ou, equivalentemente, $val^{\mathfrak{E}}(\varphi)[\sigma] = 1$. Para tal, considere $f : \mathcal{C} \rightarrow \{0, 1\}$ onde $\mathcal{C}$ é o conjunto das fórmulas básicas de $\mathcal{L}$ que são subfórmulas de φ. Considere ainda $\mathcal{B}$ o conjunto de todas as fórmulas básicas de $\mathcal{L}$, $v : \mathcal{B} \rightarrow \{0, 1\}$ tal que $v \upharpoonright_{\mathcal{C}} \; = f$ e $v(\psi) = 0$ para toda ψ em $\mathcal{B} \setminus \mathcal{C}$. Então v é uma atribuição verdade, e pelas Definições 2.7 e 2.27 temos que $\overline{v}(\varphi) = val^{\mathfrak{E}}(\varphi)[\sigma]$. Sendo φ uma tautologia segue que $\overline{v}(\varphi) = 1$ e, portanto, $val^{\mathfrak{E}}(\varphi)[\sigma] = 1$, como queríamos. □

3 Sintaxe

Neste capítulo veremos as noções sintáticas de prova formal na Seção 3.1 e formalizaremos alguns argumentos clássicos da matemática na Seção 3.2. Fazendo um paralelo com a gramática, a ideia da sintaxe neste contexto é analisar as sentenças de uma linguagem de primeira ordem e definir uma relação entre elas de forma a compor um texto, e, no nosso caso, compor uma prova. As principais referências bibliográficas para este capítulo são [3] e [5].

3.1 A noção de prova formal

Nosso objetivo nesta seção é definir rigorosamente a noção de prova ou demonstração. Informalmente, uma demonstração é uma sequência finita de sentenças que obtemos a partir de um certo conjunto de premissas (axiomas) por meio da aplicação de regras de inferência. No que segue, adotaremos uma única regra de inferência, denominada Modus Ponens.

Definição 3.1 *Sejam φ e ψ sentenças de uma linguagem de primeira ordem $\mathcal{L}$. A única* ***regra de inferência*** *que adotaremos, denominada* ***Modus Ponens****, diz o seguinte: de φ e $\varphi \to \psi$ concluímos ψ (ou, ainda, inferimos ψ).*

Vamos agora definir e fixar um conjunto de axiomas, que chamaremos de *axiomas lógicos*. Os axiomas lógicos são sentenças que gostaríamos que fossem válidas (e que são, em algum nível, intuitivamente válidas) e que usaremos como base para as provas formais.

Definição 3.2 *Um* ***axioma lógico*** *de uma linguagem de primeira ordem $\mathcal{L}$ é uma sentença de $\mathcal{L}$ que é um fecho universal de uma fórmula de um dos seguintes tipos:*

1. *tautologias proposicionais;*

2. *$\varphi \to \forall x \varphi$, onde x não é livre em φ;*

3. *$\forall x(\varphi \to \psi) \to (\forall x \varphi \to \forall x \psi)$;*

4. $\forall x\varphi \to [\varphi]_x^\tau$, *onde* τ *é um termo livre para* x *em* φ;

5. $[\varphi]_x^\tau \to \exists x\varphi$, *onde* τ *é um termo livre para* x *em* φ;

6. $\forall x\neg\varphi \leftrightarrow \neg\exists x\varphi$;

7. $x = x$;

8. $x = y \leftrightarrow y = x$;

9. $x = y \wedge y = z \to x = z$;

10. $(x_1 = y_1 \wedge x_2 = y_2 \wedge ... \wedge x_n = y_n) \to f(x_1, x_2, ..., x_n) = f(y_1, y_2, ..., y_n)$, *para todo* $n > 0$ *e* $f \in \mathcal{F}_n$;

11. $(x_1 = y_1 \wedge x_2 = y_2 \wedge ... \wedge x_n = y_n) \to p(x_1, x_2, ..., x_n) \leftrightarrow p(y_1, y_2, ..., y_n)$, *para todo* $n > 0$ *e* $p \in \mathcal{P}_n$.

Note ainda que, se omitíssemos a hipótese de τ ser um termo livre para x em φ no Axioma 4, então tal esquema iria gerar um axioma indesejado para nossa lista. Para ver isto, considere a sentença $\forall x\exists y(\neg(x = y))$. O termo y não é livre para a variável x na fórmula $\exists y(\neg(x = y))$. Se pudéssemos invocar o Axioma 4 neste caso, teríamos que $\forall x\exists y(\neg(x = y)) \to [\exists y(\neg(x = y))]_x^y$, ou seja, que $\forall x\exists y(\neg(x = y)) \to \exists y(\neg(y = y))$, que é falsa em uma $\mathcal{L}$-estrutura cujo universo possui ao menos dois elementos distintos.

Teorema 3.3 *Todos os axiomas lógicos são logicamente válidos.*

Demonstração: Para os itens abaixo, mostraremos que a lista de fórmulas dada na Definição 3.2 é uma lista de fórmulas logicamente válidas. Sendo φ uma fórmula logicamente válida, mostramos que $\forall x\varphi$ é logicamente válida da seguinte maneira: fixando $\mathfrak{E}$ uma $\mathcal{L}$-estrutura e σ uma atribuição para φ, como φ é logicamente válida, para todo $a \in A$ temos que $val^{\mathfrak{E}}(\varphi)[\sigma + (x/a)] = 1$. Generalizando este resultado para n variáveis obtemos que se φ é logicamente válida então um fecho universal qualquer de φ também o é.

1. Segue do Teorema 2.28.

2. Sejam φ uma fórmula, $\mathfrak{E}$ uma $\mathcal{L}$-estrutura e σ uma atribuição para a fórmula $\varphi \to \forall x\varphi$ em $\mathfrak{E}$, onde x não é livre em φ. Se $val^{\mathfrak{E}}(\varphi)[\sigma] = 0$, pela tabela verdade da implicação segue que $val^{\mathfrak{E}}(\varphi \to \forall x\varphi)[\sigma] = 1$. Suponha portanto que $val^{\mathfrak{E}}(\varphi)[\sigma] = 1$. Para concluir o resultado devemos mostrar que $val^{\mathfrak{E}}(\forall x\varphi)[\sigma] =$

1. Por sua vez, para isto, devemos mostrar que $val^{\mathfrak{E}}(\varphi)[\sigma + (x/a)] = 1$ para todo a no universo de $\mathfrak{E}$. Note que, como x não é livre em φ, então toda ocorrência de x (quando houver) é limitada. Desta forma, podemos trocar as ocorrências de x por outra variável diferente de x e que não esteja no domínio de σ e manteremos o valor lógico de φ (pois as fórmulas $\forall x\psi$ e $\forall y\psi$ possuem a mesma valoração, e o mesmo ocorre para o quantificador existencial). Dessa forma φ não possui mais nenhuma ocorrência de x, e portanto $val^{\mathfrak{E}}(\varphi)[\sigma + (x/a)] = val^{\mathfrak{E}}(\varphi)[\sigma] = 1$, como queríamos mostrar.

3. Sejam φ, ψ fórmulas, $\mathfrak{E}$ uma $\mathcal{L}$-estrutura e σ uma atribuição para a fórmula $\forall x(\varphi \to \psi) \to (\forall x\varphi \to \forall x\psi)$ em $\mathfrak{E}$. Vamos mostrar que $val^{\mathfrak{E}}(\forall x(\varphi \to \psi) \to (\forall x\varphi \to \forall x\psi))[\sigma] = 1$. Pela definição de valoração, se $val^{\mathfrak{E}}(\forall x(\varphi \to \psi))[\sigma] = 0$ temos o resultado. Suponha portanto que $val^{\mathfrak{E}}(\forall x(\varphi \to \psi))[\sigma] = 1$. Queremos mostrar que, neste caso, vale $val^{\mathfrak{E}}(\forall x\varphi \to \forall x\psi)[\sigma] = 1$. Novamente, se $val^{\mathfrak{E}}(\forall x\varphi)[\sigma] = 0$ segue o resultado. Suponha então que $val^{\mathfrak{E}}(\forall x\varphi)[\sigma] = 1$ e vejamos que $val^{\mathfrak{E}}(\forall x\psi)[\sigma] = 1$ — e disto seguirá que $val^{\mathfrak{E}}(\forall x\varphi \to \forall x\psi)[\sigma] = 1$, como desejado. Para tal, fixe a uma constante arbitrária no universo da estrutura $\mathfrak{E}$. Como $val^{\mathfrak{E}}(\forall x(\varphi \to \psi))[\sigma] = 1$ então $val^{\mathfrak{E}}(\varphi \to \psi)[\sigma + (x/a)] = 1$. E como $val^{\mathfrak{E}}(\forall x\varphi)[\sigma] = 1$, então $val^{\mathfrak{E}}(\varphi)[\sigma + (x/a)] = 1$. Assim, decorre da definição de valoração para a implicação que $val^{\mathfrak{E}}(\psi)[\sigma + (x/a)] = 1$ e, portanto, $val^{\mathfrak{E}}(\forall x\psi)[\sigma] = 1$. Esta última igualdade é a desejada.

4. Sejam φ uma fórmula, $\mathfrak{E}$ uma $\mathcal{L}$-estrutura e σ uma atribuição para a fórmula $\forall x\varphi \to [\varphi]^{\tau}_{x}$, onde τ é um termo livre para x em φ. Suponha que $val^{\mathfrak{E}}(\forall x\varphi)[\sigma] = 1$. Então $val^{\mathfrak{E}}(\varphi)[\sigma + (x/a)] = 1$, para todo $a \in A$, e em particular, para $a = val^{\mathfrak{E}}(\tau)[\sigma]$. Pelo Teorema 2.22 segue que $val^{\mathfrak{E}}([\varphi]^{\tau}_{x})[\sigma] = 1$, e disto decorre que $val^{\mathfrak{E}}(\forall x\varphi \to [\varphi]^{\tau}_{x}) = 1$, como queríamos.

5. Análogo ao item anterior.

6. Análogo ao exemplo feito após a Definição 2.14.

7. Se $x = x$ segue da definição de valoração para a igualdade que $val^{\mathfrak{E}}(x)[\sigma] = val^{\mathfrak{E}}(x)[\sigma]$, para toda $\mathcal{L}$-estrutura $\mathfrak{E}$ e toda atribuição σ. Desta forma $val^{\mathfrak{E}}(x = x)[\sigma] = 1$.

8. Segue da definição de valoração para a igualdade usando que $val^{\mathfrak{E}}(x)[\sigma] = val^{\mathfrak{E}}(y)[\sigma]$ se, e somente se, $val^{\mathfrak{E}}(y)[\sigma] = val^{\mathfrak{E}}(x)[\sigma]$.

9. Análogo ao item anterior.

10. Basta notar que $val^{\mathfrak{E}}(x_1 = y_1 \wedge ... \wedge x_n = y_n)[\sigma] = 1$ se, e somente se, $val^{\mathfrak{E}}(x_i = y_i)[\sigma] = 1$, o que, por sua vez, equivale a $val^{\mathfrak{E}}(x_i)[\sigma] = val^{\mathfrak{E}}(y_i)[\sigma]$, para todo $i \in \{1, ..., n\}$. Então neste caso vale

$$\begin{aligned} val^{\mathfrak{E}}(f(x_1,...,x_n))[\sigma] =& f^{\mathfrak{E}}(val^{\mathfrak{E}}(x_1)[\sigma],...,val^{\mathfrak{E}}(x_n)[\sigma]) \\ =& f^{\mathfrak{E}}(val^{\mathfrak{E}}(y_1)[\sigma],...,val^{\mathfrak{E}}(y_n)[\sigma]) \\ =& val^{\mathfrak{E}}(f(y_1,...,y_n))[\sigma]. \end{aligned}$$

Portanto temos $\mathfrak{E} \vDash f(x_1,...,x_n) = f(y_1,...,y_n)$, e disto segue o resultado.

11. Análogo ao item anterior, usando a definição de valoração para o bicondicional. □

Podemos definir uma prova formal partindo de um conjunto de sentenças.

Definição 3.4 *Se Σ é um conjunto de sentenças de uma linguagem de primeira ordem $\mathcal{L}$, então uma **prova formal partindo de** Σ é uma sequência finita (e não vazia) φ_0, φ_1, ..., φ_n de sentenças de $\mathcal{L}$ tal que para cada $i \in \{0,1,...,n\}$, ou $\varphi_i \in \Sigma$, ou φ_i é um axioma lógico, ou para certos $j,k < i$ tem-se que φ_i decorre de φ_j e φ_k por Modus Ponens (isto é, φ_k é a fórmula $\varphi_j \rightarrow \varphi_i$). Dessa forma, dizemos que a sequência φ_0, φ_1, ..., φ_n é uma **prova formal de** φ_n.*

Definição 3.5 *Se Σ é um conjunto de sentenças de uma linguagem de primeira ordem $\mathcal{L}$ e φ é uma sentença de $\mathcal{L}$, dizemos que φ é **consequência sintática de** Σ, e escrevemos $\Sigma \vdash_{\mathcal{L}} \varphi$, quando existe uma prova formal de φ partindo de Σ.*

Se $\Sigma = \{\psi\}$ denotamos, usualmente, $\Sigma \vdash \varphi$ por $\psi \vdash \varphi$.

Vejamos um exemplo das duas definições acima. Afirmamos que existe uma prova formal para $\neg\varphi$ partindo de $\Sigma = \{\varphi \rightarrow \psi, \neg\psi\}$. Para verificar tal afirmação, considere a seguinte sentença: $(\varphi \rightarrow \psi) \rightarrow ((\neg\psi) \rightarrow (\neg\varphi))$. Vejamos que tal sentença é uma tautologia. Note que únicas subfórmulas básicas da fórmula acima são φ e ψ. Logo, há 4 casos a considerar.

- $v_1(\varphi) = 0$ e $v_1(\psi) = 0$. Neste caso temos que $\overline{v}_1(\varphi \rightarrow \psi) = 1$ e $\overline{v}_1((\neg\psi) \rightarrow (\neg\varphi)) = 1$, logo $\overline{v}_1((\varphi \rightarrow \psi) \rightarrow ((\neg\psi) \rightarrow (\neg\varphi))) = 1$.

- $v_2(\varphi) = 1$ e $v_2(\psi) = 1$. Este caso é análogo ao caso anterior.

- $v_3(\varphi) = 0$ e $v_3(\psi) = 1$. Neste caso temos que $\overline{v}_3(\varphi \rightarrow \psi) = 1$ e $\overline{v}_3((\neg\psi) \rightarrow (\neg\varphi)) = 1$, logo $\overline{v}_3((\varphi \rightarrow \psi) \rightarrow ((\neg\psi) \rightarrow (\neg\varphi))) = 1$.

- $v_4(\varphi) = 1$ e $v_4(\psi) = 0$. Este caso é análogo ao caso anterior.

Portanto tal fórmula é uma tautologia, e, consequentemente, é um axioma lógico.

Por hipótese $\varphi \to \psi \in \Sigma$, logo segue da sentença anterior (que vimos ser um axioma) e da regra de inferência Modus Ponens que $(\neg\psi) \to (\neg\varphi)$ é uma consequência sintática de Σ. E sendo, por hipótese, $\neg\psi \in \Sigma$, segue da regra de inferência Modus Ponens que $\neg\varphi$ é uma consequência sintática de Σ.

O Teorema 3.6 é a implicação direta da equivalência

$$\Sigma \vdash_{\mathcal{L}} \varphi \text{ se, e somente se, } \Sigma \vDash \varphi.$$

Ele nos diz, em outras palavras, que consequência sintática implica consequência semântica. A recíproca dessa implicação é o chamado Teorema da Completude, que veremos posteriormente[1].

Teorema 3.6 (Teorema da Correção) *Sejam $\mathcal{L}$ uma linguagem de primeira ordem, Σ um conjunto de sentenças de $\mathcal{L}$ e φ uma sentença de $\mathcal{L}$. Se $\Sigma \vdash_{\mathcal{L}} \varphi$ então $\Sigma \vDash \varphi$.*

Demonstração: Suponha que $\Sigma \vdash_{\mathcal{L}} \varphi$ e seja $\mathcal{M}$ uma estrutura para $\mathcal{L}$ tal que $\mathcal{M} \vDash \Sigma$. Queremos mostrar que $\mathcal{M} \vDash \varphi$. Sejam $\varphi_0, \varphi_1, ..., \varphi_n$ sentenças de $\mathcal{L}$ tais que $\varphi_0, \varphi_1, ..., \varphi_n$ é uma prova formal de φ partindo de Σ. Note que φ_n é a fórmula φ. Mostraremos, por indução em i, que $\mathcal{M} \vDash \varphi_i$. Se $i = 0$, então ou $\varphi_0 \in \Sigma$ ou φ_0 é um axioma lógico. Se $\varphi_0 \in \Sigma$, então como $\mathcal{M} \vDash \Sigma$, segue que $\mathcal{M} \vDash \varphi_0$. Se φ_0 é um axioma lógico, então pelo Teorema 3.3 φ_0 é uma sentença logicamente válida. E sendo $\mathcal{M}$ uma estrutura para $\mathcal{L}$, segue que $\mathcal{M} \vDash \varphi_0$.

Suponha agora que $\mathcal{M} \vDash \varphi_j$ para todo $j < i$ e vejamos que o resultado vale para i. Se $\varphi_i \in \Sigma$ ou φ_i é uma axioma lógico, então o mesmo argumento apresentado acima garante que $\mathcal{M} \vDash \varphi_i$. Resta então tratar o caso em que φ_i não satisfaz nenhuma destas duas condições. A única possibilidade é φ_i ter sido inferido por Modus Ponens aplicado a sentenças que ocorrem antes de φ_i na prova de φ, isto é, devem existir $j, k < i$ tais que φ_k é a sentença $\varphi_j \to \varphi_i$. Como $j, k < i$ então, por hipótese de indução, temos que $\mathcal{M} \vDash \varphi_j$ e $\mathcal{M} \vDash \varphi_k$, e desta segunda decorre que $\mathcal{M} \vDash \varphi_j \to \varphi_i$. Do Corolário 2.8 segue que $\mathcal{M} \vDash \varphi_j \to \varphi_i$ se, e somente se, $\mathcal{M} \vDash \varphi_i$ ou não ocorre $\mathcal{M} \vDash \varphi_j$. Dessa forma, segue que $\mathcal{M} \vDash \varphi_i$. □

[1]A equivalência é usualmente chamada de Teorema da Completude, mas a recíproca é a implicação menos trivial do teorema.

3.2 Formalização de argumentos clássicos da matemática

Nesta seção veremos a formalização rigorosa, se valendo da definição de prova formal dada na seção anterior, de argumentos clássicos de demonstração. O primeiro deles é o Teorema da Dedução (dado pelo Teorema 3.7). Nele, formalizamos a ideia de que para demonstrar uma implicação do tipo $p \to q$ é suficiente que, ao assumir válida a afirmação p, consigamos concluir que q é válida.

Teorema 3.7 (Teorema da Dedução) *Se Σ é um conjunto de sentenças da linguagem de primeira ordem $\mathcal{L}$ e φ e ψ são sentenças de $\mathcal{L}$, então $\Sigma \vdash_{\mathcal{L}} \varphi \to \psi$ se, e somente se, $\Sigma \cup \{\varphi\} \vdash_{\mathcal{L}} \psi$.*

Demonstração: ($\Rightarrow$) Suponha que $\Sigma \vdash_{\mathcal{L}} \varphi \to \psi$. Assim, existe uma sequência $\varphi_0, \varphi_1, ..., \varphi_n$ que é uma prova de $\varphi \to \psi$ partindo de Σ. Adicionando as sentenças φ_{n+1} igual a φ e φ_{n+2} igual a ψ, e notando que φ_{n+2} pode ser obtido por Modus Ponens a partir das sentenças φ_n, que é $\varphi \to \psi$, e φ_{n+1}, temos que a sequência $\varphi_0, \varphi_1, ..., \varphi_n, \varphi_{n+1}, \varphi_{n+2}$ é uma prova de ψ partindo de $\Sigma \cup \{\varphi\}$.

($\Leftarrow$) Suponha agora que $\Sigma \cup \{\varphi\} \vdash_{\mathcal{L}} \psi$. Então existe uma sequÊncia $\psi_0, \psi_1, ..., \psi_n$ que é uma prova formal de ψ partindo de $\Sigma \cup \{\varphi\}$. Mostraremos, por indução em i, que $\Sigma \vdash \varphi \to \psi_i$, e sendo ψ_n igual a ψ, teremos que $\Sigma \vdash \varphi \to \psi$. Suponha então que vale $\Sigma \vdash_{\mathcal{L}} (\varphi \to \psi_j)$ para todo $j < i$. Há três possíveis casos (note que os dois primeiros casos não utilizam a hipótese de indução, e são estes os únicos casos possíveis para ψ_0):

Caso 1: ψ_i é um axioma lógico ou $\psi_i \in \Sigma$.

Neste caso, note que a sentença $\psi_i \to (\varphi \to \psi_i)$ é uma tautologia. Para isto, basta considerar a seguinte tabela de atribuição verdade:

φ	ψ_i	$\varphi \to \psi_i$	$\psi_i \to (\varphi \to \psi_i)$
V	V	V	V
V	F	F	V
F	V	V	V
F	F	V	V

Dessa forma, a seguinte sequência é uma prova formal para $\varphi \to \psi_i$:

1. ψ_i
2. $\psi_i \to (\varphi \to \psi_i)$
3. $\varphi \to \psi_i$

onde o último item é inferido por Modus Ponens a partir dos dois itens anteriores. Assim, obtemos $\Sigma \vdash_{\mathcal{L}} \varphi \to \psi_i$.

Caso 2: ψ_i é φ.

Neste caso, $\varphi \to \psi_i$ é uma tautologia, logo a sequência formada por essa única sentença é uma prova formal de $\varphi \to \psi_i$ partindo de Σ.

Caso 3: existem $j, k < i$ tais que ψ_i é inferido de ψ_j e ψ_k por Modus Ponens — e, portanto, ψ_k é a sentença $\psi_j \to \psi_i$.

Vejamos primeiro que a sentença $(\varphi \to \psi_j) \to ((\varphi \to (\psi_j \to \psi_i)) \to (\varphi \to \psi_i))$, a qual chamaremos de α, é uma tautologia. Denotando $(\varphi \to (\psi_j \to \psi_i)) \to (\varphi \to \psi_i)$ por β, a seguinte tabela de atribuição verdade mostra que α é uma tautologia.

φ	ψ_i	ψ_j	$\psi_j \to \psi_i$	$\varphi \to \psi_i$	$\varphi \to \psi_j$	$\varphi \to (\psi_j \to \psi_i)$	β	α
V	V	V	V	V	V	V	V	V
V	V	F	V	V	F	V	V	V
V	F	V	F	F	V	F	V	V
V	F	F	V	F	F	V	F	V
F	V	V	V	V	V	V	V	V
F	V	F	V	V	V	V	V	V
F	F	V	F	V	V	V	V	V
F	F	F	V	V	V	V	V	V

Logo, o que segue mostra que existe uma prova de $\varphi \to \psi_i$ partindo de Σ:

1. $\Sigma \vdash_{\mathcal{L}} \varphi \to \psi_j$ (por hipótese de indução em $j < i$)
2. $\Sigma \vdash_{\mathcal{L}} \varphi \to (\psi_j \to \psi_i)$ (por hipótese de indução em $k < i$)
3. $\Sigma \vdash_{\mathcal{L}} (\varphi \to \psi_j) \to ((\varphi \to (\psi_j \to \psi_i)) \to (\varphi \to \psi_i))$ (pois tal sentença é uma tautologia)
4. $\Sigma \vdash_{\mathcal{L}} (\varphi \to (\psi_j \to \psi_i)) \to (\varphi \to \psi_i)$ (pelos itens 1 e 3 e Modus Ponens)
5. $\Sigma \vdash_{\mathcal{L}} \varphi \to \psi_i$ (pelos itens 2 e 4 e Modus Ponens)

Note que uma prova formal para a sentença descrita no item 4 é obtida usando uma prova formal da sentença $\varphi \to \psi_j$ (cuja existência é garantida pelo item 1) e a tautologia descrita no item 3: aplicaríamos Modus Ponens na sentença $\varphi \to \psi_j$ e na tautologia, obtendo finalmente uma prova formal para a sentença $\varphi \to (\psi_j \to \psi_i) \to (\varphi \to \psi_i)$. O mesmo vale para o item 5. Dessa forma, mostramos como obter uma prova formal indiretamente — sem de fato explicitar a sequência, e sim indicando um caminho para obter tal sequência. $\square$

Nosso próximo passo é considerar as provas por contradição (ou redução ao absurdo).

Definição 3.8 *Se Σ é um conjunto de sentenças de uma linguagem de primeira ordem $\mathcal{L}$, dizemos que Σ é **sintaticamente inconsistente**, e escrevemos $\neg Con_{\vdash,\mathcal{L}}(\Sigma)$, se existe alguma sentença φ de $\mathcal{L}$ tal que $\Sigma \vdash_{\mathcal{L}} \varphi$ e $\Sigma \vdash_{\mathcal{L}} \neg\varphi$. E dizemos que Σ é **sintaticamente consistente** se não for sintaticamente inconsistente.*

Veremos no resultado a seguir que a inconsistência sintática de um conjunto Σ de sentenças de uma linguagem de primeira ordem $\mathcal{L}$ é equivalente a conseguir provar qualquer sentença de $\mathcal{L}$ partindo de Σ.

Lema 3.9 *Se Σ é um conjunto de sentenças de uma linguagem de primeira ordem $\mathcal{L}$, então são equivalentes:*

1. *$\neg Con_{\vdash,\mathcal{L}}(\Sigma)$.*

2. *$\Sigma \vdash_{\mathcal{L}} \psi$, para toda sentença ψ de $\mathcal{L}$.*

Demonstração: ($1 \Rightarrow 2$) Suponha que vale o item 1 e seja φ uma sentença de $\mathcal{L}$ que atesta que $\neg Con_{\vdash,\mathcal{L}}(\Sigma)$, ou seja, $\Sigma \vdash_{\mathcal{L}} \varphi$ e $\Sigma \vdash_{\mathcal{L}} \neg\varphi$. Note que, para uma sentença arbitrária ψ de $\mathcal{L}$, a sentença $\varphi \to (\neg\varphi \to \psi)$ é uma tautologia. De fato, basta considerar a seguinte tabela de atribuição verdade:

φ	ψ	$\neg\varphi$	$\neg\varphi \to \psi$	$\varphi \to (\neg\varphi \to \psi)$
V	V	F	V	V
V	F	F	V	V
F	V	V	V	V
F	F	V	F	V

Dessa forma, como vale $\Sigma \vdash_{\mathcal{L}} \varphi$, conseguimos uma prova formal de φ partindo de Σ, e então podemos aplicar Modus Ponens na sentença φ e na tautologia citada acima, inferindo a sentença $\neg\varphi \to \psi$. Como vale $\Sigma \vdash_{\mathcal{L}} \neg\varphi$, então existe uma prova de $\neg\varphi$ partindo de Σ, e então podemos aplicar Modus Ponens nas sentenças $\neg\varphi$ e $\neg\varphi \to \psi$, inferindo ψ. Assim, concluímos que $\Sigma \vdash_{\mathcal{L}} \psi$.

($2 \Rightarrow 1$) Assumindo o item 2, basta tomar uma sentença φ de $\mathcal{L}$ e a sentença $\neg\varphi$, e teremos que $\Sigma \vdash_{\mathcal{L}} \varphi$ e $\Sigma \vdash_{\mathcal{L}} \neg\varphi$, logo $\neg Con_{\vdash,\mathcal{L}}(\Sigma)$. $\square$

Teorema 3.10 (Prova por Contradição) *Se Σ é um conjunto de sentenças de uma linguagem de primeira ordem $\mathcal{L}$ e φ é uma sentença de $\mathcal{L}$, então valem:*

1. *$\Sigma \vdash_{\mathcal{L}} \varphi$ se, e somente se, $\neg Con_{\vdash,\mathcal{L}}(\Sigma \cup \{\neg\varphi\})$.*

2. *$\Sigma \vdash_{\mathcal{L}} \neg\varphi$ se, e somente se, $\neg Con_{\vdash,\mathcal{L}}(\Sigma \cup \{\varphi\})$.*

Demonstração: Mostraremos que vale o item 1, e o item 2 segue de forma análoga. Supondo que $\Sigma \vdash_{\mathcal{L}} \varphi$, então em particular temos que $\Sigma \cup \{\neg\varphi\} \vdash_{\mathcal{L}} \varphi$, pois $\Sigma \subseteq \Sigma \cup \{\neg\varphi\}$ e, portanto, a mesma prova que atesta $\Sigma \vdash_{\mathcal{L}} \varphi$ também atesta que $\Sigma \cup \{\neg\varphi\} \vdash_{\mathcal{L}} \varphi$. E como $\neg\varphi \in \Sigma \cup \{\neg\varphi\}$, a sequência formada unicamente pela sentença $\neg\varphi$ atesta que $\Sigma \cup \{\neg\varphi\} \vdash_{\mathcal{L}} \neg\varphi$. Portanto, $\neg Con_{\vdash,\mathcal{L}}(\Sigma \cup \{\neg\varphi\})$.

Supondo agora que $\neg Con_{\vdash,\mathcal{L}}(\Sigma \cup \{\neg\varphi\})$, pelo Lema 3.9 temos que $\Sigma \cup \{\neg\varphi\} \vdash_{\mathcal{L}} \varphi$. Logo, pelo Teorema da Dedução, segue que $\Sigma \vdash_{\mathcal{L}} \neg\varphi \to \varphi$. Note agora que $(\neg\varphi \to \varphi) \to \varphi$ é uma tautologia, e desta tautologia e da sentença $\neg\varphi \to \varphi$ podemos inferir por Modus Ponens a sentença φ. Logo temos que $\Sigma \vdash_{\mathcal{L}} \varphi$. □

A Definição 3.11 e os Teoremas 3.12 e 3.13 generalizam o raciocínio apresentado no fim do Teorema 3.10.

Definição 3.11 *Dizemos que uma sentença φ **segue tautologicamente** de $\varphi_1, ..., \varphi_n$ se $(\varphi_1 \wedge ... \wedge \varphi_n) \to \varphi$ é uma tautologia proposicional.*

Teorema 3.12 *Se $\varphi, \varphi_1, ..., \varphi_n$ são sentenças de uma linguagem de primeira ordem $\mathcal{L}$ e φ segue tautologicamente de $\varphi_1, ..., \varphi_n$, então $\{\varphi_1, ..., \varphi_n\} \vdash_{\mathcal{L}} \varphi$.*

Demonstração: Primeiro, note que $\varphi_1 \to (\varphi_2 \to (... \to (\varphi_n \to \varphi)...))$ possui o mesmo valor lógico (quando analisamos a tabela de atribuição verdade) que $(\varphi_1 \wedge ... \wedge \varphi_n) \to \varphi$. Para isso, basta observar que as seguintes sentenças possuem o mesmo valor lógico:

1. $\neg(\neg((\varphi_1 \wedge ... \wedge \varphi_n) \to \varphi))$

2. $(\neg\varphi_1) \vee ... \vee (\neg\varphi_n) \vee \varphi$

3. $(\neg\varphi_1) \vee ... \vee (\neg\varphi_{n-1}) \vee (\varphi_n \to \varphi)$

4. $(\neg\varphi_1) \vee ... \vee (\neg\varphi_{n-2}) \vee ((\varphi_{n-1} \to (\varphi_n \to \varphi))$

$\vdots$

$n+2$. $\varphi_1 \to (\varphi_2 \to (... \to (\varphi_n \to \varphi)...))$

E como a primeira sentença possui, pela definição de $\neg$, o mesmo valor lógico de $(\varphi_1 \wedge ... \wedge \varphi_n) \to \varphi$, e esta por sua vez é uma tautologia, então segue que $\varphi_1 \to (\varphi_2 \to (... \to (\varphi_n \to \varphi)...))$ é uma tautologia. Assim, basta aplicar Modus Ponens n

vezes nesta tautologia e nas φ_i para obtermos uma prova de φ partindo de $\{\varphi_1,...,\varphi_n\}$. □

O Teorema 3.13 pode ser visto como uma espécie de transitividade do símbolo $\vdash$.

Teorema 3.13 *Seja uma linguagem de primeira ordem $\mathcal{L}$. Se $\{\varphi_1,...,\varphi_n\} \vdash_{\mathcal{L}} \psi$ e $\Sigma \vdash_{\mathcal{L}} \varphi_i$ para todo $i \in \{1,...,n\}$, então $\Sigma \vdash_{\mathcal{L}} \psi$.*

Demonstração: Uma prova formal de ψ partindo de Σ pode começar listando, para cada $i \in \{1,\dots,n\}$, uma prova formal de φ_i partindo de Σ e finalizar listando uma prova formal de ψ partindo de $\{\varphi_1,\dots,\varphi_n\}$. □

Note que os principais teoremas demonstrados nesta seção, como o Teorema da Dedução e o da Prova por Contradição, visam formalizar o modo como nós demonstramos resultados usualmente. Cada um deles justifica alguma técnica específica usada. Veremos no próximo teorema outras formalizações de técnicas, desta vez com o uso dos quantificadores.

Teorema 3.14 (Regras para quantificadores) *Sejam $\mathcal{L}$ uma linguagem de primeira ordem, Σ um conjunto de sentenças de $\mathcal{L}$ e $\varphi(x)$ uma fórmula de $\mathcal{L}$ com no máximo a variável x ocorrendo livre. Valem as seguintes regras para o uso de quantificadores:*

UI: $\{\forall x\varphi(x)\} \vdash_{\mathcal{L}} \varphi(\tau)$.

UG: *De $\Sigma \vdash_{\mathcal{L}'} \varphi(c)$ concluímos que $\Sigma \vdash_{\mathcal{L}} \forall x\varphi(x)$.*

EI: *De $\Sigma \cup \{\varphi(c)\} \vdash_{\mathcal{L}'} \psi$ concluímos que $\Sigma \cup \{\exists x\varphi(x)\} \vdash_{\mathcal{L}} \psi$.*

EG: $\{\varphi(\tau)\} \vdash_{\mathcal{L}} \exists x\varphi(x)$.

Em UI e EG, τ é um termo de $\mathcal{L}$ sem variáveis. Em UG e EI, c é um símbolo de constante que não está em $\mathcal{L}$ e $\mathcal{L}' = \mathcal{L} \cup \{c\}$, e em EI, ψ é uma sentença de $\mathcal{L}$.

As letras U, E, I, G vêm de "Universal", "Existencial", "Instância"e "Generalização", respectivamente. Vejamos alguns exemplos que demonstram na prática o argumento que cada uma das sentenças acima formaliza.

A sentença UI formaliza o argumento de que se uma sentença universal $\forall x\varphi(x)$ é verdadeira então podemos concluir que uma instância $\varphi(\tau)$ é verdadeira. Por exemplo, se $\forall x(x+2=2+x)$ é verdadeiro, então, em particular $1+2=2+1$.

A afirmação EG permite concluir que, se conseguimos provar φ para um termo τ específico, então é verdadeira a generalização existencial de que existe algum x que satisfaz $\varphi(x)$.

Para exemplificar a sentença UG considere a seguinte afirmação: para todo $x \in \mathbb{R}$ existe $y \in \mathbb{R}$ tal que $x = y^3$. Tal afirmação é, em símbolos, a sentença $\forall x\varphi(x)$, onde $\varphi(x)$ é a sentença $\exists y(x = y^3)$. Para demonstrar essa afirmação, usualmente iríamos fixar um $c \in \mathbb{R}$ arbitrário e mostrar que para este c existe um $y \in \mathbb{R}$ que satisfaz $c = y^3$. E como c era arbitrário, então a afirmação vale para todo $x \in \mathbb{R}$. A afirmação UG é a formalização de "como c era arbitrário, então vale que $\forall x\varphi(x)$".

Por fim, quando queremos provar um resultado que tem como hipótese uma afirmação do tipo "existe um elemento x que satisfaz $\varphi(x)$", então para demonstrar a tese fixaríamos um c que satisfaz φ e ao concluir que vale a tese, concluiríamos que ela decorre da hipótese $\exists x\varphi(x)$. A afirmação EI corresponde a esse tipo de raciocínio.

Exemplo 3.15 *Se ψ é uma fórmula de uma linguagem de primeira ordem $\mathcal{L}$ com nenhuma variável diferente de x livre, então $\emptyset \vdash_{\mathcal{L}} \neg\forall x\psi(x) \to \exists x\neg\psi(x)$.*

Seja c um símbolo de constante que não está em $\mathcal{L}$ e considere $\mathcal{L}' = \mathcal{L} \cup \{c\}$.

1. $\emptyset \vdash_{\mathcal{L}} \forall x\neg\neg\psi(x) \leftrightarrow \neg\exists x\neg\psi(x)$ (axioma lógico do tipo 6)
2. $\neg\neg\psi(c) \vdash_{\mathcal{L}'} \psi(c)$ (tautologia e Teorema 3.12)
3. $\forall x\neg\neg\psi(x) \vdash_{\mathcal{L}'} \psi(c)$ (2, UI e Teorema3.13)
4. $\forall x\neg\neg\psi(x) \vdash_{\mathcal{L}} \forall x\psi(x)$ (3 e UG)
5. $\emptyset \vdash_{\mathcal{L}} \forall x\neg\neg\psi(x) \to \forall x\psi(x)$ (4 e Teorema da Dedução)
6. $\emptyset \vdash_{\mathcal{L}} \neg\forall x\psi(x) \to \exists x\neg\psi(x)$ (1, 5 e tautologia)

Demonstração do Teorema 3.14: Para demonstrar UI, note que a sentença $\forall x\varphi(x) \to \varphi(\tau)$ é um axioma lógico do tipo 4. Desta forma temos que $\emptyset \vdash_{\mathcal{L}} \forall x\varphi(x) \to \varphi(\tau)$, e pelo Teorema da Dedução segue que $\{\forall x\varphi(x)\} \vdash_{\mathcal{L}} \varphi(\tau)$, como desejado.

Para demonstrar EG, basta notar que a sentença $\varphi(\tau) \to \exists x\varphi(x)$ é um axioma lógico do tipo 5 e um raciocínio análogo ao anterior mostra que $\{\varphi(\tau)\} \vdash_{\mathcal{L}} \exists x\varphi(x)$.

Para demonstrar UG, suponha que $\Sigma \vdash_{\mathcal{L}'} \varphi(c)$ e seja $\varphi_0, ..., \varphi_n$ uma prova formal em $\mathcal{L}'$ de $\varphi(c)$. Então φ_n é a sentença $\varphi(c)$. Seja y uma variável que não ocorre em nenhuma das sentenças φ_i, e seja $\psi_i(y)$ a fórmula resultante da substituição de todas as ocorrências de c em φ_i pela variável y. Mostraremos, por indução em i, que $\Sigma \vdash_{\mathcal{L}} \forall y\psi_i(y)$. Note que, ao mostrarmos isto, teremos que $\Sigma \vdash_{\mathcal{L}} \forall y\varphi(y)$ (pois $\psi_n(y)$ é a sentença $\varphi(y)$) e a seguinte sequência mostra que $\forall y\varphi(y) \vdash_{\mathcal{L}} \forall x\varphi(x)$:

$1.\forall y\varphi(y)$	(por hipótese)
$2.\forall x(\forall y\varphi(y) \to \varphi(x))$	(axioma lógico do tipo 4)
$3.\forall x(\forall y\varphi(y) \to \varphi(x)) \to (\forall x\forall y\varphi(y) \to \forall x\varphi(x))$	(axioma lógico do tipo 3)
$4.\forall x\forall y\varphi(y) \to \forall x\varphi(x)$	(pelos itens 3, 2 e Modus Ponens)
$5.\forall y\varphi(y) \to \forall x\forall y\varphi(y)$	(axioma lógico do tipo 2)
$6.\forall x\forall y\varphi(y)$	(pelos itens 5, 1 e Modus Ponens)
$7.\forall x\varphi(x)$	(pelos itens 4, 6 e Modus Ponens)

Logo, segue de $\Sigma \vdash_{\mathcal{L}} \forall y\varphi(y)$, de $\{\forall y\varphi(y)\} \vdash_{\mathcal{L}} \forall x\varphi(x)$ e da transitividade de $\vdash$, Teorema 3.13, que $\Sigma \vdash_{\mathcal{L}} \forall x\varphi(x)$.

Procedamos à indução. Há três casos a serem considerados. O Caso 1 a seguir evidencia por que motivo precisamos exigir que y seja uma variável que não ocorre em lugar algum na prova $\varphi_0, ..., \varphi_n$.

Caso 1. φ_i é um axioma lógico. Note primeiro que se c não ocorre em φ_i, então $\psi_i(y)$ é a própria sentença φ_i, e então temos o axioma lógico do tipo 2, $\varphi_i \to \forall y\varphi_i$, e sendo φ_i um axioma lógico, podemos inferir $\forall y\varphi_i$, isto é, $\forall y\psi_i(y)$. No caso em que há ocorrência de c em φ_i, temos que a sentença $\forall y\psi_i(y)$ é um axioma lógico do mesmo tipo de φ_i [2].

Caso 2. $\varphi_i \in \Sigma$. Neste caso, como c é uma constante que não está em $\mathcal{L}$ e Σ é um conjunto de sentenças de $\mathcal{L}$, então φ_i não contém nenhuma ocorrência de c. Assim, $\psi_i(y)$ é a própria sentença φ_i. Notando que $\varphi_i \to \forall y\varphi_i$ é um axioma lógico do tipo 2 e usando que $\varphi_i \in \Sigma$, podemos inferir $\forall y\varphi_i$, o que atesta que $\Sigma \vdash_{\mathcal{L}} \forall y\psi_i(y)$ (usando, claro, que φ_i é a sentença $\psi_i(y)$).

Caso 3. Existem $j, k < i$ tais que φ_i é inferido de φ_j e φ_k por Modus Ponens — e, portanto, φ_k é a sentença $\varphi_j \to \varphi_i$. Neste caso, a seguinte sequência de afirmações

[2]Por exemplo, se φ_i é a sentença $\forall z\exists xp(z,x) \to \exists xp(c,x)$, então a sentença $\psi_i(y)$ é a dada por $\forall z\exists xp(z,x) \to \exists xp(y,x)$. Assim, a sentença $\forall y\psi_i(y)$ é o fecho universal da sentença $\psi_i(y)$, a qual é também um axioma lógico do tipo 4. Lembre-se de que, no início, havíamos tomado y como uma variável que não ocorre em nenhuma das sentenças φ_i. Se y fosse, por exemplo, a variável x, que ocorre na sentença $\forall z\exists xp(z,x) \to \exists xp(c,x)$, então $\psi_i(y)$ seria a sentença $\forall z\exists xp(z,x) \to \exists xp(x,x)$, que não é um axioma lógico, já que x não é livre para z em $\exists xp(z,x)$.

nos garante que existe uma prova formal de $\forall y \psi_i(y)$ partindo de Σ.

$1.\Sigma \vdash_{\mathcal{L}} \forall y \psi_j(y)$	(por hipótese de indução em $j < i$)
$2.\Sigma \vdash_{\mathcal{L}} \forall y(\psi_j(y) \to \psi_i(y))$	(por hipótese de indução em $k < i$)
$3.\Sigma \vdash_{\mathcal{L}} \forall y(\psi_j(y) \to \psi_i(y)) \to (\forall y \psi_j(y) \to \forall y \psi_i(y))$	(axioma lógico do tipo 3)
$4.\Sigma \vdash_{\mathcal{L}} \forall y \psi_j(y) \to \forall y \psi_i(y)$	(pelos itens 3, 2 e Modus Ponens)
$5.\Sigma \vdash_{\mathcal{L}} \forall y \psi_i(y)$	(pelos itens 4, 1 e Modus Ponens)

Assim, concluímos a demonstração de UG.

Vejamos agora que vale EI. Para tal, suponha que $\Sigma \cup \{\varphi(c)\} \vdash_{\mathcal{L}'} \psi$. Do Teorema 3.10 (Prova por Contradição) segue que $\neg Con_{\vdash,\mathcal{L}'}(\Sigma \cup \{\varphi(c), \neg\psi\})$, e aplicando novamente o mesmo teorema temos que $\Sigma \cup \{\neg\psi\} \vdash_{\mathcal{L}'} \neg\varphi(c)$. Agora, por UG (que já mostramos ser válida) segue que $\Sigma \cup \{\neg\psi\} \vdash_{\mathcal{L}} \forall x \neg\varphi(x)$. Assim, novamente pelo Teorema 3.10 segue que $\neg Con_{\vdash,\mathcal{L}}(\Sigma \cup \{\neg\psi, \neg(\forall x \neg\varphi(x))\})$, e aplicando novamente o mesmo teorema obtemos $\Sigma \cup \{\neg(\forall x \neg\varphi(x))\} \vdash_{\mathcal{L}} \psi$. Agora, note que $\forall x \neg\varphi(x) \leftrightarrow \neg(\exists x \varphi(x))$ é um axioma lógico do tipo 6, e que $\neg(\forall x \neg\varphi(x))$ segue tautologicamente deste axioma e de $\exists x \varphi(x)$. Assim, do Teorema 3.12 segue que $\{\exists x \varphi(x)\} \vdash_{\mathcal{L}} \neg(\forall x \neg\varphi(x))$. Como vimos que $\Sigma \cup \{\neg(\forall x \neg\varphi(x))\} \vdash_{\mathcal{L}} \psi$, decorre do Teorema 3.13 que $\Sigma \cup \{\exists x \varphi(x)\} \vdash_{\mathcal{L}} \psi$. $\square$

4 O Teorema da Completude

O objetivo deste capítulo é demonstrar o Teorema da Completude, que relaciona as noções de consistência semântica e consistência sintática. As principais referências bibliográficas para este capítulo são [3] e [5].

Teorema 4.1 (Teorema da Completude) *Seja Σ um conjunto de sentenças de uma linguagem de primeira ordem $\mathcal{L}$. Então:*

1. $Con_{\models}(\Sigma)$ *se, e somente se,* $Con_{\vdash,\mathcal{L}}(\Sigma)$.

2. *Para toda sentença φ de $\mathcal{L}$, $\Sigma \models \varphi$ se, e somente se, $\Sigma \vdash_{\mathcal{L}} \varphi$.*

O item 1 do Teorema da Completude diz que as noções de consistência sintática e semântica são equivalentes, ou seja, existe uma $\mathcal{L}$-estrutura que modela Σ se, e somente se, Σ não leva a contradições. Uma vez demonstrado este item, não será mais necessário explicitar os símbolos $\models$ e $\vdash$ para nos referirmos à consistência. O item 2 do Teorema da Completude diz que φ é consequência semântica de um conjunto de sentenças Σ se, e somente se, φ é consequência sintática de Σ. Note que já havíamos visto (no Teorema da Correção) que, se φ é consequência sintática de Σ, então φ é consequência semântica de Σ. Assim, resta verificar que, se φ é consequência semântica de Σ, então φ é consequência sintática de Σ.

Vamos primeiro mostrar que as afirmações (1) e (2) do Teorema da Completude são, na verdade, equivalentes. Assim, para demonstrar o Teorema 4.1, bastará mostrar que vale alguma das afirmações.

Teorema 4.2 *Seja Σ um conjunto de sentenças de uma linguagem de primeira ordem $\mathcal{L}$. São equivalentes:*

1. $Con_{\models}(\Sigma)$ *se, e somente se,* $Con_{\vdash,\mathcal{L}}(\Sigma)$.

2. *Para toda sentença φ de $\mathcal{L}$, $\Sigma \models \varphi$ se, e somente se, $\Sigma \vdash_{\mathcal{L}} \varphi$.*

Demonstração: $(1 \to 2)$ Seja φ uma sentença de $\mathcal{L}$. Note que, pelo Teorema 2.13, $\Sigma \models \varphi$ ocorre se, e somente se, $\neg Con_{\models}(\Sigma \cup \{\neg\varphi\})$ e, por hipótese, isto ocorre se, e somente se, $\neg Con_{\vdash,\mathcal{L}}(\Sigma \cup \{\neg\varphi\})$. Por sua vez, pelo Teorema 3.10, isto ocorre se, e somente se, $\Sigma \vdash_{\mathcal{L}} \varphi$, como queríamos.

($2 \to 1$) Vamos assumir (2) e provar, por contrapositiva, a ida e a volta de (1). Suponha então que $\neg Con_{\vdash,\mathcal{L}}(\Sigma)$. Então existe uma sentença φ de $\mathcal{L}$ tal que $\Sigma \vdash_{\mathcal{L}} \varphi$ e $\Sigma \vdash_{\mathcal{L}} \neg\varphi$. Assim, por hipótese, vale que $\Sigma \vDash_{\mathcal{L}} \varphi$ e $\Sigma \vDash_{\mathcal{L}} \neg\varphi$. Dessa forma não pode haver uma $\mathcal{L}$-estrutura $\mathcal{M}$ tal que $\mathcal{M} \vDash \Sigma$, pois se houvesse uma tal $\mathcal{M}$, de $\Sigma \vDash_{\mathcal{L}} \varphi$ obteríamos $\mathcal{M} \vDash \varphi$, e de $\Sigma \vDash_{\mathcal{L}} \neg\varphi$ obteríamos $\mathcal{M} \vDash \neg\varphi$, o que contradiz a Proposição 2.9. Logo, $\neg Con_{\vDash}(\Sigma)$.

Suponha agora que vale $\neg Con_{\vDash}(\Sigma)$ e seja $\varphi \in \Sigma$. Então $\Sigma = \Sigma \cup \{\varphi\}$, e $\neg Con_{\vDash}(\Sigma)$ se traduz em $\neg Con_{\vDash}(\Sigma \cup \{\varphi\})$. Do Teorema 2.13 segue que $\Sigma \vDash \neg\varphi$, do item 2 segue que $\Sigma \vdash_{\mathcal{L}} \neg\varphi$ e do Teorema 3.10 segue que $\neg Con_{\vdash,\mathcal{L}}(\Sigma \cup \{\varphi\})$, isto é, $\neg Con_{\vdash,\mathcal{L}}(\Sigma)$, como queríamos. □

O próximo resultado mostra que, para demonstrar o Teorema da Completude, basta provar que consistência sintática implica consistência semântica.

Teorema 4.3 *Seja Σ um conjunto de sentenças de uma linguagem de primeira ordem $\mathcal{L}$. Se $Con_{\vdash,\mathcal{L}}(\Sigma)$ implica $Con_{\vDash}(\Sigma)$, então vale o Teorema da Completude.*

Demonstração: Basta notar que, na demonstração do Teorema 4.2, mostramos que o Teorema da Correção é suficiente para concluir que $Con_{\vDash}(\Sigma) \to Con_{\vdash,\mathcal{L}}(\Sigma)$. □

Desta forma, basta provar o seguinte resultado.

Lema 4.4 *Seja Σ um conjunto de sentenças de uma linguagem de primeira ordem $\mathcal{L}$. Se $Con_{\vdash,\mathcal{L}}(\Sigma)$, então $Con_{\vDash}(\Sigma)$.*

Assim, nosso objetivo (e é a parte que dará mais trabalho) é demonstrar o Lema 4.4. O Teorema da Completude foi provado pela primeira vez por Kurt Gödel em 1929. No mesmo ano, de forma independente, Jacques Herbrand apresentou um método para construir modelos usando os termos da linguagem. Em 1949 Leon Henkin percebeu que o método de Herbrand poderia ser usado para demonstrar o Teorema da Completude. A demonstração que apresentaremos do Teorema da Completude baseia-se nessa ideia de Henkin.

Para provar o Lema 4.4 precisamos, a partir da consistência sintática de Σ, mostrar a consistência semântica, ou seja, temos que exibir uma $\mathcal{L}$-estrutura e mostrar que tal estrutura modela Σ. Sendo assim, parece natural construir um modelo para Σ usando os objetos sintáticos da linguagem. Note (na Definição 2.1) que, fixada uma estrutura para a linguagem $\mathcal{L}$, alguns termos de $\mathcal{L}$ são associados a elementos do universo por uma interpretação — por exemplo, termos do tipo constante. Sendo assim, seja lá o que for nosso modelo, o universo da estrutura desejada deve ter elementos que se associam a estes termos da linguagem. Um bom início, então, seria colocar tais termos da linguagem dentro do universo que estamos construindo (e, assim, poderíamos associá-los a si mesmos no universo da estrutura). Mas note que isto não pode ser feito para *todos* os termos da linguagem. Por exemplo, não faz sentido colocar uma variável no universo da estrutura — justamente porque variáveis não possuem valores determinados até que seja fixada uma atribuição, diferente das constantes citadas acima.

Assim, primeiro iremos inserir no universo da estrutura que estamos construindo os termos da linguagem $\mathcal{L}$ que não contêm nenhuma variável; logo, o valor de uma valoração para um tal termo em uma estrutura fixada é o mesmo para toda atribuição, e isto fixa a interpretação desse termo — diferente do que ocorre na interpretação de termos que contém variáveis. Vamos destacar tais termos na definição a seguir.

Definição 4.5 *Um termo τ de uma linguagem de primeira ordem $\mathcal{L}$ é dito **fechado** quando τ não contém nenhuma variável. Denotamos por $CT_0(\mathcal{L})$ o conjunto de todos os termos fechados de $\mathcal{L}$.*

Agora, como sugerido anteriormente, definiremos uma $\mathcal{L}$-estrutura que tem como universo o conjunto dos termos fechados de $\mathcal{L}$ e usaremos as noções sintáticas de prova para definir a interpretação.

Definição 4.6 *Seja Σ um conjunto de sentenças de uma linguagem de primeira ordem $\mathcal{L}$. Supondo que $\mathcal{L}$ contenha ao menos um símbolo de constante (isto é, $\mathcal{F}_0 \neq \emptyset$), definimos a **estrutura de termos fechados** $\mathcal{M}_0 = \mathcal{CT}_0(\mathcal{L}, \Sigma)$ como a $\mathcal{L}$-estrutura cujo universo é o conjunto $CT_0(\mathcal{L})$ e cuja interpretação é dada, recursivamente, da seguinte maneira:*

- *Se $c \in \mathcal{F}_0$ então $c^{\mathcal{M}_0} = c$;*
- *Se $p \in \mathcal{P}_0$ então $p^{\mathcal{M}_0} = 1$ se, e somente se, $\Sigma \vdash_{\mathcal{L}} p$;*
- *Se $f \in \mathcal{F}_n$ com $n > 0$, e $\tau_1, ..., \tau_n \in CT_0(\mathcal{L})$, então $f^{\mathcal{M}_0}(\tau_1, ..., \tau_n)$ é o termo fechado $f(\tau_1, ..., \tau_n)$.*
- *Se $p \in \mathcal{P}_n$ com $n > 0$, e $\tau_1, ..., \tau_n \in CT_0(\mathcal{L})$, então $(\tau_1, ..., \tau_n) \in p^{\mathcal{M}_0}$ se, e somente se, $\Sigma \vdash_{\mathcal{L}} p(\tau_1, ..., \tau_n)$.*

Note que, como não admitimos uma estrutura cujo conjunto universo é vazio, a definição acima só faz sentido quando existe ao menos um termo de $\mathcal{L}$ que não contém variáveis — e tal termo existe, pois estamos assumindo que $\mathcal{F}_0 \neq \emptyset$. Note também que não pedimos que Σ satisfaça nenhuma condição especial. Se, por exemplo, Σ for sintaticamente inconsistente, a definição acima ainda faz sentido, mas teremos que $\mathcal{M}_0$ não é um modelo para Σ, pois já vimos que consistência semântica implica consistência sintática. Isto nos indica que o modelo que estamos buscando construir deve ter outro conjunto universo. Mas, ainda assim, vejamos quais propriedades já são satisfeitas por esta estrutura.

Teorema 4.7 *Seja Σ um conjunto de sentenças de uma linguagem de primeira ordem $\mathcal{L}$. Se $\tau \in CT_0(\mathcal{L})$, então $val^{\mathcal{M}_0}(\tau) = \tau$.*

Demonstração: Faremos esta prova por indução no comprimento de τ. Se $|\tau| = 1$, a única opção é τ ser uma constante, já que τ é um termo fechado. Se τ é uma constante c, então pela Definição 2.4 teremos que $val^{\mathcal{M}_0}(c) = c^{\mathcal{M}_0} = c$. Suponha agora que o enunciado seja válido para todo termo com comprimento estritamente menor que $|\tau| > 1$. Neste caso existem $f \in \mathcal{F}_n$ e $\tau_1, ..., \tau_n \in CT_0(\mathcal{L})$ tais que τ é o termo $f(\tau_1, ..., \tau_n)$. Note que τ_i possui comprimento estritamente menor que τ, logo, vale por hipótese de indução que $val^{\mathcal{M}_0}(\tau_i) = \tau_i$. Assim, usando a definição de valoração, temos que

$$\begin{aligned} val^{\mathcal{M}_0}(f(\tau_1, ..., \tau_n)) &= f^{\mathcal{M}_0}(val^{\mathcal{M}_0}(\tau_1), ..., val^{\mathcal{M}_0}(\tau_n)) \\ &= f^{\mathcal{M}_0}(\tau_1, ..., \tau_n) \\ &= f(\tau_1, ..., \tau_n), \end{aligned}$$

como queríamos. □

Note ainda que a interpretação dos símbolos de funções dada pela Definição 4.6 independe de Σ, o que pode nos trazer alguns problemas. Considere, por exemplo, $\mathcal{L} = \{0, +\}$ e Σ um conjunto de sentenças que contém a sentença $\forall x(x + 0 = x)$. O conjunto universo de $\mathcal{M}_0, CT_0(\mathcal{L})$, contém os termos fechados $0, 0 + 0, 0 + (0 + 0)$, e assim por diante, que são todos distintos. Sendo todos distintos, do Teorema 4.7 e do item (3) da Definição 2.5 segue que $\mathcal{M}_0 \nvDash (0 + 0 = 0)$. Por outro lado, como Σ possui o axioma $\forall x(x+0 = x)$, a regra UI de quantificadores UI e o Teorema 3.13 nos permitem concluir que $\Sigma \vdash_{\mathcal{L}} (0 + 0 = 0)$. Disto segue que $\mathcal{M}_0$ não é um modelo para Σ, pois de $\Sigma \vdash_{\mathcal{L}} (0 + 0 = 0)$ segue que $\Sigma \vDash (0 + 0 = 0)$, isto é, $\mathcal{M} \vDash (0 + 0 = 0)$ para todo modelo $\mathcal{M}$ de Σ, e vimos que isto não ocorre para a $\mathcal{L}$-estrutura $\mathcal{M}_0$.

Em resumo, como estamos buscando um modelo para Σ e queremos que valha a equivalência entre consequência sintática e semântica, temos mais um indício de que $CT_0(\mathcal{L})$ não deve ser o universo da estrutura que estamos buscando e, ainda, que devemos levar em consideração o conjunto Σ na interpretação dos símbolos de função na estrutura desejada — já que o problema no exemplo anterior surgiu ao notar que os elementos 0, $0+0$, $0+(0+0)$ etc. são todos distintos em $\mathcal{M}_0$. O que podemos fazer para lidar com esse problema é "identificar"os termos que queremos que sejam de alguma forma equivalentes. Faremos isto definindo uma relação de equivalência que reúna em uma mesma classe de equivalência termos que gostaríamos que fossem iguais e consideraremos uma estrutura que tenha o conjunto de todas estas classes de equivalência como conjunto universo. Vamos primeiro definir tal relação em $CT_0(\mathcal{L})$.

Definição 4.8 *Seja Σ um conjunto de sentenças de uma linguagem de primeira ordem $\mathcal{L}$. Definimos a relação $\sim_{\mathcal{L},\Sigma}$, a qual abreviaremos por $\sim$, em $CT_0(\mathcal{L})$ por:*

$$\tau \sim \sigma \text{ se, e somente se, } \Sigma \vdash_{\mathcal{L}} (\tau = \sigma).$$

Vejamos que $\sim$ é, de fato, uma relação de equivalência em $CT_0(\mathcal{L})$.

Teorema 4.9 *Seja Σ um conjunto de sentenças de uma linguagem de primeira ordem $\mathcal{L}$. Então a relação $\sim$ definida acima é uma relação de equivalência em $CT_0(\mathcal{L})$.*

Demonstração: Vejamos primeiro que $\sim$ é reflexiva, isto é, dado $\tau \in CT_0(\mathcal{L})$, ocorre $\Sigma \vdash_{\mathcal{L}} (\tau = \tau)$. Para tal, basta notar que $\forall x(x = x)$ é um axioma lógico do tipo 7 e, portanto, $\Sigma \vdash_{\mathcal{L}} \forall x(x = x)$. Agora, como τ é um termo de $\mathcal{L}$ sem variáveis, da regra de quantificadores UI segue que $\forall x(x = x) \vdash_{\mathcal{L}} (\tau = \tau)$, e pela transitividade de $\vdash_{\mathcal{L}}$ temos que $\Sigma \vdash_{\mathcal{L}} (\tau = \tau)$ e, portanto, $\tau \sim \tau$.

Vejamos agora que $\sim$ é simétrica. Dados $\tau, \sigma \in CT_0(\mathcal{L})$, queremos verificar que $\tau \sim \sigma$ se, e somente se, $\sigma \sim \tau$, isto é, $\Sigma \vdash_{\mathcal{L}} (\tau = \sigma)$ se, e somente se, $\Sigma \vdash_{\mathcal{L}} (\sigma = \tau)$. Faremos uma implicação, e a outra segue de forma inteiramente análoga. Suponha que vale $\Sigma \vdash_{\mathcal{L}} (\tau = \sigma)$. Note que a sentença $\forall x \forall y(x = y \leftrightarrow y = x)$ é um axioma lógico do tipo 8, e sendo τ e σ termos sem variáveis, então pela regra UI (aplicada duas vezes), segue que $\forall x \forall y(x = y \leftrightarrow y = x) \vdash_{\mathcal{L}} (\tau = \sigma \leftrightarrow \sigma = \tau)$. Como $\forall x \forall y(x = y \leftrightarrow y = x)$ é um axioma lógico, segue que $\emptyset \vdash_{\mathcal{L}} (\tau = \sigma \leftrightarrow \sigma = \tau)$. Note agora que $\sigma = \tau$ segue tautologicamente de $\tau = \sigma \leftrightarrow \sigma = \tau$ e $\tau = \sigma$, e como estamos assumindo que vale $\Sigma \vdash_{\mathcal{L}} (\tau = \sigma)$, então decorre que $\Sigma \vdash_{\mathcal{L}} (\sigma = \tau)$.

Vejamos por fim que $\sim$ é transitiva. Sejam $\tau, \sigma, \rho \in CT_0(\mathcal{L})$ tais que $\tau \sim \sigma$ e $\sigma \sim \rho$. Então vale $\Sigma \vdash_{\mathcal{L}} (\tau = \sigma)$ e $\Sigma \vdash_{\mathcal{L}} (\sigma = \rho)$. Note que a sentença[1] $\forall x, y, z((x = y \wedge y = z) \rightarrow x = z)$ é um axioma lógico do tipo 9, logo pelo mesmo argumento dos

itens anteriores segue que $\emptyset \vdash_{\mathcal{L}} ((\tau = \sigma \wedge \sigma = \rho) \rightarrow \tau = \rho)$. E como $\tau = \rho$ segue tautologicamente de $(\tau = \sigma \wedge \sigma = \rho) \rightarrow \tau = \rho$, $\tau = \sigma$ e $\sigma = \rho$ então segue do Teorema 3.12 que $\{(\tau = \sigma \wedge \sigma = \rho) \rightarrow \tau = \rho, \tau = \sigma, \sigma = \rho\} \vdash_{\mathcal{L}} \tau = \rho$. E como vale $\Sigma \vdash_{\mathcal{L}} (\tau = \sigma)$, $\Sigma \vdash_{\mathcal{L}} (\sigma = \rho)$ e $\Sigma \vdash_{\mathcal{L}} (\tau = \sigma \wedge \sigma = \rho \rightarrow \tau = \rho)$, segue do Teorema 3.13 que $\Sigma \vdash_{\mathcal{L}} (\tau = \rho)$.
□

Dessa forma, a relação $\sim$ definida acima é uma relação de equivalência em $CT_0(\mathcal{L})$ e, portanto, podemos considerar o conjunto $CT_0(\mathcal{L})/\sim$ de todas as classes de equivalência de $\sim$ em $CT_0(\mathcal{L})$. Dado $\tau \in CT_0(\mathcal{L})$, denotaremos sua classe de equivalência por $[\tau]$. O quociente $CT_0(\mathcal{L})/\sim$ será o universo da nova estrutura que iremos construir, cuja interpretação será definida a seguir.

Definição 4.10 *Sejam $\mathcal{L}$ uma linguagem de primeira ordem e Σ um conjunto de sentenças de $\mathcal{L}$. Suponha que $\mathcal{F}_0 \neq \emptyset$ e defina $CT(\mathcal{L},\Sigma) = CT_0(\mathcal{L})/\sim$ e a* ***estrutura de Herbrand*** *$\mathcal{M} = \mathcal{CT}(\mathcal{L},\Sigma)$ como a $\mathcal{L}$-estrutura cujo universo é $CT(\mathcal{L},\Sigma)$ e cuja interpretação se dá, recursivamente, da seguinte maneira:*

- *Se $c \in \mathcal{F}_0$, então $c^{\mathcal{M}} = [c]$.*
- *Se $p \in \mathcal{P}_0$, então $p^{\mathcal{M}} = 1$ se, e somente se, $\Sigma \vdash_{\mathcal{L}} p$.*
- *Se $f \in \mathcal{F}_n$ com $n > 0$ e $[\tau_1],...,[\tau_n] \in CT(\mathcal{L},\Sigma)$, então $f^{\mathcal{M}}([\tau_1],...,[\tau_n])$ é a classe de equivalência $[f(\tau_1,...,\tau_n)]$.*
- *Se $p \in \mathcal{P}_n$ com $n > 0$ e $[\tau_1],...,[\tau_n] \in CT(\mathcal{L},\Sigma)$, então $([\tau_1],...,[\tau_n]) \in p^{\mathcal{M}}$ se, e somente se, $\Sigma \vdash_{\mathcal{L}} p(\tau_1,...,\tau_n)$.*

Como estamos trabalhando com classes de equivalência, precisamos verificar que a Definição 4.10 está bem definida, isto é, que a interpretação independe do representante de uma classe.

Justificativa: Os únicos casos em que precisamos verificar que a interpretação está bem definida são quando $n > 0$, que é quando escolhemos representantes das classes de equivalência e definimos a interpretação usando tais representantes. Sejam $f \in \mathcal{F}_n$ com $n > 0$ e $\tau_1,...,\tau_n,\sigma_1,...,\sigma_n$ termos fechados de $\mathcal{L}$ tais que $\tau_i \sim \sigma_i$ para todo $i \in \{1,...,n\}$. Precisamos verificar que $f(\tau_1,...,\tau_n) \sim f(\sigma_1,...,\sigma_n)$. Do Teorema 3.12 segue que $\{(\tau_1 = \sigma_1 \wedge \ldots \wedge \tau_n = \sigma_n) \rightarrow f(\tau_1,\ldots,\tau_n) = f(\sigma_1,\ldots,\sigma_n), \tau_1 = \sigma_1, \ldots, \tau_n = \sigma_n\} \vdash_{\mathcal{L}} f(\tau_1,\ldots,\tau_n) = f(\sigma_1,\ldots,\sigma_n)$.Como $\Sigma \vdash_{\mathcal{L}} \tau_i = \sigma_i$ para todo $i \in \{1,\ldots,n\}$ e de uma aplicação de um axioma lógico do tipo 10 e a regra de quantificadores UI segue que

[1]Usaremos a notação $\forall x, y\varphi$ para expressar $\forall x \forall y \varphi$, para todas as variáveis x, y e fórmula φ.

$\emptyset \vdash_{\mathcal{L}} (\tau_1 = \sigma_1 \wedge \ldots \wedge \tau_n = \sigma_n) \rightarrow f(\tau_1, \ldots, \tau_n) = f(\sigma_1, \ldots, \sigma_n)$, do Teorema 3.13 obtemos $\Sigma \vdash_{\mathcal{L}} f(\tau_1, \ldots, \tau_n) = f(\sigma_1, \ldots, \sigma_n)$.

De forma análoga, dados $p \in \mathcal{P}_n$ com $n > 0$ e $\tau_1, \ldots, \tau_n, \sigma_1, \ldots, \sigma_n$ termos fechados de $\mathcal{L}$ tais que $\tau_i \sim \sigma_i$ para todo $i \in \{1, \ldots, n\}$ basta repetir o argumento anterior, notando agora que

$$\forall x_1, ..., x_n, y_1, ..., y_n ((x_1 = y_1 \wedge ... \wedge x_n = y_n) \rightarrow (p(x_1, ..., x_n) \leftrightarrow p(y_1, ..., y_n))$$

é um axioma lógico do tipo 11, para concluirmos que $\Sigma \vdash_{\mathcal{L}} p(\tau_1, ..., \tau_n)$ se, e somente se, $\Sigma \vdash_{\mathcal{L}} p(\sigma_1, ..., \sigma_n)$. □

No conjunto quociente, a relação $\sim$ colocou em uma mesma classe de equivalência elementos que, de fato, deveriam ser iguais. No exemplo que demos, onde $\mathcal{L} = \{0, +\}$ e Σ continha a sentença $\forall x(x + 0 = x)$, temos que $[0] = [0 + 0]$, pois vimos que $\Sigma \vdash_{\mathcal{L}} (0 + 0 = 0)$, e então segue que $\mathcal{CT}(\mathcal{L}, \Sigma) \models (0 + 0 = 0)$.

Vamos explorar quais outras propriedades são válidas para a $\mathcal{L}$-estrutura $\mathcal{CT}(\mathcal{L}, \Sigma)$ que ainda independem da consistência sintática de Σ.

Teorema 4.11 *Sejam $\mathcal{L}$ uma linguagem de primeira ordem tal que $\mathcal{F}_0 \neq \emptyset$, Σ um conjunto de sentenças de $\mathcal{L}$ e $\mathcal{M} = \mathcal{CT}(\mathcal{L}, \Sigma)$. Valem as seguintes afirmações:*

1. *Se τ é um termo fechado de $\mathcal{L}$, então $val^{\mathcal{M}}(\tau) = [\tau]$.*

2. *Se φ é uma sentença de $\mathcal{L}$ da forma $\forall x_1, ..., x_n \psi(x_1, ..., x_n)$, então $\mathcal{M} \models \varphi$ se, e somente se, $\mathcal{M} \models \psi(\tau_1, ..., \tau_n)$ quaisquer que sejam os termos fechados $\tau_1, ..., \tau_n$.*

3. *Se φ é uma sentença atômica (isto é, uma fórmula atômica que também é uma sentença), então $\Sigma \vdash_{\mathcal{L}} \varphi$ se, e somente se, $\mathcal{M} \models \varphi$.*

4. *Se $\Sigma \vdash_{\mathcal{L}} \varphi$, onde φ é um fecho universal de uma fórmula atômica, então $\mathcal{M} \models \varphi$.*

Demonstração:

1. Análoga ao Teorema 4.7.

2. Seja φ uma sentença da forma $\forall x_1 ... \forall x_n \psi(x_1, ..., x_n)$. Temos que $\mathcal{M} \models \varphi$ se, e somente se, $val^{\mathcal{M}}(\varphi) = 1$, e isso equivale a $val^{\mathcal{M}}(\forall x_2 ... \forall x_n \psi(x_1, x_2, .., x_n))[\emptyset + (x_1/[\tau_1])] = 1$ para todo termo fechado τ_1. Pelo item 1, dado um termo fechado τ_1, temos que $val^{\mathcal{M}}(\tau_1) = [\tau_1]$. Logo, pelo Teorema 2.22, temos que $val^{\mathcal{M}}(\forall x_2, \ldots, x_n \psi(x_1, x_2, \ldots, x_n))[\emptyset + (x_1/[\tau_1])] = 1$ se, e somente se, $val^{\mathcal{M}}(\forall x_2 ... \forall x_n \psi(\tau_1, x_2, .., x_n)) = 1$. Prosseguindo dessa maneira, concluímos que $val^{\mathcal{M}}(\varphi) = 1$

ocorre se e somente se $val^{\mathcal{M}}(\psi(\tau_1,...,\tau_n)) = 1$, isto é, $\mathcal{M} \vDash \psi(\tau_1,...,\tau_n)$, quaisquer que sejam os termos fechados $\tau_1,...,\tau_n$.

3. Sejam φ uma sentença atômica e σ uma valoração para φ. Há 3 casos possíveis a considerar. Se φ é a sentença formada por um único p, onde $p \in \mathcal{P}_0$, então $val^{\mathcal{M}}(p)[\sigma] = p^{\mathcal{M}}$. Pela Definição 4.10 temos que $p^{\mathcal{M}} = 1$ se, e somente se, $\Sigma \vdash_{\mathcal{L}} p$, e desta forma vale que $\Sigma \vdash_{\mathcal{L}} \varphi$ se, e somente se, $\mathcal{M} \vDash \varphi$.

   Se φ é a fórmula $p(\tau_1,...,\tau_n)$ para $p \in \mathcal{P}_n$ com $n > 0$ e $\tau_1,...,\tau_n$ termos fechados, temos que

$$\mathcal{M} \vDash \varphi \Leftrightarrow (val^{\mathcal{M}}(\tau_1),...,val^{\mathcal{M}}(\tau_n)) \in p^{\mathcal{M}} \Leftrightarrow ([\tau_1],...,[\tau_n]) \in p^{\mathcal{M}} \Leftrightarrow \Sigma \vdash_{\mathcal{L}} p(\tau_1,...,\tau_n),$$

   onde a segunda equivalência é dada pelo item 1 deste teorema, e as demais equivalências são dadas pelas respectivas definições.

   Por último, se φ for a fórmula $\tau_1 = \tau_2$ para τ_1 e τ_2 termos fechados, temos que

$$\mathcal{M} \vDash \varphi \Leftrightarrow val^{\mathcal{M}}(\tau_1) = val^{\mathcal{M}}(\tau_2) \Leftrightarrow [\tau_1] = [\tau_2] \Leftrightarrow \Sigma \vdash_{\mathcal{L}} (\tau_1 = \tau_2).$$

4. Suponha que φ seja uma sentença da forma $\forall x_1...\forall x_n \psi(x_1,...,x_n)$, com ψ uma fórmula atômica (ou seja, φ é um fecho universal de uma fórmula atômica). Se mostrarmos que $\mathcal{M} \vDash \psi(\tau_1,...,\tau_n)$ para todos os termos fechados $\tau_1,...,\tau_n$, então teremos, pelo item 2, que vale $\mathcal{M} \vDash \varphi$. Sejam então $\tau_1,...,\tau_n$ termos fechados. Aplicando a regra de quantificadores UI na fórmula $\forall x_1 \forall x_2...\forall x_n \psi(x_1,x_2...,x_n)$, obtemos $\forall x_1 \forall x_2...\forall x_n \psi(x_1,x_2...,x_n) \vdash_{\mathcal{L}} \forall x_2...\forall x_n \psi(\tau_1,x_2,...,x_n)$, e repetindo este argumento teremos que

$$\forall x_2 \forall x_3...\forall x_n \psi(\tau_1,x_2,...,x_n) \vdash_{\mathcal{L}} \forall x_3...\forall x_n \psi(\tau_1,\tau_2,x_3,...,x_n).$$

   Do Teorema 3.13 obtemos uma prova formal para $\forall x_3...\forall x_n \psi(\tau_1,\tau_2,x_3,...,x_n)$ partindo da sentença inicial. Repetindo tal processo n vezes, obtemos uma prova formal de $\psi(\tau_1,...,\tau_n)$ partindo da sentença inicial, isto é, obtemos a sentença $\forall x_1 \forall x_2...\forall x_n \psi(x_1,x_2...,x_n) \vdash_{\mathcal{L}} \psi(\tau_1,...,\tau_n)$. Como $\forall x_1 \forall x_2...\forall x_n \psi(x_1,x_2, ...,x_n)$ é a sentença φ, segue de $\Sigma \vdash_{\mathcal{L}} \varphi$ e do Teorema 3.13 que $\Sigma \vdash_{\mathcal{L}} \psi(\tau_1,...,\tau_n)$. Como $\psi(\tau_1,...,\tau_n)$ é uma sentença atômica, segue do item 3 que $\mathcal{M} \vDash \psi(\tau_1,...,\tau_n)$, como queríamos. $\square$

Do item 4 do Teorema 4.11 segue que se Σ for um conjunto composto apenas por sentenças que são fechos universais de fórmulas atômicas então $\mathcal{CT}(\mathcal{L},\Sigma)$ será um modelo para Σ, pois para toda sentença $\varphi \in \Sigma$ tem-se de imediato que $\Sigma \vdash_{\mathcal{L}} \varphi$ e do item 4 segue que $\mathcal{CT}(\mathcal{L}, \Sigma) \vDash \varphi$ e, portanto, que $\mathcal{CT}(\mathcal{L}, \Sigma) \vDash \Sigma$. Precisamos agora cuidar para que o mesmo ocorra para as demais sentenças.

Um exemplo em que $\mathcal{CT}(\mathcal{L}, \Sigma)$ não é modelo para um Σ é o caso em que Σ é sintaticamente inconsistente. Embora este seja um caso trivial, pois a hipótese do resultado que queremos demostrar é justamente a consistência sintática, há casos em que nem mesmo a consistência sintática de Σ é capaz de garantir que $\mathcal{CT}(\mathcal{L}, \Sigma)$ seja um modelo para Σ. Para exemplificar isto, considere $\mathcal{L} = \{a, b, <\}$ onde a e b são constantes distintas e um conjunto de sentenças Σ que diz que $<$ é uma ordem total estrita sem elemento máximo — isto é, Σ é o conjunto:

1. $\forall x \forall y \forall z((x < y \wedge y < z) \rightarrow x < z)$ (transitividade)
2. $\forall x \neg(x < x)$ (irreflexividade)
3. $\forall x \forall y(x < y \vee y < x \vee x = y)$ (tricotomia)
4. $\forall y \exists x(y < x)$ (sem elemento máximo)

Note que a e b são os únicos termos fechados de $\mathcal{L}$.

Afirmamos que não ocorre $\Sigma \vdash_{\mathcal{L}} a = b$. De fato, tome a $\mathcal{L}$-estrutura $\mathcal{N}$ dada pelo conjunto ω com a ordem usual e a interpretação que associa a e b aos números 0 e 1, respectivamente. Tal $\mathcal{L}$-estrutura é um modelo para Σ e, como $a^{\mathcal{N}} = 0$ e $b^{\mathcal{N}} = 1$, segue que $val^{\mathcal{N}}(a) \neq val^{\mathcal{N}}(b)$, logo $\mathcal{N} \nvDash a^{\mathcal{N}} = b^{\mathcal{N}}$ e consequentemente $\Sigma \nvDash a = b$. Do Teorema da Correção segue que não ocorre $\Sigma \vdash_{\mathcal{L}} a = b$.

Afirmamos ainda que não ocorre $\Sigma \vdash_{\mathcal{L}} \tau < \sigma$ para quaisquer $\tau, \sigma \in \{a, b\}$. De fato, tomando a estrutura $\mathcal{N}'$ que associa a e b ao 0, temos que $\mathcal{N}'$ é um modelo onde não é satisfeito $0 < 0$, logo, não é satisfeito $a^{\mathcal{N}'} <^{\mathcal{N}'} b^{\mathcal{N}'}$ e, por um argumento análogo ao feito no parágrafo anterior, obtemos que não ocorre $\Sigma \vdash_{\mathcal{L}} a < b$. De forma análoga mostramos que as demais desigualdades não podem ser provadas em Σ, justificando a afirmação em questão. Disto segue que $<^{\mathcal{M}}$ é a relação vazia, onde $\mathcal{CT}(\mathcal{L}, \Sigma)$.

E ainda, do que mostramos acima temos que Σ é semanticamente consistente, logo, pelo comentário feito na demonstração do Teorema 4.3, segue que Σ é sintaticamente consistente.

Temos aqui dois problemas. O primeiro é que da quarta sentença da lista acima e da aplicação da regra de quantificadores UI para o termo b segue que $\Sigma \vdash_{\mathcal{L}} \exists x(b < x)$. Contudo, temos que não ocorre $\mathcal{M} \vDash \exists x(b < x)$. De fato, se σ é uma atribuição para a fórmula $b < x$, então $val^{\mathcal{M}}(\exists x(b < x)) = 1$ se, e somente se, $val^{\mathcal{M}}(b < x)[\sigma +$

$(x/[a])] = 1$ ou $val^{\mathcal{M}}(b < x)[\sigma + (x/[b])] = 1$. No entanto, $val^{\mathcal{M}}(b < x)[\sigma + (x/[a])] = 0$ e $val^{\mathcal{M}}(b < x)[\sigma + (x/[b])] = 0$, já que $<^{\mathcal{M}}$ é a relação vazia. Logo, $val^{\mathcal{M}}(\exists x(b < x)) = 0$, ou seja, $\mathcal{M} \nvDash \exists x(b < x)$. Disto segue que $\mathcal{M}$ não é um modelo para Σ.

O segundo problema é o seguinte: a tricotomia (terceira sentença da lista acima) e a regra UI aplicada duas vezes para os termos a e b nos fornecem que $\Sigma \vdash_{\mathcal{L}} (a < b \vee b < a \vee a = b)$, mas $a < b \vee b < a \vee a = b$ é falsa em $\mathcal{M}$ porque $<^{\mathcal{M}}$ é a relação vazia e vimos que não ocorre $\Sigma \vdash_{\mathcal{L}} a = b$.

Os próximos passos para construir um modelo para Σ são inspirados em soluções para cada um desses problemas. Para o primeiro problema, podemos acrescentar a $\mathcal{L}$ uma "constante testemunha"c e adicionar a Σ a sentença $b < c$. Note que, agora, considerando a sentença $\exists x(c < x)$, o problema se repetiria — e isto ocorre, em suma, porque a ordem considerada não possui elemento máximo. Teríamos então que adicionar uma nova constante c' junto do axioma $c < c'$, e faríamos isso um número infinito de vezes.

Para o segundo problema, podemos acrescentar a Σ uma das seguintes sentenças: $a < b, a > b$ ou $a = b$. No fundo, o problema neste caso é que Σ "não tem sentenças suficientes".

Para resolver o segundo tipo de problema, vamos considerar um conjunto Σ' que contenha o conjunto Σ, que "tenha sentenças o suficiente", e que ainda mantenha a consistência sintática. Veremos isso na próxima definição.

Definição 4.12 *Um conjunto de sentenças Σ de uma linguagem de primeira ordem $\mathcal{L}$ é dito **maximalmente consistente em relação a** $(\vdash, \mathcal{L})$ se valem:*

1. $Con_{\vdash,\mathcal{L}}(\Sigma)$*;*

2. *para todo conjunto Π de sentenças de $\mathcal{L}$ tal que $Con_{\vdash,\mathcal{L}}(\Pi)$ e $\Sigma \subseteq \Pi$ tem-se $\Sigma = \Pi$.*

É como se o conjunto maximalmente consistente Σ' tomasse para si todas as pontas soltas de Σ de modo a ainda preservar a consistência sintática. Na solução para o Problema 2, adicionamos a Σ uma das sentenças $a < b$, $b < a$ ou $a = b$ e, ao fazer isso, ainda preservamos a consistência sintática. Note que precisamos fazer isso de forma controlada, pois se adicionarmos dois desses axiomas perderíamos a consistência sintática.

Vejamos agora algumas propriedades que os conjuntos maximalmente consistentes possuem.

Teorema 4.13 *Seja Σ um conjunto de sentenças de uma linguagem de primeira ordem $\mathcal{L}$. Se Σ é maximalmente consistente em relação a $(\vdash, \mathcal{L})$, então para quaisquer sentenças φ e ψ de $\mathcal{L}$ tem-se que:*

1. *$\Sigma \vdash \varphi$ se, e somente se, $\varphi \in \Sigma$.*

2. *$\neg\varphi \in \Sigma$ se, e somente se, $\varphi \notin \Sigma$.*

3. *$(\varphi \vee \psi) \in \Sigma$ se, e somente se, $\varphi \in \Sigma$ ou $\psi \in \Sigma$.*

Demonstração:

1. $(\Rightarrow)$ Por hipótese, temos que $Con_{\vdash,\mathcal{L}}(\Sigma)$, e junto com $\Sigma \vdash_{\mathcal{L}} \varphi$ obtemos $Con_{\vdash,\mathcal{L}}(\Sigma \cup \{\varphi\})$, pelo Teorema 3.10 (Prova por Contradição). Como Σ é maximalmente consistente em relação a $(\vdash, \mathcal{L})$, segue que $\Sigma \cup \{\varphi\} = \Sigma$, isto é, $\varphi \in \Sigma$.

   $(\Leftarrow)$ Basta tomar a prova formal dada pela sequência formada pela única sentença φ.

2. $(\Rightarrow)$ Se $\neg\varphi \in \Sigma$, então a sequência unitária $\neg\varphi$ é uma prova para $\neg\varphi$ partindo de Σ, ou seja, $\Sigma \vdash_{\mathcal{L}} \neg\varphi$. Assim, se por absurdo tivéssemos $\varphi \in \Sigma$, também teríamos que $\Sigma \vdash_{\mathcal{L}} \varphi$, o que contraria $Con_{\vdash,\mathcal{L}}(\Sigma)$. Logo, $\varphi \notin \Sigma$.

   $(\Leftarrow)$ Se $\varphi \notin \Sigma$, então Σ está contido propriamente no conjunto $\Sigma \cup \{\varphi\}$. Da maximalidade de Σ segue que $\neg Con_{\vdash,\mathcal{L}}(\Sigma \cup \{\varphi\})$. Mas então, do Teorema 3.10 (Prova por Contradição) segue que $\Sigma \vdash_{\mathcal{L}} \neg\varphi$, e do item 1 demonstrado acima, segue que $\neg\varphi \in \Sigma$, como queríamos.

3. $(\Rightarrow)$ Suponha, por absurdo, que $(\varphi \vee \psi) \in \Sigma$, $\varphi \notin \Sigma$ e $\psi \notin \Sigma$. Então do item 2 demonstrado acima segue que $\neg\varphi \in \Sigma$ e $\neg\psi \in \Sigma$. Note que $((\neg\varphi) \wedge (\neg\psi)) \rightarrow \neg(\varphi \vee \psi)$ é uma tautologia, logo pelo Teorema 3.12 segue que $\{\neg\varphi, \neg\psi\} \vdash_{\mathcal{L}} \neg(\varphi \vee \psi)$. Disso e de $\neg\varphi \in \Sigma$ e $\neg\psi \in \Sigma$ segue que $\Sigma \vdash_{\mathcal{L}} \neg(\varphi \vee \psi)$, o que contradiz $Con_{\vdash,\mathcal{L}}(\Sigma)$, já que $\varphi \vee \psi \in \Sigma$.

   $(\Leftarrow)$ Se $\varphi \in \Sigma$, como $\varphi \rightarrow (\varphi \vee \psi)$ é uma tautologia, segue do Teorema 3.12 que $\{\varphi\} \vdash_{\mathcal{L}} \varphi \vee \psi$, e como $\varphi \in \Sigma$ temos que $\Sigma \vdash_{\mathcal{L}} \varphi \vee \psi$. Assim, pelo item 1 provado acima, segue que $(\varphi \vee \psi) \in \Sigma$. O caso em que $\psi \in \Sigma$ é análogo. $\square$

E veremos agora que tomar um conjunto maximalmente consistente já resolve nosso problema caso Σ seja formado por um tipo particular de sentenças.

Teorema 4.14 *Seja Σ um conjunto de sentenças de uma linguagem de primeira ordem $\mathcal{L}$. Suponha que $\mathcal{F}_0 \neq \emptyset$ e que Σ é maximalmente consistente em relação a $(\vdash, \mathcal{L})$, e considere*

$\mathcal{M} = \mathcal{CT}(\mathcal{L}, \Sigma)$. Se φ é uma sentença de $\mathcal{L}$ na qual não ocorre nenhum quantificador, então $\varphi \in \Sigma$ se, e somente se, $\mathcal{M} \vDash \varphi$.

Demonstração: Mostraremos o resultado por indução no comprimento da sentença φ. O caso base da indução é quando $|\varphi| = 1$, e portanto φ deve ser uma fórmula atômica. Mas tal caso pode ser tratado da mesma forma para uma fórmula atômica φ de qualquer comprimento — assim, no passo indutivo, não precisaremos mais tratar este caso. Para tal, note que o item 1 do Teorema 4.13 nos dá que $\varphi \in \Sigma$ se, e somente se, $\Sigma \vdash_{\mathcal{L}} \varphi$, e o item 3 do Teorema 4.11 nos dá que $\Sigma \vdash_{\mathcal{L}} \varphi$ se, e somente se, $\mathcal{M} \vDash \varphi$. Logo $\varphi \in \Sigma$ se, e somente se, $\mathcal{M} \vDash \varphi$, como queríamos.

Suponha agora que o enunciado seja válido para toda sentença de comprimento estritamente menor que $|\varphi|$. Como já tratamos o caso em que a sentença φ é atômica e em nossa sentença não ocorre nenhum quantificador, então pela regra de formação de fórmulas temos que φ pode ser da forma $\neg\psi$, $\psi \wedge \phi$, $\psi \vee \phi$, $\psi \to \phi$ ou $\psi \leftrightarrow \phi$.

Se φ é da forma $\neg\psi$, então a sentença ψ possui comprimento estritamente menor que a sentença φ, logo pela hipótese de indução vale $\psi \notin \Sigma$ se, e somente se, $\mathcal{M} \nvDash \psi$. E por sua vez, temos que $\mathcal{M} \nvDash \psi$ se, e somente se, $\mathcal{M} \vDash \neg\psi$. E pelo item 2 do Teorema 4.13 temos que $\neg\psi \in \Sigma$ se, e somente se, $\psi \notin \Sigma$. Assim, juntando essas três equivalências, obtemos $\varphi \in \Sigma$ se, e somente se, $\mathcal{M} \vDash \varphi$.

Os casos em que φ é da forma $\psi \wedge \phi$, $\psi \vee \phi$, $\psi \to \phi$ ou $\psi \leftrightarrow \phi$ são semelhantes. Faremos somente o caso em que φ é da forma $\psi \leftrightarrow \phi$.

Suponha que $\psi \in \Sigma$ e $\phi \in \Sigma$. Então $\{\psi, \phi\} \subseteq \Sigma$, e notando que $(\psi \wedge \phi) \to (\psi \leftrightarrow \phi)$ é uma tautologia, segue do Teorema 3.12 que $\Sigma \vdash_{\mathcal{L}} \varphi$. Assim, do item 1 do Teorema 4.13 segue que $\varphi \in \Sigma$. De forma análoga, assumindo que $\psi \notin \Sigma$ e $\phi \notin \Sigma$, do item 2 do Teorema 4.13 segue que $\{\neg\psi, \neg\phi\} \subseteq \Sigma$, e como $(\neg\psi \wedge \neg\phi) \to \varphi$ é uma tautologia, temos que $\Sigma \vdash_{\mathcal{L}} \varphi$ e, portanto, $\varphi \in \Sigma$.

Agora, se $\psi \in \Sigma$ e $\phi \notin \Sigma$ (e de forma inteiramente análoga, $\psi \notin \Sigma$ e $\phi \in \Sigma$), então pelo item 2 do Teorema 4.13 segue que $\{\psi, \neg\phi\} \subseteq \Sigma$. E sendo $(\psi \wedge (\neg\phi)) \to \neg(\psi \leftrightarrow \phi)$ uma tautologia, segue do Teorema 3.12 que $\Sigma \vdash_{\mathcal{L}} \neg\varphi$. Logo, do item 1 do Teorema 4.14, $\neg\varphi \in \Sigma$.

Concluímos que $\varphi \in \Sigma$ se, e somente se, $\psi \in \Sigma$ e $\phi \in \Sigma$, ou $\neg\psi \in \Sigma$ e $\neg\phi \in \Sigma$. Pela hipótese de indução aplicada nas sentenças ψ e ϕ, temos que $\psi \in \Sigma$ e $\phi \in \Sigma$ se, e somente se, $\mathcal{M} \vDash \psi$ e $\mathcal{M} \vDash \phi$, bem como $\neg\psi \in \Sigma$ e $\neg\phi \in \Sigma$ se, e somente se, $\mathcal{M} \nvDash \psi$ e $\mathcal{M} \nvDash \phi$. Logo, $\varphi \in \Sigma$ se, e somente se, $val^{\mathcal{M}}(\psi) = val^{\mathcal{M}}(\phi)$, ou seja, se, e somente se, $val^{\mathcal{M}}(\varphi) = 1$, o que significa que $\mathcal{M} \vDash \varphi$. □

Estando já convencidos de que o conceito de consistência maximal resolve parte dos nossos problemas, precisamos garantir que o conjunto Σ do Lema 4.4 admite uma extensão maximalmente consistente. Veremos no Teorema 4.17 que, de fato, a consistência sintática de Σ é suficiente para garantir a existência de uma extensão maximalmente consistente em relação a $(\vdash, \mathcal{L})$. Para mostrar tal resultado, usaremos uma ferramenta equivalente ao Lema de Kuratowski-Zorn — o que é, de certa forma, esperado quando tentamos mostrar resultados acerca da existência de um conjunto maximal em relação a alguma ordem parcial, como a inclusão. Para tal, veremos uma definição antes de introduzir o referido resultado.

Definição 4.15 *Sejam A um conjunto e $\mathcal{F} \subseteq \wp(A)$. Dizemos que $\mathcal{F}$ é de **caráter finito** quando para todo $X \subseteq A$ tem-se que $X \in \mathcal{F}$ se, e somente se, todo subconjunto finito de X pertence a $\mathcal{F}$.*

Definição 4.16 (Lema de Tukey) *Se $\mathcal{F} \subseteq \wp(A)$ é de caráter finito e $X \in \mathcal{F}$, então existe um conjunto maximal $Y \in \mathcal{F}$ que contém X.*

Como dito antes, o Lema de Tukey é uma afirmação equivalente ao Lema de Zorn —e portanto, equivalente a todas as demais afirmações que são equivalentes ao Lema de Zorn, como por exemplo o Axioma da Escolha. Esta equivalência está demonstrada em [5]. Com tal resultado conseguimos demonstrar o seguinte teorema:

Teorema 4.17 *Se Δ é um conjunto de sentenças de uma linguagem de primeira ordem $\mathcal{L}$ tal que $Con_{\vdash,\mathcal{L}}(\Delta)$, então existe um conjunto de sentenças Σ tal que $\Delta \subseteq \Sigma$ e Σ é maximalmente consistente em relação a $(\vdash, \mathcal{L})$.*

Demonstração: Defina S como o conjunto de todas as sentenças de $\mathcal{L}$ e note que $\Delta \in \wp(S)$. Tome $\mathcal{F} = \{\Pi \in \wp(S) : Con_{\vdash,\mathcal{L}}(\Pi)\}$ e vejamos que $\mathcal{F}$ é de caráter finito. Seja $\Pi \subseteq S$. Suponha que $\Pi \in \mathcal{F}$ e seja $\Gamma \subseteq \Pi$. Então vale $Con_{\vdash,\mathcal{L}}(\Gamma)$, pois se Γ levasse a contradições, então Π também levaria, o que contradiz $Con_{\vdash,\mathcal{L}}(\Pi)$, uma vez que $\Pi \in \mathcal{F}$. Portanto, pela definição de $\mathcal{F}$, temos que $\Gamma \in \mathcal{F}$ — e em particular, isto vale para todo subconjunto finito de Π. Reciprocamente, suponha que todo subconjunto finito de Π é um elemento de $\mathcal{F}$ e vejamos que $\Pi \in \mathcal{F}$. Se, por absurdo, $\Pi \notin \mathcal{F}$, existiriam entenças $\psi_1, ..., \psi_n$, $\phi_1, ..., \phi_m \in \Pi$ s que atestam, respectivamente, que $\Pi \vdash_{\mathcal{L}} \varphi$ e $\Pi \vdash_{\mathcal{L}} \neg\varphi$ para alguma fórmula φ de $\mathcal{L}$, pois toda prova formal é finita. Dessa forma $\{\psi_1, ..., \psi_n, \phi_1, ..., \phi_n\}$ é um subconjunto finito de Π sintaticamente inconsistente, o que contraria nossa hipótese. Então $\Pi \in \mathcal{F}$, o que conclui que $\mathcal{F}$ é de caráter finito. Portanto, pelo Lema de Tukey, $\mathcal{F}$ possui um elemento maximal Σ (e, portanto, Σ é maximalmente consistente em relação a $(\vdash, \mathcal{L})$) que contém o conjunto Δ, como queríamos. $\square$

Vamos agora tratar do primeiro problema apontado pelo exemplo algumas páginas atrás. Ele surgiu porque algumas sentenças existenciais apontavam para objetos que deveriam existir, mas cujas existências não eram testemunhadas. Nossa solução para o exemplo foi adicionar constantes na linguagem e novas sentenças em Σ que atestavam que a sentença existencial seria verdadeira na estrutura. Vamos destacar estas ideias na definição a seguir.

Definição 4.18 *Chamamos de* ***sentença existencial*** *uma sentença da forma* $\exists x\varphi(x)$*. Se* Σ *é um conjunto de sentenças de uma linguagem de primeira ordem* $\mathcal{L}$ *e* $\exists x\varphi(x)$ *é uma sentença existencial, dizemos que o termo* τ *é uma* ***testemunha para*** $\exists x\varphi(x)$ ***com respeito a*** Σ ***e*** $\mathcal{L}$ *se* $\tau \in CT_0(\mathcal{L})$ *e* $\Sigma \vdash_{\mathcal{L}} (\exists x\varphi(x) \to \varphi(\tau))$*. Por fim, dizemos que* Σ ***possui testemunhas em*** $\mathcal{L}$ *se toda sentença existencial de* $\mathcal{L}$ *possui testemunha.*

Vamos agora mostrar que a solução que arranjamos para os dois problemas garante, de fato, que a estrutura de Herbrand é um modelo para Σ, caso Σ satisfaça as duas condições estudadas para a resolução dos problemas: a consistência maximal e a existência de testemunhas na linguagem.

Teorema 4.19 *Seja* Σ *um conjunto de sentenças de uma linguagem de primeira ordem* $\mathcal{L}$*. Tomando* $\mathcal{M} = \mathcal{CT}(\mathcal{L}, \Sigma)$*, se* Σ *for maximalmente consistente em relação a* $(\vdash, \mathcal{L})$ *e* Σ *possuir testemunhas em* $\mathcal{L}$*, então* $\mathcal{M} \vDash \Sigma$*.*

Demonstração: Fixada uma sentença φ de $\mathcal{L}$, mostraremos que $\varphi \in \Sigma$ se, e somente se, $\mathcal{M} \vDash \varphi$. Seja $S(\varphi)$ o número de ocorrências de algum dos símbolos $\wedge$, $\vee$, $\neg$, $\to$, $\leftrightarrow$, $\forall$, $\exists$ em φ. Mostraremos o resultado por indução em $S(\varphi)$. Se $S(\varphi) = 0$, então em particular φ não contém nenhuma ocorrência de quantificadores e, portanto, segue do Teorema 4.14 a equivalência desejada.

Suponha agora $S(\varphi) > 0$ e que o resultado seja válido para toda sentença ψ tal que $S(\psi) < S(\varphi)$. Para o caso em que φ é da forma $\neg\psi$, $\psi \wedge \phi$, $\psi \vee \phi$, $\psi \to \phi$ ou $\psi \leftrightarrow \phi$, de forma análoga ao que foi feito na demonstração do Teorema 4.14 conseguimos concluir o resultado.

Vamos tratar então o caso dos quantificadores. Suponha primeiro que φ é do tipo $\exists x\psi(x)$ e seja τ uma testemunha para tal sentença existencial, isto é, τ é um termo fechado de $\mathcal{L}$ tal que $\Sigma \vdash_{\mathcal{L}} (\exists x\psi(x) \to \psi(\tau))$. Note que a sentença $\psi(\tau)$ tem um quantificador a menos que a sentença φ, logo $S(\psi(\tau)) < S(\varphi)$, e assim pela hipótese de indução segue que $\psi(\tau) \in \Sigma$ se, e somente se, $\mathcal{M} \vDash \psi(\tau)$.

Agora, supondo que $\varphi \in \Sigma$, então a partir de $\Sigma \vdash_{\mathcal{L}} \varphi$ e $\Sigma \vdash_{\mathcal{L}} (\exists x \psi(x) \to \psi(\tau))$ inferimos por Modus Ponens que vale $\Sigma \vdash_{\mathcal{L}} \psi(\tau)$. Assim, pelo item 1 do Teorema 4.13, segue que $\psi(\tau) \in \Sigma$, e então segue da hipótese de indução que $\mathcal{M} \vDash \psi(\tau)$. Logo, da Definição 2.7 e do Teorema 2.22 segue que $\mathcal{M} \vDash \varphi$.

Reciprocamente, suponha que $\mathcal{M} \vDash \varphi$. Novamente pela Definição 2.7, existe algum termo fechado a tal que $\mathcal{M} \vDash \psi(x)[\emptyset + (x/[a])]$. Como vimos que $val^{\mathcal{M}}(a) = [a]$, segue do Teorema 2.22 que $\mathcal{M} \vDash [\psi(x)]^a_x$, ou seja $\mathcal{M} \vDash \psi(a)$. Novamente, note que $\psi(a)$ possui um quantificador a menos que φ, logo podemos usar a hipótese de indução em $\psi(a)$ e teremos $\psi(a) \in \Sigma$. Pela regra de quantificadores EG, temos que $\{\psi(a)\} \vdash_{\mathcal{L}} \exists x \psi(x)$, logo de $\psi(a) \in \Sigma$ concluímos que $\Sigma \vdash_{\mathcal{L}} \varphi$, e então pelo item 1 do Teorema 4.13 segue que $\varphi \in \Sigma$, como queríamos.

Vamos tratar agora o caso em que φ é da forma $\forall x \psi(x)$. Se $\varphi \in \Sigma$, então pelo item 1 do Teorema 4.13 segue que $\Sigma \vdash_{\mathcal{L}} \varphi$, e pela regra de quantificadores UI segue que $\{\varphi\} \vdash_{\mathcal{L}} \psi(\tau)$ para todo termo fechado τ. Sendo $\varphi \in \Sigma$, obtemos $\Sigma \vdash_{\mathcal{L}} \psi(\tau)$ e, usando novamente o item 1 do Teorema 4.13, concluímos que $\psi(\tau) \in \Sigma$. Assim, por hipótese de indução, temos que $\mathcal{M} \vDash \psi(\tau)$ para todo termo fechado τ e, portanto, $\mathcal{M} \vDash \varphi$.

Reciprocamente, suponha que $\varphi \notin \Sigma$. Então pela maximalidade de Σ e do item 2 do Teorema 4.13 segue que $\neg\varphi \in \Sigma$. Tome uma testemunha τ para a sentença existencial $\exists x \neg\psi(x)$. Assim $\Sigma \vdash_{\mathcal{L}} (\exists x \neg\psi(x) \to \neg\psi(\tau))$. Vimos no exemplo 3.15 que $\emptyset \vdash_{\mathcal{L}} \neg\forall x \psi(x) \to \exists x \neg\psi(x)$, o que implica $\Sigma \vdash_{\mathcal{L}} \neg\psi(\tau)$ e, como Σ é consistente, $\psi(\tau) \notin \Sigma$. Então aplicando a hipótese de indução para $\psi(\tau)$ segue que $\mathcal{M} \nvDash \psi(\tau)$, e portanto, $\mathcal{M} \nvDash \varphi$, como queríamos. □

Note que uma indução no comprimento da fórmula φ poderia não funcionar na demonstração do Teorema 4.19 pois, ao substituir um termo τ em ψ, poderia ocorrer de $\psi(\tau)$ ter um comprimento maior que φ, e então não poderíamos usar a hipótese de indução para $\psi(\tau)$.

Mostraremos a seguir que, ao adicionarmos a $\mathcal{L}$ uma constante que faça o papel de testemunha para uma sentença existencial $\exists x \varphi(x)$, a adição da sentença $\exists x \varphi(x) \to \varphi(c)$ a Σ preserva consistência sintática. Este será o primeiro passo do nosso processo de adicionar constantes à linguagem que sejam testemunhas para as sentenças existenciais, a fim de obter um conjunto que possua testemunha na linguagem dada pela união da linguagem inicial com as constantes adicionadas.

E ainda, já havíamos garantido que todo conjunto Σ sintaticamente consistente admite extensão maximalmente consistente em relação a uma linguagem e o Teorema 4.19 diz que, se garantimos que Σ possui testemunhas em $\mathcal{L}$, então a consistência maximal garante a consistência semântica. Sendo assim, alcançaremos nosso objetivo seguindo os seguintes passos: a partir de $\mathcal{L}$ e Σ obtemos $\mathcal{L}'$ (contendo $\mathcal{L}$) e Σ' (contendo Σ) que possui testemunhas em $\mathcal{L}'$; aumentamos Σ' para Σ^* de forma a obter consistência maximal sem perder as testemunhas e aplicamos o Teorema 4.19 para garantir que o modelo de Herbrand $\mathcal{M}$ é um modelo para Σ^* e $\mathcal{L}'$; por fim mostraremos que tal modelo, quando restrito a Σ e $\mathcal{L}$, é um modelo para Σ e $\mathcal{L}$.

Teorema 4.20 *Sejam Σ um conjunto de sentenças de uma linguagem de primeira ordem $\mathcal{L}$, $\exists x\varphi(x)$ uma sentença existencial de $\mathcal{L}$, $\mathcal{L}' = \mathcal{L} \cup \{c\}$ onde c é um símbolo de constante tal que $c \notin \mathcal{L}$ e $\Sigma' = \Sigma \cup \{\exists x\varphi(x) \to \varphi(c)\}$. Se $Con_{\vdash,\mathcal{L}}(\Sigma)$, então $Con_{\vdash,\mathcal{L}'}(\Sigma')$.*

Demonstração: Mostraremos a contrapositiva dessa afirmação, isto é, $\neg Con_{\vdash,\mathcal{L}'}(\Sigma')$ implica $\neg Con_{\vdash,\mathcal{L}}(\Sigma)$. De fato, se $\neg Con_{\vdash,\mathcal{L}'}(\Sigma')$, então, pela definição de Σ', segue do Teorema 3.10 que $\Sigma \vdash_{\mathcal{L}'} \neg(\exists x\varphi(x) \to \varphi(c))$. Note agora que $\neg(\exists x\varphi(x) \to \varphi(c)) \to \exists x\varphi(x)$ é uma tautologia, logo inferimos que $\Sigma \vdash_{\mathcal{L}'} \exists x\varphi(x)$. De forma análoga, note que $\neg(\exists x\varphi(x) \to \varphi(c)) \to \neg\varphi(c)$ também é uma tautologia, logo segue que $\Sigma \vdash_{\mathcal{L}'} \neg\varphi(c)$. Assim, como a constante c não está em $\mathcal{L}$, segue pela regra de quantificadores UG que $\Sigma \vdash_{\mathcal{L}} \forall x\neg\varphi(x)$. Note agora que a sentença $\forall x\neg\varphi(x) \leftrightarrow \neg\exists x\varphi(x)$ é um axioma lógico do tipo 6, assim, deste axioma e de $\Sigma \vdash_{\mathcal{L}} \forall x\neg\varphi(x)$ inferimos que $\Sigma \vdash_{\mathcal{L}} \neg\exists x\varphi(x)$.

Por fim, usando a regra de quantificadores UG em $\Sigma \vdash_{\mathcal{L}'} \exists x\varphi(x)$ (que havíamos inferido inicialmente), obtemos que $\Sigma \vdash_{\mathcal{L}} \forall y(\exists x\varphi(x))$. Mas como $\forall y(\exists x\varphi(x)) \to (\exists x\varphi(x))$ é um axioma lógico do tipo 4, já que $\exists x\varphi(x)$ é uma sentença de $\mathcal{L}$, segue que $\Sigma \vdash_{\mathcal{L}} \exists x\varphi(x)$ (e, mais geralmente, mostramos aqui que se ϕ é uma sentença de $\mathcal{L}$ e vale $\Sigma \vdash_{\mathcal{L}'} \phi$, então vale $\Sigma \vdash_{\mathcal{L}} \phi$).

Dessa forma, obtemos $\Sigma \vdash_{\mathcal{L}} \neg\exists x\varphi(x)$ e $\Sigma \vdash_{\mathcal{L}} \exists x\varphi(x)$, logo $\neg Con_{\vdash,\mathcal{L}}(\Sigma)$, como queríamos. □

Usaremos o resultado anterior para provar uma generalização do mesmo. Iremos, indutivamente, adicionar à linguagem tantas constantes quanto forem necessárias, e mostrar que o conjunto de sentenças final é sintaticamente consistente em relação à linguagem final.

Teorema 4.21 *Sejam Σ um conjunto de sentenças de uma linguagem de primeira ordem $\mathcal{L}$ e δ um ordinal qualquer. Para cada $\alpha < \delta$ considere c_α um novo símbolo de constante que não está em $\mathcal{L}$ e é distinto de c_β para todo $\beta < \alpha$. Considere ainda, para $\alpha \leq \delta$, o conjunto $\mathcal{L}_\alpha = \mathcal{L} \cup \{c_\xi : \xi < \alpha\}$, e para cada $\alpha < \delta$ seja $\exists x\varphi_\alpha(x)$ uma sentença existencial de $\mathcal{L}_\alpha$. Por fim, seja $\Sigma_\delta = \Sigma \cup \{\exists x\varphi_\alpha(x) \to \varphi(c_\alpha) : \alpha < \delta\}$. Se $Con_{\vdash,\mathcal{L}}(\Sigma)$, então $Con_{\vdash,\mathcal{L}_\delta}(\Sigma_\delta)$.*

Demonstração: Mostraremos o resultado por indução transfinita em δ. Para $\delta = 0$, ele é imediato, já que temos $\mathcal{L}_0 = \mathcal{L}$ e $\Sigma_0 = \Sigma$.

Suponha agora que $\delta > 0$ e que o resultado seja válido para todo ordinal $\alpha < \delta$. Se δ é um ordinal sucessor, então existe um ordinal β tal que $\delta = \beta + 1$. Por hipótese de indução, temos $Con_{\vdash,\mathcal{L}_\beta}(\Sigma_\beta)$. E sendo $\delta = \beta + 1$, segue que

$$\begin{aligned}\Sigma_\delta &= \Sigma \cup \{\exists x \varphi_\alpha(x) \to \varphi(c_\alpha) : \alpha < \delta\}\\ &= \Sigma \cup \{\exists x \varphi_\alpha(x) \to \varphi(c_\alpha) : \alpha < \beta\} \cup \{\exists x \varphi_\beta(x) \to \varphi(c_\beta)\}\\ &= \Sigma_\beta \cup \{\exists x \varphi_\beta(x) \to \varphi(c_\beta)\}.\end{aligned}$$

E ainda, $\mathcal{L}_\delta = \mathcal{L} \cup \{c_\xi : \xi < \delta\} = \mathcal{L} \cup \{c_\xi : \xi < \beta\} \cup \{c_\beta\} = \mathcal{L}_\beta \cup \{c_\beta\}$. Então como $Con_{\vdash,\mathcal{L}_\beta}(\Sigma_\beta)$, segue do Teorema 4.20 que $Con_{\vdash,\mathcal{L}_\delta}(\Sigma_\delta)$.

Agora, suponha que δ seja um ordinal limite. Suponha, por absurdo, que ocorre $\neg Con_{\vdash,\mathcal{L}_\delta}(\Sigma_\delta)$, e seja φ uma sentença que ateste isto. Então existem sentenças $\psi_1, ..., \psi_n$ e $\phi_1, ..., \phi_m$ de $\mathcal{L}_\delta$ que atestam, respectivamente, que $\Sigma_\delta \vdash_{\mathcal{L}_\delta} \varphi$ e $\Sigma_\delta \vdash_{\mathcal{L}_\delta} \neg\varphi$ pois cada sentença possui apenas uma quantidade finita de símbolos. Como δ é um ordinal limite, existe um ordinal $\alpha < \delta$ tal que $\psi_1, \ldots, \psi_n, \phi_1, \ldots, \phi_m$ são sentenças de $\mathcal{L}_\alpha$. Temos então que $\Sigma_\alpha \vdash_{\mathcal{L}_\alpha} \varphi$ e $\Sigma_\alpha \vdash_{\mathcal{L}_\alpha} \neg\varphi$, o que é um absurdo, pois, por hipótese, $Con_{\vdash,\mathcal{L}_\alpha}(\Sigma_\alpha)$. □

Lema 4.22 *Seja Σ um conjunto de sentenças de uma linguagem de primeira ordem $\mathcal{L}$ tal que $Con_{\vdash,\mathcal{L}}(\Sigma)$. Se $\kappa = \max\{|\mathcal{L}|, \aleph_0\}$, então existem uma linguagem de primeira ordem $\mathcal{L}'$ e um conjunto Σ' de sentenças de $\mathcal{L}'$ tais que:*

1. *$\mathcal{L}' = \mathcal{L} \cup \mathcal{C}$, onde $\mathcal{C}$ é um conjunto de símbolos de constantes;*
2. *$|\mathcal{L}'| = |\mathcal{C}| = \kappa$*
3. *$\Sigma \subseteq \Sigma'$;*
4. *$Con_{\vdash,\mathcal{L}'}(\Sigma')$;*
5. *Σ' possui testemunhas em $\mathcal{L}'$.*

Demonstração: Tome $\mathcal{L}' = \mathcal{L}_{\kappa\cdot\omega} = \mathcal{L} \cup \mathcal{C}$, com $\mathcal{C} = \{c_\alpha : \alpha < \kappa \cdot \omega\}$ um conjunto constituído de símbolos de constantes dois a dois distintos que não estão em $\mathcal{L}$ dado pelo Teorema 4.21. Temos que o item 1 segue imediatamente. Para o item 2 basta notar que $|\mathcal{C}| = |\kappa \cdot \omega| = \kappa$, já que κ é maior ou igual a ω, e sendo κ maior ou igual a $|\mathcal{L}|$, então $\mathcal{L}' = |\mathcal{L}| + |\mathcal{C}| = |\mathcal{L}| + \kappa = \kappa$. Usando o Teorema 4.21 para o ordinal $\delta = \kappa \cdot \omega$ obtemos os itens 3 e 4, considerando $\Sigma' = \Sigma_{\kappa\cdot\omega}$.

Para o item 5, note que, como o alfabeto de $\mathcal{L}_{\kappa\cdot n}$ tem cardinalidade κ e cada sequência existencial de $\mathcal{L}_{\kappa\cdot n}$ é uma sequência finita de símbolos desse alfabeto, o número de sequências existenciais de $\mathcal{L}_{\kappa\cdot n}$ é menor ou igual a $\sum_{n\in\omega}\kappa^n = \sum_{n\in\omega}\kappa = \max\{\aleph_0, \kappa\} = \kappa$.

Assim, há no máximo κ sentenças existenciais de $\mathcal{L}_{\kappa\cdot n}$. E ainda, para cada $\alpha < \kappa$ podemos considerar a sentença existencial $\exists x(x = c_\alpha)$, o que mostra que existem pelo menos $|\kappa \cdot n| = \kappa$ sentenças existenciais distintas de $\mathcal{L}_{\kappa\cdot n}$. Logo, há exatamente κ sentenças existenciais de $\mathcal{L}_{\kappa\cdot n}$. Portanto, podemos indexar o conjunto das sentenças existenciais de $\mathcal{L}_{\kappa\cdot n}$ como $\{\exists x\varphi_\alpha(x) : \kappa \cdot n \leq \alpha < \kappa \cdot (n+1)\}$.

Vejamos agora que o conjunto $\{\exists x\varphi_\alpha(x) : \alpha < \kappa \cdot \omega\}$ lista todas as sentenças existenciais de $\mathcal{L}'$. De fato, seja φ uma sentença existencial de $\mathcal{L}'$. Como φ é finita e como a sequência $\{\kappa \cdot n : n \in \omega\}$ é ilimitada em $\kappa \cdot \omega$, existe $n \in \omega$ tal que φ é uma sentença existencial da linguagem $\mathcal{L}_{\kappa\cdot n}$ e, portanto, é da forma $\exists x\varphi_\alpha(x)$ para algum $\alpha \in [\kappa \cdot n, \kappa \cdot (n+1)[$. Assim o conjunto $\{\exists x\varphi_\alpha(x) : \alpha < \kappa \cdot \omega\}$ de fato lista todas as sentenças existenciais de $\mathcal{L}'$.

Dessa forma, dada uma sentença existencial φ de $\mathcal{L}'$, temos que φ é a sentença $\exists x\varphi_\alpha(x)$ para algum $\alpha < \kappa \cdot \omega$ e, portanto, c_α é uma testemunha para φ com respeito a Σ' e $\mathcal{L}'$. Logo Σ' possui testemunhas em $\mathcal{L}'$. $\square$

Já temos todos os elementos de que precisamos para demonstrar o Lema 4.4.

Demonstração do Lema 4.4: Seja Σ um conjunto de sentenças de uma linguagem de primeira ordem $\mathcal{L}$ tal que $Con_{\vdash,\mathcal{L}}(\Sigma)$. Vamos mostrar que $Con_{\models}(\Sigma)$, isto é, vamos construir uma $\mathcal{L}$-estrutura que modela Σ.

Pelo Lema 4.22 existem uma linguagem de primeira ordem $\mathcal{L}'$ e um conjunto Σ' de sentenças de $\mathcal{L}'$ tais que $\Sigma \subseteq \Sigma'$, $Con_{\vdash,\mathcal{L}'}(\Sigma')$ e Σ' possui testemunhas em $\mathcal{L}'$.

Pelo Teorema 4.17 existe um conjunto Σ^* de sentenças de $\mathcal{L}'$ tal que $\Sigma' \subseteq \Sigma^*$ e Σ^* é maximalmente consistente em relação a $(\vdash, \mathcal{L}')$. E como Σ' possui testemunha em $\mathcal{L}'$, então toda sentença existencial de $\mathcal{L}'$ possui testemunha com respeito a Σ' e $\mathcal{L}'$ e, portanto, possui testemunha com respeito a Σ^* e $\mathcal{L}'$. Logo, Σ^* também possui testemunhas em $\mathcal{L}'$.

Estamos portanto nas condições do Teorema 4.19 (já que Σ^* é um conjunto maximalmente consistente em relação a $(\vdash, \mathcal{L}')$ e possui testemunhas em $\mathcal{L}'$), que garante que $\mathcal{M}' := \mathcal{CT}(\mathcal{L}', \Sigma^*)$ é um modelo para Σ^*, isto é, $\mathcal{M}' \models \Sigma^*$.

Considere agora a redução $\mathcal{M} = \mathcal{M}'\restriction_{\mathcal{L}}$. Dado $\varphi \in \Sigma$, como $\mathcal{M}' \models \Sigma^*$ e $\Sigma \subseteq \Sigma^*$, então $\mathcal{M}' \models \varphi$ e assim $\mathcal{M}' \models \Sigma$. Como $\mathcal{L} \subseteq \mathcal{L}'$, pelo Teorema 2.25 ($2 \to 1$), a redução $\mathcal{M}$ é um modelo para Σ, isto é $\mathcal{M} \models \Sigma$, como queríamos. $\square$

Com a demonstração deste lema, encerramos a prova do Teorema da Completude.

5 Os Teoremas da Incompletude

Nosso objetivo neste capítulo é construir os conceitos necessários para enunciar e demonstrar os Teoremas da Incompletude de Gödel. Na primeira seção apresentaremos uma teoria formal, baseada nos axiomas de Peano, que é capaz de provar os resultados elementares da aritmética de números naturais. Na segunda seção estudaremos os conceitos de relações exprimíveis e funções representáveis numa dada teoria. Na terceira seção estudaremos o conceito de funções recursivas numa dada teoria e sua relação com os conceitos de exprimibilidade e representabilidade. Na quarta seção estudaremos o conceito de número de Gödel. E finalmente, na quinta e sexta seção veremos, respectivamente, o primeiro e o segundo Teorema da Incompletude de Gödel. As principais referências bibliográficas para este capítulo são [5] e [6].

5.1 Aritmética de Peano

Uma das primeiras tentativas de axiomatização da teoria dos números naturais foi dada por Giuseppe Peano através dos seguintes postulados, que ficaram conhecidos como axiomas de Peano:

(P1) 0 é um número natural.

(P2) Se n é um número natural, então existe outro número natural, $s(n)$.

(P3) Para todo número natural n tem-se que $s(n) \neq 0$.

(P4) Se $s(n) = s(m)$, então $n = m$.

(P5) Se P é uma propriedade acerca de números naturais, e se valem:

   (i) 0 possui a propriedade P; e

   (ii) se um número natural n possui a propriedade P, então $s(n)$ também possui a propriedade P,

então todos os números naturais possuem a propriedade P.

Estes foram os axiomas considerados mais adequados à época para formalizar a teoria dos números naturais. Observe, contudo, que na lista acima, a noção de propriedade não é claramente definida, o que faz com que esse conjunto de axiomas não seja considerado uma formalização rigorosa da teoria em questão. No que segue, os utilizaremos como inspiração para construir uma teoria formal capaz de expressar a aritmética dos naturais.

Para isto, considere a linguagem de primeira ordem $\mathcal{L}_\mathcal{A} = \{0, s, +, \cdot\}$, onde $0 \in \mathcal{F}_0$, $s \in \mathcal{F}_1$ e $+, \cdot \in \mathcal{F}_2$. Chamaremos a função s de função sucessora. Os axiomas não lógicos da nossa teoria são fechos universais das fórmulas de um dos tipos listados abaixo.

(A1) $0 \neq s(x)$;

(A2) $s(x) = s(y) \to x = y$;

(A3) $x + 0 = x$;

(A4) $x + s(y) = s(x + y)$;

(A5) $x \cdot 0 = 0$;

(A6) $x \cdot s(y) = (x \cdot y) + x$;

E ainda, vale:

(A7) para cada fórmula $\varphi(x)$ de $\mathcal{L}_\mathcal{A}$ os fechos universais de $\varphi(0) \to (\forall x(\varphi(x) \to \varphi(s(x))) \to \forall x \varphi(x))$ são axiomas não lógicos.

Note que o axioma $(A7)$ é, na verdade, um esquema de axiomas, chamado de **Princípio da Indução Finita**.

Os postulados $(P1)$ e $(P2)$ correspondem à presença do símbolo constante 0 e do símbolo de função s em $\mathcal{L}_\mathcal{A}$. Já $(P3)$, $(P4)$ correspondem aos axiomas $(A1)$ e $(A2)$, respectivamente. Por fim, o esquema $(A9)$ é a versão rigorosa de $(P5)$. O símbolo de função + relaciona os termos desta linguagem de acordo com $(A3)$ e $(A4)$, e o símbolo de função $\cdot$ relaciona os termos de acordo com $(A5)$ e $(A6)$.

Vamos agora verificar que esta teoria, a qual denotaremos por $\mathcal{P}$ e chamaremos de **aritmética de Peano**, é, de fato, capaz de expressar e provar os resultados elementares da teoria dos números naturais.

Teorema 5.1 *Sejam t, r, v termos da linguagem $\mathcal{L}_\mathcal{A}$. Então as sentenças dadas pelos fechos universais das seguintes fórmulas podem ser provadas em $\mathcal{P}$:*

1. $0 \neq s(t)$
2. $s(t) = s(r) \rightarrow t = r$
3. $t + 0 = t$
4. $t + s(r) = s(t + r)$
5. $t \cdot 0 = 0$
6. $t \cdot s(r) = (t \cdot r) + t$
7. $t = r \rightarrow (r = v \rightarrow t = v)$
8. $t = r \rightarrow s(t) = s(r)$
9. $0 \cdot t = 0$
10. $0 + t = t$
11. $t + v = r + v \rightarrow t = r$
12. $s(t) + r = s(t + r)$

Demonstração: Nesta prova usaremos frequentemente o axioma lógico do tipo 4. Para garantir que possamos usá-lo livremente, mudaremos, em cada fórmula listada no enunciado, todas as variáveis limitadas por outras variáveis que não aparecem nos respectivos termos envolvidos. Desta forma garantimos que os termos envolvidos sejam livres para todas as variáveis nas respectivas fórmulas.

(1). Se $x_1, ..., x_n$ são as variáveis livres da fórmula $0 \neq s(t)$, devemos mostrar $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \forall x_1 ... \forall x_n(0 \neq s(t))$. Por UG aplicada n vezes, basta mostrar que $\mathcal{P} \vdash_{\mathcal{L}'_\mathcal{A}} 0 \neq s(t')$, onde $\mathcal{L}'_\mathcal{A} = \mathcal{L}_\mathcal{A} \cup \{c_1, ..., c_n\}$, $c_1, ..., c_n$ são constantes que não estão em $\mathcal{L}_\mathcal{A}$ e t' é o termo obtido ao fazer a substituição de cada ocorrência de x_i por c_i em t, para cada $i \in \{1, ..., n\}$. Por (A1) segue que $\mathcal{P} \vdash_{\mathcal{L}'_\mathcal{A}} \forall x(0 \neq s(x))$. Do axioma lógico do tipo 4, dado na Definição 3.2, temos que $\mathcal{P} \vdash_{\mathcal{L}'_\mathcal{A}} \forall x(0 \neq s(x)) \rightarrow 0 \neq s(t')$. Portanto inferimos por Modus Ponens que $\mathcal{P} \vdash_{\mathcal{L}'_\mathcal{A}} 0 \neq s(t')$, como queríamos.

Os itens **(2)–(6)** podem ser provados de maneira análoga.

(7). De forma análoga a feita no item 1, se $x_1, ..., x_n$ são as variáveis livres da fórmula $t = r \rightarrow (r = v \rightarrow t = v)$, então devemos mostrar $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \forall x_1 ... \forall x_n(t = r \rightarrow (r = v \rightarrow t = v))$. Por UG, aplicada n vezes à fórmula $t = r \rightarrow (r = v \rightarrow t = v)$, basta mostrar que $\mathcal{P} \vdash_{\mathcal{L}'_\mathcal{A}} t' = r' \rightarrow (r' = v' \rightarrow t' = v')$, onde $\mathcal{L}'_\mathcal{A} = \mathcal{L}_\mathcal{A} \cup \{c_1, ..., c_n\}$, $c_1, ..., c_n$ são constantes que não estão em $\mathcal{L}_\mathcal{A}$ e t', r' e v' são os termos obtidos ao fazer a substituição de cada ocorrência de x_i por c_i para cada $i \in \{1,...,n\}$, em t, r e v, respectivamente. Por sua vez, pelo Teorema da Dedução, basta mostrar que $\mathcal{P} \cup \{t' = r', r' = v'\} \vdash_{\mathcal{L}'_{\mathcal{A}}} t' = v'$. O axioma lógico do tipo 9 nos dá $\mathcal{P} \vdash_{\mathcal{L}'_{\mathcal{A}}} \forall x \forall y \forall z((x = y \wedge y = z) \rightarrow x = z)$. Pelo axioma lógico do tipo 4, fazendo as substituições sucessivas das variáveis x, y, z pelos termos t', r', v' respectivamente, inferimos que $\mathcal{P} \vdash_{\mathcal{L}_{\mathcal{A}}} (t' = r' \wedge r' = v') \rightarrow t' = v'$, e consequentemente inferimos que $\mathcal{P} \cup \{t' = r', r' = v'\} \vdash_{\mathcal{L}'_{\mathcal{A}}} t' = v'$, como desejado.

(8). Se $x_1, ..., x_n$ são as variáveis livres da fórmula $t = r \rightarrow s(t) = s(r)$, então devemos mostrar $\mathcal{P} \vdash_{\mathcal{L}_{\mathcal{A}}} \forall x_1 ... \forall x_n (t = r \rightarrow s(t) = s(r))$. Por UG, aplicada n vezes à fórmula $t = r \rightarrow s(t) = s(r)$, basta mostrar que $\mathcal{P} \vdash_{\mathcal{L}'_{\mathcal{A}}} t' = r' \rightarrow s(t') = s(r')$, onde $\mathcal{L}'_{\mathcal{A}} = \mathcal{L}_{\mathcal{A}} \cup \{c_1, ..., c_n\}$, $c_1, ..., c_n$ são constantes que não estão em $\mathcal{L}_{\mathcal{A}}$ e t' e r' são os termos obtidos ao fazer a substituição de cada ocorrência de x_i por c_i para cada $i \in \{1, ..., n\}$, em t e r, respectivamente. Aplicando o axioma lógico do tipo 10 para a função sucessora obtemos que $\mathcal{P} \vdash_{\mathcal{L}'_{\mathcal{A}}} \forall x \forall y (x = y \rightarrow s(x) = s(y))$. Basta então aplicar o axioma lógico do tipo 4 para as substituições de x, y por t', r' respectivamente e inferimos que $\mathcal{P} \vdash_{\mathcal{L}'_{\mathcal{A}}} t' = r' \rightarrow s(t') = s(r')$, como queríamos.

(9). Se $x_1, ..., x_n$ são as variáveis livres da fórmula $0 \cdot t = 0$, então devemos mostrar $\mathcal{P} \vdash_{\mathcal{L}_{\mathcal{A}}} \forall x_1 ... \forall x_n (0 \cdot t = 0)$. Por UG, aplicada n vezes à fórmula $0 \cdot t = 0$, basta mostrar que $\mathcal{P} \vdash_{\mathcal{L}'_{\mathcal{A}}} 0 \cdot t' = 0$, onde $\mathcal{L}'_{\mathcal{A}} = \mathcal{L}_{\mathcal{A}} \cup \{c_1, ..., c_n\}$, $c_1, ..., c_n$ são constantes que não estão em $\mathcal{L}_{\mathcal{A}}$ e t' é o termo obtido ao fazer a substituição de cada ocorrência de x_i por c_i em t, para cada $i \in \{1, ..., n\}$. Em primeiro lugar, mostraremos por indução (isto é, usando o axioma $(A7)$) que $\mathcal{P} \vdash_{\mathcal{L}'_{\mathcal{A}}} \forall x (0 \cdot x = 0)$. Para tal, tomando $\varphi(x)$ como a fórmula $0 \cdot x = 0$, mostraremos que $\mathcal{P} \vdash_{\mathcal{L}'_{\mathcal{A}}} \varphi(0)$ e $\mathcal{P} \vdash_{\mathcal{L}'_{\mathcal{A}}} \forall x (\varphi(x) \rightarrow \varphi(s(x)))$. Note que, por (5), temos que $\mathcal{P} \vdash_{\mathcal{L}'_{\mathcal{A}}} 0 \cdot 0 = 0$, logo $\mathcal{P} \vdash_{\mathcal{L}'_{\mathcal{A}}} \varphi(0)$. Por UG, para mostrar que $\mathcal{P} \vdash_{\mathcal{L}'_{\mathcal{A}}} \forall x (\varphi(x) \rightarrow \varphi(s(x)))$, basta mostrar que $\mathcal{P} \vdash_{\mathcal{L}''_{\mathcal{A}}} \varphi(c) \rightarrow \varphi(s(c))$ para alguma constante c que não está em $\mathcal{L}'_{\mathcal{A}}$ e, sendo $\mathcal{L}''_{\mathcal{A}} = \mathcal{L}'_{\mathcal{A}} \cup \{c\}$. Por sua vez, pelo Teorema da Dedução basta mostrar que $\mathcal{P} \cup \{\varphi(c)\} \vdash_{\mathcal{L}''_{\mathcal{A}}} \varphi(s(c))$. Por (6) temos que $\mathcal{P} \cup \{\varphi(c)\} \vdash_{\mathcal{L}''_{\mathcal{A}}} 0 \cdot s(c) = (0 \cdot c) + 0$ e por (3) temos que $\mathcal{P} \cup \{\varphi(c)\} \vdash_{\mathcal{L}''_{\mathcal{A}}} (0 \cdot c) + 0 = 0 \cdot c$. Usando um axioma lógico do tipo 9 inferimos que $\mathcal{P} \cup \{\varphi(c)\} \vdash_{\mathcal{L}''_{\mathcal{A}}} 0 \cdot s(c) = 0 \cdot c$. Como $\varphi(c)$ expressa $0 \cdot c = 0$, segue novamente por um axioma lógico do tipo 9 que $\mathcal{P} \cup \{\varphi(c)\} \vdash_{\mathcal{L}''_{\mathcal{A}}} 0 \cdot s(c) = 0$, isto é, $\mathcal{P} \cup \{\varphi(c)\} \vdash_{\mathcal{L}''_{\mathcal{A}}} \varphi(s(c))$, o que conclui a prova de que $\mathcal{P} \vdash_{\mathcal{L}_{\mathcal{A}}} \forall x (0 \cdot x = 0)$.

Como nos itens anteriores, aplicamos um axioma lógico do tipo 4 para a fórmula $\varphi(x)$ igual a $0 \cdot x = 0$ substituindo as ocorrências de x pelo termo t' e obtemos $\mathcal{P} \vdash_{\mathcal{L}'_{\mathcal{A}}} 0 \cdot t' = 0$, como desejado.

(10). Pode ser provado de maneira análoga ao item 9.

(11). Se $x_1,...,x_n$ são as variáveis livres da fórmula $(t+v=r+v)\to t=r$, então devemos mostrar $\mathcal{P}\vdash_{\mathcal{L}_\mathcal{A}} \forall x_1...\forall x_n(t+v=r+v\to t=r)$. Por UG, aplicada n vezes à fórmula $t+v=r+v\to t=r$, basta mostrar que $\mathcal{P}\vdash_{\mathcal{L}'_\mathcal{A}} t'+v'=r'+v'\to t'=r'$, onde $\mathcal{L}'_\mathcal{A}=\mathcal{L}_\mathcal{A}\cup\{c_1,...,c_n\}$, $c_1,...,c_n$ são constantes que não estão em $\mathcal{L}_\mathcal{A}$ e t',r' e v' são termo obtidos ao fazer a substituição de cada ocorrência de x_i por c_i para cada $i\in\{1,...,n\}$, em t,r e v, respectivamente.

Mostraremos por indução em z que $\mathcal{P}\vdash_{\mathcal{L}'_\mathcal{A}} \forall z\forall x\forall y(x+z=y+z\to x=y)$. Para tal, considerando $\varphi(z)$ a fórmula $\forall x\forall y(x+z=y+z\to x=y)$, basta mostrarmos que $\mathcal{P}\vdash_{\mathcal{L}'_\mathcal{A}} \varphi(0)$ e $\mathcal{P}\vdash_{\mathcal{L}'_\mathcal{A}} \forall z(\varphi(z)\to\varphi(s(z)))$.

Por UG, para mostrar que $\mathcal{P}\vdash_{\mathcal{L}'_\mathcal{A}} \varphi(0)$ basta mostrarmos que $\mathcal{P}\vdash_{\mathcal{L}''_\mathcal{A}} c+0=d+0\to c=d$, onde c e d são constantes que não estão em $\mathcal{L}'_\mathcal{A}$ e $\mathcal{L}''_\mathcal{A}=\mathcal{L}'_\mathcal{A}\cup\{c,d\}$. De (3) segue que $\mathcal{P}\vdash_{\mathcal{L}''_\mathcal{A}} c+0=c$ e $\mathcal{P}\vdash_{\mathcal{L}''_\mathcal{A}} d+0=d$. Usando axiomas lógicos dos tipos 8 e 9 e o Teorema da Dedução, inferimos que $\mathcal{P}\vdash_{\mathcal{L}''_\mathcal{A}} c+0=d+0\to c=d$, com queríamos.

De forma análoga, para verificar que $\mathcal{P}\vdash_{\mathcal{L}'_\mathcal{A}} \forall z(\varphi(z)\to\varphi(s(z))$, basta mostrarmos que $\mathcal{P}\vdash_{\mathcal{L}'''_\mathcal{A}} \varphi(a)\to\varphi(s(a)))$, onde a é uma constante que não está em $\mathcal{L}'_\mathcal{A}$ e $\mathcal{L}'''_\mathcal{A}=\mathcal{L}''_\mathcal{A}\cup\{a\}$. Por sua vez, por UG e pelo Teorema da Dedução é suficiente mostrar que $\mathcal{P}''''=\mathcal{P}\cup\{c+a=d+a\to c=d, c+s(a)=d+s(a)\}\vdash_{\mathcal{L}''''_\mathcal{A}} c=d$, onde c e d são constantes que não estão em $\mathcal{L}'''_\mathcal{A}$ e $\mathcal{L}''''_\mathcal{A}=\mathcal{L}'''_\mathcal{A}\cup\{c,d\}$. Por 4 temos que $\mathcal{P}''''\vdash_{\mathcal{L}''''_\mathcal{A}} c+s(a)=s(c+a)$ e $\mathcal{P}''''\vdash_{\mathcal{L}''''_\mathcal{A}} d+s(a)=s(d+a)$. Consequentemente, inferimos via (7), axioma lógico do tipo 8 e pelo fato da sentença $c+s(a)=d+s(a)$ ser um elemento de $\mathcal{P}''''$ que $\mathcal{P}''''\vdash_{\mathcal{L}''''_\mathcal{A}} s(d+a)=s(c+a)$. Logo por (2) inferimos que $\mathcal{P}''''\vdash_{\mathcal{L}''''_\mathcal{A}} d+a=c+a$. Como $c+a=d+a\to c=d$ é uma sentença de $\mathcal{P}''''$ inferimos que $\mathcal{P}''''\vdash_{\mathcal{L}''''_\mathcal{A}} c=d$, o que conclui a indução.

Pelo axioma lógico do tipo 4, fazendo substituições sucessivas em $\mathcal{P}\vdash_{\mathcal{L}'_\mathcal{A}} \forall z\forall x\forall y$ $(x+z=y+z\to x=y)$ de x,y e z por t',r' e v', segue que $\mathcal{P}\vdash_{\mathcal{L}'_\mathcal{A}} t'+v'=r'+v'\to t'=r'$, como queríamos.

(12). Se $x_1,...,x_n$ são as variáveis livres da fórmula $s(t)+r=s(t+r)$, então devemos mostrar $\mathcal{P}\vdash_{\mathcal{L}_\mathcal{A}} \forall x_1...\forall x_n(s(t)+r=s(t+r))$. Por UG, aplicada n vezes à fórmula $s(t)+r=s(t+r)$, basta mostrar que $\mathcal{P}\vdash_{\mathcal{L}'_\mathcal{A}} s(t')+r'=s(t'+r')$, onde $\mathcal{L}'_\mathcal{A}=\mathcal{L}_\mathcal{A}\cup\{c_1,...,c_n\}$, $c_1,...,c_n$ são constantes que não estão em $\mathcal{L}_\mathcal{A}$ e t' e r' são termos obtidos ao fazer a substituição de cada ocorrência de x_i por c_i para cada $i\in\{1,...,n\}$, em t,r e v, respectivamente.

Mostraremos por indução em y que $\mathcal{P}\vdash_{\mathcal{L}'_\mathcal{A}} \forall y\forall x(s(x)+y=s(x+y))$. Para tal, considerando $\varphi(y)$ a fórmula $\forall x(s(x)+y=s(x+y))$, basta mostrarmos que $\mathcal{P}\vdash_{\mathcal{L}'_\mathcal{A}} \varphi(0)$ e $\mathcal{P}\vdash_{\mathcal{L}'_\mathcal{A}} \forall y(\varphi(y)\to\varphi(s(y)))$.

Por UG, para mostrar que $\mathcal{P}\vdash_{\mathcal{L}'_\mathcal{A}} \varphi(0)$ basta mostrarmos que $\mathcal{P}\vdash_{\mathcal{L}''_\mathcal{A}} s(c)+0=$

$s(c+0)$, onde c é uma uma constante que não está em $\mathcal{L}'_{\mathcal{A}}$ e $\mathcal{L}''_{\mathcal{A}} = \mathcal{L}'_{\mathcal{A}} \cup \{c\}$. E isto segue dos itens 3, 7 e 8 deste teorema.

De forma análoga, para verificar que $\mathcal{P} \vdash_{\mathcal{L}'_{\mathcal{A}}} \forall y(\varphi(y) \rightarrow \varphi(s(y)))$, basta mostrarmos que $\mathcal{P} \vdash_{\mathcal{L}'''_{\mathcal{A}}} \varphi(a) \rightarrow \varphi(s(a))$, onde a é uma constante que não está em $\mathcal{L}'_{\mathcal{A}}$ e $\mathcal{L}'''_{\mathcal{A}} = \mathcal{L}''_{\mathcal{A}} \cup \{a\}$. Por sua vez, por UG e pelo Teorema da Dedução é suficiente mostrar que $\mathcal{P}'''' = \mathcal{P} \cup \{s(c)+a = s(c+a)\} \vdash_{\mathcal{L}''''_{\mathcal{A}}} s(c)+s(a) = s(c+s(a))$, onde c é uma constante que não está em $\mathcal{L}'''_{\mathcal{A}}$ e $\mathcal{L}''''_{\mathcal{A}} = \mathcal{L}'''_{\mathcal{A}} \cup \{c\}$. Para isso, basta considerar a seguinte lista:

1. $s(c)+a = s(c+a)$	Hipótese
2. $s(c)+s(a) = s(s(c)+a)$	Item 4
3. $s(s(c)+a) = s(s(c+a))$	Linha 1, item 8 e Modus Ponens
4. $s(c)+s(a) = s(s(c+a))$	Linhas 2, 3, item 7 e Modus Ponens
5. $c+s(a) = s(c+a)$	Item 4
6. $s(c+s(a)) = s(s(c+a))$	Linha 5, reflexividade e Modus Ponens
7. $s(c)+s(a) = s(c+s(a))$	Linhas 4, 7, reflexividade, item 7 e Modus Ponens.

□

Note que no início de cada demonstração do teorema anterior tivemos que invocar UG, tantas vezes quanto necessário, para trocar as variáveis das respectivas fórmulas por constantes de uma linguagem expandida $\mathcal{L}'_{\mathcal{A}}$, e então trabalhar com sentenças de $\mathcal{L}'_{\mathcal{A}}$ — uma vez que provas formais provam e se valem de sentenças. Este processo, como pode ser visto, carrega bastante a notação e acaba sendo repetitivo. Uma vez que está subentendido que devemos aplicar UG logo de início para trabalhar com sentenças na linguagem expandida, no que segue denotaremos, quando conveniente, as constantes da linguagem expandida pelos mesmo símbolos das variáveis, e a linguagem expandida pelo mesmo símbolo da linguagem original.

Para expressar sentenças corretamente no que se segue, denotaremos as variáveis por $x_1, x_2, x_3, ...$, onde x_1 é a primeira variável de $\mathcal{P}$, x_2 é a segunda e assim por diante. De forma análoga, denotaremos por $a_1, a_2, a_3, ...$ as constantes de $\mathcal{P}$. Denotaremos ainda por f^n_k o k-ésimo símbolo de função de aridade n em T e por p^n_k o k-ésimo símbolo de relação de aridade n em $\mathcal{P}$.

Definição 5.2 *Sejam t e r termos de $\mathcal{P}$. Escrevemos*

- *$t < r$ para abreviar $\exists w(w \neq 0 \wedge w + t = r)$, onde w é a primeira variável que não está em t ou em r.*

- $t \leq r$ *para abreviar* $t < r \vee t = r$
- $t > r$ *para abreviar* $r < t$
- $t \geq r$ *para abreviar* $r \leq t$
- $t \nless r$ *para abreviar* $\neg(t < r)$.

Os termos $0, s(0), s(s(0)), s(s(s(0))), \ldots$ de $\mathcal{L}_{\mathcal{A}}$ serão denominados **numerais** e denotados por $\overline{0}, \overline{1}, \overline{2}, \overline{3}, \ldots$ respectivamente. De forma geral, definimos recursivamente que 0 é o numeral $\overline{0}$ e se $\overline{n}$ é um numeral, então o numeral $\overline{n+1}$ é $s(\overline{n})$. Assim o numeral $\overline{n}$ é o resultado da aplicação da função sucessor n vezes no número 0, isto é, $s^n(0)$.

Teorema 5.3 *Sejam m e n números naturais.*

1. *Se $m \neq n$, então $\mathcal{P} \vdash_{\mathcal{L}_{\mathcal{A}}} \overline{m} \neq \overline{n}$.*
2. *$\mathcal{P} \vdash_{\mathcal{L}_{\mathcal{A}}} \overline{m+n} = \overline{m} + \overline{n}$ e $\mathcal{P} \vdash_{\mathcal{L}_{\mathcal{A}}} \overline{m \cdot n} = \overline{m} \cdot \overline{n}$.*

Demonstração:

1. Se $m \neq n$, então ou $m < n$ ou $n < m$. Suponha, sem perda de generalidade, que $m < n$. Vamos mostrar que $\mathcal{P} \cup \{\overline{m} = \overline{n}\}$ é inconsistente, e teremos, pelo Teorema 3.10 (Prova por Contradição), que $\mathcal{P} \vdash_{\mathcal{L}_{\mathcal{A}}} \overline{m} \neq \overline{n}$. De fato, por hipótese temos que $\overline{m} = \overline{n}$, ou seja, $s^m(0) = s^n(0)$. Aplicando o Teorema 5.1 (2) e Modus Ponens m vezes inferimos que $0 = s^{n-m}(0)$. Note que, como $m < n$, então $n - m > 0$ e $n - m - 1 \geq 0$. Assim, definindo $t = s^{(n-m-1)}(0)$ temos que $0 = s(t)$. Mas do Teorema 5.1 (1) segue que $0 \neq s(t)$. Logo, $\mathcal{P} \cup \{\overline{m} = \overline{n}\}$ é inconsistente.

2. Mostraremos que $\mathcal{P} \vdash_{\mathcal{L}_{\mathcal{A}}} \overline{m+n} = \overline{m} + \overline{n}$ por indução em n. Para o caso base note que $\overline{m+0}$ é $\overline{m}$, logo segue do Teorema 5.1 (3) que $\mathcal{P} \vdash_{\mathcal{L}_{\mathcal{A}}} \overline{m+0} = \overline{m} + \overline{0}$. Para o passo indutivo, suponha que $\mathcal{P} \vdash_{\mathcal{L}_{\mathcal{A}}} \overline{m+n} = \overline{m} + \overline{n}$. Então pela hipótese de indução e pelo Teorema 5.1 (4), respectivamente, segue que $\mathcal{P} \vdash_{\mathcal{L}_{\mathcal{A}}} s(\overline{m+n}) = \overline{m} + s(\overline{n})$. Note que $\overline{m+(n+1)} = s(\overline{m+n})$ e $\overline{n+1} = s(\overline{n})$, assim segue que $\mathcal{P} \vdash_{\mathcal{L}_{\mathcal{A}}} \overline{m+(n+1)} = \overline{m} + (\overline{n+1})$. Concluímos então a indução que mostra que $\mathcal{P} \vdash_{\mathcal{L}_{\mathcal{A}}} \overline{m+n} = \overline{m} + \overline{n}$.

   Vamos agora mostrar que $\mathcal{P} \vdash_{\mathcal{L}_{\mathcal{A}}} \overline{m \cdot n} = \overline{m} \cdot \overline{n}$. Como $m \cdot 0 = 0$, temos que $\overline{m \cdot 0}$ é $\overline{0}$. Por outro lado, o Teorema 5.1 (5) nos dá que $\mathcal{P} \vdash_{\mathcal{L}_{\mathcal{A}}} \overline{m} \cdot \overline{0} = \overline{0}$ e, portanto, $\mathcal{P} \vdash_{\mathcal{L}_{\mathcal{A}}} \overline{m \cdot 0} = \overline{m} \cdot \overline{0}$. Assuma agora que $\mathcal{P} \vdash_{\mathcal{L}_{\mathcal{A}}} \overline{m \cdot n} = \overline{m} \cdot \overline{n}$. Temos que $m \cdot (n+1) = m \cdot n + m$. Assim pelo item 1, pelo que foi mostrado no parágrafo anterior, pela hipótese de indução segue, respectivamente, que $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \overline{m \cdot (n+1)} = \overline{m} \cdot \overline{n} + \overline{m}$. Por outro lado, segue do Teorema 5.1 (9) que $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \overline{m} \cdot (\overline{n+1}) = \overline{m} \cdot \overline{n} + \overline{m}$. Desta forma segue que $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \overline{m \cdot (n+1)} = \overline{m} \cdot (\overline{n+1})$, o que conclui a indução. □

Podemos ainda expressar a noção de ordem em $\mathcal{P}$.

Teorema 5.4 *Sejam t, r, v termos da linguagem $\mathcal{L}_\mathcal{A}$. Então as sentenças dadas pelos fechos universais das seguintes fórmulas podem ser provadas em $\mathcal{P}$:*

1. $t \not< t$
2. $t \leq v \to (v < r \to t < r)$
3. $t < r \to r \not< t$
4. $t < s(t)$
5. $0 \leq t$
6. $0 < t \to \exists w(t = s(w))$
7. $t < r \to s(t) \leq r$
8. $t = r \vee t < r \vee r < t$
9. $(t \leq r \wedge r \leq t) \to t = r$

Demonstração: De forma análoga ao que fizemos no Teorema 5.1, usaremos o axioma lógico 4 em alguns itens e, para isso, mudaremos, em cada fórmula listada no enunciado, todas as variáveis limitadas por outras variáveis que não aparecem nos respectivos termos envolvidos. Desta forma garantimos que os termos envolvidos sejam livres para todas as variáveis nas respectivas fórmulas.

1. A lista abaixo mostra que $\neg Con_{\vdash, \mathcal{L}_\mathcal{A}}(\mathcal{P} \cup \{t < t\})$ — e então basta aplicar o Teo-

rema 3.10.

1. $t < t$ Hipótese
2. $\exists w(w \neq 0 \wedge w + t = t)$ Expansão de (1)
3. $b \neq 0 \wedge b + t = t$ Por EI em (2)
4. $b + t = t$ Conjunção em (3)
5. $0 + t = t$ Proposição 5.1 (10)
6. $b + t = 0 + t$ Inferido de 4, 5, Proposição 5.1 (7) e axioma lógico 8
7. $b = 0$ Inferido de 6 e Proposição 5.1 (11)
8. $b \neq 0$ Inferido de 3

De 7 e 8 segue que $\neg Con_{\vdash,\mathcal{L}_\mathcal{A}}(\mathcal{P} \cup \{t < t\})$.

2. Pelo Teorema da Dedução, basta mostrar que $\mathcal{P} \cup \{t \leq v, v < r\} \vdash_{\mathcal{L}_\mathcal{A}} t < r$. Se $t = v$, considere a seguinte lista:

   1. $t = v$ Hipótese
   2. $v < r$ Hipótese
   3. $c \neq 0 \wedge c + v = r$ Por EI na expansão de (2)
   4. $c + t = r$ Por (2) do Teorema 5.1 e Modus Ponens
   5. $t < r$ Pela definição de $<$, usando que $c \neq 0$ e EI

   Se $t < v$ considere a seguinte lista.

   1. $t < v$ Hipótese
   2. $v < r$ Hipótese
   3. $b \neq 0 \wedge b + t = v$ Por EI na expansão de (1)
   4. $c \neq 0 \wedge c + v = r$ Por EI na expansão de (2)
   5. $b + c + t = r$ Por (2) do Teorema 5.1 e Modus Ponens
   6. $t < r$ Pela definição de $<$, usando que $b + c \neq 0$ e EI

   Na última linha usamos que $b \neq 0$ e $c \neq 0$ implicam $b+c \neq 0$, pois caso contrário teríamos $b < c$.

3. Pelo Teorema da Dedução basta mostrar que $\mathcal{P} \cup \{t < s\} \vdash_{\mathcal{L}_\mathcal{A}} s \not< t$ e para tal, pelo Teorema 3.10 basta mostrar que $\neg Con_{\vdash,\mathcal{L}_\mathcal{P}}(\mathcal{P} \cup \{t < s, s < t\})$. Para tal, considere a seguinte lista.

1. $t < s$	Hipótese
2. $s < t$	Hipótese
3. $t < t$	Pelo item 2 deste teorema, linhas 1 e 2 e Modus Ponens
4. $t \not< t$	Pelo item 1 deste teorema

   As linhas 3 e 4 mostram a inconsistência desejada.

4. Mostraremos que $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \forall x(x < s(x))$ e, como fizemos anteriormente, o resultado segue por um axioma lógico do tipo 4 para a substituição de x por t, em que inferimos que $\mathcal{P}$ prova um fecho universal de $t < s(t)$. Por UG, basta mostrar que $\mathcal{P} \vdash_{\mathcal{L}'_\mathcal{A}} a < s(a)$ onde a é uma constante que não está em $\mathcal{L}_\mathcal{A}$ e $\mathcal{L}'_\mathcal{A} = \mathcal{L}_\mathcal{A} \cup \{a\}$. Pelo item 4 do Teorema 5.1 temos que $a + s(0) = s(a + 0)$, pelo item 3 temos que $a + 0 = a$ e, consequentemente, do item 8 inferimos que $s(a + 0) = s(a)$. Desta forma, do item 7 inferimos que $a + s(0) = s(a)$. Do item 1 temos que $s(0) \neq 0$, logo vale $s(0) \neq 0 \wedge a + s(0) = s(a)$. Assim por EG segue que $\mathcal{P} \vdash_{\mathcal{L}'_\mathcal{A}} \exists w(w \neq 0 \wedge a + w = s(a))$, isto é, $\mathcal{P} \vdash_{\mathcal{L}'_\mathcal{A}} a < s(a)$.

5. Mostraremos por indução que $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \forall x(0 \leq x)$ e, análogo ao que fizemos na demonstração do Teorema 5.1, pelo axioma lógico do tipo 4 segue o resultado. Tome $\varphi(x)$ como $0 \leq x$. Por indução basta mostrar que $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \varphi(0)$ e $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \forall x(\varphi(x) \to \varphi(s(x)))$. Para mostrar que $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \varphi(0)$ basta notar que de $0 = 0$ inferimos que $0 \leq 0$ pela definição de $\leq$. Para mostrar que $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \forall x(\varphi(x) \to \varphi(s(x)))$, por UG, basta mostrar que $\mathcal{P} \vdash_{\mathcal{L}'_\mathcal{A}} \varphi(c) \to \varphi(s(c))$ onde c é uma constante que não está em $\mathcal{L}_\mathcal{A}$ e $\mathcal{L}'_\mathcal{A} = \mathcal{L}_\mathcal{A} \cup \{c\}$. Do Teorema da Dedução, basta mostrar que $\mathcal{P} \cup \{\varphi(c)\} \vdash_{\mathcal{L}'_\mathcal{A}} \varphi(s(c))$. Do item 4 temos que $c < s(c)$ e por hipótese $0 \leq c$. Se assim, do item 2 e de Modus Ponens temos que $0 < c$ e, em particular, $\mathcal{P} \cup \{0 \leq c\} \vdash_{\mathcal{L}'_\mathcal{A}} 0 \leq s(c)$, como queríamos.

6. Mostraremos que $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \forall x(0 < x \to \exists w(x = s(w)))$. Disto, como feito anteriormente usando um axioma lógico do tipo 4 para substituir x segue que $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} 0 < t \to \exists w(t = s(w))$. Faremos isto por indução (isto é, usaremos o axioma $(A7)$). Definindo $\varphi(x)$ como a fórmula $0 < x \to \exists w(x = s(w))$, basta

mostrarmos que $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \varphi(0)$ e $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \forall x(\varphi(x) \rightarrow \varphi(s(x)))$.

Pelo Teorema da Dedução, para mostrar que $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \varphi(0)$ basta mostrar que $\mathcal{P}' = \mathcal{P} \cup \{0 < 0\} \vdash_{\mathcal{L}_\mathcal{A}} \exists w(0 = s(w))$. Pelo item 1 temos que $\mathcal{P}' \vdash_{\mathcal{L}_\mathcal{A}} \neg(0 < 0)$, e como $0 < 0$ é uma sentença de $\mathcal{P}'$ também temos $\mathcal{P}' \vdash_{\mathcal{L}_\mathcal{A}} 0 < 0$. Note agora que $(\psi \wedge \neg\psi) \rightarrow \phi$ é uma tautologia, para quaisquer fórmulas ψ e ϕ, logo, tomando ψ como a fórmula $0 < 0$ e ϕ como fórmula $\exists w(0 = s(w))$, inferimos que $\mathcal{P}' \vdash_{\mathcal{L}_\mathcal{A}} \exists w(0 = s(w))$, como desejado.

Para mostrar que $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \forall x(\varphi(x) \rightarrow \varphi(s(x)))$, por UG, basta mostrar que $\mathcal{P} \vdash_{\mathcal{L}'_\mathcal{A}} \varphi(a) \rightarrow \varphi(s(a))$, onde a é uma constante fora de $\mathcal{L}_\mathcal{A}$ e $\mathcal{L}'_\mathcal{A} = \mathcal{L}_\mathcal{A} \cup \{a\}$. Para tal, pelo Teorema da Dedução basta mostrar que $\mathcal{P} \cup \{\varphi(a)\} \vdash_{\mathcal{L}'_\mathcal{A}} \varphi(s(a))$, e expandindo $\varphi(a)$ e usando novamente o Teorema da Dedução, basta mostrar que $\mathcal{P}' = \mathcal{P} \cup \{\varphi(a), 0 < s(a)\} \vdash_{\mathcal{L}'_\mathcal{A}} \exists w(s(a) = s(w))$. Mas para tal basta notar que, por um axioma lógico do tipo 7, $\mathcal{P}' \vdash_{\mathcal{L}'_\mathcal{A}} s(a) = s(a)$. Definindo $\varphi(w)$ como a fórmula $s(a) = s(w)$, temos que $\mathcal{P}' \vdash_{\mathcal{L}'_\mathcal{A}} \varphi(a)$, logo por EG segue que $\mathcal{P}' \vdash_{\mathcal{L}'_\mathcal{A}} \exists w\varphi(w)$, isto é, $\mathcal{P}' \vdash_{\mathcal{L}'_\mathcal{A}} \exists w(s(a) = s(w))$, como queríamos.

7. Mostraremos que $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \forall x\forall y(x < y \rightarrow s(x) \leq y)$. Disto, como feito anteriormente usando um axioma lógico do tipo 4 para substituir x por t e y por r, segue que $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} t < r \rightarrow s(t) \leq r$.

   Aplicando UG duas vezes para as variáveis x e y, basta mostrar que $\mathcal{P} \vdash_{\mathcal{L}'_\mathcal{A}} a < b \rightarrow s(a) \leq b$ onde a e b são constantes que não estão em $\mathcal{L}_\mathcal{A}$ e $\mathcal{L}'_\mathcal{A} = \mathcal{L}_\mathcal{A} \cup \{a, b\}$. E pelo Teorema da Dedução, basta mostrar que $\mathcal{P}' = \mathcal{P} \cup \{a < b\} \vdash_{\mathcal{L}'_\mathcal{A}} s(a) \leq b$. Assim, por EI, para obtermos o resultado desejado basta mostrar que $\mathcal{P}'' = \mathcal{P}' \cup \{c \neq 0 \wedge a + c = b\} \vdash_{\mathcal{L}''_\mathcal{A}} s(a) \leq b$ onde c é uma constante que não está em $\mathcal{L}'_\mathcal{A}$ e $\mathcal{L}''_\mathcal{A} = \mathcal{L}'_\mathcal{A} \cup \{c\}$. Temos que $\mathcal{P}'' \vdash_{\mathcal{L}''_\mathcal{A}} c \neq 0$, então de (2) segue que $\mathcal{P}'' \vdash_{\mathcal{L}''_\mathcal{A}} 0 < c$. Por (6) temos que $\mathcal{P}'' \vdash_{\mathcal{L}''_\mathcal{A}} 0 < c \rightarrow \exists w(c = s(w))$, assim, novamente por EI, basta mostrar que $\mathcal{P}''' = \mathcal{P}'' \cup \{c = s(d)\} \vdash_{\mathcal{L}'''_\mathcal{A}} s(a) \leq b$, onde d é uma constante que não está em $\mathcal{L}''_\mathcal{A}$ e $\mathcal{L}'''_\mathcal{A} = \mathcal{L}''_\mathcal{A} \cup \{d\}$. Por fim, basta notar que, do item 12 do Teorema 5.1 vale $s(a) + d = s(a + d)$, do item 4 temos $s(a + d) = a + s(d)$, e como $s(d) = c$ e $a + c = b$, segue que $s(a) + d = a + s(d) = a + c = b$. Desta forma temos que $s(a) + d = b$. Se $d = 0$ então $b = s(a) + 0 = s(a)$, do item 3, e neste caso vale $s(a) \leq b$. Se $d \neq 0$, então por EG segue que $\exists w(w \neq 0 \wedge s(a) + w = b)$, isto é, $s(a) < b$, e em particular $s(a) \leq b$, como queríamos.

8. Mostraremos por indução que $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \forall x\forall y(x \leq y \vee y \leq x)$. Disto, como feito anteriormente usando um axioma lógico do tipo 4 para substituir x por t e y

por r, segue que $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} t \leq r \vee r \leq t$. Notando que $(t \leq r \vee r \leq t) \to (t = r \vee t < r \vee r < t)$ é uma tautologia, concluiremos o resultado desejado.

Desta forma, definindo $\varphi(x)$ como a fórmula $\forall y(x \leq y \vee y \leq x)$, basta mostrar que $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \varphi(0)$ e $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \forall x(\varphi(x) \to \varphi(s(x)))$. Note que $\varphi(0)$ é a fórmula $\forall y(0 \leq y \vee y \leq 0)$, e por UG, para concluirmos que $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \forall y(0 \leq y \vee y \leq 0)$ basta mostrar que $\mathcal{P} \vdash_{\mathcal{L}'_\mathcal{A}} 0 \leq a \vee a \leq 0$ onde a é uma constante que não estão em $\mathcal{L}_\mathcal{A}$ e $\mathcal{L}'_\mathcal{A} = \mathcal{L}_\mathcal{A} \cup \{a\}$. Pelo item 2 temos que $\mathcal{P} \vdash_{\mathcal{L}'_\mathcal{A}} 0 \leq a$, e como $0 \leq a \to (0 \leq a \vee a \leq 0)$ é uma tautologia, segue que $\mathcal{P} \vdash_{\mathcal{L}'_\mathcal{A}} 0 \leq a \vee a \leq 0$ como desejado.

Para mostrar que $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \forall x(\varphi(x) \to \varphi(s(x)))$, ao expandir $\varphi(x)$ temos, por UG, que basta mostrar $\mathcal{P} \vdash_{\mathcal{L}''_\mathcal{A}} \forall y(b \leq y \vee y \leq b) \to \forall y(s(b) \leq y \vee y \leq s(b))$ onde b é uma constante que não está em $\mathcal{L}_\mathcal{A}$ e $\mathcal{L}''_\mathcal{A} = \mathcal{L}_\mathcal{A} \cup \{b\}$. Pelo Teorema da Dedução basta mostrar que $\mathcal{P} \cup \{\forall y(b \leq y \vee y \leq b)\} \vdash_{\mathcal{L}''_\mathcal{A}} \forall y(s(b) \leq y \vee y \leq s(b))$. Por sua vez, por UG, basta mostrar que $\mathcal{P}''' = \mathcal{P} \cup \{\forall y(b \leq y \vee y \leq b)\} \vdash_{\mathcal{L}'''_\mathcal{A}} s(b) \leq c \vee c \leq s(b)$, onde c é uma constante que não está em $\mathcal{L}''_\mathcal{A}$ e $\mathcal{L}'''_\mathcal{A} = \mathcal{L}''_\mathcal{A} \cup \{c\}$.

Note que, por UI, temos que $\mathcal{P}''' \vdash_{\mathcal{L}'''_\mathcal{A}} b \leq c \vee c \leq b$, pois $\forall y(b \leq y \vee y \leq b)$ é uma sentença de $\mathcal{P}'''$. Vamos mostrar que $\mathcal{P}''' \vdash_{\mathcal{L}'''_\mathcal{A}} (b \leq c) \to (s(b) \leq c \vee c \leq s(b))$ e $\mathcal{P}''' \vdash_{\mathcal{L}'''_\mathcal{A}} (c \leq b) \to (s(b) \leq c \vee c \leq s(b))$, pois disso e de $\mathcal{P}''' \vdash_{\mathcal{L}'''_\mathcal{A}} b \leq c \vee c \leq b$ seguirá (por uma tautologia) que $\mathcal{P}'' \vdash_{\mathcal{L}'''_\mathcal{A}} s(b) \leq c \vee c \leq s(b)$.

Se $c \leq b$ com $c = b$, pelo item 5 temos que $b < s(b)$, logo por um axioma lógico do tipo 11 para a relação $<$ segue que $c < s(b)$. Assim, vale em particular que $s(b) \leq c \vee c \leq s(b)$. Se $b < c$, pelo item 7 inferimos que $s(b) \leq c$ e, em particular, também vale $s(b) \leq c \vee c \leq s(b)$. Se $b \leq c$ com $b = c$, então em particular $c \leq b$ e podemos aplicar o caso anterior. Se $b < c$, pelo item 6 inferimos que $s(b) \leq c$. Em particular, vale $s(b) \leq c \vee c \leq s(b)$, como queríamos.

9. Pelo Teorema da Dedução basta mostrar que $\mathcal{P} \cup \{t \leq s \wedge r \leq t\} \vdash_{\mathcal{L}_\mathcal{A}} t = r$ e para tal, pelo Teorema 3.10 basta mostrar que $\neg Con_{\vdash, \mathcal{L}_\mathcal{P}}(\mathcal{P} \cup \{t \leq s \wedge r \leq t, t \neq r\})$. Para

tal, considere a seguinte lista.

1. $t \neq r$	Hipótese
2. $t \leq r$	Instância da hipótese
3. $r \leq t$	Instância da hipótese
4. $t < r$	Por (1) e (2)
5. $r \nless t$	Por (4) e pelo item 3 deste teorema
6. $r < t$	Por (1) e (3)

As duas últimas linhas da sequência acima mostram que $\neg Con_{\vdash,\mathcal{L}_\mathcal{P}}(\mathcal{P} \cup \{t \leq s \wedge r \leq t, t \neq r\})$. □

Lema 5.5 *Para todo número natural $k > 0$ e para toda fórmula φ com no máximo uma variável livre, valem:*

1. $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \forall x((x = 0 \vee ... \vee x = \overline{k}) \leftrightarrow x \leq \overline{k})$.
2. $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} (\varphi(0) \wedge \varphi(\overline{1}) \wedge ... \wedge \varphi(\overline{k-1})) \leftrightarrow \forall x(x < \overline{k} \rightarrow \varphi(x))$.

Demonstração:

1. Faremos esta prova por indução em k. Para o caso em que $k = 0$ queremos mostrar que $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} x = \overline{0} \leftrightarrow x \leq \overline{0}$. Pela definição de ordem, temos que $x \leq 0$ abrevia $x < 0 \vee x = 0$. Portanto, $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} x = \overline{0} \rightarrow x \leq \overline{0}$. Reciprocamente, assuma $x \leq 0$. Pelo Teorema 5.4 itens (5) e (9), respectivamente, segue que $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \overline{0} \leq x$ e $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} (x \leq \overline{0}) \wedge (\overline{0} \leq x) \rightarrow x = \overline{0}$. Desta forma vale, pelo Teorema da Dedução, que $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} x \leq \overline{0} \rightarrow x = \overline{0}$. Portanto $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} x = \overline{0} \leftrightarrow x \leq \overline{0}$.

   Assuma agora que $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} x = \overline{0} \vee ... \vee x = \overline{k} \leftrightarrow x \leq \overline{k}$. Devemos mostrar que $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} (x = \overline{0} \vee ... \vee x = \overline{k} \vee x = \overline{k+1}) \leftrightarrow x \leq \overline{k+1}$. Para isto, vamos nos valer do Teorema da Dedução para mostrar cada implicação. Para a implicação direta, se $x = 0 \vee ... \vee x = \overline{k}$, então por hipótese, $x \leq \overline{k}$ e pelo item 4 do Teorema 5.4 vale $\overline{k} < \overline{k+1}$ e do item 2 do mesmo teorema segue que $x \leq \overline{k+1}$. E claro que, se $x = \overline{k+1}$ então $x \leq \overline{k+1}$, logo, $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} x = \overline{0} \vee ... \vee x = \overline{k} \vee x = \overline{k+1} \rightarrow x \leq \overline{k+1}$. Reciprocamente, se $x \leq \overline{k+1}$ então $x = \overline{k+1}$ ou $x < \overline{k+1}$. Se $x = \overline{k+1}$ então, em particular, $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} x = \overline{0} \vee ... \vee x = \overline{k} \vee x = \overline{k+1}$, e se $x < \overline{k+1}$, por hipótese de indução, também temos que $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} x = \overline{0} \vee ... \vee x = \overline{k} \vee x = \overline{k+1}$. Disto segue o resultado.

2. Faremos esta prova por indução em k. Para o caso em que $k = 0$ devemos mostrar que $\mathcal{P} \vdash_{\mathcal{L}_A} \varphi(\overline{0}) \leftrightarrow \forall x(x < \overline{0} \to \varphi(x))$. Pelo Teorema da Dedução seguido de UI, basta mostrar que $\mathcal{P} \cup \{\varphi(\overline{0})\} \vdash_{\mathcal{L}'_A} c < \overline{0} \to \varphi(c)$ onde $\mathcal{L}'_A = \mathcal{L}_A \cup \{c\}$ e c é uma constante que não está em $\mathcal{L}_A$. Novamente, pelo Teorema da Dedução, basta mostrar que $\mathcal{P} \cup \{\varphi(\overline{0}), c < \overline{0}\} \vdash_{\mathcal{L}_A} \varphi(c)$. Mas note que $\neg Con_{\vdash,\mathcal{L}'_A}(\mathcal{P} \cup \{\varphi(\overline{0}), c < \overline{0}\})$ pois, pelo item 5 do Teorema 5.4 e da hipótese $c < 0$ temos que $\mathcal{P} \cup \{\varphi(0), c < \overline{0}\} \vdash_{\mathcal{L}_A} \overline{0} < c$; e do item 3 deste mesmo teorema, a hipótese $c < 0$ e Modus Ponens temos que $\mathcal{P} \cup \{\varphi(\overline{0}), c < \overline{0}\} \vdash_{\mathcal{L}_A} \overline{0} \not< c$. Logo, do Lema 3.9 temos que o conjunto inconsistente prova qualquer sentença de $\mathcal{L}'_A$, em particular, $\mathcal{P} \cup \{\varphi(\overline{0}), c < \overline{0}\} \vdash_{\mathcal{L}_A} \varphi(c)$.

   Para o passo indutivo, assuma que $\mathcal{P} \vdash_{\mathcal{L}_A} (\varphi(\overline{0}) \land \varphi(\overline{1}) \land ... \land \varphi(\overline{k-1})) \leftrightarrow \forall x(x < \overline{k} \to \varphi(x))$. Devemos mostrar que $\mathcal{P} \vdash_{\mathcal{L}_A} (\varphi(\overline{0}) \land \varphi(\overline{1}) \land ... \land \varphi(\overline{k-1}) \land \varphi(\overline{k})) \leftrightarrow \forall x(x < \overline{k+1} \to \varphi(x))$. Para tal, basta provar as duas implicações separadamente. Para a implicação direta, pelo Teorema da Dedução, por UI e novamente pelo Teorema da Dedução, respectivamente, basta provarmos que $\mathcal{P} \cup \{\varphi(\overline{0}) \land \varphi(\overline{1}) \land ... \land \varphi(\overline{k-1}) \land \varphi(\overline{k}), c < \overline{k+1}\} \vdash_{\mathcal{L}'_A} \varphi(c)$. De $c < \overline{k+1}$, da contrapositiva do item 3 do Teorema 5.4 e do item 8 deste mesmo teorema segue, por Modus Ponens, que $c \leq \overline{k}$. Por disjunção da sentença $\varphi(\overline{0}) \land \varphi(\overline{1}) \land ... \land \varphi(\overline{k-1}) \land \varphi(\overline{k})$ e por UI na hipótese de indução inferimos, por Modus Ponens, que vale $\mathcal{P} \cup \{\varphi(\overline{0}) \land \varphi(\overline{1}) \land ... \land \varphi(\overline{k-1}) \land \varphi(\overline{k}), c < \overline{k+1}\} \vdash_{\mathcal{L}'_A} \varphi(c)$. A outra implicação segue de forma análoga. □

Podemos também expressar a noção de divisibilidade em $\mathcal{P}$.

Definição 5.6 *Escrevemos que $t \mid u$ para abreviar $\exists z(u = t \cdot z)$, onde z é a primeira variável que não ocorre em t ou u.*

E disto podemos derivar os diversos resultados acerca de divisibilidade. Destacamos aqui um resultado que usaremos posteriormente.

Teorema 5.7 (Divisão Euclidiana) *Temos*

$$\mathcal{P} \vdash_{\mathcal{L}_A} \forall x \forall y(y \neq 0 \to \exists v \exists u(x = y \cdot u + v \land v < y \land \forall v_1 \forall u_1((x = y \cdot u_1 + v_1 \land v_1 < y) \to u = u_1 \land v = v_1))).$$

Finalmente, a "estrutura"cujo conjunto universo é o conjunto dos inteiros não negativos, a interpretação do símbolo de constante 0 é o inteiro 0, cuja interpretação do símbolo de função s é a função que associa cada inteiro não negativo n ao inteiro

$n+1$, cuja interpretação dos símbolos de função $+$ e $\cdot$ são, respectivamente, a soma e o produto usual nos inteiros será chamada de interpretação padrão de $\mathcal{P}$.

5.2 Relações exprimíveis e funções representáveis

Definição 5.8 *Dado um número natural k, chamaremos uma função $f : \mathbb{N}^k \to \mathbb{N}$ de* ***função de números naturais*** *e uma relação $R \subseteq \mathbb{N}^k$ de* ***relação de números naturais****.*

Definição 5.9 *Seja T uma teoria na linguagem $\mathcal{L}_\mathcal{A}$. Dizemos que uma relação n-ária de números naturais é* ***exprimível*** *em T quando existe uma fórmula $\varphi(x_1,...,x_n)$ de $\mathcal{L}_\mathcal{A}$ com variáveis livres $x_1,...,x_n$ tal que, para quaisquer números naturais $k_1,...,k_n$, valem as seguintes condições:*

1. *Se $(k_1,...,k_n) \in R$ então $T \vdash_{\mathcal{L}_\mathcal{A}} \varphi(\overline{k}_1,...,\overline{k}_n)$.*

2. *Se $(k_1,...,k_n) \notin R$ então $T \vdash_{\mathcal{L}_\mathcal{A}} \neg\varphi(\overline{k}_1,...,\overline{k}_n)$.*

Neste caso, dizemos que φ ***exprime*** *R.*

Exemplo 5.10 *A igualdade de números naturais é uma relação exprimível em $\mathcal{P}$ pela fórmula $\varphi(x_1,x_2)$ dada por $x_1 = x_2$. Isto segue do item 1 do Teorema 5.3 e do fato de que se k_1 e k_2 são tais que $k_1 = k_2$ (isto é, k_1 e k_2 denotam o mesmo número natural), então $\overline{k}_1$ e $\overline{k}_2$ denotam o mesmo termo, o que implica que $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \overline{k}_1 = \overline{k}_2$.*

Exemplo 5.11 *A relação $<$ é exprimível em $\mathcal{P}$ pela fórmula $x_1 < x_2$. De fato, sejam k_1, k_2 números naturais. Se $k_1 < k_2$, existe um natural $n \neq 0$ satisfazendo $n + k_1 = k_2$. Do Teorema 5.3 (2) segue que $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \overline{n} + \overline{k}_1 = \overline{k}_2$. E ainda, sendo $n \neq 0$, do Exemplo 5.10 segue que $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \overline{n} \neq 0$. Assim, por uma conjunção e pela regra de quantificadores EG segue que $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \exists w(w \neq 0 \ \wedge w + \overline{k}_1 = \overline{k}_2)$, isto é, $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \overline{k}_1 < \overline{k}_2$. Por outro lado, se $k_1 \not< k_2$, então $k_2 < k_1$ ou $k_2 = k_1$. Se $k_2 < k_1$, acabamos de ver que obtemos $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \overline{k}_2 < \overline{k}_1$, pelo item 3 do Teorema 5.4 segue que $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \overline{k}_1 \not< \overline{k}_2$. E se $k_2 = k_1$, pelo item 1 do Teorema 5.4 temos que $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \overline{k}_1 \not< \overline{k}_2$. Em ambos os casos, concluímos o desejado.*

Definição 5.12 *Seja T uma teoria na linguagem $\mathcal{L}_\mathcal{A}$. Dizemos que uma função de números naturais com n argumentos f é* ***representável*** *em T quando existe uma fórmula $\varphi(x_1,...,x_n,y)$ de $\mathcal{L}_\mathcal{A}$ com variáveis livres $x_1,...,x_n,y$ tal que, para quaisquer números naturais $k_1,...,k_n,m$, valem as seguintes condições:*

(1) *Se $f(k_1,...,k_n) = m$ então $T \vdash_{\mathcal{L}_\mathcal{A}} \varphi(\overline{k}_1,...,\overline{k}_n,\overline{m})$.*

(2) $T \vdash_{\mathcal{L}_A} \exists! y\varphi(\overline{k}_1, ..., \overline{k}_n, y)$[1].

*Neste caso, dizemos que φ **representa** f. Se substituirmos a condição* (2) *acima pela condição*

(2′) $T \vdash_{\mathcal{L}_A} \forall x_1 ... \forall x_n \exists! y\varphi(x_1, ..., x_n, y)$,

*então f será dita **fortemente representável** em T. Neste caso, dizemos que φ **representa fortemente** f.*

Uma questão natural acerca das definições de relações exprimíveis e funções representáveis é a seguinte: por que não pedir que, para que uma função f seja representável, valha $T \vdash_{\mathcal{L}_A} \neg\varphi(\overline{k}_1, ..., \overline{k}_n, \overline{m})$ sempre que $f(k_1, ..., k_n) \neq m$, de forma análoga ao que exigimos para as relações exprimíveis? A resposta é dada pelo resultado a seguir, que mostra que as condições 1 e 2 da representabilidade são suficientes para concluir tal fato.

Proposição 5.13 *Seja $f(x_1, ..., x_n)$ uma função representada por $\varphi(x_1, ..., x_{n+1})$ em $\mathcal{P}$. Se $k_1, ..., k_n, m \in \mathbb{N}$ são tais que $f(k_1, ..., k_n) \neq m$ então $\mathcal{P} \vdash_{\mathcal{L}_A} \neg\varphi(\overline{k_1}, ..., \overline{k}_n, \overline{m})$.*

Demonstração: Seja $f(k_1, ..., k_n) = l$. Então $l \neq m$ e pelo item 1 do Teorema 5.3 temos que $\mathcal{P} \vdash_{\mathcal{L}_A} \overline{m} \neq \overline{l}$. Pela condição 1 da representabilidade de f segue que $\mathcal{P} \vdash_{\mathcal{L}_A} \varphi(\overline{k}_1, ..., \overline{k}_n, \overline{l})$. E ainda, da condição 2 de representabilidade temos que $\mathcal{P} \vdash_{\mathcal{L}_A} \forall y \forall x((\varphi(\overline{k}_1, ..., \overline{k}_n, y) \wedge \varphi(\overline{k}_1, ..., \overline{k}_n, x)) \to y = x)$. Por UI podemos instanciar tal fórmula para $\mathcal{P} \vdash_{\mathcal{L}_A} (\varphi(\overline{k}_1, ..., \overline{k}_n, \overline{m}) \wedge \varphi(\overline{k}_1, ..., \overline{k}_n, \overline{l})) \to \overline{m} = \overline{l}$. Note que, para quaisquer fórmulas A, B e C, a fórmula $(((A \wedge B) \to C) \wedge \neg C) \to (\neg A \vee \neg B)$ é uma tautologia. Desta forma, como valem em $\mathcal{P}$ as sentenças $(\varphi(\overline{k}_1, ..., \overline{k}_n, \overline{m}) \wedge \varphi(\overline{k}_1, ..., \overline{k}_n, \overline{l})) \to \overline{m} = \overline{l}$ e $\overline{m} \neq \overline{l}$, inferimos que $\mathcal{P} \vdash_{\mathcal{L}_A} \neg\varphi(\overline{k}_1, ..., \overline{k}_n, \overline{m}) \vee \neg\varphi(\overline{k}_1, ..., \overline{k}_n, \overline{l})$. Note agora que $((\neg A \vee B) \wedge A) \to B$ também é uma tautologia, logo, de $\mathcal{P} \vdash_{\mathcal{L}_A} \varphi(\overline{k}_1, ..., \overline{k}_n, \overline{m}) \wedge \varphi(\overline{k}_1, ..., \overline{k}_n, \overline{l})$ e de $\mathcal{P} \vdash_{\mathcal{L}_A} \varphi(\overline{k}_1, ..., \overline{k}_n, \overline{l})$ segue que $\mathcal{P} \vdash_{\mathcal{L}_A} \neg\varphi(\overline{k}_1, ..., \overline{k}_n, \overline{m})$. □

Não é difícil ver que toda função fortemente representável é, também, representável. O surpreendente é que a definição de função fortemente representável, que a priori parece mais restritiva, é, na verdade, equivalente à de função representável, como veremos a seguir.

Proposição 5.14 *Seja T uma teoria na linguagem $\mathcal{L}_A$. Uma função de números naturais é representável em T se, e somente se, é fortemente representável em T.*

[1]A fórmula $\exists! x\varphi(x)$ é uma abreviação de "existe um único x satisfazendo φ", isto é, de $\exists x\varphi(x) \wedge \forall x \forall y((\varphi(x) \wedge \varphi(y)) \to x = y)$.

Demonstração: ($\Leftarrow$) Basta aplicar a regra UI para cada numeral $\overline{k}_1, ..., \overline{k}_n$.

($\Rightarrow$) Seja $f(x_1, ..., x_n)$ uma função representável em T pela fórmula $\mathcal{F}(x_1, ..., x_n, y)$. Vejamos que f é fortemente representável em T pela fórmula $\mathcal{C}(x_1, ..., x_n, y)$ dada por

$$((\exists! z \mathcal{F}(x_1, ..., x_n, z)) \wedge \mathcal{F}(x_1, ..., x_n, y)) \vee (\neg(\exists! z \mathcal{F}(x_1, .., x_n, z)) \wedge y = 0).$$

Para verificar que $\mathcal{C}$ satisfaz a condição (1) da definição de fortemente representável, considere $k_1, ..., k_n, m$ números naturais tais que $f(k_1, ..., k_n) = m$. Como $\mathcal{F}$ representa f segue que $T \vdash_{\mathcal{L}_\mathcal{A}} \mathcal{F}(\overline{k}_1, ..., \overline{k}_n, \overline{m})$ e $T \vdash_{\mathcal{L}_\mathcal{A}} \exists! y \mathcal{F}(\overline{k}_1, ..., \overline{k}_n, y)$. Por uma conjunção destas duas sentenças e uma disjunção com a fórmula $\neg(\exists! y \mathcal{F}(\overline{k}_1, ..., \overline{k}_n, y)) \wedge \overline{m} = 0$, teremos que $T \vdash_{\mathcal{L}_\mathcal{A}} \mathcal{C}(\overline{k}_1, ..., \overline{k}_n, \overline{m})$.

Para a condição (2′) da definição de fortemente representável, precisamos mostrar que $T \vdash_{\mathcal{L}_\mathcal{A}} \forall x_1 ... \forall x_n \exists! y \mathcal{C}(x_1, ..., x_n, y)$. Para tal, é suficiente mostrar $T \vdash_{\mathcal{L}'_\mathcal{A}} \exists! y \mathcal{C}(a_1, ..., a_n, y)$ onde $a_1, ..., a_n$ são constantes que não estão em $\mathcal{L}_\mathcal{A}$ e $\mathcal{L}'_\mathcal{A} = \mathcal{L}_\mathcal{A} \cup \{a_1, ..., a_n\}$, podemos aplicar UG n vezes e obter $T \vdash_{\mathcal{L}_\mathcal{A}} \forall x_1 ... \forall x_n \exists! y \mathcal{C}(x_1, ..., x_n, y)$.

Note agora que, para quaisquer sentenças A e B, a sentença $((A \to B) \wedge (\neg A \to B)) \to B$ é uma tautologia. Sendo assim, tomando A como a sentença $\exists! y \mathcal{F}(a_1, ..., a_n, y)$ e B como a sentença $\exists! y \mathcal{C}(a_1, ..., a_n, y)$, mostraremos que $T \vdash_{\mathcal{L}'_\mathcal{A}} A \to B$ e que $T \vdash_{\mathcal{L}'_\mathcal{A}} \neg A \to B$, e disto podemos inferir $T \vdash_{\mathcal{L}'_\mathcal{A}} \exists! y \mathcal{C}(a_1, ..., a_n, y)$.

(i) $T \vdash_{\mathcal{L}'_\mathcal{A}} (A \to B)$: de fato, para mostrar $T \vdash_{\mathcal{L}'_\mathcal{A}} \exists! y \mathcal{F}(a_1, ..., a_n, y) \to \exists! y \mathcal{C}(a_1, ..., a_n, y)$, pelo Teorema da Dedução basta mostrar que $T \cup \{\exists! y \mathcal{F}(a_1, ..., a_n, y)\} \vdash_{\mathcal{L}'_\mathcal{A}} \exists! y \mathcal{C}(a_1, ..., a_n, y)$. E por EI, para mostrar $T \cup \{\exists! y \mathcal{F}(a_1, ..., a_n, y)\} \vdash_{\mathcal{L}'_\mathcal{A}} \exists! y \mathcal{C}(a_1, ..., a_n, y)$ é suficiente mostrar $T'' := T \cup \{\exists! y \mathcal{F}(a_1, ..., a_n, y), \mathcal{F}(a_1, ..., a_n, b)\} \vdash_{\mathcal{L}''_\mathcal{A}} \exists! y \mathcal{C}(a_1, ..., a_n, y)$, onde b é uma constante que não está em $\mathcal{L}'_\mathcal{A}$ e $\mathcal{L}''_\mathcal{A} = \mathcal{L}'_\mathcal{A} \cup \{b\}$.

Como $\exists! y \mathcal{F}(a_1, ..., a_n, y)$ e $\mathcal{F}(a_1, ..., a_n, b)$ são sentenças de T'', temos que $T'' \vdash_{\mathcal{L}''_\mathcal{A}} \exists! y \mathcal{F}(a_1, ..., a_n, y) \wedge \mathcal{F}(a_1, ..., a_n, b)$. Logo, $T'' \vdash_{\mathcal{L}''_\mathcal{A}} \mathcal{C}(a_1, ..., a_n, b)$, e por EG e o Teorema 3.13 segue que $T'' \vdash_{\mathcal{L}''_\mathcal{A}} \exists y \mathcal{C}(a_1, ..., a_n, y)$.

Para a unicidade, queremos mostrar que $T'' \vdash_{\mathcal{L}''_\mathcal{A}} \forall u \forall v (\mathcal{C}(a_1, ..., a_n, u) \wedge \mathcal{C}(a_1, ..., a_n, v)) \to u = v$. Por UG basta mostrar que $T'' \vdash_{\mathcal{L}'''_\mathcal{A}} (\mathcal{C}(a_1, ..., a_n, c_1) \wedge \mathcal{C}(a_1, ..., a_n, c_2)) \to c_1 = c_2$, onde c_1 e c_2 são constantes que não estão em $\mathcal{L}''_\mathcal{A}$ e $\mathcal{L}'''_\mathcal{A} = \mathcal{L}''_\mathcal{A} \cup \{c_1, c_2\}$. Por fim, pelo Teorema da Dedução basta mostrar que $T''' := T'' \cup \{\mathcal{C}(a_1, ..., a_n, c_1) \wedge \mathcal{C}(a_1, ..., a_n, c_2)\} \vdash_{\mathcal{L}'''_\mathcal{A}} c_1 = c_2$. O que faremos é mostrar que $T''' \vdash_{\mathcal{L}'''_\mathcal{A}} \mathcal{F}(a_1, ..., a_n, c_1)$, pois de forma análoga teremos $T''' \vdash_{\mathcal{L}'''_\mathcal{A}} \mathcal{F}(a_1, ..., a_n, c_2)$, e como $T''' \vdash_{\mathcal{L}'''_\mathcal{A}} \exists! y \mathcal{F}(a_1, ..., a_n, y)$ teremos que $c_1 = c_2$, como desejado. Sendo assim, note que a fórmula $(((C \wedge D) \vee (\neg C \wedge E)) \wedge C) \to D$ é uma tautologia. Tomando C como a sentença $\exists! y \mathcal{F}(a_1, ..., a_n, y)$, D como a sentença $\mathcal{F}(a_1, ..., a_n, c_1)$ e E a sentença $c_1 = 0$, obtemos que $\mathcal{C}(a_1,...,a_n,c_1)$ é justamente a fórmula $(C \wedge D) \vee (\neg C \wedge E)$, e temos que C é uma sentença de T'''. Desta forma, por Modus Ponens temos que $T''' \vdash_{\mathcal{L}'''_\mathcal{A}} \exists! y \mathcal{F}(a_1,...,a_n,c_1)$, como queríamos.

(ii) $T \vdash_{\mathcal{L}'_\mathcal{A}} (\neg A \to B)$: temos que mostrar que $T \vdash_{\mathcal{L}'_\mathcal{A}} \neg(\exists! y \mathcal{F}(a_1,...,a_n,y)) \to \exists! y \mathcal{C}(a_1, ..., a_n, y)$. Pelo Teorema da Dedução, basta mostrar que

$$T' := T \cup \{\neg(\exists! y \mathcal{F}(a_1,...,a_n,y))\} \vdash_{\mathcal{L}'_\mathcal{A}} \exists! y \mathcal{C}(a_1,...,a_n,y).$$

Para a existência, como $\neg(\exists! y \mathcal{F}(a_1,...,a_n,y))$ é uma sentença de T' então podemos fazer a conjunção com a sentença $0 = 0$ (que é um axioma lógico) e obtemos $T' \vdash_{\mathcal{L}'_\mathcal{A}} \neg(\exists! y \mathcal{F}(a_1,...,a_n,y)) \wedge 0 = 0$. Fazendo a disjunção desta sentença com $\exists! y \mathcal{F}(a_1,...,a_n,y) \wedge \mathcal{F}(a_1,...,a_n,0)$ obtemos em T' uma prova para $\mathcal{C}(a_1,...,a_n, 0)$ e por EG $T' \vdash_{\mathcal{L}'_\mathcal{A}} \exists y \mathcal{C}(a_1,...,a_n,y)$.

Para a unicidade, sejam c_1, c_2 constantes fora de $\mathcal{L}'_\mathcal{A}$ e assuma que seja válido em T' a fórmula $\mathcal{C}(a_1,...,a_n,c_1) \wedge \mathcal{C}(a_1,...,a_n,c_2)$. De forma análoga ao item anterior, note que a fórmula $(((C \wedge D) \vee (\neg C \wedge E)) \wedge \neg C) \to E$ é uma tautologia. Tomando C como a sentença $\exists! y \mathcal{F}(a_1,...,a_n,y)$, D como a sentença $\mathcal{F}(a_1,...,a_n,c_1)$ e E a sentença $c_1 = 0$, obtemos que a fórmula $(C \wedge D) \vee (\neg C \wedge E)$ é justamente $\mathcal{C}(a_1,...,a_n,c_1)$, que podemos inferir de $\mathcal{C}(a_1,...,a_n,u) \wedge \mathcal{C}(a_1,...,a_n,v)$, e temos por hipótese $\neg C$, logo inferimos por Modus Ponens que $c_1 = 0$. De forma análoga conseguimos inferir que $c_2 = 0$. Portanto, $c_1 = c_2$, do que segue a unicidade.

$\square$

No que segue, usaremos as expressões "função representável" e "função fortemente representável" como sinônimos uma da outra.

A noção de relação exprimível se relaciona com a de função representável em uma teoria T na linguagem $\mathcal{L}_\mathcal{A}$ que satisfaz $T \vdash_{\mathcal{L}_\mathcal{A}} 0 \neq \overline{1}$, e tal relação é estabelecida pela função característica de uma relação de números naturais.

Definição 5.15 *Seja $R \subseteq \mathbb{N}^n$ uma relação. Definimos a **função característica** $\chi_R : \mathbb{N}^n \to \mathbb{N}$ de R por*

$$\chi_R(x_1,...,x_n) = \begin{cases} 1, & se\ (x_1,...,x_n) \in R \\ 0, & caso\ contrário. \end{cases}$$

Proposição 5.16 *Seja T uma teoria na linguagem $\mathcal{L}_\mathcal{A}$ tal que $T \vdash_{\mathcal{L}_\mathcal{A}} 0 \neq \overline{1}$. Uma relação de números naturais é exprimível em T se, e somente se, sua função característica é representável em T.*

Demonstração: ($\Rightarrow$) Sejam R uma relação n-ária de números naturais exprimível em T e $\varphi(x_1, ..., x_n)$ uma fórmula que a exprime. Mostraremos que a fórmula $\psi(x_1, ..., x_n, y)$ dada por $(\varphi(x_1, ..., x_n) \wedge y = \overline{1}) \vee (\neg\varphi(x_1, ..., x_n) \wedge y = 0)$ representa χ_R. Sejam $k_1, ..., k_n$ naturais quaisquer. Se $\chi_R(k_1, ..., k_n) = 0$, então $(k_1, ..., k_n) \notin R$. Como φ exprime R, segue que $T \vdash_{\mathcal{L}_A} \neg\varphi(\overline{k_1}, ..., \overline{k_n})$. Como $T \vdash_{\mathcal{L}_A} 0 = 0$, logo $T \vdash_{\mathcal{L}_A} \neg\varphi(\overline{k_1}, ..., \overline{k_n}) \wedge 0 = 0$. Como $A \to (A \vee B)$ é uma tautologia para quaisquer sentenças A e B, temos que $T \vdash_{\mathcal{L}_A} (\varphi(\overline{k_1}, ..., \overline{k_n}) \wedge 0 = \overline{1}) \vee (\neg\varphi(\overline{k_1}, ..., \overline{k_n}) \wedge 0 = 0)$, isto é, $T \vdash_{\mathcal{L}_A} \psi(\overline{k}_1, ..., \overline{k}_n, 0)$. Se $\chi_R(k_1, ..., k_n) = 1$ obtemos, de forma análoga, que vale $T \vdash_{\mathcal{L}_A} \psi(\overline{k}_1, ..., \overline{k}_n, \overline{1})$.

Com o desenvolvimento acima mostramos que $T \vdash_{\mathcal{L}_A} \exists y(\psi(\overline{k}_1, ..., \overline{k}_n, y))$. Resta, então, mostrar a unicidade, ou seja, que $T \vdash_{\mathcal{L}_A} \forall u \forall v((\psi(\overline{k}_1, ..., \overline{k}_n, u) \wedge \psi(\overline{k}_1, ..., \overline{k}_n, v)) \to u = v)$. Faremos apenas o caso em que $\chi_R(k_1, ..., k_n) = 1$, já que o outro caso é tratado de forma análoga. Pelo Teorema da Dedução e UG, basta mostrar que $T' := T \cup \{\psi(\overline{k}_1, ..., \overline{k}_n, a) \wedge \psi(\overline{k}_1, ..., \overline{k}_n, b)\} \vdash_{\mathcal{L}'_A} a = b$ onde a e b são constantes que não estão em $\mathcal{L}_A$ e $\mathcal{L}'_A = \mathcal{L}_A \cup \{a, b\}$.

Sabemos que, para quaisquer fórmulas A, B e C, a fórmula $(((A \wedge B) \vee (\neg A \wedge C)) \wedge A) \to B$ é uma tautologia. Tomando A como $\varphi(\overline{k}_1, ..., \overline{k}_n)$, B como $a = \overline{1}$ e C como $a = \overline{0}$ temos que a sentença $(A \wedge B) \vee (\neg A \wedge C)$ é justamente $\psi(\overline{k}_1, ..., \overline{k}_n, \overline{a})$, que é um elemento de T'. Como $\chi_R(k_1, ..., k_n) = 1$, vale $T' \vdash_{\mathcal{L}'} \varphi(\overline{k}_1, ..., \overline{k}_n)$, isto é, vale A. Inferimos, portanto, que vale B em T', isto é, $T' \vdash_{\mathcal{L}'_A} a = \overline{1}$. De forma análoga mostramos que $T' \vdash_{\mathcal{L}'_A} b = \overline{1}$ e, portanto, $T' \vdash_{\mathcal{L}'_A} a = b$, como queríamos.

($\Leftarrow$) Seja R uma relação n-ária de números naturais cuja função característica χ_R é representável pela fórmula $\psi(x_1, ..., x_n, y)$. Vejamos que a fórmula $\varphi(x_1, ..., x_n)$ dada por $\psi(x_1, ..., x_n, \overline{1})$ exprime R. Dados $k_1, ..., k_n$ naturais, suponha que $(k_1, ..., k_n) \in R$. Logo, $\chi_R(k_1, ..., k_n) = 1$. Como ψ representa χ_R temos que $T \vdash_{\mathcal{L}_A} \psi(\overline{k_1}, ..., \overline{k_n}, \overline{1})$ assim, $T \vdash_{\mathcal{L}_A} \varphi(\overline{k_1}, ..., \overline{k_n})$ e, portanto, a condição (1) da definição de relação exprimível se verifica.

Suponha agora que $(k_1, ..., k_n) \notin R$. Logo $\chi_R(k_1, ..., k_n) = 0$ e como ψ representa χ_R, segue que $T \vdash_{\mathcal{L}_A} \psi(\overline{k_1}, ..., \overline{k_n}, 0)$. Pela unicidade de ψ temos que $T \vdash_{\mathcal{L}_A} \forall x \forall y((\psi(\overline{k_1}, ..., \overline{k_n}, x) \wedge \psi(\overline{k_1}, ..., \overline{k_n}, y)) \to x = y)$. Note que a fórmula $(((A \wedge B) \to C) \wedge \neg C \wedge A) \to \neg B$ é uma tautologia. Tomando A como a sentença $\psi(\overline{k_1}, ..., \overline{k_n}, 0)$, B como a sentença $\psi(\overline{k_1}, ..., \overline{k_n}, \overline{1})$ e C como $0 = \overline{1}$ temos por UI que $T \vdash_{\mathcal{L}_A} (A \wedge B) \to C$ e, por hipótese, $T \vdash_{\mathcal{L}_A} \neg C$. Desta forma inferimos pela tautologia anteriormente citada que vale $T \vdash_{\mathcal{L}_A} \neg B$, isto é, $T \vdash_{\mathcal{L}_A} \neg\varphi(\overline{k}_1, ..., \overline{k}_n)$, como queríamos. $\square$

5.3 Funções e relações recursivas

Definição 5.17 *Uma **função inicial** é uma função de números naturais de um dos seguintes tipos:*

1. *A **função nula** $z(x) = 0$ para todo x.*

2. *A **função sucessor** $S(x) = x + 1$ para todo x.*

3. *A **i-ésima projeção** $p_i^n(x_1, ..., x_n) = x_i$ para quaisquer $x_1, ..., x_n$.*

Considere as seguintes regras para obter novas funções de números naturais a partir de funções dadas:

I. ***Substituição**. Dadas as funções de números naturais $g(y_1, ..., y_m), h_1(x_1, ..., x_n), ...,$ $h_m(x_1, ..., x_n)$, dizemos que a função $f : \mathbb{N}^n \to \mathbb{N}$ dada por*

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

é obtida a partir de $g, h_1, \ldots, h_m$ por substituição.

II. ***Recursão**. Dadas as funções de números naturais $g(x_1, ..., x_n), h(y_1, ..., y_n, y_{n+1}, y_{n+2})$, dizemos que a função $f : \mathbb{N}^{n+1} \to \mathbb{N}$ dada por*

$$f(x_1, ..., x_n, 0) = g(x_1, ..., x_n)$$

$$f(x_1, ..., x_n, y + 1) = h(x_1, ..., x_n, y, f(x_1, ..., x_n, y))$$

é obtida a partir de g e h por recursão.

III. ***Operador de minimização restrito**. Seja $g(x_1, ..., x_n, y)$ uma função de números naturais tal que, para quaisquer $x_1, ..., x_n$, existe y satisfazendo $g(x_1, ..., x_n, y) = 0$. Denotaremos por $\mu y(g(x_1, ..., x_n, y) = 0)$ o menor y tal que $g(x_1, ..., x_n, y) = 0$. Dizemos que a função $f : \mathbb{N}^n \to \mathbb{N}$ dada por*

$$f(x_1, ..., x_n) = \mu y(g(x_1, ..., x_n, y) = 0)$$

é obtida a partir de g pelo operador de minimização restrito.

*Uma função de números naturais é dita **primitiva recursiva** se puder ser obtida a partir das funções iniciais por meio de finitas substituições e recursões, e é dita **recursiva** quando puder ser obtida a partir das funções iniciais por meio de finitas substituições, recursões e aplicações do operador de minimização restrito.*

Segue imediatamente da definição acima que toda função primitiva recursiva é, em particular, recursiva.

Veremos alguns exemplos de funções primitivas recursivas e recursivas no Exemplo 5.19, mas antes demonstraremos um resultado que irá nos auxiliar.

Proposição 5.18 *Seja $g(y_1,...,y_k)$ uma função primitiva recursiva. Sejam ainda $x_1,...,x_n$ variáveis duas a duas distintas, e para cada $i \in \{1,...,k\}$ seja $z_i \in \{x_1,...,x_n\}$. Então a função f dada por $f(x_1,...,x_n) = g(z_1,...,z_k)$ é primitiva recursiva.*

Demonstração: Note que $z_i = x_{j_i}$ para algum $j_i \in \{1,...,n\}$. Assim $z_i = p^n_{j_i}(x_1,...,x_n)$. Então

$$f(x_1,...,x_n) = g(p^n_{j_1}(x_1,...,x_n),...,p^n_{j_k}(x_1,...,x_n)).$$

Disto segue que f é primitiva recursiva, pois é obtida por substituição a partir de g, que é primitiva recursiva, e das projeções. □

Do resultado anterior segue que podemos permutar a ordem das variáveis de uma função sem afetar sua recursividade. Por exemplo, se tivermos $g(x_1,x_2)$ primitiva recursiva, então $f(x_1,x_2) = g(x_2,x_1)$ é primitiva recursiva — basta tomar $z_1 = x_2$ e $z_2 = x_1$ na Proposição 5.18. Podemos também adicionar variáveis extras a uma função primitiva recursiva e manter a recursividade. Por exemplo, se tivermos $g(x_1,x_2)$ primitiva recursiva, então $f(x_1,x_2,x_3) = g(x_1,x_2)$ também é primitiva recursiva — basta tomar $z_1 = x_2$ e $z_2 = x_3$ na Proposição 5.18. E ainda, reduzir o número de variáveis também mantém a recursividade. Por exemplo, se $g(x_1,x_2,x_3) = x_1 + 2x_2 + 3x_3$ é primitiva recursiva, então $f(x_1,x_2) = g(x_1,x_2,x_1) = 4x_1 + 2x_2$ também é primitiva recursiva — basta tomar $z_1 = x_1, z_2 = x_2$ e $z_3 = x_1$ na Proposição 5.18.

Exemplo 5.19 *As seguintes funções são primitivas recursivas.*

1. *A função zero $Z(x_1,...,x_n) = 0$.*

2. *A função constante $C^n_k(x_1,...,x_n) = k$.*

3. *A função identidade $i(x) = x$.*

4. *A função soma $f(x,y) = x + y$.*

5. *A função multiplicação $g(x,y) = x \cdot y$.*

6. *A função exponenciação $e(x,y) = x^y$.*

7. *A função predecessor* $\delta(x) = \begin{cases} x-1, & se\ x > 0 \\ 0, & se\ x = 0 \end{cases}$

8. *A função* $x \dot{-} y = \begin{cases} x-y, & se\ x \geq y \\ 0, & se\ x < y \end{cases}$

9. *A função* $|x-y| = \begin{cases} x-y, & se\ x \geq y \\ y-x, & se\ x < y \end{cases}$

10. *A função* $sg(x) = \begin{cases} 0, & se\ x = 0 \\ 1, & se\ x \neq 0 \end{cases}$

11. *A função* $\overline{sg}(x) = \begin{cases} 1, & se\ x = 0 \\ 0, & se\ x \neq 0 \end{cases}$

12. *A função* $\min(x, y)$

13. *A função* $\min(x_1, ..., x_n)$

14. *A função* $rd(x, y)$ *que retorna o resto da divisão de* y *por* x *quando* $x \neq$ *e retorna* 0 *se* $x = 0$.

15. *A função* $qt(x, y)$ *que retorna o quociente da divisão de* y *por* x *quando* $x \neq$ *e retorna* 0 *se* $x = 0$.

Demonstração:

1. Basta aplicar a Proposição 5.18 na função nula e tomar $z_1 = x_1$, e teremos $Z(x_1, ..., x_n) = z(x_1)$.

2. Mostraremos o resultado por indução em k. Se $k = 0$, então $C_0(x_1, ..., x_n) = 0 = Z(x_1, ..., x_n)$, e segue do item anterior que C_0 é primitiva recursiva. Suponha agora que C_k^n é primitiva recursiva para $k \geq 0$. Note que $C_{k+1}^{n(x_1,...,x_n)} = S(C_k^n(x_1, ..., x_n))$. Como S é primitiva recursiva, segue, por substituição, que C_{k+1}^n é primitiva recursiva.

3. Basta notar que $i(x) = p_1^1(x)$, onde p_1^1 é a projeção na primeira (e única) coordenada.

4. Basta notar que:

$$f(x,0) = x = p_1^1(x),$$
$$f(x,y+1) = x + (y+1) = S(x+y).$$

Como p_1^1 e S são funções primitivas recursivas, segue por recursão que f é primitiva recursiva.

5. Basta notar que:

$$g(x,0) = 0 = z(x),$$
$$g(x,y+1) = x \cdot (y+1) = x \cdot y + x = f(g(x,y),x),$$

onde f denota a função soma definida no item anterior. Como f e z são funções primitivas recursivas, segue por recursão e substituição que g é primitiva recursiva.

6. Basta notar que:

$$e(x,0) = 1 = C_1(x),$$
$$e(x,y+1) = x^{y+1} = x^y \cdot x = e(x,y) \cdot i(x).$$

onde C_1^1 denota a função constante igual a 1 e i denota a função identidade. Como C_1, i e a multiplicação são funções primitivas recursivas, segue por recursão e substituição que e é primitiva recursiva.

7. Basta notar que:

$$\delta(0) = 0 = z(0),$$
$$\delta(y+1) = y = i(y).$$

Como z e i são funções primitivas recursivas, segue por recursão que δ é primitiva recursiva.

8. Basta notar que:

$$x \dot{-} 0 = x - 0 = x = i(x),$$
$$x \dot{-} y + 1 = \delta(x \dot{-} y).$$

Como δ e i são funções primitivas recursivas, segue por recursão que δ é primitiva recursiva.

9. Basta notar que:

$$|x - y| = (x \dot{-} y) + (y \dot{-} x).$$

Como as funções $\dot{-}$ e $+$ são primitivas recursivas, segue, por substituição, que $|\cdot|$ é uma função primitiva recursiva.

10. Basta notar que:

$$sg(x) = x \dot{-} \delta(x).$$

Como as funções $\dot{-}$ e i são primitivas recursivas, segue, por substituição, que sg é uma função primitiva recursiva.

11. Basta notar que:

$$sg(x) = 1 \dot{-} sg(x).$$

Como as funções $\dot{-}$, sg e C_1^1 são primitivas recursivas, segue, por substituição, que $\overline{sg}$ é uma função primitiva recursiva.

12. Basta notar que $\min(x, y) = x \dot{-} (x \dot{-} y)$. Como $\dot{-}$ e p_1^2 são funções primitivas recursivas, segue, por substituição, que min é primitiva recursiva.

13. Mostraremos o resultado por indução em n. Para $n = 2$ o resultado vale pelo item anterior. Suponha agora que $\min(x_1, ..., x_n)$ seja primitiva recursiva. Note que

$$\min(x_1, ..., x_n, x_{n+1}) = \min(\min(x_1, ..., x_n), x_{n+1}).$$

Pela hipótese de indução, pelo item anterior, pois p_{n+1}^{n+1} é primitiva recursiva e por substituição segue que $\min(x_1, ..., x_n, x_{n+1})$ é primitiva recursiva.

14. Note primeiro que $rd(x, 0) = 0$. E ainda, sejam q e r naturais tais que $0 \leq r < x$ e $y = x \cdot q + r$. Então temos que $y + 1 = x \cdot q + r + 1$. Como $r < x$ então $r + 1 \leq x$. Assim há duas possibilidades: ou $r + 1 < x$, e neste caso o resto da divisão de $y + 1$ por x é $r + 1$; ou $r + 1 = x$, e neste caso o resto da divisão de $y + 1$ por x é

0. Com isto, temos que:

$$rd(x, y+1) = \mathrm{S}(rd(x, y)) \cdot sg(|x - \mathrm{S}(rd(x, y))|).$$

Como S, rd, sg, p_1^2 e $|\cdot|$ e a multiplicação são funções primitivas recursivas, segue, por recursão e substituição, que rd é primitiva recursiva.

15. Note primeiro que $qt(x, 0) = 0$. Como no caso anterior, dados naturais x e y, existem q e r naturais tais que $0 \leq r < x$ e $y = x \cdot q + r$. Como $y + 1 = x \cdot q + r + 1$ então, se $r + 1 < x$ então o quociente da divisão de $y + 1$ por x é q, e se $r + 1 = x$ então o quociente da divisão de $y + 1$ por x é $q + 1$. Com isto, temos que:

$$qt(x, y+1) = qt(x, y) + \overline{sg}(|x - \mathrm{S}(rd(x, y))|).$$

Como S, $\overline{sg}$, $|\cdot|$, rd e p_1^2 e a soma são funções primitivas recursivas, segue, por recursão e substituição, que qt é primitiva recursiva. $\square$

Vejamos outros exemplos de construção de funções primitivas recursivas e recursivas.

Teorema 5.20 *Dada uma função $f(x_1, .., x_n, y)$ primitiva recursiva, as seguintes funções também são primitivas recursivas:*

1. $\sum_{y<z} f(x_1, ..., x_n, y) = \begin{cases} 0, & se\ z = 0 \\ f(x_1, ..., x_n, 0) + ... + f(x_1, ..., x_n, z-1), & se\ z > 0 \end{cases}$
2. $\sum_{y \leq z} f(x_1, ..., x_n, y) = \sum_{y<z+1} f(x_1, ..., x_n, y)$
3. $\prod_{y<z} f(x_1, ..., x_n, y) = \begin{cases} 1, & se\ z = 0 \\ f(x_1, ..., x_n, 0) \cdot ... \cdot f(x_1, ..., x_n, z-1), & se\ z > 0 \end{cases}$
4. $\prod_{y \leq z} f(x_1, ..., x_n, y) = \prod_{y<z+1} f(x_1, ..., x_n, y)$

Demonstração:

1. Considere $g(x_1, ..., x_n, z) = \sum_{y<z} f(x_1, ..., x_n, y)$. Então g pode ser definida recursivamente da seguinte forma:

$$\begin{aligned} g(x_1, ..., x_n, 0) &= 0 \\ g(x_1, ..., x_n, z+1) &= g(x_1, ..., x_n, z) + f(x_1, ..., x_n, z). \end{aligned}$$

Assim, por recursão e substituição, segue que g é primitiva recursiva.

2. Considere $h(x_1, ..., x_n, z) = \sum_{y \leq z} f(x_1, ..., x_n, y)$ e note que:

$$h(x_1, ..., x_n, z) = g(x_1, ..., x_n, z+1).$$

Assim, por substituição e pelo item anterior, segue que g é primitiva recursiva.

3. Considere $g(x_1, ..., x_n, z) = \prod_{y<z} f(x_1, ..., x_n, y)$. Então g pode ser definida recursivamente da seguinte forma:

$$\begin{aligned} g(x_1, ..., x_n, 0) &= 1 \\ g(x_1, ..., x_n, z+1) &= g(x_1, ..., x_n, z) \cdot f(x_1, ..., x_n, z). \end{aligned}$$

Assim, por recursão e substituição, segue que g é primitiva recursiva.

4. Considere $h(x_1, ..., x_n, z) = \prod_{y \leq z} f(x_1, ..., x_n, y)$ e note que:

$$h(x_1, ..., x_n, z) = g(x_1, ..., x_n, z+1).$$

Assim, por substituição, segue que h é primitiva recursiva. □

Exemplo 5.21 *Seja $\tau(x)$ a quantidade de divisores de x, se $x > 0$, e $\tau(0) = 1$. A função τ é primitiva recursiva. De fato, basta notar que $\tau(x) = \sum_{y \leq x} \overline{sg}(rd(y, x))$, e dos Teoremas 5.19 e 5.20 segue que τ é primitiva recursiva.*

Definição 5.22 *Uma relação n-ária de números naturais é dita **primitiva recursiva** (respectivamente, **recursiva**) quando sua função característica é primitiva recursiva (respectivamente, recursiva).*

Teorema 5.23 *As seguintes relações são primitivas recursivas:*

1. *A relação de igualdade: $x_1 = x_2$.*

2. *A relação "menor que": $x_1 < x_2$.*

3. *A relação de divisibilidade: $x_1 \mid x_2$.*

4. *A relação unária $Pr(x)$: x é um número primo.*

Demonstração:

1. Basta notar que a função característica da relação de igualdade $x_1 = x_2$ pode ser escrita como $\overline{sg}(|x_1 - x_2|)$, que é primitiva recursiva pelo Teorema 5.19.

2. Note que $x_1 < x_2$ se e somente se $x_2 - x_1 > 0$. Assim, a função característica de tal relação pode ser escrita como $sg(x_2 \dot{-} x_1)$, que é primitiva recursiva pelo Teorema 5.19.

3. Note que $x_1 \mid x_2$ se e somente se o resto da divisão de x_2 por x_1 é 0. Assim, a função característica de tal relação pode ser escrita como $\overline{sg}(rd(x_1, x_2))$, que é primitiva recursiva pelo Teorema 5.19.

4. Note que x é um número primo se, e somente se, x possui exatamente 2 divisores: 1 e x. Desta forma, a função característica da relação $\mathrm{Pr}(x)$ é dada por $\overline{sg}(|\tau(x) - 2|)$. Logo, do Teorema 5.19 e do Exemplo 5.21, segue que Pr é uma relação primitiva recursiva. □

Teorema 5.24 *Se $R_1(x_1, ..., x_n)$ e $R_2(y_1, ..., y_m)$ são relações primitivas recursivas, então as seguintes relações também são primitivas recursivas:*

1. $\neg R_1(x_1, ..., x_n)$;

2. $R_1(x_1, ..., x_n) \wedge R_2(y_1, ..., y_m)$;

3. $R_1(x_1, ..., x_n) \vee R_2(y_1, ..., y_m)$.

Demonstração: Como R_1 e R_2 são relações primitivas recursivas, χ_{R_1} e χ_{R_2} são funções primitivas recursivas.

1. Basta notar que $\chi_{\neg R_1}(x_1, ..., x_n) = 1 \dot{-} \chi_{R_1}(x_1, ..., x_n)$, e como χ_{R_1}, $\dot{-}$ e C_1^n são primitivas recursivas, segue que $\chi_{\neg R_1}$ é primitiva recursiva, e portanto $\neg R_1$ é uma relação primitiva recursiva.

2. Basta notar que $\chi_{R_1 \wedge R_2}(x_1, ..., x_n) = \chi_{R_1}(x_1, ..., x_n) \cdot \chi_{R_2}(x_1, ..., x_n)$, e como χ_{R_1}, χ_{R_2} e a multiplicação são funções primitivas recursivas, segue que $\chi_{R_1 \wedge R_2}$ é primitiva recursiva, e portanto $R_1 \wedge R_2$ é uma relação primitiva recursiva.

3. Basta notar que $\chi_{R_1 \vee R_2}(x_1, ..., x_n) = 1 \dot{-} (\chi_{\neg R_1}(x_1, ..., x_n) \cdot \chi_{\neg R_2}(x_1, ..., x_n))$, e como χ_{R_1}, χ_{R_2}, a multiplicação e, pelo item 1, a função característica da negação são funções primitivas recursivas, segue que $\chi_{R_1 \wedge R_2}$ é primitiva recursiva, e portanto $R_1 \vee R_2$ é uma relação primitiva recursiva. □

Teorema 5.25 *Se $A \subseteq \mathbb{N}$ é um conjunto finito, então a relação unária A é primitiva recursiva.*

Demonstração: Seja $A = \{a_1, \ldots, a_n\}$. Do Teorema 5.18 e do item 1 do Teorema 5.23, as relações $x = a_i$ são primitivas recursivas, para cada $i \in \{1, ..., n\}$. Disto e do item 3 do Teorema 5.24, aplicado $n - 1$ vezes, segue que $x = a_1 \vee x = a_2 \vee \ldots \vee x = a_n$ é uma relação primitiva recursiva. Basta notar agora que x é um elemento de A se, e somente se, $x = a_1 \vee x = a_2 \vee \ldots \vee x = a_n$. □

Teorema 5.26 *Se $R(x_1, ..., x_n, y)$ é uma relação primitiva recursiva então as seguintes relações, denominadas relações com quantificadores limitados, são primitivas recursivas:*

1. $(\exists y)_{y<z} R(x_1, ..., x_n, y)$;
2. $(\exists y)_{y \leq z} R(x_1, ..., x_n, y)$;
3. $(\forall y)_{y<z} R(x_1, ..., x_n, y)$;
4. $(\forall y)_{y \leq z} R(x_1, ..., x_n, y)$.

Demonstração:

1. Definindo a relação $S(x_1, ..., x_n, z)$ como $(\exists y)_{y<z} R(x_1, ..., x_n, y)$, basta notar que $\chi_S(x_1, ..., x_n, z) = \mathrm{sg}(\sum_{y<z} \chi_R(x_1, ..., x_n, y))$. Por hipótese $\chi_R(x_1, ..., x_n, y)$ é uma função primitiva recursiva, assim, o resultado segue do Teorema 5.20.

2. Definindo a relação $S(x_1, ..., x_n, z)$ como $(\exists y)_{y \leq z} R(x_1, ..., x_n, y)$, basta notar que $\chi_S(x_1, ..., x_n, z) = \mathrm{sg}(\sum_{y \leq z} \chi_R(x_1, ..., x_n, y))$, assim, o resultado segue do Teorema 5.20.

3. Definindo a relação $S(x_1, ..., x_n, z)$ como $(\forall y)_{y<z} R(x_1, ..., x_n, y)$, basta notar que $\chi_S(x_1, ..., x_n, z) = \mathrm{sg}(\prod_{y<z} \chi_R(x_1, ..., x_n, y))$, assim, o resultado segue do Teorema 5.20.

4. Definindo a relação $S(x_1, ..., x_n, z)$ como $(\forall y)_{y \leq z} R(x_1, ..., x_n, y)$, basta notar que $\chi_S(x_1, ..., x_n, z) = \mathrm{sg}(\prod_{y \leq z} \chi_R(x_1, ..., x_n, y))$, assim, o resultado segue do Teorema 5.20. □

Teorema 5.27 *A função $f(x_1, ..., x_n)$ é recursiva se, e somente se, a relação $R(x_1, \ldots, x_n, y)$ dada por $f(x_1, ..., x_n) = y$ é uma relação recursiva.*

Demonstração: $(\Rightarrow)$ Note que $\chi_R(x_1, ..., x_n, y) = \overline{sg}(|f(x_1, ..., x_n) \dot{-} y|)$. Como f é recursiva, segue do Teorema 5.19 que χ_R é recursiva, e portanto a relação $R(x_1, \ldots, x_n, y)$ é recursiva.

($\Leftarrow$) Se R é uma relação recursiva, do item 1 do Teorema 5.24 segue que $\neg R$ é uma relação recursiva. Note agora que $f(x_1,...,x_n) = \mu y(\chi_{\neg R}(x_1,...,x_n,y) = 0)$ e, portanto, f é recursiva. $\square$

Teorema 5.28 *Se $R(x_1,...,x_n,y)$ é uma relação primitiva recursiva, então a seguinte função, obtida por meio da aplicação do operador de minimização limitado, é primitiva recursiva:*

$$\mu y_{y<z}R(x_1,...,x_n,y) = \begin{cases} \textit{o menor } y < z \textit{ satisfazendo } R(x_1,...,x_n,y), & \textit{se um tal } y \textit{ existir} \\ z, & \textit{caso contrário.} \end{cases}$$

Demonstração: Fixe $y < z$. Note que $\prod_{u\leq y}\chi_{\neg R}(x_1,...,x_n,u)$ vale 1 quando $R(x_1,...,x_n,u)$ não é satisfeita para nenhum $u \leq y$, e vale 0 caso exista ao menos um $u \leq y$ tal que $R(x_1,...,x_n,u)$ vale. Assim, $\sum_{y<z}(\prod_{u\leq y}\chi_{\neg R}(x_1,...,x_n,u))$ fornece a quantidade de naturais $y < z$ tais que não vale $R(x_1,...,x_n,u)$ para nenhum $u \leq y$. Portanto $\sum_{y<z}(\prod_{u\leq y}\chi_{\neg R}(x_1,...,x_n,u))$ é igual a $\mu y_{y<z}R(x_1,...,x_n,y)$. Do Teorema 5.20 segue que $\mu y_{y<z}R(x_1,...,x_n,y)$ é primitiva recursiva. $\square$

Teorema 5.29 *Seja $R(x_1,...,x_n,y)$ uma relação recursiva. Se, para quaisquer números naturais $x_1,...,x_n$, é possível encontrar um natural y tal que vale $R(x_1,...,x_n,y)$, então a função $f(x_1,...,x_n) = \mu yR(x_1,...,x_n,y)$ é recursiva.*

Demonstração: Note que um tal y satisfaz $\chi_R(x_1,...,x_n,y) = 1$, e portanto satisfaz $\chi_{\neg R}(x_1,...,x_n,y) = 0$. Portanto $f(x_1,...,x_n) = \mu y(\chi_{\neg R}(x_1,...,x_n,y) = 0)$ é recursiva. $\square$

Teorema 5.30 *Denote o x-ésimo número primo por p_x. Valem:*

1. *A função $p(n)$ que associa cada natural n ao n-ésimo número primo é primitiva recursiva.*

2. *Para cada $x > 1$, considere $p_0^{a_0}p_1^{a_1}\dots p_k^{a_k}$ a fatoração de x em fatores primos. Denotaremos por $(x)_j$ o expoente a_j. Para $x = 0$, declaramos $(x)_j = 0$ para todo natural j. E para $x = 1$, fazemos $(x)_j = 1$ para todo natural j. Esta função que mapeia x, j para $(x)_j$ é primitiva recursiva.*

3. *Para cada $x > 0$, designamos por $lh(x)$ o número de expoentes não nulos na fatoração de x por números primos, e definimos $lh(0) = 0$. Esta função é primitiva recursiva.*

4. *Se $x = 2^{a_0}3^{a_1}...p_k^{a_k}$ e $y = 2^{b_0}3^{b_1}...p_m^{b_m}$, então a função **concatenação**, denotada por $*$, é definida da seguinte maneira:*

$$x * y = 2^{a_0}3^{a_1}...p_k^{a_k}p_{k+1}^{b_0}p_{k+2}^{b_1}\cdots p_{k+1+m}^{b_m}.$$

Esta função é primitiva recursiva.

Demonstração:

1. Primeiro afirmamos que para cada número natural n vale $p_{n+1} \leq p_n! + 1$. De fato, fixado n, considere $k = p_n! + 1$. Então $k \geq 2$, logo existe um número primo p tal que $p \mid k$. Note que $p \geq p_i$ para cada $i \in \{1, ..., n\}$, pois caso contrário, teríamos que $p \mid k$ e $p \mid p_n!$, logo $p \mid (k - p_n!) = 1$, o que é uma contradição. Logo $p \geq p_i$, e portanto, $p \geq p_{n+1}$. Assim $p_n! + 1 = k \geq p \geq p_{n+1}$.

   Podemos, então, definir recursivamente a função p_x da seguinte forma:

$$p_0 = 2,$$
$$p_{x+1} = \mu y_{y \leq (p_x)!+1}(p_x < y \wedge \Pr(y)).$$

   Pelo Teorema 5.28 e pelo item 4 do Teorema 5.23 a função $\mu y_{y \leq (p_x)!+1}(p_x < y \wedge \Pr(y)$ é primitiva recursiva, logo segue, por recursão, que $p(x)$ é primitiva recursiva.

2. Se $x = p_0^{a_0} p_1^{a_1} ... p_k^{a_k}$, então

$$(x)_j = \mu y_{y<x}(p_j^y \mid x \wedge \neg(p_j^{y+1} \mid x)).$$

   Pelo item anterior, p_j é uma função primitiva recursiva, logo, $(x)_j$ é primitiva recursiva.

3. Considere a relação $R(x, y)$ dada por $\Pr(y) \wedge y \mid x \wedge x \neq 0$. Note que a função característica de $\neg R(x, y)$ vale 0 exatamente quando y é um número primo que aparece com expoente não nulo na fatoração de x e, portanto, $\overline{\mathrm{sg}}(\chi_{\neg R}(x, y))$ retorna o valor 1 sempre que isto ocorre. Assim, para $x > 0$,

$$\mathrm{lh}(x) = \sum_{y \leq x} \overline{\mathrm{sg}}(\chi_{\neg R}(x, y)).$$

4. Basta notar que

$$x * y = x \cdot (\prod_{j < \mathrm{lh}(y)} (p_{\mathrm{lh}(x)+j})^{(y)_j}).$$

□

Definição 5.31 *Dada $f(x_1, \ldots, x_n, y)$ uma função de números naturais, defina*

$$f\#(x_1, ..., x_n, y) = \prod_{u<y} p_u^{f(x_1, ..., x_n, u)}.$$

Note que $f(x_1,...,x_n,y) = (f\#(x_1,...,x_n,y+1))_y$.

Teorema 5.32 *Se $h(x_1,...,x_n,y,z)$ é uma função primitiva recursiva e*

$$f(x_1,...,x_n,y) = h(x_1,...,x_n,y,f\#(x_1,...,x_n,y)),$$

então f é primitiva recursiva.

Demonstração: Note que:

$$\begin{aligned} f\#(x_1,...,x_n,0) &= \prod_{u<0} p_u^{f(x_1,...,x_n,u)} = 1, \\ f\#(x_1,...,x_n,y+1) &= \prod_{u<y+1} p_u^{f(x_1,...,x_n,u)} \\ &= \left(\prod_{u<y} p_u^{f(x_1,...,x_n,u)}\right) \cdot p_y^{f(x_1,...,x_n,y)} \\ &= f\#(x_1,...,x_n,y) \cdot p_y^{f(x_1,...,x_n,y)} \\ &= f\#(x_1,...,x_n,y) \cdot p_y^{h(x_1,...,x_n,f\#(x_1,...,x_n,y))}. \end{aligned}$$

Assim, pela regra de recursão, pela hipótese de h ser primitiva recursiva e pelo Exemplo 5.19, segue que $f\#$ é primitiva recursiva, e como $f(x_1,...,x_n,y) = (f\#(x_1,...,x_n, y+1))_y$, segue que f é primitiva recursiva. □

Teorema 5.33 *Se $H(x_1,...,x_n,y,z)$ é uma relação primitiva recursiva e $R(x_1,...,x_n,y)$ vale exatamente quando $H(x_1,...,x_n,y,(\chi_R)\#(x_1,...,x_n,y))$ vale, onde χ_R é a função característica de R, então R é primitiva recursiva.*

Demonstração: Primeiro note que, como $R(x_1,...,x_n,y)$ vale exatamente quando $H(x_1, ...,x_n,y,(\chi_R)\#(x_1,...,x_n,y))$, então $\chi_\mathrm{R}(x_1,...,x_n,y) = \chi_H(x_1,...,x_n,y,(\chi_\mathrm{R})\#(x_1,...,x_n,y))$. E como a relação H é primitiva recursiva, a função χ_H é primitiva recursiva. Assim, segue do Teorema 5.32 que a função χ_R é primitiva recursiva, e portanto a relação R é primitiva recursiva. □

Encerraremos esta seção mostrando que toda função recursiva é representável em $\mathcal{P}$.

Definição 5.34 *Defina a **função β de Gödel** por $\beta(x_1,x_2,x_3) = rd(1+(x_3+1)\cdot x_2, x_1)$.*

Lema 5.35 *A função β de Gödel é primitiva recursiva e representável em $\mathcal{P}$ pela fórmula $\mathcal{B}t(x_1, x_2, x_3, y)$ dada por*

$$\exists w(x_1 = (1 + (x_3 + 1) \cdot x_2) \cdot w + y \ \wedge \ y < 1 + (x_3 + 1) \cdot x_2).$$

Demonstração: Segue do Exemplo 5.19 que a função é primitiva recursiva. Sejam k_1, k_2, k_3 números naturais. Pelo Teorema 5.7 segue que $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \exists! y \mathcal{B}t(\overline{k}_1, \overline{k}_2, \overline{k}_3, y)$, que é a condição (2) de representabilidade. Para verificar a condição (1) de representabilidade suponha que $\beta(k_1, k_2, k_3) = m$, isto é, $rd(1 + (k_3 + 1) \cdot k_2, k_1) = m$. Então existe um natural k tal que $k_1 = (1 + (k_3 + 1) \cdot k_2) \cdot k + m$ e $m < 1 + (k_3 + 1) \cdot k_2$. Do Teorema 5.3 segue que $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \overline{k}_1 = (\overline{1} + (\overline{k}_3 + 1) \cdot \overline{k}_2) \cdot \overline{k} + \overline{m}$. Pelos Exemplo 5.11 e Teorema 5.3, de $m < 1 + (k_3 + 1) \cdot k_2$ obtemos que $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \overline{m} < \overline{1} + (\overline{k}_3 + \overline{1}) \cdot \overline{k}_2$. Dessa forma segue que $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} (\overline{k}_1 = (\overline{1} + (\overline{k}_3 + \overline{1}) \cdot \overline{k}_2) \cdot \overline{k} + \overline{m} \ \wedge \ \overline{m} < \overline{1} + (\overline{k}_3 + \overline{1}) \cdot \overline{k}_2)$, e pela regra de quantificadores EG segue que $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \exists w((\overline{k}_1 = (\overline{1} + (\overline{k}_3 + \overline{1}) \cdot \overline{k}_2) \cdot w + \overline{m} \ \wedge \ \overline{m} < \overline{1} + (\overline{k}_3 + \overline{1}) \cdot \overline{k}_2))$, isto é, $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \mathcal{B}t(\overline{k}_1, \overline{k}_2, \overline{k}_3, \overline{m})$, o que conclui a verificação da condição (1) de representabilidade. □

Lema 5.36 *Para toda sequência finita de números naturais $k_0, k_1, ..., k_n$ existem naturais b e c tais que $\beta(b, c, i) = k_i$ para cada $i \in \{0, ..., n\}$.*

Demonstração: Sejam $j = \max\{n, k_0, ..., k_n\}$ e $c = j!$. Para cada $i \in \{0, ..., n\}$ defina $u_i = 1 + (i + 1)c$. Vejamos que u_i e u_l são coprimos, quaisquer que sejam $i, l \in \{0, ..., n\}$. De fato, suponha, por absurdo, que exista um número primo p que divide u_i e u_l. E suponha, sem perda de generalidade, que $i < l$. Como p divide u_i e u_l, então p divide $u_l - u_i = (l - i)c$. E sendo p primo, segue que p deve dividir $l - i$ ou c. Por um lado, se p dividisse c, então p dividiria $(i + 1)c$ e $1 + (i + 1)c = u_i$, logo p dividiria a subtração $1 + (i + 1)c - (i + 1)c = 1$, o que é um absurdo pois $p > 1$. Logo, p não divide c. Por outro lado, se p dividisse $l - i$, como $l - i \leq n \leq j$, então $l - i$ é um fator de $j! = c$ e, portanto, $l - i$ divide c. Mas p divide $l - i$, que por sua vez divide c, e teríamos novamente que p divide c, o que vimos não ocorrer. Desta forma, p também não divide $l - i$, o que é uma contradição.

Sendo assim, os termos da sequência u_i são dois a dois coprimos. E ainda, para cada $i \in \{0, ..., n\}$ temos que $k_i \leq j \leq j! = c < 1 + (i + 1)c = u_i$, isto é, $k_i < u_i$. Assim, pelo Teorema Chinês dos Restos[2] existe um único $b < u_0 u_1 ... u_n$ satisfazendo $rd(u_i, b) = k_i$ para cada $i \in \{0, ..., n\}$. Pela definição da função β segue que $\beta(b, c, i) = rd(1 + (i + 1)c, b) = rd(u_i, b) = k_i$, como queríamos. □

[2]Teorema Chinês dos Restos: se $u_0, u_1, ..., u_n$ é uma sequência de números dois a dois primos entre

Para os resultados que se seguem, convém lembrar que comentamos após o Teorema 5.1 que, uma vez que só provamos e nos valemos de sentenças para provas formais, precisamos usar UG no início de cada demonstração em que seja necessário provar fechos universais de fórmulas. E para simplificar a notação, trabalharemos, quando conveniente, denotando as constantes da linguagem expandida pelos mesmos símbolos das variáveis.

Teorema 5.37 *Toda função recursiva é representável em $\mathcal{P}$.*

Demonstração: As funções recursivas são construídas recursivamente; assim, mostraremos este resultado por indução nos tipos de funções recursivas. Para o caso base, vejamos que as funções iniciais são representáveis em $\mathcal{P}$.

1. **A função nula $z(x)$ é representável em $\mathcal{P}$.** De fato, vejamos que a fórmula $\varphi(x,y)$ dada por $x = x \wedge y = 0$ representa a função $z(x)$. Sejam k e m números naturais satisfazendo $z(k) = m$. Então $m = 0$. Como $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \bar{k} = \bar{k}$ e $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} 0 = 0$, por conjunção segue que $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \overline{k} = \overline{k} \wedge \overline{m} = 0$, ou seja, que $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \varphi(\bar{k}, 0)$. Assim a condição 1 da definição de representabilidade é satisfeita. E ainda, sejam y_1, y_2 variáveis satisfazendo $x = x \wedge y_1 = 0$ e $x = x \wedge y_2 = 0$. Pelos axiomas dos tipos 8 e 9 inferimos que $y_1 = y_2$, logo, $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \exists! y(x = x \wedge y = 0)$, e portanto a condição $2'$ da definição de representabilidade é satisfeita. Assim z é fortemente representável (e em particular, é representável).

2. **A função sucessora $S(x)$ é representável em $\mathcal{P}$.** Tal função é representável pela fórmula $\varphi(x,y)$ dada por $y = s(x)$ e a demonstração deste fato é análoga à do item 1.

3. **A i-ésima projeção p_i é representável em $\mathcal{P}$.** Tal função é representável pela fórmula $(x_1 = x_1) \wedge ... \wedge (x_n = x_n) \wedge (y = x_i)$ e a demonstração deste fato é análoga à do item 1.

Vejamos agora que a substituição, a recursão e a aplicação do operador de minimização restrito retornam funções representáveis quando aplicados em funções representáveis.

I. **Substituição:** sejam $g(x_1, ..., x_m), h_1(x_1, ..., x_n), ..., h_m(x_1, ..., x_n)$ funções representáveis em $\mathcal{P}$, e sejam $\mathcal{G}(y_1, ..., y_m, z)$, $\mathcal{H}_1(x_1, ..., x_n, y_1), ..., \mathcal{H}_m(x_1, ..., x_n, y_m)$ fórmulas de $\mathcal{P}$

si, e $k_0, ..., k_n$ é uma sequência de inteiros tais que $0 \leq k_i < u_i$ para quaisquer $i \in \{0, ..., n\}$, então existe um único b satisfazendo $0 \leq b < u_0 ... u_n$ e $rd(u_i, b) = k_i$ para todo $i \in \{0, ..., n\}$.

que as representem (fortemente), respectivamente. Vejamos que a função

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

obtida a partir das funções $g(x_1, \ldots, x_m), h_1(x_1, \ldots, x_n), \ldots, h_m(x_1, \ldots, x_n)$ por substituição é representável em $\mathcal{P}$ pela fórmula $\mathcal{F}(x_1, ..., x_n, z)$ dada por

$$\exists y_1 ... \exists y_m(\mathcal{H}_1(x_1, ..., x_n, y_1) \wedge ... \wedge \mathcal{H}_m(x_1, ..., x_n, y_m) \wedge \mathcal{G}(y_1, ..., y_m, z)).$$

Para verificar a condição 1 de representabilidade considere $k_1, ..., k_n, p$ naturais tais que $f(k_1, ..., k_n) = p$ e vejamos que $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \mathcal{F}(\overline{k}_1, ..., \overline{k}_n, \overline{p})$. Temos que $f(k_1, ..., k_n) = g(h_1(k_1, ..., k_n), ..., h_m(k_1, ..., k_n))$, e fazendo $h_i(k_1, ..., k_n) = r_i$ para $i \in \{1, ..., m\}$ obtemos $g(r_1, ..., r_m) = p$. Como $\mathcal{H}_i$ e $\mathcal{G}$ representam, respectivamente, h_i e g em $\mathcal{P}$, temos que $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \mathcal{H}_i(\overline{k}_1, ..., \overline{k}_n, \overline{r_i})$ e $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \mathcal{G}(\overline{r}_1, ..., \overline{r}_m, \overline{p})$. Assim, por conjunção, segue que $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \mathcal{H}_1(\overline{k}_1, ..., \overline{k}_n, \overline{r}_1) \wedge ... \wedge \mathcal{H}_m(\overline{k}_1, ..., \overline{k}_n, \overline{r}_m) \wedge \mathcal{G}(\overline{r}_1, ..., \overline{r}_m, \overline{p})$. Da regra de quantificadores EG aplicada m vezes segue que

$$\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \exists y_1 ... \exists y_m(\mathcal{H}_1(\overline{k}_1, ..., \overline{k}_n, y_1) \wedge ... \wedge \mathcal{H}_m(\overline{k}_1, ..., \overline{k}_n, y_m) \wedge \mathcal{G}(y_1, ..., y_m, \overline{p}))$$

e, portanto $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \mathcal{F}(\overline{k}_1, ..., \overline{k}_n, \overline{p})$, o que conclui a verificação da condição 1 da representabilidade.

Para verificar a condição 2 de representabilidade vejamos que $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \exists z \mathcal{F}(x_1, ..., x_2, z)$. Por hipótese temos que $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \exists y_i \mathcal{H}_i(x_1, ..., x_n, y_i)$ para cada $i \in \{1, ..., m\}$ e $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \exists z \mathcal{G}(y_1, ..., y_m, z)$. Aplicando a regra de quantificadores EG consecutivamente, para $y_m, ..., y_1$ e z obtemos que $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \exists z \exists y_1 ... \exists y_m(\mathcal{H}_1(x_1, ..., x_n, y_1) \wedge ... \wedge \mathcal{H}_m(x_1, ..., x_n, y_m) \wedge \mathcal{G}(y_1, ..., y_m, z))$, isto é, $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \exists z \mathcal{F}(x_1, ..., x_n, z)$, como desejado.

Vejamos agora que $T \vdash_{\mathcal{L}_\mathcal{A}} \exists! z \mathcal{F}(x_1, ..., x_n, z)$. Suponha válido $\mathcal{F}(x_1, ..., x_n, v) \wedge \mathcal{F}(x_1, ..., x_n, u)$. Então são válidos:

$$\exists y_1 ... \exists y_m(\mathcal{H}_1(x_1, ..., x_n, y_1) \wedge ... \wedge \mathcal{H}_m(x_1, ..., x_n, y_m) \wedge \mathcal{G}(y_1, ..., y_m, v) \tag{5.1}$$

e

$$\exists y_1 ... \exists y_m(\mathcal{H}_1(x_1, ..., x_n, y_1) \wedge ... \wedge \mathcal{H}_m(x_1, ..., x_n, y_m) \wedge \mathcal{G}(y_1, ..., y_m, u). \tag{5.2}$$

Por EG aplicada m vezes nas Equações 5.1 e 5.2 obtemos:

$$\mathcal{H}_1(x_1,...,x_n,b_1) \wedge ... \wedge \mathcal{H}_m(x_1,...,x_n,b_m) \wedge \mathcal{G}(b_1,...,b_m,v) \tag{5.3}$$

e

$$\mathcal{H}_1(x_1,...,x_n,c_1) \wedge ... \wedge \mathcal{H}_m(x_1,...,x_n,c_m) \wedge \mathcal{G}(c_1,...,c_m,u). \tag{5.4}$$

Sendo h_i fortemente representável segue que $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \exists! y_i \mathcal{H}_i(x_1,...,x_n,y_i)$ para todo $i \in \{1,...,m\}$. Dessa forma, de $\mathcal{H}_i(x_1,...,x_n,b_i)$ e $\mathcal{H}_i(x_1,...,x_n,c_i)$ inferimos $b_i = c_i$. Assim de $\mathcal{G}(b_1,...,b_m,v)$ e $b_i = c_i$ obtemos pelo axioma lógico do tipo 10 e 11 que vale $\mathcal{G}(c_1,...,c_m,v)$. E como $\mathcal{G}$ representa fortemente g, de $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \exists! z\mathcal{G}(x_1,...,x_n,z)$, de $\mathcal{G}(c_1,...,c_m,u)$ e $\mathcal{G}(c_1,...,c_m,v)$ inferimos que $u = v$. Dessa forma obtemos $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \mathcal{F}(x_1,...,x_n,u) \wedge \mathcal{F}(x_1,...,x_n,v) \to (u = v)$, e portanto $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \exists! z\mathcal{F}(x_1,...,x_n,z)$.

II. **Recursão:** sejam $g(x_1,...,x_n)$ e $h(x_1,...,x_n,y,z)$ funções representáveis em $\mathcal{P}$ pelas fórmulas $\mathcal{G}(x_1,...,x_n,x_{n+1})$ e $\mathcal{H}(x_1,...,x_n,x_{n+1},x_{n+2},x_{n+3})$ respectivamente, e seja $f(x_1,...,x_n,y)$ dada por

$$f(x_1,...,x_n,0) = g(x_1,...,x_n),$$

$$f(x_1,...,x_n,y+1) = h(x_1,...x_n,y,f(x_1,...,x_n,y)).$$

Vamos mostrar que f é representada em $\mathcal{P}$ pela fórmula $\mathcal{F}(x_1,...,x_{n+2})$ dada por

$$\exists u \exists v((\exists w(\mathcal{B}t(u,v,0,w) \wedge \mathcal{G}(x_1,...,x_n,w))) \wedge \mathcal{B}t(u,v,x_{n+1},x_{n+2})$$

$$\wedge(\forall w(w < x_{n+1} \to \exists y \exists z(\mathcal{B}t(u,v,w,y) \wedge \mathcal{B}t(u,v,s(w),z) \wedge \mathcal{H}(x_1,...,x_n,w,y,z)))).$$

Para tal, mostraremos que as duas condições de representabilidade são satisfeitas.

(1) Sejam $k_1,...,k_n,p,m$ números naturais tais que $f(k_1,...,k_n,p) = m$. Vamos mostrar que $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \mathcal{F}(\overline{k_1},...,\overline{k_n},\overline{p},\overline{m})$.
Suponha primeiro que $p = 0$. Neste caso, $m = f(k_1,...,k_n,0) = g(k_1,...,k_n)$. Tomando a sequência unitária dada por m no Lema 5.36 encontramos b e c números naturais tais que $\beta(b,c,0) = m$. Assim, pelo Lema 5.35, temos que

$$\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \mathcal{B}t(\overline{b},\overline{c},0,\overline{m}). \tag{5.5}$$

Como $\mathcal{G}$ representa a função g em $\mathcal{P}$, de $g(k_1,...,k_n) = m$ segue que $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \mathcal{G}(\overline{k}_1,...,\overline{k}_n,\overline{m})$. Por conjunção e pela regra de quantificadores EG segue que

$$\exists w(\mathcal{B}t(\overline{b},\overline{c},0,w) \wedge \mathcal{G}(\overline{k}_1,...,\overline{k}_n,w)). \tag{5.6}$$

Note agora que dadas fórmulas φ,ψ temos que, a fórmula $\neg\varphi \to (\varphi \to \psi)$ é uma tautologia. E como $w \not< 0$ é válido em $\mathcal{P}$ segue que $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} w < 0 \to \exists y\exists z(\mathcal{B}t(\overline{b},\overline{c},w,y) \wedge (\mathcal{B}t(\overline{b},\overline{c},s(w),z) \wedge \mathcal{H}(\overline{k}_1,...,\overline{k}_n,w,y,z))$. E aplicando a regra de quantificadores UG obtemos

$$\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \forall w(w < 0 \to \exists y\exists z(\mathcal{B}t(\overline{b},\overline{c},w,y)\wedge\mathcal{B}t(\overline{b},\overline{c},s(w),z)\wedge\mathcal{H}(\overline{k}_1,...,\overline{k}_n,w,y,z))). \tag{5.7}$$

Aplicando a regra de quantificadores EG na conjunção das afirmações feitas em 5.5, 5.6 e 5.7 obtemos que $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \mathcal{F}(\overline{k_1},...,\overline{k_n},0,\overline{m})$.

Suponha agora $p > 0$. Considere, para cada $i \in \{0,\dots,p\}$, $r_i = f(k_1,...,k_n,i)$. Pelo Lema 5.36, dada a sequência finita $r_0,...,r_p$ conseguimos encontrar b,c números naturais tais que $\beta(b,c,i) = r_i$ para cada $i \in \{0,...,p\}$, e pelo Lema 5.35 segue que $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \mathcal{B}t(\overline{b},\overline{c},\overline{i},\overline{r}_i)$. Em particular, temos que $\beta(b,c,0) = r_0 = f(k_1,...,k_n,0) = g(k_1,...,k_n)$. Logo, da representatividade de β e g em $\mathcal{P}$, segue que $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \mathcal{B}t(\overline{b},\overline{c},0,\overline{r}_0) \wedge \mathcal{G}(\overline{k}_1,...,\overline{k}_n,\overline{r}_0)$, e pela regra de quantificadores EG obtemos

$$\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \exists w(\mathcal{B}t(\overline{b},\overline{c},0,w) \wedge \mathcal{G}(\overline{k}_1,...,\overline{k}_n,w)). \tag{5.8}$$

Além disso, como $r_p = f(k_1,...,k_n,p) = m$, então $\beta(b,c,p) = m$. Assim,

$$\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \mathcal{B}t(\overline{b},\overline{c},\overline{p},\overline{m}). \tag{5.9}$$

E para $i \in \{0,...,p-1\}$ temos que $\beta(b,c,i) = r_i = f(k_1,...,k_n,i)$ e $\beta(b,c,i+1) = r_{i+1} = f(k_1,...,k_n,i+1) = h(k_1,...,k_n,i,f(k_1,...,k_n,i)) = h(k_1,...,k_n,i,r_i)$. Disto segue, por conjunção, que

$$\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \mathcal{B}t(\overline{b},\overline{c},\overline{i},\overline{r}_i) \wedge \mathcal{B}t(\overline{b},\overline{c},\overline{s(i)},\overline{r}_{i+1}) \wedge \mathcal{H}(\overline{k}_1,...,\overline{k}_n,\overline{i},\overline{r}_i,\overline{r}_{i+1}).$$

Finalmente, da regra de quantificadores EG segue que

$$\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \exists y\exists z(\mathcal{B}t(\overline{b},\overline{c},\overline{w},y) \wedge \mathcal{B}t(\overline{b},\overline{c},\overline{s(i)},z) \wedge \mathcal{H}(\overline{k}_1,...,\overline{k}_n,\overline{i},y,z)).$$

Sendo assim, dos dois parágrafos anteriores e do Lema 5.5 segue que

$$\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \forall w(w < \overline{p} \to \exists y \exists z(\mathcal{B}t(\overline{b}, \overline{c}, w, y) \wedge \mathcal{B}t(\overline{b}, \overline{c}, s(w), z) \wedge \mathcal{H}(\overline{k}_1, ..., \overline{k}_n, w, y, z))). \tag{5.10}$$

Aplicando a regra de quantificadores EG na conjunção das afirmações feitas em 5.8, 5.9 e 5.10 obtemos $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \mathcal{F}(\overline{k}_1, ..., \overline{k}_n, \overline{p}, \overline{m})$, como queríamos.

(2) De $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \mathcal{R}(\overline{k_1}, \ldots, \overline{k_n}, \overline{p}, \overline{m})$ segue, via aplicação da regra de quantificadores EG, que $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \exists x_{n+2} \mathcal{F}(\overline{k}_1, ..., \overline{k}_n, \overline{p}, x_{n+2})$. Sendo assim, resta mostrar a unicidade. Faremos isto por indução em p. Assuma então que $p = 0$ e defina $\alpha = f(k_1, ..., k_n, 0) = g(k_1, ..., k_n)$. Mostraremos que se $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \mathcal{F}(\overline{k}_1, ..., \overline{k}_n, \overline{p}, x_{n+2})$ então $x_{n+2} = \overline{\alpha}$. Pela representabilidade de g segue que α é o único número natural que satisfaz $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \mathcal{G}(\overline{k}_1, ..., \overline{k}_n, \overline{\alpha})$ e pelo que vimos no item (i) temos que $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \mathcal{F}(\overline{k}_1, ..., \overline{k}_n, 0, \overline{\alpha})$. Desta forma, por EG existem constantes b e c tais que vale, em particular, as conjunções $\exists w(\mathcal{B}t(b, c, 0, w) \wedge \mathcal{G}(\overline{k}_1, ..., \overline{k}_n, w))$ e $\mathcal{B}t(b, c, x_{n+1}, x_{n+2})$. Se fixarmos, por EG, uma constante w satisfazendo $\mathcal{B}t(b, c, 0, w) \wedge \mathcal{G}(\overline{k}_1, ..., \overline{k}_n, w)$, pela unicidade de α dada pela representabilidade de $\mathcal{G}$ obtemos que $w = \overline{\alpha}$, logo temos que vale $\mathcal{B}t(b, c, 0, \overline{\alpha})$. E por sua vez, pela representabilidade forte de β por $\mathcal{B}t$, segue que $x_{n+2} = \overline{\alpha}$, como queríamos para o caso base.

Suponha agora que $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \exists! x_{n+2} \mathcal{F}(\overline{k}_1, ..., \overline{k}_n, \overline{p}, x_{n+2})$ e vejamos que $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \exists! x_{n+2} \mathcal{F}(\overline{k}_1, ..., \overline{k}_n, \overline{p+1}, x_{n+2})$. Novamente, resta mostrar a unicidade. Defina $\alpha = g(k_1, ..., k_n)$, $\beta = f(k_1, ..., k_n, p)$ e $\gamma = f(k_1, ..., k_n, p+1) = h(k_1, ..., k_n, p, \beta)$. Destas definições seguem que:

1. $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \mathcal{H}(\overline{k}_1, ..., \overline{k}_n, \overline{p}, \overline{\beta}, \overline{\gamma})$
2. $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \mathcal{G}(\overline{k}_1, ..., \overline{k}_n, \overline{\alpha})$
3. $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \mathcal{F}(\overline{k}_1, ..., \overline{k}_n, \overline{p}, \overline{\beta})$
4. $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \mathcal{F}(\overline{k}_1, ..., \overline{k}_n, \overline{p+1}, \overline{\gamma})$
5. $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \exists! x_{n+2} \mathcal{F}(\overline{k}_1, ..., \overline{k}_n, \overline{p}, x_{n+2})$

Para mostrar a unicidade, suponha ainda que seja válido em $\mathcal{P}$

$$6. \ \mathcal{F}(\overline{k}_1, ..., \overline{k}_n, \overline{p+1}, x_{n+2}).$$

Mostremos que vale $x_{n+2} = \overline{\gamma}$. De 6. e de EG temos existem b e c constantes tais que:

a. $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \exists w(\mathcal{B}t(b, c, 0, w) \wedge \mathcal{G}(\overline{k}_1, ..., \overline{k}_n, w))$

b. $\mathcal{P} \vdash_{\mathcal{L}_A} \mathcal{B}t(b, c, \overline{p+1}, x_{n+2})$

c. $\mathcal{P} \vdash_{\mathcal{L}_A} \forall w(w < \overline{p+1} \to \exists y \exists z(\mathcal{B}t(b, c, w, y) \wedge \mathcal{B}t(b, c, s(w), z) \wedge \mathcal{H}(\overline{k}_1, ..., \overline{k}_n, w, y, z)$.

E sendo $\overline{p} < \overline{p+1}$, então de (c) obtemos

d. $\mathcal{P} \vdash_{\mathcal{L}_A} \forall w(w < \overline{p} \to \exists y \exists z(\mathcal{B}t(b, c, w, y) \wedge \mathcal{B}t(b, c, s(w), z) \wedge \mathcal{H}(\overline{k}_1, ..., \overline{k}_n, w, y, z)$.

Usando $w = \overline{p}$ em (c) e aplicando UI, existem números naturais d e e tais que

e. $\mathcal{P} \vdash_{\mathcal{L}_A} Bt(b, c, \overline{p}, d) \wedge \mathcal{B}t(b, c, \overline{p+1}, e) \wedge \mathcal{H}(\overline{k}_1, ..., \overline{k}_n, \overline{p}, d, e)$.

Agora, de (a), (d) e (e) segue que

f. $\mathcal{P} \vdash_{\mathcal{L}_A} \mathcal{F}(\overline{k}_1, ..., \overline{k}_n, \overline{p}, d)$.

E pela unicidade dada (5) e de (f) e (3) inferimos que $\mathcal{P} \vdash_{\mathcal{L}_A} d = \overline{\beta}$. Disto e de (e) inferimos que

g. $\mathcal{P} \vdash_{\mathcal{L}_A} \mathcal{H}(\overline{k}_1, ..., \overline{k}_n, \overline{p}, \overline{\beta}, e)$.

Como $\mathcal{H}$ representa h, obtemos de (1) e (g) que $\mathcal{P} \vdash_{\mathcal{L}_A} \overline{\gamma} = e$. Disto e de (e) inferimos

h. $\mathcal{P} \vdash_{\mathcal{L}_A} \mathcal{B}t(b, c, \overline{p+1}, \overline{\gamma})$.

Como $\mathcal{B}t$ representa fortemente a função β, segue de (b) e de (h) que $\mathcal{P} \vdash_{\mathcal{L}_A} x_{n+2} = \overline{\gamma}$, como queríamos.

III. **Operador de minimização restrito:** seja $g : \mathbb{N}^{n+1} \to \mathbb{N}$ tal que, para quaisquer números naturais $x_1, \ldots, x_n$ exista um natural y tal que $g(x_1, \ldots, x_n, y) = 0$. Suponhamos que g seja representada em $\mathcal{P}$ pela fórmula $\mathcal{G}(x_1, ..., x_{n+2})$. Vamos mostrar que $f : \mathbb{N}^n \to \mathbb{N}$ dada por

$$f(x_1, ..., x_n) = \mu y(g(x_1, ..., x_n, y) = 0)$$

é representada em $\mathcal{P}$ pela fórmula $\mathcal{F}(x_1, ..., x_{n+1})$ dada por

$$\mathcal{G}(x_1, ..., x_{n+1}, 0) \wedge \forall y(y < x_{n+1} \to \neg\mathcal{G}(x_1, ..., x_n, y, 0)).$$

Para tal, sejam $k_1, ..., k_n, m$ números naturais tais que $f(k_1, ..., k_n) = m$. Então $g(k_1, ..., k_n, m) = 0$ e m é o menor número natural satisfazendo tal condição, ou seja, para $k < m$ temos que $g(k_1, ..., k_n, k) \neq 0$. Como $\mathcal{G}$ representa g segue em $\mathcal{P}$ temos que $\mathcal{P} \vdash_{\mathcal{L}_A} \mathcal{G}(\overline{k}_1, ..., \overline{k}_n, \overline{m}, 0)$ e, para $k < m$ temos, pela Proposição 5.13, que $\mathcal{P} \vdash_{\mathcal{L}_A} \neg\mathcal{G}(\overline{k}_1, ..., \overline{k}_n, \overline{k}, 0)$. Desta forma, segue do item 2 do Lema 5.5 que $\mathcal{P} \vdash_{\mathcal{L}_A} \forall y(y < \overline{m} \to \neg\mathcal{G}(\overline{k}_1, ..., \overline{k}_n, y, 0))$. Assim obtemos, por conjunção, que

$\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \mathcal{F}(\overline{k}_1, ..., \overline{k}_n, \overline{m})$. Com isto mostramos a condição (1) da definição de representabilidade e, por meio de uma aplicação da regra de quantificadores EG, obtemos $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \exists x_{n+1} \mathcal{F}(\overline{k}_1, ..., \overline{k}_n, x_{n+1})$. Sendo assim, resta verificar a unicidade. Suponha então que $\mathcal{G}(\overline{k}_1, ..., \overline{k}_n, u, 0) \wedge \forall y(y < u \rightarrow \neg\mathcal{G}(\overline{k}_1, ..., \overline{k}_n, y, 0))$ seja válido em $\mathcal{P}$. Pelo Teorema 5.4 (8) temos que

$$\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \overline{m} < u \vee \overline{m} = u \vee u < \overline{m}. \tag{5.11}$$

Note que $((A \vee B \vee C) \wedge (\neg A) \wedge (\neg C)) \rightarrow B$ é uma tautologia e tome A como $\overline{m} < u$, B como $\overline{m} = u$, e C como $u < \overline{m}$. Por UI aplicado à segunda sentença de $\mathcal{G}(\overline{k}_1, ..., \overline{k}_n, u, 0) \wedge \forall y(y < u \rightarrow \neg\mathcal{G}(\overline{k}_1, ..., \overline{k}_n, y, 0))$ temos que $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \overline{m} < u \rightarrow \neg\mathcal{G}(\overline{k}_1, ..., \overline{k}_n, \overline{m}, 0)$, e por contrapositiva e Modus Ponens segue que $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \neg(\overline{m} < u)$. De forma análoga, por UI, contrapositiva e Modus Ponens em $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \forall y(y < \overline{m} \rightarrow \neg\mathcal{G}(\overline{k}_1, ..., \overline{k}_n, y, 0))$ segue que $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \neg(u < \overline{m})$. Da tautologia dada pela afirmação 5.11 segue que $\mathcal{P} \vdash_{\mathcal{L}_\mathcal{A}} \overline{m} = u$, provando a unicidade desejada. $\square$

Corolário 5.38 *Toda relação recursiva é exprimível em $\mathcal{P}$.*

Demonstração: Seja R uma relação recursiva em $\mathcal{P}$. então χ_R é uma função recursiva. Pelo do 5.37, χ_R é representável e da Proposição 5.16 segue que R é exprimível. $\square$

5.4 Números de Gödel

Vamos apresentar, nesta seção, uma das principais ferramentas para a demonstração dos Teoremas da Incompletude: os números de Gödel. A ideia é associar a cada símbolo, fórmula e sequência de fórmulas de uma teoria de primeira ordem T um inteiro positivo.

Para adequar a nossa teoria $\mathcal{P}$ de forma a obter unicidade na associação aos núneros de Gödel, vamos reescrever $\mathcal{L}_\mathcal{A} = \{a_1, f_1^1, f_1^2, f_2^2\}$, onde a_1 é o símbolo de constante 0, f_1^1 é o símbolo de função s, f_1^2 é o símbolo de função + e f_2^2 é o símbolo de função $\cdot$.

E ainda, no que se segue, iremos flexibilizar o uso da palavra "expressão"[3] para abarcar qualquer sequência finita de símbolos de $\mathcal{L}$.

[3]Conceito definido na Definição 1.1 como um sinônimo para uma expressão bem formada.

Definição 5.39 *Seja T uma teoria de primeira ordem. A cada símbolo u de T iremos associar um inteiro positivo, denominado **número de Gödel do símbolo** u e denotado por $g(u)$, da seguinte maneira:*

- $g(=) = 3$;
- $g(\neg) = 5$;
- $g(\wedge) = 7$;
- $g(\vee) = 9$;
- $g(\Rightarrow) = 11$;
- $g(\leftrightarrow) = 13$;
- $g(\forall) = 15$;
- $g(\exists) = 17$;
- $g(x_k) = 13 + 8k$, *para* $k \geq 1$;
- $g(a_k) = 15 + 8k$, *para* $k \geq 1$;
- $g(f_k^n) = 1 + 8(2^n 3^k)$, *para* $k, n \geq 1$;
- $g(p_k^n) = 3 + 8(2^n 3^k)$, *para* $k, n \geq 1$.

Definição 5.40 *Sejam T uma teoria de primeira ordem e $u_0 u_1 ... u_r$ uma expressão de T onde cada u_j é um símbolo de T. Definimos o **número de Gödel** de $u_0 u_1 ... u_r$, denotado por $g(u_0 u_1 ... u_r)$, da seguinte forma*

$$g(u_0 u_1 ... u_r) = 2^{g(u_0)} 3^{g(u_1)} ... p_r^{g(u_r)}$$

onde p_j denota o j-ésimo número primo e $p_0 = 2$.

Definição 5.41 *Sejam T uma teoria de primeira ordem e $e_0, e_1, ..., e_r$ uma sequência finita de expressões de T. Definimos o **número de Gödel** de $e_0, e_1, ..., e_r$, denotado por $g(e_0, e_1, ..., e_r)$, da seguinte forma*

$$g(e_0, e_1, ..., e_r) = 2^{g(e_0)} 3^{g(e_1)} ... p_r^{g(u_r)}$$

onde p_j denota o j-ésimo número primo e $p_0 = 2$.

Há diversas observações a serem feitas acerca da definição anterior. Primeiro, note que, dado um símbolo u qualquer de T, o número de Gödel de u é um inteiro positivo *ímpar*. E ainda, o resto da divisão de $g(u)$ por 8 é 5 quando u é uma variável, 7 quando u é um símbolo de constante, 1 quando u é um símbolo de função e 3 quando u é uma relação. Dessa forma, símbolos diferentes possuem números de Gödel diferentes.

Para as expressões, como a decomposição por fatores primos é única, temos que expressões distintas possuem números de Gödel diferentes. Note também que símbolos e expressões possuem números de Gödel distintos, já que todo símbolo possui número de Gödel ímpar e o número de Gödel de cada expressão possui um fator 2^k em sua decomposição, com k ímpar, sendo, portanto, par. Um símbolo u pode ser considerado uma expressão constituída de um único símbolo, e neste caso, u irá possuir números de Gödel diferentes quando considerado como símbolo e quando considerado como expressão. Por exemplo, o símbolo de variável x_1 possui número de Gödel 21 quando visto como um símbolo, e número de Gödel 2^{21} quando visto como expressão unitária.

Para sequências de expressões, note que pela unicidade da decomposição por fatores primos, sequências distintas possuem números de Gödel diferentes. Pelo mesmo motivo apresentado no parágrafo anterior temos que as sequências de expressões possuem números de Gödel diferentes dos de símbolos. E como expressões possuem número de Gödel par, as sequências de expressões possuem um fator 2^m em sua decomposição, com m par, diferente do que ocorre com os números de Gödel de expressões. Desta forma, as sequências de expressões possuem números de Gödel distintos dos de expressões. E uma expressão vista como uma sequência unitária de expressões terá número de Gödel diferente quando visto como expressão e quando vista como sequência unitária de expressões.

Com isto concluímos que a função cujo domínio é o conjunto dos símbolos, expressões e sequências finitas de expressões em T e cujo contradomínio é o conjunto dos inteiros positivos, a qual associa a cada elemento do domínio seu respectivo número de Gödel, é injetora.

Definição 5.42 *Seja T uma teoria de primeira ordem. Dizemos que T possui um* ***alfabeto primitivo recursivo (respectivamente, recursivo)*** *se as seguintes relações unárias são primitivas recursivas (respectivamente, recursivas):*

- *$C(x)$: x é o número de Gödel de um símbolo de constante de T.*
- *$F(x)$: x é o número de Gödel de um símbolo de função de T.*

- *$R(x)$: x é o número de Gödel de um símbolo de relação de T.*

Teorema 5.43 *A teoria $\mathcal{P}$ possui um alfabeto primitivo recursivo.*

Demonstração: Basta notar que $\mathcal{P}$ possui uma quantidade finita de símbolos de constantes, funções e relações e, portanto, as relações C, F e R são subconjuntos finitos de $\mathbb{N}$. Do Teorema 5.25 segue que tais relações são primitivas recursivas. □

Um resultado intuitivo que usaremos no que se segue é o seguinte.

Teorema 5.44 *Seja φ uma fórmula de uma teoria de primeira ordem $\mathcal{L}$. Se T prova um fecho universal de φ, então T prova todo fecho universal de φ.*

Demonstração: Sejam ψ e ϕ fechos universais de φ. Pelo Teorema 2.16 temos que ψ e ϕ são logicamente equivalentes, isto é $T \vDash \psi \leftrightarrow \phi$. Do Teorema da Completude segue que $T \vdash_{\mathcal{L}} \psi \leftrightarrow \phi$. Por hipótese, $T \vdash_{\mathcal{L}} \psi$, portanto segue por Modus Ponens que $T \vdash_{\mathcal{L}} \phi$. □

Teorema 5.45 *Seja T uma teoria de primeira ordem com um alfabeto primitivo recursivo (respectivamente, recursivo). As seguintes relações e funções são primitivas recursivas (respectivamente, recursivas):*

1. *$EV(x)$: x é o número de Gödel de uma expressão constituída por um único símbolo de variável.*

2. *$EC(x)$: x é o número de Gödel de uma expressão constituída por um único símbolo de constante.*

3. *$EF(x)$: x é o número de Gödel de uma expressão constituída por um único símbolo de função.*

4. *$ER(x)$: x é o número de Gödel de uma expressão constituída por um único símbolo de relação.*

5. *A função $Arg_f(x)$ definida da seguinte maneira: se x é o número de Gödel do símbolo de função f_j^n, então $Arg_f(x) = n$.*

6. *A função $Arg_r(x)$ definida da seguinte maneira: se x é o número de Gödel do símbolo de relação p_j^n, então $Arg_r(x) = n$.*

7. *$Gd(x)$: x é o número de Gödel de uma expressão em T.*

8. *$MP(x, y, z)$: x é o número de Gödel de uma fórmula φ, z é o número de Gödel de uma fórmula ψ e y é o número de Gödel da fórmula $\varphi \rightarrow \psi$.*

9. *Trm*(x): *x é o número de Gödel de uma expressão que é um termo de T.*

10. *Atfml*(x): *x é o número de Gödel de uma fórmula atômica de T.*

11. *Fml*(x): *x é o número de Gödel de uma fórmula de T.*

12. *Sub*(x, y, u, v): *y é o número de Gödel de uma expressão φ, u é o número de Gödel de uma expressão que é um termo t, v é o número de Gödel de uma variável w e x é o número de Gödel da expressão $[\varphi]^t_w$.*

13. *A função Sub*(y, u, v) *definida da seguinte maneira: se y é o número de Gödel de uma expressão $\varphi(w)$, u é o número de Gödel de um termo t, v é o número de Gödel de uma variável w e x é o número de Gödel da expressão $[\varphi]^t_w$, então Sub*$(y, u, v) = x$.

14. *Fr*(y, v): *y é o número de Gödel de uma fórmula ou de uma expressão que é um termo de T que contém ocorrências livres da variável com número de Gödel v.*

15. *Ff*(u, v, w): *u é o número de Gödel de uma expressão que é um termo que é livre para a variável com número de Gödel v na fórmula com número de Gödel w.*

16. *A função Neg*(x), *que retorna o número de Gödel da expressão $\neg\varphi$, onde φ é a expressão com número de Gödel x.*

17. *A função Cond*(x, y), *que retorna o número de Gödel da expressão $\varphi \to \psi$, onde φ é a expressão com número de Gödel x e ψ é a expressão com número de Gödel y.*

18. *A função Clos*(u), *que retorna o número de Gödel do fecho universal no qual as variáveis aparecem em ordem decrescente da fórmula cujo número de Gödel é u.*

19. *LAx*(x): *x é o número de Gödel de um axioma lógico de T, onde T é uma teoria na linguagem $\mathcal{L}_{\mathcal{A}}$.*

Demonstração: Mostraremos que tais funções são primitivas recursivas assumindo que T possui um alfabeto primitivo recursivo, e para a recursividade a prova é igual — a recursividade seguirá do fato de C, F e R serem recursivas, ao invés de primitivas recursivas. A estratégia é escrevê-las usando outras funções e relações que já sabemos que são primitivas recursivas, tais como relações com quantificadores limitados (dado pelo Teorema 5.26) e a disjunção e conjunção de relações recursivas (dado pelo Teorema 5.24). Mostraremos alguns itens de forma detalhada e indicaremos os que podem ser mostrados de forma análoga.

1. EV(x): seja x o número de Gödel de uma expressão constituída de um único símbolo de variável, digamos v. Então o número de Gödel do símbolo v é $13 + 8z$ é para algum $z \geq 1$. E assim o número de Gödel x da expressão v é 2^{13+8z}. Por indução podemos mostrar que, para todo z natural, ocorre $z < 2^z$, e como $z \leq 13 + 8z$, segue que $z < 2^{13+8z} = x$. Logo, podemos nos limitar a $z < x$, sem perda de generalidade. Defina agora a relação unária E da seguinte forma: $x \in E$ exatamente quando $\exists z_{z<x}(1 \leq z \wedge x = 2^{13+8z})$. Com o que vimos acima segue que EV $\subseteq E$. E note que vale a inclusão reversa, pois se existe $z < x$ satisfazendo $z \geq 1$ e $x = 2^{13+8z}$ então x é o número de Gödel da expressão constituída do único símbolo de variável z. Logo EV $= E$.

   Vejamos agora que a relação $R(x, z)$ dada por $1 \leq z \wedge x = 2^{13+8z}$ é primitiva recursiva. Pelo Teorema 5.19 temos que a função identidade i, as funções constantes e a função produto são primitivas recursivas. Dessa forma, obtemos por substituição que a função $8z = \cdot(8, z)$ é primitiva recursiva. Também temos que a soma é uma função primitiva recursiva, logo obtemos por substituição que a função $13 + 8z = +(13, 8z)$ é primitiva recursiva. Assim a função 2^{13+8z} é uma substituição das funções primitivas recursivas 2 e $13 + 8z$ na função primitiva recursiva exponencial u^v, e portanto a função 2^{13+8z} é também primitiva recursiva. Assim, pelo Teorema 5.27 segue que a relação $x = 2^{13+8z}$ é primitiva recursiva. E ainda, a relação $1 \leq z$ é a abreviação de $1 = z \vee 1 < z$. A igualdade e a relação $<$ são primitivas recursivas, logo, por substituição obtemos que as relações $1 = z$ e $1 < z$ são primitivas recursivas. Logo, temos que a relação $1 \leq z$ é a disjunção de relações primitivas recursivas e pelo Teorema 5.24 é também primitiva recursiva. Por este mesmo teorema, segue que a relação $1 \leq z \wedge x = 2^{13+8z}$ é primitiva recursiva. Agora note que, pelo Teorema 5.26, a relação dada pelo quantificador existencial limitado $\exists z_{z<x} R(x, z)$ é primitiva recursiva desde que a relação $R(x, z)$ seja primitiva recursiva. Do que segue acima, temos portanto que $\exists z_{z<x}(1 \leq z \wedge x = 2^{13+8z})$ é uma relação primitiva recursiva. Como já havíamos visto que EV(x) vale exatamente quando temos $\exists z_{z<x}(1 \leq z \wedge x = 2^{13+8z})$, segue portanto que EV é uma relação primitiva recursiva.

2. EC(x): seja x o número de Gödel de uma expressão dada por um único símbolo de constante c. Então se y for o número de Gödel do símbolo c vale C(y) e o número de Gödel da expressão constituída pelo símbolo c é 2^y. Como vimos no item anterior, podemos considerar, sem perda de generalidade, que $y < 2^y$. Dessa forma EC é dada pela relação $\exists y_{y<x}(C(y) \wedge x = 2^y)$. De forma análoga

ao caso anterior verifica-se que tal relação é primitiva recursiva, se valendo da hipótese de que C é uma relação primitiva recursiva.

3. EF(x): seja x o número de Gödel de uma expressão constituída por um único símbolo de função. Temos que EF(x) é dada pela relação $\exists y_{y<x}(F(y) \wedge x = 2^y)$. Como F é, por hipótese, primitiva recursiva, segue que EF é primitiva recursiva.

4. ER(x): seja x o número de Gödel de uma expressão constituída por um único símbolo de relação. Temos que ER(x) é dada pela relação $\exists y_{y<x}(R(y) \wedge x = 2^y)$. Como R é, por hipótese, primitiva recursiva, segue que ER é primitiva recursiva.

5. $\mathrm{Arg}_f(x)$: seja x o número de Gödel do símbolo de função f_j^n. Note que $\mathrm{Arg}_f(x) = qt(8, x \dot{-} 1)_0$, e vimos no Teorema 5.19 que as funções $\dot{-}$ e qt são primitivas recursivas. Portanto Arg_f é primitiva recursiva.

6. $\mathrm{Arg}_r(x)$: seja x o número de Gödel do símbolo de relação p_j^n. Basta notar que $\mathrm{Arg}_r(x) = qt(8, x \dot{-} 3)_0$.

7. Gd(x): seja x o número de Gödel de uma expressão de T. As expressões que consistem de um único símbolo são constituídas de um símbolo lógico, símbolo de função ou símbolo de relação. Assim, se uma expressão é constituída por um único símbolo, podemos representá-la pela relação EV(x) $\vee$ EC(x) $\vee$EF(x) $\vee$ ER(x) $\vee$ $x = 2^3 \vee x = 2^5 \vee x = 2^7 \vee x = 2^9 \vee x = 2^{11}$. Para expressões constituídas por dois ou mais símbolos, pela regra de formação de expressões, conseguimos definir o número de Gödel desta expressão com a concatenação do número de Gödel das expressões mais simples que a compõem. Neste caso, temos que $\exists u_{u<x} \exists v_{v<x}(x = u * v \wedge \mathrm{Gd}(u) \wedge \mathrm{Gd}(v))$. Vejamos então que a seguinte relação (que expressa Gd(x)) é primitiva recursiva:

$$\mathrm{EV}(x) \vee \mathrm{EC}(x) \vee \mathrm{EF}(x) \vee \mathrm{ER}(x) \vee x = 2^3 \vee x = 2^5 \vee x = 2^7 \vee x = 2^9 \vee x = 2^{11} \vee$$

$$x = 2^{13} \vee x = 2^{15} \vee x = 2^{17} \vee \exists u_{u<x} \exists v_{v<x}(x = u * v \wedge \mathrm{Gd}(u) \wedge \mathrm{Gd}(v)).$$

Das funções e relações utilizadas acima, o único trecho que nos impede de afirmar a recursividade primitiva da expressão é a relação Gd(u) para cada $u < x$. A priori, somente a regra de recursão não é suficiente para garantir que essa expressão seja primitiva recursiva (pois a recursão usa a avaliação somente no termo com número de Gödel imediatamente anterior a y), mas o Teorema 5.33 nos permitirá concluir a recursividade primitiva.

Denotando por χ_{Gd} a função característica de Gd, e $\chi_{Gd}\#$ como na Definição 5.31, fixado $u < x$ note que:

$$((\chi_{Gd})\#(x))_u = \left(\prod_{k<x} p_k^{\chi_{Gd}(k)}\right)_u = \chi_{Gd}(u) = \begin{cases} 1, & \text{se vale } Gd(u), \\ 0, & \text{caso contrário.} \end{cases}$$

Dessa forma, vale Gd(u) se, e somente se, $((\chi_{Gd})\#(x))_u = 1$. Defina agora a relação $H(x,z)$ por:

$$EV(x) \vee EC(x) \vee EF(x) \vee ER(x) \vee x = 2^3 \vee x = 2^5 \vee x = 2^7 \vee x = 2^9 \vee x = 2^{11} \vee$$

$$x = 2^{13} \vee x = 2^{15} \vee x = 2^{17} \vee \exists u_{u<x} \exists v_{v<x} (x = u * v \ \wedge \ (z)_u = 1 \ \wedge \ (z)_v = 1).$$

Do que vimos acima, vale Gd(x) se, e somente se, vale $H(x, (\chi_{Gd})\#(x))$. E note que $H(x,z)$ é primitiva recursiva, pois se vale de funções e relações que já sabemos serem primitivas recursivas. Assim, segue do Teorema 5.33 que Gd(x) é primitiva recursiva.

8. MP(x,y,z): seja x o número de Gödel da expressão φ, z o número de Gödel da expressão ψ e y o número de Gödel da expressão $\varphi \to \psi$. Então vale MP(x,y,z) se, e somente se, vale Gd(x)$\wedge$Gd(z)$\wedge y = 2^{11} * x * z$. Como Gd é uma relação primitiva recursiva, segue que MP é uma relação primitiva recursiva.

9. Trm(x): sejam τ um termo de T e x o número de Gödel da expressão dada por τ. Pelo Teorema 1.10, τ é uma variável, um símbolo de constante, ou existe um símbolo de função f_k^n e termos $\tau_1,...,\tau_n$ tais que τ é o termo $f_k^n \tau_1 ... \tau_n$. Os dois primeiros casos valem quando EV(x) $\vee$ EC(x).

Para o terceiro caso, considere a seguinte sequência.

1.	f_k^n
2.	$f_k^n\tau_1$
3.	$f_k^n\tau_1\tau_2$
$\vdots$	
$n.$	$f_k^n\tau_1\tau_2...\tau_{n-1}$
$n+1.$	$f_k^n\tau_1\tau_2...\tau_{n-1}\tau_n$

Note que x é o número de Gödel do termo $f_k^n\tau_1...\tau_n$ exatamente quando: x é o número de Gödel da última expressão da sequência acima (cujo comprimento é $n+1$), isto é, $x = (y)_{lh(y)\dot{-}1}$, onde y é o número de Gödel desta sequência; n é a aridade do símbolo de função f_k^n, e portanto vale $lh(y) = \text{Arg}_f((x)_0)+1$; a primeira expressão da sequência acima possui comprimento 1 e é constituída de um símbolo de função n-ária, isto é, $\text{F}(((y)_0)_0)\ \wedge\ lh((y)_0) = 1$; e as demais expressões desta sequência são formadas pela concatenação de um termo à expressão anterior, isto é, $\forall u_{u<lh(y)\dot{-}1}\exists v_{v<u}((y)_{u+1} = (y)_u * v \wedge Trm(v))$.

Note agora que se x_i for o número de Gödel da i-ésima expressão da lista acima, então ocorre $x_i < x_j$ se $i < j$. Desta forma vale que $x_i < x$ para cada $i \in 1,...,n$. Logo, segue que $y < 2^x 3^x...p_n^x = (2\cdot 3\cdot ...\cdot p_n)^x < (p_n!)^x < (p_x!)^x$, onde a última desigualdade vale pois $n < x$ (já que $x = 2^{x_1}3^{x_2}...p_n^{x_{n+1}}$ e, em geral, $n \leq p_n$ para $n \geq 1$). Portanto podemos nos limitar aos valores de y que satisfazem $y < (p_x!)^x$.

Sendo assim, de forma geral, a relação $\text{Trm}(x)$ pode ser escrita da seguinte forma:

$$\text{EV}(x) \vee \text{EC}(x)\ \vee\ \exists y_{y<(p_x!)^x}(x = (y)_{lh(y)\dot{-}1}\ \wedge\ lh(y) = \text{Arg}_f((x)_0)+1\ \wedge\ \text{F}(((y)_0)_0)\ \wedge$$

$$lh((y)_0) = 1\ \wedge \forall u_{u<lh(y)\dot{-}1}\exists v_{v<x}((y)_{u+1} = (y)_u * v \wedge Trm(v))).$$

Das funções e relações utilizadas acima, o único trecho que nos impede de afirmar a recursividade primitiva da expressão é a relação $\text{Trm}(v)$ para $v < u$. Note que, como $u <\text{lh}(y)\dot{-}1 = n \leq p_n \leq y$, então $u < y$. Estamos portanto usando a avaliação de Trm em todos os termos τ_i (e fazemos isso variando $u < y$)

para definir Trm em $f\tau_1...\tau_n$. De forma análoga ao que fizemos para a relação Gd, podemos concluir a recursividade primitiva dessa relação utilizando o Teorema 5.33.

10. Atfml(x): seja x o número de Gödel de uma fórmula atômica de T. Então ou tal fórmula é da forma $= \tau_1\tau_2$, com τ_1, τ_2 termos, e neste caso vale $\exists u_{u<x}\exists v_{v<x}(x = 2^3 * u * v \ \wedge \ Trm(u) \ \wedge \ Trm(v))$, ou então existe um símbolo de relação p_n^k e termos $\tau_1, ..., \tau_n$ tais que tal fórmula é da forma $p_n^k\tau_1...\tau_n$. Neste caso, de forma análoga à relação Trm, considere a seguinte sequência de expressões.

1.	p_k^n
2.	$p_k^n\tau_1$
3.	$p_k^n\tau_1\tau_2$
$\vdots$	
n.	$p_k^n\tau_1\tau_2...\tau_{n-1}$
$n+1$.	$p_k^n\tau_1\tau_2...\tau_{n-1}\tau_n$

Como visto na demonstração da relação Trm, x é o número de Gödel da última expressão da sequência acima, y é o número de Gödel da sequência e podemos supor $y < (p_x!)^x$. Desta forma temos que $x = (y)_{lh(y)\dot{-}1}$. Note que a aridade do símbolo de relação é n (logo $n = Arg_p((x)_0)$) e a sequência acima tem $n+1$ elementos, logo $lh(y) = Arg_p((x)_0) + 1$. E ainda, a primeira expressão da sequência acima possui comprimento 1 e é constituída de um símbolo de relação n-ária, logo vale $\mathrm{R}(((y)_0)_0) \wedge lh((y)_0) = 1$. E ainda, as demais expressões desta sequência são formadas pela concatenação de um termo à expressão anterior, isto é, $\forall u_{u<lh(y)\dot{-}1}\exists v_{v<u}((y)_{u+1} = (y)_u * v \wedge Trm(v))$.

De forma análoga à demonstração dada na relação Trm(x) mostra-se que seguinte expressão, que expressa a relação Atfml(x), é primitiva recursiva:

$$\exists u_{u<x}\exists v_{v<x}(x = 2^3 * u * v \ \wedge \ Trm(u) \ \wedge \ Trm(v)) \vee$$

$$\exists y_{y<(p_x!)^x}(x = (y)_{lh(y)\dot{-}1} \ \wedge \ lh(y) = \mathrm{Arg}_p((x)_0) + 1 \ \wedge$$

$$\mathrm{R}(((y)_0)_0) \ \wedge \ lh((y)_0) = 1 \ \wedge \forall u_{u<lh(y)\dot{-}1}\exists v_{v<x}((y)_{u+1} = (y)_u * v \wedge Trm(v))).$$

11. Fml(y): seja x o número de Gödel de uma fórmula φ de T. Pela Definição 1.8 temos que φ é uma fórmula atômica, e neste caso vale Atfml(x), ou existem fórmulas ψ_1, ψ_2 tais que φ é uma das seguintes fórmulas: $\neg\psi_1$, $\wedge\psi_1\psi_2$, $\vee\psi_1\psi_2$, $\rightarrow \psi_1\psi_2$, $\leftrightarrow \psi_1\psi_2$, $\forall y\psi_1$ ou $\exists y\psi_1$. Cada um destes casos pode ser expresso, respectivamente, pelas seguintes relações:

$$\exists z(\mathrm{Fml}(z) \wedge y = 2^5 * z)$$

$$\exists z_0 \exists z_1 (\mathrm{Fml}(z_0) \wedge \mathrm{Fml}(z_1) \wedge y = 2^7 * z_0 * z_1)$$

$$\exists z_0 \exists z_1 (\mathrm{Fml}(z_0) \wedge \mathrm{Fml}(z_1) \wedge y = 2^9 * z_0 * z_1)$$

$$\exists z_0 \exists z_1 (\mathrm{Fml}(z_0) \wedge \mathrm{Fml}(z_1) \wedge y = 2^{11} * z_0 * z_1)$$

$$\exists z_0 \exists z_1 (\mathrm{Fml}(z_0) \wedge \mathrm{Fml}(z_1) \wedge y = 2^{13} * z_0 * z_1)$$

$$\exists z_0 \exists z_1 (\mathrm{Fml}(z_0) \wedge \mathrm{EV}(z_1) \wedge y = 2^{15} * z_0 * z_1)$$

$$\exists z_0 \exists z_1 (\mathrm{Fml}(z_0) \wedge \mathrm{EV}(z_1) \wedge y = 2^{17} * z_0 * z_1)$$

Se φ é uma sequência unitária de símbolo, então φ é uma fórmula atômica e vale $\mathrm{Atfml}(y) \vee \exists z_{z<3^y}((\mathrm{Fml}(z) \wedge y = 2^5 * z)$. Se φ é uma sequência com dois ou mais símbolo, existe z que é o número de Gödel de uma expressão (para contemplar o caso da negação) ou o número de Gödel de uma sequência de expressões (para contemplar os demais casos que necessitam de 2 expressões). Caso z seja uma sequência de expressões, precisamos de, no mínimo, uma sequência com 2 expressões. Suponha assim que tenhamos z o número de Gödel de uma sequência com 2 expressões de tal forma que $(z)_0 = 2^{a_0} \cdot \ldots \cdot p_n^{a_n}$ e $(z)_1 = 2^{b_0} \cdot \ldots \cdot p_l^{b_l}$. Então $z = 2^{(z)_0} \cdot 3^{(z)_1} = 2^{2^{a_0} \cdot \ldots \cdot p_n^{a_n}} \cdot 3^{2^{b_0} \cdot \ldots \cdot p_l^{b_l}}$. Para o caso da conjunção temos que y é da seguinte forma: $y = 2^7 \cdot 3^{a_0} \cdot \ldots \cdot p_{n+1}^{a_n} \cdot p_{n+2}^{b_0} \cdot \ldots \cdot p_{l+n+1}^{b_l}$. Logo temos que: $z = 2^{(z)_0} \cdot 3^{(z)_1} < 3^{(z)_0} \cdot 3^{(z)_1} = 3^{(z)_0 + (z)_1} < 3^{(z)_0 \cdot (z)_1} = 3^{2^{a_0} \cdot \ldots \cdot p_n^{a_n} \cdot 2^{b_0} \cdot \ldots \cdot p_l^{b_l}} < 3^{2^7 \cdot 3^{a_0} \cdot \ldots \cdot p_{n+1}^{a_n} \cdot p_{n+2}^{b_0} \cdot \ldots \cdot p_{l+n+1}^{b_l}} = 3^y$.

Para os demais tipos de fórmulas se mostra de forma análoga que podemos supor sem perda de generalidade que $z < 3^y$. Com isto podemos reformular a relação Fml(y) da seguinte forma:

$\mathrm{Atfml}(y) \vee \exists z_{z<3^y}((\mathrm{Fml}(z) \wedge y = 2^5 * z) \vee (\mathrm{Fml}((z)_0) \wedge \mathrm{Fml}((z)_1) \wedge y = 2^7 * (z)_0 * (z)_1) \vee$

$(\mathrm{Fml}((z)_0) \wedge \mathrm{Fml}((z)_1) \wedge y = 2^9 * (z)_0 * (z)_1) \vee (\mathrm{Fml}((z)_0) \wedge \mathrm{Fml}((z)_1) \wedge y = 2^{11} * (z)_0 * (z)_1) \vee$

$$(\mathrm{Fml}((z)_0) \wedge \mathrm{Fml}((z)_1) \wedge y = 2^{13} * (z)_0 * (z)_1) \vee (\mathrm{Fml}((z)_0) \wedge \mathrm{Fml}((z)_1) \wedge y = 2^{15} * (z)_0 * (z)_1) \vee$$
$$(\mathrm{Fml}((z)_0) \wedge \mathrm{Fml}((z)_1) \wedge y = 2^{17} * (z)_0 * (z)_1)).$$

Note que em todos os casos usamos recursivamente o valor de Fml calculado em um número de Gödel estritamente menor que y: no primeiro caso usamos $\mathrm{Fml}(z)$ onde $y = 2^5 * z$ e portanto $z < y$, e nos demais usamos $\mathrm{Fml}((z)_0)$ e $\mathrm{Fml}((z)_1)$ onde $y = 2^i * (z)_0 * (z)_1$ e portanto $(z)_0 < y$ e $(z)_1 < y$. Desta forma a recursividade primitiva da relação acima segue, de forma análoga ao que fizemos anteriormente, do Teorema 5.33.

12. $\mathrm{Subst}(x, y, z, v)$: seja y o número de Gödel de uma expressão φ, u o número de Gödel de um termo t e v o número de Gödel de uma variável w. Então valem $\mathrm{Gd}(y)$, $\mathrm{Trm}(u)$ e $\mathrm{EV}(2^v)$. Como feito nas demonstrações anteriores, nossa estratégia para avaliar a substituição de uma variável por um termo será partir a expressão em expressões com número de Gödel estritamente menor que o número de Gödel da expressão inicial para que possamos aplicar recursividade nestas novas menores, avaliar a substituição das ocorrências livres de w por t e invocar o Teorema 5.33. Para isto, trataremos primeiro o caso em que φ é uma expressão com um único símbolo. Nesta caso há duas possibilidades: φ é a expressão constituída pelo símbolo w ou φ é a expressão constituída por um símbolo diferente de w. No primeiro caso a substituição $[\varphi]^t_w$ resulta na expressão t, e então x, o número de Gödel de $[\varphi]^t_w$, é igual a u. Assim vale que $y = 2^v \wedge x = u$. No segundo caso, a substituição $[\varphi]^t_w$ não muda a fórmula φ, e portanto o número de Gödel da expressão $[\varphi]^t_w$ é ainda y, e existe algum s que é o número de Gödel do símbolo que constitui φ e $y = 2^s$. Vale portanto que $\exists s_{s<y}(y = 2^s \ \wedge \ y \neq 2^v \ \wedge x = y)$.

   Já tratamos o caso em que φ é uma expressão constituída por um único símbolo. Vamos considerar agora que φ possui ao menos dois símbolos. Suponha, por exemplo, que φ seja a fórmula $\forall w = ww$ (isto é, $\forall w(w = w)$ na notação usual). Ao tentar partir esta expressão em duas expressões menores poderíamos tentar separar nas expressões $\forall$ e $w = ww$. Mas note que na segunda expressão a ocorrência de w é livre, sendo assim ao realizar a substituição das ocorrências livres de w por t obteríamos a expressão $t\,t = t$, quando na verdade estamos interessados na substituição $[\varphi]^t_w$ que é a própria fórmula φ, já que a ocorrência de w não é livre. O mesmo problema iria ocorrer se φ fosse uma fórmula ou uma expressão que se inicie com um quantificador existencial.

Para evitar que isto ocorra, vamos separar em dois casos: quando φ é uma expressão que se inicia com um quantificador universal ou existencial com w sendo a variável que segue os símbolos $\forall$ e $\exists$, e quando isto não ocorre. No primeiro caso iremos manter a numeração de Gödel da fórmula inicial e usar a recursividade no restante da expressão, e no segundo caso olharemos para as subexpressões formadas pelo primeiro símbolo de φ e pelo restante dos símbolos (lembre-se de que estamos no caso em que φ possui ao menos 2 símbolos).

(a) Caso 1: existe uma fórmula ψ com número de Gödel s tal que φ se inicia com a fórmula $\forall w\psi$ ou $\exists w\psi$. Neste caso note que podemos expressar a relação $\mathrm{Subst}(x, y, u, v)$ pela seguinte relação:

$$\exists z_{z<y}\exists s_{s<y}(\mathrm{Fml}(s) \wedge (y = 2^{15} * 2^{v} * s * z \vee y = 2^{17} * 2^{v} * s * z)\wedge$$

$$\exists \alpha_{\alpha<x}((x = 2^{15} * 2^{v} * s * \alpha \vee x = 2^{17} * 2^{v} * s * \alpha) \wedge \mathrm{Subst}(\alpha, z, u, v))).$$

(b) Caso 2: não existe uma fórmula ψ com número de Gödel s tal que φ se inicia com a fórmula $\forall w\psi$ ou $\exists w\psi$. Neste caso iremos separar a subexpressão dada pelo primeiro símbolo da expressão φ, que tem número de Gödel $(y)_0$, e vamos analisar separadamente as substituições dadas por Subst nessa expressão e na expressão formada pelo restante da expressão φ. Note então que podemos expressar relação $\mathrm{Subst}(x, y, u, v)$ pela seguinte relação:

$$\neg(\exists z_{z<y}\exists s_{s<y}(\mathrm{Fml}(s) \wedge (y = 2^{15} * 2^{v} * s * z \vee y = 2^{17} * 2^{v} * s * z)) \wedge$$

$$\exists \alpha_{\alpha<x}\exists \beta_{\beta<x}\exists z_{z<y}(1 < z \ \wedge \ y = 2^{(y)_0} * z \ \wedge \ x = \alpha * \beta \ \wedge \ \mathrm{Subst}(\alpha, 2^{(y)_0}, u, v) \ \wedge$$

$$\mathrm{Subst}(\beta, z, u, v))).$$

Com isto, podemos expressar $\mathrm{Subst}(x, y, u, v)$ da seguinte forma:

$$\mathrm{Gd}(y) \wedge \mathrm{Trm}(u) \wedge \mathrm{EV}(2^{v}) \wedge ((y = 2^{v} \wedge x = u) \ \vee \ \exists s_{s<y}(y = 2^{s} \ \wedge \ y \neq 2^{v} \ \wedge x = y) \ \vee$$

$$\exists z_{z<y}\exists s_{s<y}(\mathrm{Fml}(s) \wedge (y = 2^{15} * 2^{v} * s * z \vee y = 2^{17} * 2^{v} * s * z)\wedge$$

$$\exists \alpha_{\alpha<x}((x = 2^{15} * 2^{v} * s * \alpha \vee x = 2^{17} * 2^{v} * s * \alpha) \wedge \mathrm{Subst}(\alpha, z, u, v))) \ \vee$$

$$\neg((\exists z_{z<y}\exists s_{s<y}(\mathrm{Fml}(s) \wedge (y = 2^{15} * 2^{v} * s * z \vee y = 2^{17} * 2^{v} * s * z)) \wedge$$

$$\exists \alpha_{\alpha<x} \exists \beta_{\beta<x} \exists z_{z<y} (1 < z \ \wedge \ y = 2^{(y)_0} * z \ \wedge \ x = \alpha * \beta$$
$$\wedge \ \mathrm{Subst}(\alpha, 2^{(y)_0}, u, v) \ \wedge \ \mathrm{Subst}(\beta, z, u, v)))))$$

Resta agora verificar que tal relação é primitiva recursiva. Note que não podemos usar diretamente o Teorema 5.33 pois estamos usando a recursividade simultânea dos dois primeiros argumentos de Subst. Considere a relação $\mathrm{R}(q, u, v)$ dada por:

$$\mathrm{Gd}((q)_1) \wedge \mathrm{Trm}(u) \wedge \mathrm{EV}(2^v) \wedge \Big(((q)_1 = 2^v \wedge (q)_0 = u) \ \vee$$
$$\exists s_{s<(q)_1} ((q)_1 = 2^s \ \wedge \ (q)_1 \neq 2^v \ \wedge (q)_0 = (q)_1) \ \vee$$
$$\exists z_{z<(q)_1} \exists s_{s<(q)_1} (\mathrm{Fml}(s) \wedge ((q)_1 = 2^{15} * 2^v * s * z \vee (q)_1 = 2^{17} * 2^v * s * z) \wedge$$
$$\exists \alpha_{\alpha<(q)_0} (((q)_0 = 2^{15} * 2^v * s * \alpha \vee (q)_0 = 2^{17} * 2^v * s * \alpha) \wedge \mathrm{R}(2^\alpha 3^z, u, v))) \ \vee$$
$$\neg (\exists z_{z<(q)_1} \exists s_{s<(q)_1} (\mathrm{Fml}(s) \wedge ((q)_1 = 2^{15} * 2^v * s * z \vee (q)_1 = 2^{17} * 2^v * s * z)) \wedge$$
$$\exists \alpha_{\alpha<(q)_0} \exists \beta_{\beta<(q)_0} \exists z_{z<(q)_1} (1 < z \wedge (q)_1 = 2^{((q)_1)_0} * z \ \wedge \ (q)_0 = \alpha * \beta \ \wedge \ \mathrm{R}(2^\alpha 3^{2^{((q)_1)_0}}, u, v) \ \wedge$$
$$\mathrm{R}(2^\beta 3^z, u, v)))\Big).$$

Pelo Teorema 5.33 temos que $\mathrm{R}(q, u, v)$ é uma relação primitiva recursiva, e note que $\mathrm{R}(q, u, v)$ coincide com $\mathrm{Subst}(x, y, u, v)$ quando $q = 2^x 3^y$. Desta forma segue que $\mathrm{Subst}(x, y, u, v)$ é primitiva recursiva, como queríamos.

13. $\mathrm{Sub}(x, y, u, v)$: sejam y o número de Gödel de uma expressão φ, u o número de Gödel de um termo t e v o número de Gödel de uma variável w. Pela injetividade da numeração de Gödel, existe um único x que é o número de Gödel da expressão $[\varphi]^t_w$. Vimos no Teorema 5.28 que o operador de minimização restrito é primitivo recursivo quando limitado. E ainda, como vimos acima que x é único, tomar o menor x que satisfaz $\mathrm{Subst}(x, y, u, v)$ equivale a tomar o único x que satisfaz tal condição. Temos portanto que:

$$\mathrm{Sub}(y, u, v) = \mu x_{x<(p_{uy}!)^{uy}} \mathrm{Subst}(x, y, u, v),$$

e caso não exista um tal x que satisfaça $\mathrm{Subst}(x, y, u, v)$, definimos $\mathrm{Sub}(y, u, v)$ como qualquer natural. E como já vimos que Subst é uma relação primitiva recursiva, para concluir que a função Sub é primitiva recursiva basta justificar a limitação $x < (p_{uy}!)^{uy}$. Vamos analisar cada um dos casos que consideramos para a função Subst. Se $x = u$ então $x \leq p_x < p_{xy} = p_{uy} < p_{uy}! < (p_{uy}!)^{uy}$. E se $x = y$ vale um argumento análogo. Vamos então analisar o caso em que ocorre uma substituição não trivial (e onde φ não é uma expressão unitária).

Escreva $x = 2^{a_1} * 2^{a_2} * ... * 2^{a_r}$. Como x é o número de Gödel do resultado da substituição em φ de todas as ocorrências livres de w por t, então no máximo cada símbolo de φ (que tem número de Gödel y) será substituído por t (que tem número de Gödel u). Logo temos que $r < |u| \cdot |y|$, onde $|y|$ e $|u|$ representam, respectivamente, a quantidade de fatores primos com expoentes não nulo na fatoração de y e u (ou, equivalentemente, a quantidade de símbolos em φ e em t). E ainda, cada a_i é o número de Gödel de um símbolo que ocorre em t ou em φ, logo $a_i \leq y$ (note que a desigualdade é estrita pois já descartamos o caso em que φ é uma expressão unitária) e $a_i \leq u$, assim, $a_i < uy$. Portanto vale:

$$x = 2^{a_1} * 2^{a_2} * ... * 2^{a_r} < 2^{uy} \cdot 3^{uy} \cdot ... \cdot p_{uy}^{uy} = (p_{uy}!)^{uy}.$$

Com isto, concluímos a prova de que Sub é primitiva recursiva.

14. Fr(y, v): seja φ uma fórmula ou um termo com úmero de Gödel y que contém ocorrência livre de uma variável x com número de Gödel v. Então vale Fml(y) caso φ seja uma fórmula, ou Trm(y) caso φ seja um termo. E sendo x uma variável com número de Gödel v, vale EV(2^v). E ainda, se há ocorrência livre de x em φ, então se fizermos a substituição $[\varphi]_x^\tau$ onde τ é um termo constituído por uma única variável diferente de x, então a expressão $[\varphi]_x^\tau$ terá número de Gödel diferente de y, pois iremos obter uma expressão diferente. Notando que, para todo número natural v, temos que $13+8v$ é um número estritamente maior que v, e ainda é o número de Gödel de uma variável, e portanto representa uma variável diferente de x, temos que vale $\neg$Subst$(y, y, 2^{13+8v}, v)$ (isto é, a substituição em φ de todas as ocorrências livres de x por uma variável diferente de x resulta necessariamente em uma expressão diferente).

    Portanto Fr(y, v) pode ser expresso pela seguinte relação:

    $$(\mathrm{Fml}(y) \vee \mathrm{Trm}(y)) \wedge \mathrm{EV}(2^v) \wedge \neg\mathrm{Subst}(y, y, 2^{13+8v}, v).$$

    Como já vimos que Fml, Trm, EV e Subst são primitivas recursivas, segue que Fr também é.

15. Ff(u, v, w): sejam τ um termo livre para uma variável x em uma fórmula φ,

onde u é o número de Gödel de τ, w o número de Gödel de φ e v o número de Gödel da variável x. Então valem $\mathrm{Trm}(u) \wedge \mathrm{EV}(2^v) \wedge \mathrm{Fml}(w)$. Como fizemos antes, iremos partir a fórmula φ em expressões menores de modo que a recursividade dada pelo Teorema 5.33 garanta o resultado nestas expressões menores. Para isso, trataremos cada um dos tipos de fórmulas de acordo com sua regra de formação.

Para o caso em que φ é uma fórmula atômica vale $\mathrm{Atfml}(w)$. O caso em que φ é do tipo$\neg\psi$, se tomarmos por y o número de Gödel de ψ, temos que $w = 2^5 * y$ valendo $\mathrm{Ff}(u, v, y)$. O caso em que φ é de algum dos tipos $\wedge\psi_1\psi_2$, $\vee\psi_1\psi_2$, $\rightarrow \psi_1\psi_2$, $\leftrightarrow \psi_1\psi_2$ pode ser expresso pela seguinte relação:

$$\exists y_{y<w} \exists z_{z<w} (\mathrm{Ff}(u, v, y) \wedge \mathrm{Ff}(u, v, z) \wedge (w = 2^7 * y * z \ \vee \ w = 2^9 * y * z \vee \\ w = 2^{11} * y * z \ \vee \ w = 2^{13} * y * z)).$$

E o caso em que φ é da forma $\forall z\psi$ ou $\exists z\psi$, para alguma variável z, são os casos em que é necessário um cuidado especial. Vamos fazer detalhadamente o caso em que φ é do tipo $\forall z\psi$ e o outro caso segue de forma análoga.

Sendo τ um termo livre para x em φ, temos que se z ocorre em τ então nenhuma ocorrência livre de x ocorre em φ. E como τ é um termo, toda ocorrência de uma variável é livre, e portanto podemos reformular esta afirmação da seguinte maneira: se z ocorrer de forma livre em τ, então x não ocorre de forma livre em ψ, isto é, $\mathrm{Fr}(u, z) \rightarrow \neg\mathrm{Fr}(y, v)$.

Mas ainda temos que analisar a ocorrência de quantificadores existenciais ou universais dentro da fórmula ψ (e aí podemos usar a recursividade dada pelo Teorema 5.33). Há duas possibilidades: $z = x$ ou $z \neq x$. Se $z = x$, então x ocorre de forma limitada em φ, e neste caso, não há nada a se fazer. Se $z \neq x$, então temos que τ é livre para x em ψ, e portanto vale $z \neq v \rightarrow \mathrm{Ff}(u, v, y)$.

Sendo assim, quando φ é da forma $\forall z\psi$, podemos representar a relação $\mathrm{Ff}(u, v, w)$ por

$$\exists y_{y<w} \exists z_{z<w} (w = 2^{15} * 2^z * y \wedge \mathrm{EV}(2^z) \wedge (z \neq v \rightarrow \mathrm{Ff}(u, v, y)) \wedge (\mathrm{Fr}(u, z) \rightarrow \neg\mathrm{Fr}(y, v))).$$

O raciocínio para quando φ é da forma $\exists z\psi$ é semelhante, o que nos dá, no caso geral para φ da forma $\forall z\psi$ ou $\exists z\psi$, a seguinte relação:

$$\exists y_{y<w} \exists z_{z<w} ((w = 2^{15} * 2^z * y \vee w = 2^{17} * 2^z * y) \wedge \mathrm{EV}(2^z) \wedge$$

$$(z \neq v \rightarrow \mathrm{Ff}(u,v,y)) \wedge (\mathrm{Fr}(u,z) \rightarrow \neg \mathrm{Fr}(y,v))).$$

E, de forma geral, $\mathrm{Ff}(u,v,w)$ pode ser dada por:

$$\mathrm{Trm}(u) \wedge \mathrm{EV}(2^v) \wedge \mathrm{Fml}(w) \wedge (\mathrm{Atfml}(w) \ \vee \ \exists y_{y<w}(w = 2^5 * y \ \wedge \mathrm{Ff}(u,v,y)) \ \vee$$

$$\exists y_{y<w} \exists z_{z<w}(\mathrm{Ff}(u,v,y) \wedge \mathrm{Ff}(u,v,z) \wedge (w = 2^7 * y * z \ \vee \ w = 2^9 * y * z \ \vee \ w = 2^{11} * y * z \ \vee$$
$$w = 2^{13} * y * z)) \ \vee$$

$$\exists y_{y<w} \exists z_{z<w}((w = 2^{15} * 2^z * y \vee w = 2^{17} * 2^z * y) \wedge \mathrm{EV}(2^z) \wedge (z \neq v \rightarrow \mathrm{Ff}(u,v,y)) \wedge$$
$$(\mathrm{Fr}(u,z) \rightarrow \neg \mathrm{Fr}(y,v)))).$$

Segue então do Teorema 5.33 (e dos itens anteriores) que Ff é primitiva recursiva.

16. $\mathrm{Neg}(x)$: seja φ uma expressão com números de Gödel x. Basta notar que $\mathrm{Neg}(x) = 2^5 * x$.

17. $\mathrm{Cond}(x,y)$: sejam φ e ψ expressões com número de Gödel x e y, respectivamente. Basta notar que $\mathrm{Cond}(x,y) = 2^{11} * x * y$.

18. $\mathrm{Clos}(u)$: seja φ uma fórmula com número de Gödel u. Defina primeiro $\mathrm{V}(u) = \mu v_{v \leq u}(\mathrm{EV}(2^v) \wedge \mathrm{Fr}(u,v))$. Temos que $\mathrm{V}(u)$ expressa o menor número de Gödel de uma variável que ocorre de forma livre em φ — e caso uma tal variável não exista, dê quaquer valor natural para $V(u)$. Por exemplo, para uma fórmula ψ onde há ocorrência livre somente das variáveis x_2, x_3 e x_6, temos que $\mathrm{V}(g(\varphi)) = g(x_2)$. Já vimos que EV e Fr são relações primitivas recursivas, e o operador de minimização restrito também é, quando limitado. Logo $\mathrm{V}(u)$ é primitiva recursiva. Defina agora $\mathrm{Sent}(u) = \mathrm{Fml}(u) \wedge \neg(\exists v_{v \leq u} \mathrm{Fr}(u,v))$. Temos que $\mathrm{Sent}(u)$ expressa quando a fórmula φ é uma sentença ou não (isto é, quando há ocorrência de alguma variável livre em φ ou não). Sendo Fml e Fr relações primitivas recursivas, assim como quantificadores limitados, segue que Sent é uma relação primitiva recursiva. Defina assim a seguinte função:

$$G(u) = \begin{cases} 2^{15} * 2^{V(u)} * u, & \text{se } \mathrm{Fml}(u) \wedge \neg \mathrm{Sent}(u) \\ u, & \text{caso contrário.} \end{cases}$$

Isto é, se ϕ é uma fórmula que não é uma sentença, então olhamos para a variável (que ocorre livremente em ϕ) com o menor número de Gödel, digamos x, e retornamos em G(u) o número de Gödel da fórmula $\forall x\phi$. E caso ϕ seja uma sentença, retornamos em G(u) o próprio u. Pelo Exemplo 5.19, itens $2, 4, 5$ e 10 e por substituição segue que G(u) é primitiva recursiva.

A ideia é olhar para a fórmula inicial e adicionar o fecho de cada uma das variáveis livres que ocorrem nesta fórmula em ordem decrescente, e obter, ao final, a sentença dada pelo fecho universal da fórmula inicial. Faremos isto usando recursão. Defina a relação H dada, recursivamente, da seguinte forma:

$$H(u,0) = G(u),$$

$$H(u,y+1) = G(H(u,y)).$$

Por recursão, substituição e pelo que vimos acima, temos que H é primitiva recursiva. Por fim, note que:

$$\mathrm{Clos}(u) = H(u, \mu y_{y \leq u} H(u,y) = H(u,y+1)).$$

Para o exemplo do início, onde ψ era uma fórmula que tinha ocorrências livres somente das variáveis x_2, x_3 e x_6, se tomarmos por u o número de Gödel de ψ, temos que vale:

$$H(u,0) = G(u) = g(\forall x_2 \psi).$$

$$H(u,1) = G(H(u,0)) = G(g(\forall x_2 \psi)) = g(\forall x_3 \forall x_2 \psi).$$

$$H(u,2) = G(H(u,1)) = G(g(\forall x_3 \forall x_2 \psi)) = g(\forall x_6 \forall x_3 \forall x_2 \psi).$$

$$H(u,3) = G(H(u,2)) = G(g(\forall x_6 \forall x_3 \forall x_2 \psi)) = g(\forall x_6 \forall x_3 \forall x_2 \psi).$$

Logo, $\mathrm{Clos}(u) = H(u,3) = g(\forall x_6 \forall x_3 \forall x_2 \psi)$.

Por fim, como vimos que H é primitiva recursiva, assim como o operador de minimização restrito limitado, segue, por substituição, que Clos(u) é uma relação primitiva recursiva.

19. Os axiomas lógicos são sentenças que são fechos universais de certos tipos de fórmula, descritas na Definição 3.2. Note que o primeiro item da nossa lista de axiomas lógicos trata de todas as tautologias. Segue do Teorema 6.7 que todas as tautologias podem ser provadas por Modus Ponens a partir de 9 tautologias. Assim, para provarmos este item, iremos mostrar a recursividade destas

9 tautologias. E ainda, nosso conjunto de axiomas abrangia todo fecho universal de um dos esquemas dados na Definição 3.2. Para fins práticos, iremos considerar somente o fecho universal que foi fixado no item anterior — pelo Teorema 5.44 isto basta, pois a prova de todo fecho universal pode ser obtida a partir da prova de um deles:

Desta forma, considere as seguintes relações.

(a) $\mathrm{Axt}_1(x)$: x é o número de Gödel do fecho universal de uma instância de tautologia da forma $\varphi \to (\psi \to \varphi)$. Para tal, basta notar que $\mathrm{Axt}_1(x)$ pode ser reescrita como:

$$\exists u_{u<x} \exists v_{v<x} (\mathrm{Fml}(u) \wedge \mathrm{Fml}(v) \wedge \mathrm{Clos}(2^{11} * u * 2^{11} * v * u)).$$

(b) $\mathrm{Axt}_2(x)$: x é o número de Gödel de um fecho universal de uma instância de tautologia da forma $(\varphi \to (\psi \to \phi)) \to ((\varphi \to \psi) \to (\varphi \to \phi))$. Para tal, basta notar que $\mathrm{Axt}_2(x)$ pode ser reescrita como:

$$\exists u_{u<x} \exists v_{v<x} \exists w_{w<x} (\mathrm{Fml}(u) \wedge \mathrm{Fml}(v) \wedge \mathrm{Fml}(w) \wedge$$

$$x = \mathrm{Clos}(2^{11} * 2^{11} * u * 2^{11} * v * w * 2^{11} * 2^{11} * u * v * 2^{11} * u * w)).$$

(c) $\mathrm{Axt}_3(x)$: x é o número de Gödel de um fecho universal de uma instância de tautologia da forma $(\neg\varphi \to \neg\psi) \to ((\neg\varphi \to \psi) \to \varphi)$. Para tal, basta notar que $\mathrm{Axt}_3(x)$ pode ser reescrita como:

$$\exists u_{u<x} \exists v_{v<x} (\mathrm{Fml}(u) \wedge \mathrm{Fml}(v) \wedge$$

$$x = \mathrm{Clos}(2^{11} * 2^{11} * 2^{5} * u * 2^{5} * v * 2^{11} * 2^{11} * 2^{5} * u * v * u)).$$

(d) $\mathrm{Axt}_4(x)$: x é o número de Gödel de um fecho universal de uma instância de tautologia da forma $(\varphi \wedge \psi) \leftrightarrow \neg(\varphi \to \neg\psi)$. Para tal, basta notar que $\mathrm{Axt}_4(x)$ pode ser reescrita como:

$$\exists u_{u<x} \exists v_{v<x} (\mathrm{Fml}(u) \wedge \mathrm{Fml}(v) \wedge x = \mathrm{Clos}(2^{13} * 2^{7} * u * v * 2^{5} * 2^{11} * u * 2^{5} * v)).$$

(e) $\mathrm{Axt}_5(x)$: x é o número de Gödel de um fecho universal de uma instância de tautologia da forma $(\varphi \vee \psi) \leftrightarrow (\neg\varphi \to \psi)$. Para tal, basta notar que

$\mathrm{Axt}_5(x)$ pode ser reescrita como:

$$\exists u_{u<x} \exists v_{v<x} (\mathrm{Fml}(u) \land \mathrm{Fml}(v) \land x = \mathrm{Clos}(2^{13} * 2^9 * u * v * 2^{11} * 2^5 * u * v)).$$

(f) $\mathrm{Axt}_6(x)$: x é o número de Gödel de um fecho universal de uma instância de tautologia da forma $(\varphi \leftrightarrow \psi) \to (\varphi \to \psi)$. Para tal, basta notar que $\mathrm{Axt}_6(x)$ pode ser reescrita como:

$$\exists u_{u<x} \exists v_{v<x} (\mathrm{Fml}(u) \land \mathrm{Fml}(v) \land x = \mathrm{Clos}(2^{11} * 2^{13} * u * v * 2^{11} * u * v)).$$

(g) $\mathrm{Axt}_7(x)$: x é o número de Gödel de um fecho universal de uma instância de tautologia da forma $(\varphi \leftrightarrow \psi) \to (\psi \to \varphi)$. Para tal, basta notar que $\mathrm{Axt}_7(x)$ pode ser reescrita como:

$$\exists u_{u<x} \exists v_{v<x} (\mathrm{Fml}(u) \land \mathrm{Fml}(v) \land x = \mathrm{Clos}(2^{11} * 2^{13} * u * v * 2^{11} * v * u)).$$

(h) $\mathrm{Axt}_8(x)$: x é o número de Gödel de um fecho universal de uma instância de tautologia da forma $((\varphi \to \psi) \land (\psi \to \varphi)) \to (\varphi \leftrightarrow \psi)$. Para tal, basta notar que $\mathrm{Axt}_8(x)$ pode ser reescrita como:

$$\exists u_{u<x} \exists v_{v<x} (\mathrm{Fml}(u) \land \mathrm{Fml}(v) \land x = \mathrm{Clos}(2^{11} * 2^7 * 2^{11} * u * v * 2^{11} * v * u * 2^{13} * u * v)).$$

(i) $\mathrm{Axt}_9(x)$: x é o número de Gödel de um fecho universal de uma instância de tautologia da forma $\varphi \to (\psi \to (\varphi \land \psi))$. Para tal, basta notar que $\mathrm{Axt}_9(x)$ pode ser reescrita como:

$$\exists u_{u<x} \exists v_{v<x} (\mathrm{Fml}(u) \land \mathrm{Fml}(v) \land x = \mathrm{Clos}(2^{11} * u * 2^{11} * v * 2^7 * u * v)).$$

(j) $\mathrm{Ax}_2(x)$: x é o número de Gödel do fecho universal de uma instância de uma fórmula do tipo $\varphi \to \forall y \varphi$, onde y não é livre em φ. Para tal, basta notar que $\mathrm{Ax}_2(x)$ pode ser reescrita como:

$$\exists u_{u<x} \exists v_{v<x} (\mathrm{Fml}(u) \land \mathrm{EV}(2^v) \land \neg \mathrm{Fr}(u, v) \land x = \mathrm{Clos}(2^{11} * u * 2^{15} * 2^v * u)).$$

(k) $\mathrm{Ax}_3(x)$: x é o número de Gödel do fecho universal de uma instância de uma fórmula do tipo $\forall y(\varphi \to \psi) \to (\forall y \varphi \to \forall y \psi)$. Para tal, basta notar que $\mathrm{Ax}_3(x)$ pode ser reescrita como:

$$\exists u_{u<x} \exists v_{v<x} \exists w_{w<x} (\mathrm{Fml}(u) \wedge \mathrm{Fml}(v) \wedge \mathrm{EV}(2^w) \wedge$$

$$x = \mathrm{Clos}(2^{11} * 2^{15} * 2^w * 2^{11} * u * v * 2^{11} * 2^{15} * 2^w * u * 2^{15} * 2^w * v)).$$

(l) $\mathrm{Ax}_4(x)$: x é o número de Gödel do fecho universal de uma instância de uma fórmula do tipo $\forall x\varphi \to [\varphi]_y^\tau$, onde τ é um termo arbitrário, livre para y em φ. Para tal, basta notar que $\mathrm{Ax}_4(x)$ pode ser reescrita como:

$$\exists u_{u<x} \exists v_{v<x} \exists w_{w<x} (\mathrm{Fml}(u) \wedge \mathrm{Trm}(v) \wedge \mathrm{EV}(2^w) \wedge \mathrm{Ff}(v, w, u) \wedge$$

$$x = \mathrm{Clos}(2^{11} * 2^{15} * 2^w * u * \mathrm{Sub}(u, v, w))).$$

(m) $\mathrm{Ax}_5(x)$: x é o número de Gödel do fecho universal de uma instância de uma fórmula do tipo $[\varphi]_y^\tau \to \exists y\varphi$, onde τ é um termo arbitrário, livre para y em φ. Para tal, basta notar que $\mathrm{Ax}_5(x)$ pode ser reescrita como:

$$\exists u_{u<x} \exists v_{v<x} \exists w_{w<x} (\mathrm{Fml}(u) \wedge \mathrm{Trm}(v) \wedge \mathrm{EV}(2^w) \wedge \mathrm{Ff}(v, w, u) \wedge$$

$$x = \mathrm{Clos}(2^{11} * \mathrm{Sub}(u, v, w) * 2^{17} * 2^w * u)).$$

(n) $\mathrm{Ax}_6(x)$: x é o número de Gödel do fecho universal de uma instância de uma fórmula do tipo $\forall y \neg\varphi \leftrightarrow \neg\exists y\varphi$. Para tal, basta notar que $\mathrm{Ax}_6(x)$ pode ser reescrita como:

$$\exists u_{u<x} \exists w_{w<x} (\mathrm{Fml}(u) \wedge \mathrm{EV}(2^w) \wedge x = \mathrm{Clos}(2^{13} * 2^{15} * 2^w * 2^5 * u * 2^5 * 2^{17} * 2^w * u)).$$

(o) $\mathrm{Ax}_7(x)$: x é o número de Gödel do fecho universal de uma instância de uma fórmula do tipo $y = y$. Para tal, basta notar que $\mathrm{Ax}_7(x)$ pode ser reescrita como:

$$\exists w_{w<x} (\mathrm{EV}(2^w) \wedge x = \mathrm{Clos}(2^3 * 2^w * 2^w)).$$

(p) $\mathrm{Ax}_8(x)$: x é o número de Gödel do fecho universal de uma instância de uma fórmula do tipo $z = y \leftrightarrow y = z$. Para tal, basta notar que $\mathrm{Ax}_8(x)$ pode ser reescrita como:

$$\exists u_{u<x} \exists w_{w<x} (\mathrm{EV}(2^w) \wedge \mathrm{EV}(2^u) \wedge x = \mathrm{Clos}(2^{13} * 2^3 * 2^u * 2^w * 2^3 * 2^w * 2^u)).$$

(q) $\text{Ax}_9(x)$: x é o número de Gödel do fecho universal de uma instância de uma fórmula do tipo $(p = y \wedge y = z) \to p = z$. Para tal, basta notar que $\text{Ax}_9(x)$ pode ser reescrita como:

$$\exists u_{u<x} \exists v_{v<x} \exists w_{w<x} (\text{EV}(2^u) \wedge \text{EV}(2^v) \wedge \text{EV}(2^w) \wedge$$

$$x = \text{Clos}(2^{11} * 2^7 * 2^3 * 2^u * 2^v * 2^3 * 2^v * 2^w * 2^3 * 2^u * 2^w)).$$

(r) $\text{Ax}_{10}(x)$: x é o número de Gödel do fecho universal de uma instância de uma fórmula do tipo $(x_1 = y_1 \wedge x_2 = y_2 \wedge ... \wedge x_n = y_n) \to (f x_1 x_2 ... x_n = f y_1 y_2 ... y_n)$, para todo $n > 0$ e $f \in \mathcal{F}_n$. Como nossa linguagem é $\mathcal{L}_{\mathcal{A}}$, temos as funções binárias $+$ e $\cdot$ e a função unária s. Logo deve valer:

$$(x_1 = y_1 \wedge x_2 = y_2) \to x_1 + x_2 = y_1 + y_2,$$

$$(x_1 = y_1 \wedge x_2 = y_2) \to x_1 \cdot x_2 = y_1 \cdot y_2, \text{ e}$$
$$x_1 = y_1 \to s(x_1) = s(y_1).$$

Portanto $\text{Ax}_{10}(x)$ pode ser reescrita como:

$$\exists {u_1}_{u_1<x} \exists {u_2}_{u_2<x} \exists {v_1}_{v_1<x} \exists {v_2}_{v_2<x} \exists w_{w<x} (\text{EV}(2^{u_1}) \wedge \text{EV}(2^{u_2}) \wedge \text{EV}(2^{v_1}) \wedge \text{EV}(2^{v_2}) \wedge \text{EF}(w)$$

$$\wedge x = \text{Clos}(2^{11} * 2^7 * 2^3 * 2^{u_1} * 2^{v_1} * 2^3 * 2^{u_2} * 2^{v_2} * 2^{13} * 2^w * 2^{u_1} * 2^{u_2} * 2^w * 2^{v_1} * 2^{v_2}) \vee$$
$$x = \text{Clos}(2^{11} * 2^3 * 2^{u_1} * 2^{v_1} * 2^{13} * 2^w * 2^{u_1} * 2^w * 2^{v_1}))$$

(s) $\text{Ax}_{11}(x)$: x é o número de Gödel do fecho universal de uma instância de uma fórmula do tipo $(x_1 = y_1 \wedge x_2 = y_2 \wedge ... \wedge x_n = y_n) \to (p(x_1, x_2, ..., x_n) \leftrightarrow p(y_1, y_2, ..., y_n))$, para todo $n > 0$ e $p \in \mathcal{P}_n$. Para este caso, notamos que, como T é uma teoria na linguagem $\mathcal{L}_{\mathcal{A}}$ que não possui símbolo de relação, então esta relação é vazia.

Por fim, para concluir que a relação $\text{LAx}(x)$ é primitiva recursiva, basta notar que ela pode ser representada pela seguinte relação:

$$\text{Axt}_1(x) \vee \text{Axt}_2(x) \vee \text{Axt}_3(x) \vee \text{Axt}_4(x) \vee \text{Axt}_5(x) \vee \text{Axt}_6(x) \vee \text{Axt}_7(x) \vee \text{Axt}_8(x) \vee \text{Axt}_9(x)$$

$$\vee \text{Ax}_2(x) \vee \text{Ax}_3(x) \vee \text{Ax}_4(x) \vee \text{Ax}_5(x) \vee \text{Ax}_6(x) \vee \text{Ax}_7(x) \vee \text{Ax}_8(x) \vee \text{Ax}_9(x) \vee$$
$$\text{Ax}_{10}(x) \vee \text{Ax}_{11}(x). \qquad \square$$

Teorema 5.46 *Seja T uma teoria de primeira ordem com um alfabeto primitivo recursivo (respectivamente, recursivo) que contém o símbolo de constante* 0 *(isto é, a_1) e o símbolo de função f_1^1 de $\mathcal{L}_A$. As seguintes relações e funções são primitivas recursivas (respectivamente, recursivas):*

1. *A função $Num(y)$, que retorna o número de Gödel da expressão $\overline{y}$.*
2. *$Nu(x)$: x é o número de Gödel de um numeral.*
3. *A **função diagonal** $D(u)$, que retorna o número de Gödel da fórmula $\varphi(\overline{u})$, onde u é o número de Gödel de uma fórmula $\varphi(x_1)$.*

Demonstração:

1. Como $g(a_1) = 23$ e $g(f_1^1) = 49$, temos que:

$$\mathrm{Num}(0) = 2^{23}$$

$$\mathrm{Num}(y+1) = 2^{49} * \mathrm{Num}(y).$$

   Assim, Num é primitiva recursiva (respectivamente, recursiva) porque pode ser obtida usando recursão e substituição.

2. Basta notar que x é o número de Gödel de um numeral quando $\exists y_{y<x}(x = \mathrm{Num}(y))$.

3. Basta notar que se u é o número de Gödel de uma fórmula $\varphi(x_1)$, então

$$D(u) = \mathrm{Sub}(u, \mathrm{Num}(u), 21).$$ □

Definição 5.47 *Dizemos que uma teoria de primeira ordem T possui um **conjunto de axiomas primitivo recursivo*** *(respectivamente, **recursivo**) quando a seguinte relação unária for primitiva recursiva (respectivamente, recursiva):*

$$nLAx(y): y \text{ é o número de Gödel de um axioma não lógico de } T.$$

Teorema 5.48 *A teoria $\mathcal{P}$ possui um conjunto de axiomas primitivo recursivo.*

Demonstração: Note que:

1. O axioma (A1), $\forall x_1(0 \neq s(x_1))$, possui número de Gödel $k_1 = 2^{15} * 2^{21} * 2^5 * 2^3 * 2^{23} * 2^{49} * 2^{21}$.

2. O axioma (A2), $\forall x_1 \forall x_2 (s(x_1) = s(x_2) \to x_1 = x_2)$, possui número de Gödel $k_2 = 2^{15} * 2^{21} * 2^{15} * 2^{29} * 2^{11} * 2^{3} * 2^{49} * 2^{21} * 2^{49} * 2^{29} * 2^{3} * 2^{21} * 2^{29}$.

3. O axioma (A3), $\forall x_1 (x_1 + 0 = x_1)$, possui número de Gödel $k_3 = 2^{15} * 2^{21} * 2^{3} * 2^{97} * 2^{21} * 2^{23} * 2^{21}$.

4. O axioma (A4), $\forall x_1 \forall x_2 (x_1 + s(x_2) = s(x_1 + x_2))$, possui número de Gödel $k_4 = 2^{15} * 2^{21} * 2^{15} * 2^{29} * 2^{3} * 2^{97} * 2^{21} * 2^{49} * 2^{29} * 2^{49} * 2^{97} * 2^{21} * 2^{29}$.

5. O axioma (A5), $\forall x_1 (x_1 \cdot 0 = 0)$ possui número de Gödel $k_5 = 2^{3} * 2^{289} * 2^{21} * 2^{23} * 2^{23}$.

6. O axioma (A6), $\forall x_1 \forall x_2 (x_1 \cdot s(x_2) = (x_1 \cdot x_2) + x_1)$ possui número de Gödel $k_6 = 2^{15} * 2^{21} * 2^{15} * 2^{29} * 2^{3} * 2^{289} * 2^{21} * 2^{49} * 2^{29} * 2^{97} * 2^{289} * 2^{21} * 2^{29} * 2^{21}$.

7. Temos que y é o número de Gödel de uma instância do axioma esquema (A7), isto é, de $\forall x_1 (\varphi(k_1) \to ((\forall x_1 (\varphi(x_1) \to \varphi(f_1^1(x_1)))))) \to \forall x_1 \varphi(x_1)$, se, e somente se,

$$\exists v_{v<y} \exists w_{w<y} (\mathrm{EV}(2^v) \wedge \mathrm{Fml}(w) \wedge$$
$$y = 2^{15} * 2^{21} * 2^{11} * 2^{11} * \mathrm{Sub}(w, 2^{23}, v) * 2^{15} * 2^{v} * 2^{11} * w * \mathrm{Sub}(w, 2^{49} * 2^{v}, v) * 2^{15} * 2^{v} * w).$$

Denotando a relação acima por $A_7(y)$, temos que a relação $\mathrm{nLAx}(y)$ vale exatamente quando:

$$y = k_1 \ \vee \ y = k_2 \ \vee y = k_3 \ \vee y = k_4 \ \vee y = k_5 \ \vee y = k_6 \ \vee A_7(y) \text{ vale.}$$

Pelo que vimos anteriormente, $A_7(y)$ é primitiva recursiva, e, portanto, $\mathrm{nLAx}(y)$ também é. □

Teorema 5.49 *Seja T uma teoria de primeira ordem que possui um alfabeto primitivo recursivo (respectivamente, recursivo) e um conjunto de axiomas primitivo recursivo (respectivamente, recursivo). Então as seguintes relações são primitivas recursivas (respectivamente, recursivas):*

1. $\mathrm{Ax}(y)$: *y é o número de Gödel de um axioma de T.*

2. $\mathrm{Prf}(y)$: *y é o número de Gödel de uma prova em T.*

3. $\mathrm{Pf}(y, x)$: *y é o número de Gödel de uma prova em T da sentença cujo número de Gödel é x.*

Demonstração:

1. Basta notar que $\mathrm{Ax}(y)$ é a relação $\mathrm{LAx}(y) \vee \mathrm{nLAx}(y)$, e como, nas condições do enunciado, $\mathrm{LAx}(y)$ e $\mathrm{nLAx}(y)$ são primitivas recursivas, segue o resultado.

2. De acordo com a Definição 3.4, temos que $\varphi_1, ..., \varphi_{n-1}, \varphi_n$ é uma prova para φ_n se cada φ_i é um axioma (lógico ou não lógico) ou se existem φ_j e φ_k com $j, k < i$ tais que φ_i é inferido de φ_j e φ_k por Modus Ponens. Como de costume, vamos separar em dois casos principais: quando a sequência em questão é unitária (e, neste caso, só pode ocorrer deste único elemento da sequência ser um axioma, pois não há expressões anteriores para que o seja inferido por Modus Ponens) e quando a sequência possui mais de um elemento (e, neste caso, quebraremos a sequência em duas sequências menores e usaremos a recursividade).

   Se tivermos uma sequência com uma única expressão, então y é o número de Gödel da prova dada por esta sequência quando $\exists w_{w<y}(y = 2^w \wedge \mathrm{Ax}(w))$.

   Se tivermos uma sequência com ao menos duas expressões, vamos quebrar esta sequência em duas sequências menores, de modo que a segunda será constituída apenas da última expressão. Assim, daremos conta da primeira subsequência por recursão, e analisaremos os dois casos possíveis para a última expressão: ser inferida por Modus Ponens de duas outras expressões anteriores ou ser um axioma.

   Para o caso em que uma expressão é inferida por Modus Ponens de duas anteriores, temos que existem u, v, w satisfazendo:

$$\mathrm{Prf}(u) \wedge y = u * 2^v \wedge \mathrm{MP}((u)_z, (u)_w, v).$$

   E para o caso da expressão seguinte ser um axioma, temos que existe v satisfazendo:

$$\mathrm{Prf}(u) \wedge y = u * 2^v \wedge \mathrm{Ax}(v).$$

   Em todo caso, temos que y é o número de Gödel de uma prova em T quando

$$\exists u_{u<y} \exists v_{v<y} \exists z_{z<y} \exists w_{w<y}((y = 2^w \wedge \mathrm{Ax}(w)) \vee \mathrm{Prf}(u) \wedge y = u * 2^v \wedge \mathrm{MP}((u)_z, (u)_w, v)) \vee$$

$$(\mathrm{Prf}(u) \wedge y = u * 2^v \wedge \mathrm{Ax}(v)).$$

   Como todas as relações e funções usadas acima são primitivas recursivas, segue que Prf é primitiva recursiva.

3. Se y é o número de Gödel de uma prova em T da sentença cujo número de Gödel é x, então existe uma sequência $\varphi_1, ..., \varphi_n$ de sentenças de T cujo número de Gödel (da sequência) é y, vale $\mathrm{Prf}(y)$ e x é o número de Gödel de φ_n, que é o último elemento da sequência, e portanto $x = (y)_{lh(y) \dot{-} 1}$. Dessa forma, podemos reescrever a relação $\mathrm{Pf}(y, x)$ como $\mathrm{Prf}(y) \wedge x = (y)_{lh(y) \dot{-} 1}$. □

Lema 5.50 *Seja T uma teoria em uma linguagem de primeira ordem $\mathcal{L}$ que contém o símbolo de constante 0 e o símbolo de função f_1^1 de $\mathcal{L}_{\mathcal{A}}$, cujos vocabulário e conjunto de axiomas sejam primitivos recursivos. Suponha que para quaisquer números naturais r e s tenha-se $r = s$ sempre que $T \vdash_{\mathcal{L}} \overline{r} = \overline{s}$. Então toda função representável em T é recursiva.*

Demonstração: Sejam $f(x_1, ..., x_n)$ uma função representável em T e $\mathcal{F}(x_1, ..., x_n, x_{n+1})$ uma fórmula de T que a represente. Considere a relação

$$\mathrm{P}_{\mathcal{F}}(u_1, ..., u_n, u_{n+1}, y) : y \text{ é o número de Gödel de uma prova de } \mathcal{F}(\overline{u}_1, ..., \overline{u}_n, \overline{u}_{n+1}) \text{ em } T.$$

Afirmamos que se vale $\mathrm{P}_{\mathcal{F}}(u_1, ..., u_n, u_{n+1}, y)$, então vale $f(u_1, ..., u_n) = u_{n+1}$. De fato, se vale $\mathrm{P}_{\mathcal{F}}(u_1, ..., u_n, u_{n+1}, y)$, temos que $T \vdash_{\mathcal{L}_{\mathcal{A}}} \mathcal{F}(\overline{u}_1, ..., \overline{u}_n, \overline{u}_{n+1})$. E se $f(u_1, ..., u_n) = r$ então, como $\mathcal{F}$ representa f, vale $T \vdash_{\mathcal{L}_{\mathcal{A}}} \mathcal{F}(\overline{u}_1, ..., \overline{u}_n, \overline{r})$. Da condição (2) de representabilidade temos $T \vdash_{\mathcal{L}_{\mathcal{A}}} \overline{u}_{n+1} = \overline{r}$. A hipótese do enunciado garante que $r = u_{n+1}$, logo, $f(u_1, ..., u_n) = u_{n+1}$.

Seja agora m o número de Gödel da fórmula $\mathcal{F}(x_1, ..., x_n, x_{n+1})$. Note que vale $\mathrm{P}_{\mathcal{F}}(u_1, ..., u_n, u_{n+1}, y)$ se, e somente se, vale

$$\mathrm{Pf}(y, \mathrm{Sub}(...\mathrm{Sub}(\mathrm{Sub}(m, \mathrm{Num}(u_1), 21), \mathrm{Num}(u_2), 29)...\mathrm{Num}(u_{n+1}), 21 + 8n)).$$

Pelo que vimos nos resultados anteriores, $\mathrm{P}_{\mathcal{F}}$ é uma relação primitiva recursiva.

Vejamos agora que para quaisquer $x_1, ..., x_n$ existe y tal que vale $\mathrm{P}_{\mathcal{F}}(x_1, ..., x_n, (y)_0, (y)_1)$. De fato, se $k_1, ..., k_n$ são números naturais, tome $r = f(k_1, ..., k_n)$. Como $\mathcal{F}$ representa f, $T \vdash_{\mathcal{L}_{\mathcal{A}}} \mathcal{F}(\overline{k}_1, ..., \overline{k}_n, \overline{r})$. Assim, podemos tomar j como o número de Gödel de uma prova de $\mathcal{F}(\overline{k}_1, ..., \overline{k}_n, \overline{r})$ em T. Com isto, vale $\mathrm{P}_{\mathcal{F}}(k_1, ..., k_n, r, j)$. Assim, basta tomar, por exemplo, $y = 2^r 3^j$ e teremos que vale $\mathrm{P}_{\mathcal{F}}(x_1, ..., x_n, (y)_0, (y)_1)$.

Temos, pelo Teorema 5.29, que a função $\mu y(\mathrm{P}_{\mathcal{F}}(x_1, ..., x_n, (y)_0, (y)_1))$ é recursiva. Por fim, basta notar que $f(x_1, ..., x_n) = (\mu y(\mathrm{P}_{\mathcal{F}}(x_1, ..., x_n, (y)_0, (y)_1)))_0$, e portanto, segue que f é recursiva, uma vez que a função $(\cdot)_0$ é recursiva. □

Teorema 5.51 *Se $\mathcal{P}$ é consistente, então uma função de números naturais é recursiva se, e somente se, é representável em $\mathcal{P}$.*

Demonstração: ($\Rightarrow$) Segue do Teorema 5.37.

($\Leftarrow$) Pelos Teoremas 5.48 e 5.43 temos que $\mathcal{P}$ possui vocabulário e conjunto de axiomas primitivos recursivos. Da consistência e do Teorema 5.3 segue que para quaisquer números naturais r e s tenha-se $r = s$ sempre que $\vdash_{\mathcal{L}_{\mathcal{A}}} \overline{r} = \overline{s}$. Estamos portanto nas condições do Lema 5.50, desta forma, segue que toda função de números naturais representável é recursiva. □

Teorema 5.52 *Se $\mathcal{P}$ é consistente, então uma relação nos números naturais R é recursiva se, e somente se, é e exprimível em $\mathcal{P}$.*

Demonstração: Pelo axioma não lógico $(A1)$ temos que $\mathcal{P} \vdash_{\mathcal{L}_{\mathcal{A}}} 0 \neq \overline{1}$. Com isso, segue do Teorema 5.16 que uma relação de números naturais R é exprimível se, e somente se, sua função característica χ_R é representável em $\mathcal{P}$. Pelo Teorema 5.51, χ_R é representável se, e somente se, é recursiva e, por definição, R é recursiva exatamente quando χ_R o é. □

5.5 Primeiro Teorema da Incompletude de Gödel

Notação 5.53 *Seja φ uma expressão de uma teoria na linguagem $\mathcal{L}_{\mathcal{A}}$ com número de Gödel q. Denotaremos o numeral $\overline{q}$ por $\ulcorner\varphi\urcorner$.*

Podemos pensar em $\ulcorner\varphi\urcorner$ como sendo um "nome"para a expressão φ dentro da linguagem $\mathcal{L}_{\mathcal{A}}$.

Lema 5.54 (Lema da Diagonalização) *Seja T uma teoria na linguagem $\mathcal{L}_{\mathcal{A}}$. Se a função diagonal D é representável em T, então para toda fórmula $\varphi(x_1)$ existe uma sentença ψ tal que $T \vdash_{\mathcal{L}_{\mathcal{A}}} \psi \leftrightarrow \varphi(\ulcorner\psi\urcorner)$.*

Demonstração: Seja $\varphi(x_1)$ uma fórmula de T, onde x_1 é a única variável livre em φ. Como D é representável em T, tome $\delta(x_1, x_2)$ uma fórmula que represente a função D em T. Considere a fórmula $\phi(x_1)$ dada por $\forall x_2(\delta(x_1, x_2) \to \varphi(x_2))$, e seja m o número de Gödel de $\phi(x_1)$. Considere agora a sentença ψ dada por $\phi(\overline{m})$, isto é, $\forall x_2(\delta(\overline{m}, x_2) \to \varphi(x_2))$, e seja q o número de Gödel de ψ. Temos que $D(m) = q$. Como δ representa D em T, segue que $T \vdash_{\mathcal{L}_{\mathcal{A}}} \delta(\overline{m}, \overline{q})$. Sendo assim, afirmamos que:

- $T \vdash_{\mathcal{L}_{\mathcal{A}}} \psi \to \varphi(\overline{q})$.

De fato, considere a seguinte sequência de sentenças:

1.ψ	Hipótese
2.$\forall x_2(\delta(\overline{m}, x_2) \to \varphi(x_2))$	Reescrevendo ψ
3.$\delta(\overline{m}, \overline{q}) \to \varphi(\overline{q})$	Por 2 e UI
4.$\delta(\overline{m}, \overline{q})$	Pois sabemos que $T \vdash_{\mathcal{L}_A} \delta(\overline{m}, \overline{q})$
5.$\varphi(\overline{q})$	Por 3, 4 e Modus Ponens

Tal sequência mostra que $T \cup \{\psi\} \vdash_{\mathcal{L}_A} \varphi(\overline{q})$. Assim, do Teorema da Dedução segue que $T \vdash_{\mathcal{L}_A} \psi \to \varphi(\overline{q})$.

- $T \vdash_{\mathcal{L}_A} \varphi(\overline{q}) \to \psi$.

  De fato, vejamos primeiro que $T \cup \{\delta(\overline{m}, x_2), \varphi(\overline{q})\} \vdash_{\mathcal{L}_A} \varphi(x_2)$:

1.$\varphi(\overline{q})$	Hipótese
2.$\delta(\overline{m}, x_2)$	Hipótese
3.$\exists! x_2 \delta(\overline{m}, x_2)$	Pois δ representa D
4.$\delta(\overline{m}, \overline{q})$	Pois sabemos que $T \vdash_{\mathcal{L}_A} \delta(\overline{m}, \overline{q})$
5.$x_2 = \overline{q}$	Por 2, 3, 4
6.$\varphi(x_2)$	Por 1, 5

  Com isso segue do Teorema da Dedução que $T \cup \{\varphi(\overline{q})\} \vdash_{\mathcal{L}_A} \delta(\overline{m}, x_2) \to \varphi(x_2)$. Pela regra de quantificadores UG segue que $T \cup \{\varphi(\overline{q})\} \vdash_{\mathcal{L}_A} \forall x_2(\delta(\overline{m}, x_2) \to \varphi(x_2))$, e novamente pelo Teorema da Dedução temos $T \vdash_{\mathcal{L}_A} \varphi(\overline{q}) \to \forall x_2(\delta(\overline{m}, x_2) \to \varphi(x_2))$. Notando que a sentença $\forall x_2(\delta(\overline{m}, x_2) \to \varphi(x_2))$ é ψ, segue o resultado da afirmação.

  Com as duas afirmações acima concluímos que $T \vdash_{\mathcal{L}_A} (\psi \leftrightarrow \varphi(\overline{q}))$, isto é, $T \vdash_{\mathcal{L}_A} \psi \to \varphi(\ulcorner \psi \urcorner)$, como queríamos. $\square$

Teorema 5.55 (Teorema do Ponto Fixo) *Se T é uma teoria na linguagem $\mathcal{L}_A$ tal que toda função recursiva é representável em T, então para toda fórmula $\varphi(x_1)$ existe uma sentença ψ tal que $T \vdash_{\mathcal{L}_A} \psi \leftrightarrow \varphi(\ulcorner \psi \urcorner)$.*

Demonstração: Pelo Teorema 5.46, a função D é recursiva, logo é representável em T. Sendo assim, basta aplicar o Lema da Diagonalização. $\square$

Note que, em particular, o Teorema 5.55 é válido para $T = \mathcal{P}$.

Definição 5.56 *Seja T uma teoria de primeira ordem cuja linguagem $\mathcal{L}$ contém o símbolo de constante 0 e o símbolo de função f_1^1 de $\mathcal{L}_\mathcal{A}$. Dizemos que T é **ω-consistente** se, para toda fórmula $\varphi(x)$ de T, onde x é a única variável livre em φ, se $T \vdash_\mathcal{L} \neg\varphi(\overline{n})$ para todo número natural n, então não ocorre que $T \vdash_\mathcal{L} \exists x\varphi(x)$.*

Teorema 5.57 *Se T é ω-consistente, então T é consistente.*

Demonstração: Provaremos que existe uma fórmula em T que não pode ser provada em T, e seguirá do Teorema 3.9 que T é consistente. Fixe $\varphi(x)$ uma fórmula de T cuja única variável livre é x. Seja $\psi(x)$ a fórmula dada por $\varphi(x) \wedge \neg\varphi(x)$. Para todo número natural n temos que $\neg\psi(\overline{n})$ é uma tautologia, logo, $T \vdash_\mathcal{L} \neg\psi(\overline{n})$. Sendo T ω-consistente, segue que não não ocorre $T \vdash_\mathcal{L} \exists x\psi(x)$, como queríamos. □

Definição 5.58 *Uma sentença φ de uma teoria de primeira ordem T em uma linguagem $\mathcal{L}$ é dita **indecidível** quando não ocorre $T \vdash_\mathcal{L} \varphi$ nem $T \vdash_\mathcal{L} \neg\varphi$.*

Seja T uma teoria na linguagem $\mathcal{L}_\mathcal{A}$ que satisfaz as seguintes condições:

1. T possui um conjunto de axiomas recursivo;
2. $T \vdash_{\mathcal{L}_\mathcal{A}} 0 \neq \overline{1}$;
3. toda função recursiva é representável em T.

Do que vimos até então, $\mathcal{P}$ é um exemplo de teoria que satisfaz as três condições acima. T é uma teoria em $\mathcal{L}_\mathcal{A}$, e como $\mathcal{L}_\mathcal{A}$ possui uma quantidade finita de símbolos de constantes, funções e relações, então as relações C, F e R são subconjuntos finitos de $\mathbb{N}$ e do Teorema 5.25 segue que tais relações são primitivas recursivas. Assim T possui um alfabeto primitivo recursivo. Disto e da condição 1 acima segue, do Teorema 5.49, que a relação $\mathrm{Pf}(y, x)$ é primitiva recursiva. Assim, a função característica de Pf é primitiva recursiva. Pela condição 3 acima segue que a função característica de Pf é representável em T. Disto, da condição 2 acima e da Proposição 5.16 segue que Pf é exprimível. Existe, portanto, uma fórmula $\mathcal{P}f(x_2, x_1)$ de T que exprime a relação $\mathrm{Pf}(y, x)$. Seja $\mathcal{E}(x_1)$ a fórmula $\forall x_2(\neg\mathcal{P}f(x_2, x_1))$.

Pela condição 3 podemos aplicar o Teorema do Ponto Fixo e obter uma sentença $\mathcal{G}$ que satisfaz

$$T \vdash_{\mathcal{L}_\mathcal{A}} \mathcal{G} \leftrightarrow \forall x_2(\neg\mathcal{P}f(x_2, \ulcorner\mathcal{G}\urcorner)). \tag{5.12}$$

Na interpretação padrão, a sentença $\forall x_2(\neg\mathcal{P}f(x_2, \ulcorner\mathcal{G}\urcorner))$ nos diz que não existe um número natural que seja o número de Gödel de uma prova em T da sentença que possui número de Gödel $\ulcorner\mathcal{G}\urcorner$. Logo, tal sentença nos diz que não existe uma prova em T para a sentença $\mathcal{G}$. E assim, a afirmação $T \vdash_{\mathcal{L}_\mathcal{A}} (\mathcal{G} \leftrightarrow \forall x_2(\neg \mathcal{P}f(x_2, \ulcorner \mathcal{G} \urcorner)))$ nos diz que, em T, a sentença $\mathcal{G}$ é equivalente à afirmação "$\mathcal{G}$ não pode ser provada em T". Em outras palavras, a sentença $\mathcal{G}$ nos diz "eu não posso ser provada em T". Tal sentença é denominada uma **sentença de Gödel** e nosso objetivo no primeiro Teorema da Incompletude é mostrar que $\mathcal{G}$ é indecidível em T, se T é ω-consistente.

Teorema 5.59 (Primeiro Teorema da Incompletude de Gödel) *Seja T uma teoria na linguagem $\mathcal{L}_\mathcal{A}$ que satisfaz as seguintes condições:*

1. *T possui um conjunto de axiomas recursivos;*

2. *$T \vdash_{\mathcal{L}_\mathcal{A}} 0 \neq \overline{1}$;*

3. *toda função recursiva é representável em T.*

valem:

(i) Se T é consistente, então não ocorre $T \vdash_{\mathcal{L}_\mathcal{A}} \mathcal{G}$.

(ii) Se T é ω-consistente, então não ocorre $T \vdash_{\mathcal{L}_\mathcal{A}} \neg\mathcal{G}$.

Assim, pelo Teorema 5.57, se T é ω-consistente, então $\mathcal{G}$ é indecidível em T.

Demonstração: (i). Suponha que $T \vdash_{\mathcal{L}_\mathcal{A}} \mathcal{G}$ e sejam r o número de Gödel de uma prova de $\mathcal{G}$ em T e q o número de Gödel da sentença $\mathcal{G}$. Então vale Pf(r,q), e sendo Pf exprimível obtemos que $T \vdash_{\mathcal{L}_\mathcal{A}} \mathcal{P}f(\overline{r}, \overline{q})$, ou seja, $T \vdash_{\mathcal{L}_\mathcal{A}} \mathcal{P}f(\overline{r}, \ulcorner \mathcal{G} \urcorner)$.

Da afirmação feita em 5.12 e de $T \vdash_{\mathcal{L}_\mathcal{A}} \mathcal{G}$ inferimos que $T \vdash_{\mathcal{L}_\mathcal{A}} \forall x_2(\neg \mathcal{P}f(x_2, \ulcorner \mathcal{G} \urcorner))$. E pela regra de quantificadores UI para o termo $\overline{r}$ obtemos que $T \vdash_{\mathcal{L}_\mathcal{A}} \neg \mathcal{P}f(\overline{r}, \ulcorner \mathcal{G} \urcorner)$. Disto e da conclusão do parágrafo anterior segue que T é inconsistente.

(ii). Assuma agora que T seja ω-consistente e suponha, por absurdo, que $T \vdash_{\mathcal{L}_\mathcal{A}} \neg\mathcal{G}$. Disto e da afirmação feita em 5.12 inferimos que $T \vdash_{\mathcal{L}_\mathcal{A}} \neg(\forall x_2(\neg \mathcal{P}f(x_2, \ulcorner \mathcal{G} \urcorner)))$. Notando que $\neg(\forall x \neg\varphi(x)) \leftrightarrow \exists x \varphi(x)$ é uma tautologia pra toda fórmula φ, obtemos que $T \vdash_{\mathcal{L}_\mathcal{A}} \exists x_2(\mathcal{P}f(x_2, \ulcorner \mathcal{G} \urcorner))$.

Sendo T ω-consistente, do Teorema 5.57 segue que T é consistente. Como $T \vdash_{\mathcal{L}_\mathcal{A}} \neg\mathcal{G}$ então não ocorre $T \vdash_{\mathcal{L}_\mathcal{A}} \mathcal{G}$, isto é, não existe prova para $\mathcal{G}$ em T. Assim, para todo número natural n, Pf(n,q) é falsa, onde q é o número de Gödel da expressão $\mathcal{G}$. Disto segue que $T \vdash_{\mathcal{L}_\mathcal{A}} \neg \mathcal{P}f(\overline{n}, \ulcorner \mathcal{G} \urcorner)$ para todo natural n. Da ω-consistência de T segue que não ocorre $T \vdash_{\mathcal{L}_\mathcal{A}} \exists x_2(\mathcal{P}f(x_2, \ulcorner \mathcal{G} \urcorner))$, o que contradiz a conclusão obtida no parágrafo anterior. $\square$

Provaremos, mais à frente, que é possível substituir, no teorema anterior, "ω-consistência"por "consistência"ao modificarmos convenientemente a sentença $\mathcal{G}$ considerada anteriormente. Pelo item 3 das condições que T satisfaz temos que toda função recursiva é representável em T. Sendo Neg uma função recursiva, existe uma fórmula $\mathcal{N}eg(x_1, x_2)$ de T que a representa. Considere agora a sentença $\mathcal{E}(x_1)$ dada por:

$$\forall x_2(\mathcal{P}f(x_2, x_1) \to \forall x_3(\mathcal{N}eg(x_1, x_3) \to \exists x_4(x_4 \leq x_2 \wedge \mathcal{P}f(x_4, x_3)))).$$

Pelo Teorema do Ponto Fixo existe uma sentença $\mathcal{R}$ satisfazendo:

$$T \vdash_{\mathcal{L}_\mathcal{A}} (\mathcal{R} \leftrightarrow \mathcal{E}(\ulcorner \mathcal{R} \urcorner)). \tag{5.13}$$

A sentença $\mathcal{R}$ acima é dita uma **sentença de Rosser**. Em outras palavras, a sentença $\mathcal{R}$ nos diz "se $\mathcal{R}$ tem uma prova em T com número de Gödel k, então $\neg\mathcal{R}$ tem uma prova em T com número de Gödel menor ou igual a k".

O que faremos no resultado a seguir é mostrar que tal sentença é indecidível em uma teoria T que satisfaz determinadas hipóteses, se T é consistente.

Teorema 5.60 (Teorema da Incompletude de Gödel-Rosser) *Seja T uma teoria na linguagem $\mathcal{L}_\mathcal{A}$ que satisfaz as seguintes condições:*

1. *T possui um conjunto de axiomas recursivo;*
2. *$T \vdash_{\mathcal{L}_\mathcal{A}} 0 \neq \overline{1}$;*
3. *toda função recursiva é representável em T;*
4. *$T \vdash_{\mathcal{L}_\mathcal{A}} \forall x(x \leq \overline{n} \to (x = 0 \vee x = \overline{1} ... \vee x = \overline{n}))$ para todo número natural n;*
5. *$T \vdash_{\mathcal{L}_\mathcal{A}} \forall x(x \leq \overline{n} \vee \overline{n} \leq x)$ para todo número natural n.*

Se T é consistente, então $\mathcal{R}$ é indecidível em T.

Demonstração: Sejam p o número de Gödel de $\mathcal{R}$; e j o número de Gödel de $\neg\mathcal{R}$. Suponha, por absurdo, que T é consistente e $\mathcal{R}$ não é indecidível em T. Há dois casos possíveis a se considerar.

Caso 1: $T \vdash_{\mathcal{L}_\mathcal{A}} \mathcal{R}$**.** Neste caso inferimos da afirmação feita em 5.13 que $T \vdash_{\mathcal{L}_\mathcal{A}} \mathcal{E}(\ulcorner \mathcal{R} \urcorner)$, ou seja,

$$T \vdash_{\mathcal{L}_\mathcal{A}} \forall x_2(\mathcal{P}f(x_2, \overline{p}) \to \forall x_3(Neg(\overline{p}, x_3) \to \exists x_4(x_4 \leq x_2 \wedge \mathcal{P}f(x_4, x_3))).$$

Seja k o número de Gödel de uma prova de $\mathcal{R}$ em T. Então vale Pf(k,p), e consequentemente $T \vdash_{\mathcal{L}_\mathcal{A}} \mathcal{P}f(\overline{k},\overline{p})$. Aplicando a regra de quantificadores UI para o termo $\overline{k}$ na fórmula $\mathcal{E}(\ulcorner\mathcal{R}\urcorner)$ obtemos que

$$T \vdash_{\mathcal{L}_\mathcal{A}} \mathcal{P}f(\overline{k},\overline{p}) \rightarrow \forall x_3(Neg(\overline{p},x_3) \rightarrow \exists x_4(x_4 \leq \overline{k} \wedge \mathcal{P}f(x_4,x_3)).$$

Assim, do resultado acima e de $T \vdash_{\mathcal{L}_\mathcal{A}} \mathcal{P}f(\overline{k},\overline{p})$, inferimos por Modus Ponens a seguinte afirmação:

$$T \vdash_{\mathcal{L}_\mathcal{A}} \forall x_3(Neg(\overline{p},x_3) \rightarrow \exists x_4(x_4 \leq \overline{k} \wedge \mathcal{P}f(x_4,x_3)).$$

Sendo j o número de Gödel da fórmula $\neg\mathcal{R}$, temos Neg(p)= j, e assim $T \vdash_{\mathcal{L}_\mathcal{A}} Neg(\overline{p},\overline{j})$. Novamente aplicando a regra UI, para o termo $\overline{j}$, obtemos $T \vdash_{\mathcal{L}_\mathcal{A}} Neg(\overline{p},\overline{j}) \rightarrow \exists x_4(x_4 \leq \overline{k} \wedge \mathcal{P}f(x_4,\overline{j}))$. Disto e de $T \vdash_{\mathcal{L}_\mathcal{A}} Neg(\overline{p},\overline{j})$ inferimos, por Modus Ponens, a afirmação $T \vdash_{\mathcal{L}_\mathcal{A}} \exists x_4(x_4 \leq \overline{k} \wedge \mathcal{P}f(x_4,\overline{j}))$. Logo, da afirmação anterior obtemos:

$$T \vdash_{\mathcal{L}_\mathcal{A}} \neg(\forall x_4 \neg(x_4 \leq \overline{k} \wedge \mathcal{P}f(x_4,\overline{j}))). \tag{5.14}$$

Como $T \vdash_{\mathcal{L}_\mathcal{A}} \mathcal{R}$ e T é, por hipótese, consistente, então não ocorre $T \vdash_{\mathcal{L}_\mathcal{A}} \neg\mathcal{R}$. Assim, para todo número natural n temos que Pf(n,j) é falso. Pela definição de exprimibilidade, segue que $T \vdash_{\mathcal{L}_\mathcal{A}} \neg\mathcal{P}f(\overline{n},\overline{j})$ para todo número natural n. Disto, dos axiomas não lógicos do tipo 7 e 11 e da definição de expremibilidade de Pf segue que $T \vdash_{\mathcal{L}_\mathcal{A}} x_4 = \overline{n} \rightarrow \neg\mathcal{P}f(x_4,\overline{j})$ para todo natural n. Logo, da condição 4 obtemos que

$$T \vdash_{\mathcal{L}_\mathcal{A}} \forall x_4(x_4 \leq \overline{k} \rightarrow (x_4 = 0 \vee x_4 = \overline{1} \vee ... \vee x_4 = \overline{k})).$$

Pela tautologia $(p \rightarrow (p_0 \vee p_1 \vee \ldots \vee p_n)) \wedge [(p_0 \rightarrow q) \wedge \ldots \wedge (p_n \rightarrow q)] \rightarrow (p \rightarrow q)$ segue que $T \vdash_{\mathcal{L}_\mathcal{A}} x_4 \leq \overline{k} \rightarrow \neg\mathcal{P}f(x_4,\overline{j})$. Notando agora que a fórmula $(\varphi \rightarrow \neg\psi) \leftrightarrow \neg(\varphi \wedge \psi)$ é uma tautologia para todas as fórmulas φ e ψ, inferimos que $T \vdash_{\mathcal{L}_\mathcal{A}} \neg(x_4 \leq \overline{k} \wedge \mathcal{P}f(x_4,\overline{j}))$ e de UG segue que $T \vdash_{\mathcal{L}_\mathcal{A}} \forall x_4 \neg(x_4 \leq \overline{k} \wedge \mathcal{P}f(x_4,\overline{j}))$. Novamente supondo válido $T \vdash_{\mathcal{L}_\mathcal{A}} \forall x_4 \neg(x_4 \leq \overline{k} \wedge \mathcal{P}f(x_4,\overline{j}))$, obtemos uma contradição com a consistência de T e o obtido na afirmação feita em 5.14.

Caso 2: $T \vdash_{\mathcal{L}_\mathcal{A}} \neg\mathcal{R}$**.** Seja m o número de Gödel de uma prova de $\neg\mathcal{R}$ em T. Então vale Pf(m,j) e, consequentemente, $T \vdash_{\mathcal{L}_\mathcal{A}} \mathcal{P}f(\overline{m},\overline{j})$. Pela regra EG temos que $\{\overline{m} \leq x_2 \wedge \mathcal{P}f(\overline{m},\overline{j})\} \vdash_{\mathcal{L}_\mathcal{A}} \exists x_4(x_4 \leq x_2 \wedge \mathcal{P}f(x_4,\overline{j}))$. Como $T \vdash_{\mathcal{L}_\mathcal{A}} \mathcal{P}f(\overline{m},\overline{j})$, do Teorema 3.13 segue que $T \cup \{\overline{m} \leq x_2\} \vdash_{\mathcal{L}_\mathcal{A}} \exists x_4(x_4 \leq x_2 \wedge \mathcal{P}f(x_4,\overline{j}))$. Assim pelo Teorema da Dedução segue que $T \vdash_{\mathcal{L}_\mathcal{A}} \overline{m} \leq x_2 \rightarrow \exists x_4(x_4 \leq x_2 \wedge \mathcal{P}f(x_4,\overline{j}))$.

Sendo T consistente, não ocorre $T \vdash_{\mathcal{L}_\mathcal{A}} \mathcal{R}$. Assim, Pf($n,p$) é falso para todo número natural n, e então $T \vdash_{\mathcal{L}_A} \neg\mathcal{P}f(\overline{n},\overline{p})$, para todo natural n. Pela condição 4 temos que $T \vdash_{\mathcal{L}_A} x_2 \leq \overline{m} \rightarrow (x_2 = 0 \vee x_2 = \overline{1} \vee ... \vee x_2 = \overline{m})$. E por um argumento análogo ao feito no item anterior segue que $T \vdash_{\mathcal{L}_A} x_2 \leq \overline{m} \rightarrow \neg\mathcal{P}f(x_2,\overline{p})$.

Afirmação 5.61 *Afirmação:* $T \cup \{\mathcal{P}f(x_2,\overline{p}), Neg(\overline{p},x_3)\} \vdash_{\mathcal{L}_A} \exists x_4(x_4 \leq x_2 \wedge \mathcal{P}f(x_4,x_3))$.

Demonstração: De fato, a seguinte sequência de sentenças atesta tal fato:

$1.\mathcal{P}f(x_2,\overline{p})$	Hipótese
$2.Neg(\overline{p},x_3)$	Hipótese
$3.x_2 \leq \overline{m} \vee \overline{m} \leq x_2$	Condição 5
$4.\overline{m} \leq x_2 \rightarrow \exists x_4(x_4 \leq x_2 \wedge \mathcal{P}f(x_4,\overline{j}))$	Provado acima
$5.x_2 \leq \overline{m} \rightarrow \neg\mathcal{P}f(x_2,\overline{p})$	Provado acima
$6.\neg\mathcal{P}f(x_2,\overline{p}) \vee \exists x_4(x_4 \leq x_2 \wedge \mathcal{P}f(x_4,\overline{j}))$	Inferido taut. de 3, 4 e 5
$7.\exists x_4(x_4 \leq x_2 \wedge \mathcal{P}f(x_4,\overline{j}))$	Inferido taut. de 1 e 6
$8.Neg(\overline{p},\overline{j})$	Provado no item (i)
$9.\exists! x_3 Neg(\overline{p},x_3)$	Def. de representabilidade
$10.x_3 = \overline{j}$	Por 2, 8, 9 e propriedades de =
$11.\exists x_4(x_4 \leq x_2 \wedge \mathcal{P}f(x_4,x_3))$	Por 7, 10 e propriedades de =

□

Com isso, conseguimos verificar que $\mathcal{R}$ pode ser provada em T:

$i.\{\mathcal{P}f(x_2,\overline{p})\} \vdash_{\mathcal{L}_A} Neg(\overline{p},x_3) \rightarrow \exists x_4(x_4 \leq x_2 \wedge \mathcal{P}f(x_4,x_3))$

$ii.\{\mathcal{P}f(x_2,\overline{p})\} \vdash_{\mathcal{L}_A} \forall x_3(Neg(\overline{p},x_3) \rightarrow \exists x_4(x_4 \leq x_2 \wedge \mathcal{P}f(x_4,x_3)))$

$iii.T \vdash_{\mathcal{L}_A} \mathcal{P}f(x_2,\overline{p}) \rightarrow \forall x_3(Neg(\overline{p},x_3) \rightarrow \exists x_4(x_4 \leq x_2 \wedge \mathcal{P}f(x_4,x_3)))$

$iv.T \vdash_{\mathcal{L}_A} \forall x_2(\mathcal{P}f(x_2,\overline{p}) \rightarrow \forall x_3(Neg(\overline{p},x_3) \rightarrow \exists x_4(x_4 \leq x_2 \wedge \mathcal{P}f(x_4,x_3))))$

$v.T \vdash_{\mathcal{L}_A} \mathcal{R}$

onde i é válido pela afirmação acima e o Teorema da Dedução; ii segue de i e UG; iii segue de ii e do Teorema da Dedução; iv segue de iii por UG; v segue de iv e da afirmação feita em 5.13. Temos assim que $T \vdash_{\mathcal{L}_A} \mathcal{R}$ e $T \vdash_{\mathcal{L}_A} \neg\mathcal{R}$, contradizendo a consistência de T. Dos dois itens acima segue que $\mathcal{R}$ é indecidível em T. □

Já tínhamos visto que a teoria $\mathcal{P}$ satisfaz as condições 1 – 3 do Teorema 5.60, e do Teorema 5.4 e do Lema 5.5 obtemos que $\mathcal{P}$ também satisfaz 4 e 5.

5.6 Segundo Teorema da Incompletude de Gödel

Considere uma teoria T na linguagem $\mathcal{L}_A$ que seja uma extensão de $\mathcal{P}$ e que possua um conjunto de axiomas recursivo. Denote por $\mathcal{C}ons_T$ a seguinte sentença de T:

$$\forall x_1 \forall x_2 \forall x_3 \forall x_4 (\neg(\mathcal{P}f(x_1, x_3) \wedge \mathcal{P}f(x_2, x_4) \wedge \mathcal{N}eg(x_3, x_4))).$$

Em termos da interpretação padrão, a sentença acima nos diz que não há, em T, uma sentença φ tal que φ e $\neg\varphi$ podem ser provadas em T. Assim, expressa em T a consistência de T.

Para mostrar o Segundo Teorema da Incompletude mostraremos que se $\mathcal{P} \vdash_{\mathcal{L}_A} \mathcal{C}ons_T$ então ocorre $\mathcal{P} \vdash_{\mathcal{L}_A} 0 = \overline{1}$, o que é um absurdo.

Denote por $\mathcal{P}rov(x_1)$ a fórmula $\exists x_2(\mathcal{P}f(x_2, x_1))$. Em termos da interpretação padrão, tal sentença nos diz que a fórmula com número de Gödel x_1 pode ser provada em $\mathcal{P}$.

O resultado abaixo constitui o coração da demonstração do Segundo Teorema da Incompletude de Gödel e sua demonstração é longa e difícil, fugindo do escopo deste trabalho. Por este motivo, provaremos somente a primeira condição. Discussões sobre as condições HB2 e HB3 podem ser encontradas em [8] e suas demonstrações em [1] e [4].

Teorema 5.62 (Condições de Derivabilidade de Hilbert-Bernays) *Sejam φ e ψ sentenças de $\mathcal{P}$. Valem as seguintes afirmações:*

(HB1) *Se $\mathcal{P} \vdash_{\mathcal{L}_A} \varphi$, então $\mathcal{P} \vdash_{\mathcal{L}_A} \mathcal{P}rov(\ulcorner\varphi\urcorner)$.*

(HB2) *$\mathcal{P} \vdash_{\mathcal{L}_A} \mathcal{P}rov(\ulcorner\varphi \to \psi\urcorner) \to (\mathcal{P}rov(\ulcorner\varphi\urcorner) \to \mathcal{P}rov(\ulcorner\psi\urcorner))$.*

(HB3) *$\mathcal{P} \vdash_{\mathcal{L}_A} \mathcal{P}rov(\ulcorner\varphi\urcorner) \to \mathcal{P}rov(\ulcorner\mathcal{P}rov(\ulcorner\varphi\urcorner)\urcorner)$.*

A afirmação $(HB1)$ diz que se podemos provar uma sentença φ em $\mathcal{P}$, então podemos provar em $\mathcal{P}$ a sentença que diz que "a sentença φ pode ser provada em $\mathcal{P}$". A formalização da regra de inferência Modus Ponens nos diz que, se podemos provar em $\mathcal{P}$ que "se φ pode ser provada e $\varphi \to \psi$ pode ser provada, então ψ também pode ser provada". Por fim, a afirmação $(HB3)$ diz que "se $\mathcal{P}$ prova a sentença φ, então $\mathcal{P}$ prova uma fórmula com número de Gödel da sentença $\mathcal{P}rov(\ulcorner\varphi\urcorner)$".

Demonstração do Teorema 5.62 (HB1): Sejam b o número de Gödel da sentença φ e c o número de Gödel de uma prova de φ em $\mathcal{P}$. Então vale Pf(c, b). Pelo Teorema 5.49, a relação Pf é primitiva recursiva e, portanto (do item 1 do Teorema 5.1 e do Teorema 5.37), existe uma fórmula $\mathcal{P}f(x_2, x_1)$ de T que exprime a relação Pf(y, x). Logo, temos que $\mathcal{P} \vdash_{\mathcal{L}_A} \mathcal{P}f(\overline{c}, \overline{b})$, ou seja, $\mathcal{P} \vdash_{\mathcal{L}_A} \mathcal{P}f(\overline{c}, \ulcorner\varphi\urcorner)$. Pela regra de quantificadores EG segue que $\mathcal{P} \vdash_{\mathcal{L}_A} \mathcal{P}rov(\ulcorner\varphi\urcorner)$. $\square$

Dada uma fórmula φ, é usual denotar por $\square\varphi$ a fórmula $\mathcal{P}rov(\ulcorner\varphi\urcorner)$. Com isto, as Condições de Derivabilidade de Hilbert-Bernays podem ser reescritas da seguinte maneira:

(HB1) Se $\mathcal{P} \vdash_{\mathcal{L}_A} \varphi$, então $\mathcal{P} \vdash_{\mathcal{L}_A} \square\varphi$.

(HB2) $\mathcal{P} \vdash_{\mathcal{L}_A} \square(\varphi \to \psi) \to (\square\varphi \to \square\psi)$.

(HB3) $\mathcal{P} \vdash_{\mathcal{L}_A} \square\varphi \to \square\square\varphi$.

Teorema 5.63 (Teorema de Löb) *Seja φ uma sentença de $\mathcal{P}$. Se $\mathcal{P} \vdash_{\mathcal{L}_A} \square\varphi \to \varphi$, então $\mathcal{P} \vdash_{\mathcal{L}_A} \varphi$.*

Demonstração: Vamos primeiro aplicar o Teorema do Ponto Fixo para a fórmula $\mathcal{P}rov(x_1) \to \varphi$, obtendo uma sentença ψ tal que $\mathcal{P} \vdash_{\mathcal{L}_A} \psi \leftrightarrow (\mathcal{P}rov(\ulcorner\psi\urcorner) \to \varphi)$. Na notação utilizando $\square$, temos $\mathcal{P} \vdash_{\mathcal{L}_A} \psi \leftrightarrow (\square\psi \to \varphi)$. Assim, a seguinte sequência nos dá uma prova para φ em $\mathcal{P}$:

1.$\mathcal{P} \vdash_{\mathcal{L}_A} \psi \leftrightarrow (\square\psi \to \varphi)$	
2.$\mathcal{P} \vdash_{\mathcal{L}_A} \psi \to (\square\psi \to \varphi)$	Por 1
3.$\mathcal{P} \vdash_{\mathcal{L}_A} \square(\psi \to (\square\psi \to \varphi))$	Por 2 e HB1
4.$\mathcal{P} \vdash_{\mathcal{L}_A} \square\psi \to \square(\square\psi \to \varphi)$	Por 3, HB2 e Modus Ponens
5.$\mathcal{P} \vdash_{\mathcal{L}_A} \square(\square\psi \to \varphi) \to (\square\square\psi \to \square\varphi)$	Por HB2 para as sentenças $\square\psi$ e φ
6.$\mathcal{P} \vdash_{\mathcal{L}_A} \square\psi \to (\square\square\psi \to \square\varphi)$	Por 4 e 5
7.$\mathcal{P} \vdash_{\mathcal{L}_A} \square\psi \to \square\square\psi$	Por HB3
8.$\mathcal{P} \vdash_{\mathcal{L}_A} \square\psi \to \square\varphi$	Por 6, 7 e tautologia $(((p \to (q \to r)) \land (p \to q) \to)(p \to r)$.
9.$\mathcal{P} \vdash_{\mathcal{L}_A} \square\varphi \to \varphi$	Por hipótese
10.$\mathcal{P} \vdash_{\mathcal{L}_A} \square\psi \to \varphi$	Por 8 e 9
11.$\mathcal{P} \vdash_{\mathcal{L}_A} \psi$	Por 1 e 10
12.$\mathcal{P} \vdash_{\mathcal{L}_A} \square\psi$	Por 11 e HB1
13.$\mathcal{P} \vdash_{\mathcal{L}_A} \varphi$	Por 10, 12 e Modus Ponens

$\square$

Teorema 5.64 (Segundo Teorema da Incompletude de Gödel) *Se $\mathcal{P}$ é consistente, então não ocorre $\mathcal{P} \vdash_{\mathcal{L}_A} \mathcal{C}ons_{\mathcal{P}}$.*

Demonstração: Pelo axioma $(A1)$ de $\mathcal{P}$, obtemos que $\mathcal{P} \vdash_{\mathcal{L}_{\mathcal{A}}} 0 \neq \overline{1}$. Sendo $\mathcal{P}$ consistente, segue que não ocorre $\mathcal{P} \vdash_{\mathcal{L}_{\mathcal{A}}} 0 = \overline{1}$. Assim, pelo Teorema de Löb inferimos que $\mathcal{P} \vdash_{\mathcal{L}_{\mathcal{A}}} \Box(0 = \overline{1}) \to 0 = \overline{1}$ não ocorre. Pela tautologia $\neg\psi \to (\psi \to \phi)$ concluímos que $\mathcal{P} \vdash_{\mathcal{L}_{\mathcal{A}}} \neg\Box(0 = \overline{1})$ não ocorre.

Como $\mathcal{P} \vdash_{\mathcal{L}_{\mathcal{A}}} 0 \neq \overline{1}$, de (HB1) segue que $\mathcal{P} \vdash_{\mathcal{L}_{\mathcal{A}}} \Box(0 \neq \overline{1})$. Afirmamos que $\mathcal{P} \vdash_{\mathcal{L}_{\mathcal{A}}} \mathcal{C}ons_{\mathcal{P}} \to \neg\Box(0 = \overline{1})$. Com efeito, sejam n_2 o número de Gödel de uma prova de $0 \neq \overline{1}$, que ateste que $\mathcal{P} \vdash_{\mathcal{L}_{\mathcal{A}}} 0 \neq \overline{1}$ em $\mathcal{P}$, e n_3 e n_4 naturais tais que $n_3 = \ulcorner 0 = \overline{1} \urcorner$ e $n_4 = \ulcorner 0 \neq \overline{1} \urcorner$. Então valem $\mathrm{Neg}(n_3) = n_4$ e $\mathrm{Pf}(n_2, n_4)$. Assim, da sentença $\mathcal{C}ons_{\mathcal{P}}$ obtemos $\mathcal{P} \cup \{\mathcal{C}ons_{\mathcal{P}}\} \vdash_{\mathcal{L}_{\mathcal{A}}} \forall x_1(\neg\mathcal{P}f)(x_1, \overline{n}_3)$ e, portanto, $\mathcal{P} \cup \{\mathcal{C}ons_{\mathcal{P}}\} \vdash_{\mathcal{L}_{\mathcal{A}}} \neg\exists x_1(\mathcal{P}f)(x_1, \overline{n}_3)$ isto é, $\mathcal{P} \cup \{\mathcal{C}ons_{\mathcal{P}}\} \vdash_{\mathcal{L}_{\mathcal{A}}} \neg\Box(0 = \overline{1})$. Segue do Teorema da Dedução que $\mathcal{P} \vdash_{\mathcal{L}_{\mathcal{A}}} \mathcal{C}ons_{\mathcal{P}} \to \neg\Box(0 = \overline{1})$.

Como já havíamos mostrado que $\mathcal{P} \vdash_{\mathcal{L}_{\mathcal{A}}} \neg\Box(0 = \overline{1})$ não ocorre, então de $\mathcal{P} \vdash_{\mathcal{L}_{\mathcal{A}}} \mathcal{C}ons_{\mathcal{P}} \to \neg\Box(0 = \overline{1})$ decorre que $\mathcal{P} \vdash_{\mathcal{L}_{\mathcal{A}}} \mathcal{C}ons_{\mathcal{P}}$ não ocorre. $\Box$

Apêndice 1: Tabela-verdade de alguns símbolos lógicos

Os símbolos lógicos $\neg, \wedge, \vee, \rightarrow$ e $\leftrightarrow$ possuem as seguintes tabelas-verdade:

φ	ψ	$\neg\varphi$	$\varphi \wedge \psi$	$\varphi \vee \psi$	$\varphi \rightarrow \psi$	$\varphi \leftrightarrow \psi$
V	V	F	V	V	V	V
V	F	F	F	V	F	F
F	V	V	F	V	V	F
F	F	V	F	F	V	V

Apêndice 2: Completude do cálculo proposicional

Definição 6.1 *Definimos a **linguagem** L para o cálculo proposicional como o conjunto dos conectivos lógicos $\{\neg, \wedge, \vee, \rightarrow, \leftrightarrow\}$. Uma **teoria** T para o cálculo proposicional é o par formado pelo conjunto $\{B_i : i \in \omega\}$ das **letras proposicionais** e a linguagem T. Para a teoria T dizemos definimos as **proposições** da seguinte maneira:*

1. *todas as letras proposicionais são proposições;*
2. *se $\mathcal{A}$ e $\mathcal{C}$ são proposições então $\neg\mathcal{A}$, $\mathcal{A} \rightarrow \mathcal{C}$, $\mathcal{A} \wedge \mathcal{C}$, $\mathcal{A} \vee \mathcal{C}$ e $\mathcal{A} \leftrightarrow \mathcal{C}$ também são proposições.*

Se $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$ e $\mathcal{D}$ são proposições, as seguintes proposições são os axiomas lógicos de T:

(i) $\mathcal{A} \rightarrow (\mathcal{C} \rightarrow \mathcal{A})$

(ii) $(\mathcal{A} \rightarrow (\mathcal{C} \rightarrow \mathcal{D})) \rightarrow ((\mathcal{A} \rightarrow \mathcal{C}) \rightarrow (\mathcal{A} \rightarrow \mathcal{D}))$

(iii) $(\neg\mathcal{C} \rightarrow \neg\mathcal{B}) \rightarrow ((\neg\mathcal{C} \rightarrow \mathcal{B}) \rightarrow \mathcal{C})$

(iv) $(\mathcal{A} \wedge \mathcal{C}) \leftrightarrow \neg(\mathcal{A} \rightarrow \neg\mathcal{C})$

(v) $(\mathcal{A} \vee \mathcal{C}) \leftrightarrow (\neg\mathcal{A} \rightarrow \mathcal{C})$

(vi) $(\mathcal{A} \leftrightarrow \mathcal{C}) \rightarrow (\mathcal{A} \rightarrow \mathcal{C})$

(vii) $(\mathcal{A} \leftrightarrow \mathcal{C}) \rightarrow (\mathcal{C} \rightarrow \mathcal{A})$

(viii) $((\mathcal{A} \rightarrow \mathcal{C}) \wedge (\mathcal{C} \rightarrow \mathcal{A})) \rightarrow (\mathcal{A} \leftrightarrow \mathcal{C})$

(ix) $\mathcal{A} \rightarrow (\mathcal{C} \rightarrow (\mathcal{A} \wedge \mathcal{C}))$

*Uma prova em T é dada da mesma forma que a Definição 3.4, para a lista de axiomas dada acima. Se existe uma prova pata uma proposição em T, dizemos que tal proposição é um **teorema** de T.*

Definição 6.2 *Uma **atribuição-verdade** de n argumentos é uma função de n argumentos do conjunto das letras proposicionais em $\{V, F\}$ (isto é, tal função atribui valores-verdade), e se estende ao conjunto das proposições de T de acordo com a tabela-verdade dos conectivos lógicos. Uma **tautologia** (do cálculo proposicional) é uma proposição tal que toda atribuição-verdade aplicada a ela assume o valor V.*

Note que o Teorema da Dedução para o Cálculo Proposicional também pode ser aplicado a teoria T.

Teorema 6.3 (Teorema da Dedução para o Cálculo Proposicional) *Sejam T uma teoria da linguagem L e $\mathcal{A}$ e $\mathcal{B}$ proposições de T. Se $T \cup \{\mathcal{A}\} \vdash_L \mathcal{B}$ então $T \vdash_L \mathcal{A} \to \mathcal{B}$.*

Note que o Teorema da Dedução para o Cálculo Proposicional para uma lógica de primeira ordem dada no Teorema 3.7, só utiliza tautologias que são do tipo dos axiomas (i) e (ii) — na verdade, a segunda tautologia utilizada é do tipo $(\mathcal{A} \to \mathcal{C}) \to (((\mathcal{A} \to (\mathcal{C} \to \mathcal{D})) \to (\mathcal{A} \to \mathcal{D}))$, mas facilmente poderíamos trocá-la por uma tautologia do tipo (ii), uma vez que o objetivo é inferir por Modus Ponens a afirmação $\mathcal{A} \to \mathcal{D}$. Com isto obtemos uma adaptação para uma prova do Teorema da Dedução para o Cálculo Proposicional.

Para o resultado a seguir a seguinte afirmação será útil: se T é uma teoria de L e $\mathcal{B}$ é uma proposição de T então a proposição $\mathcal{B} \to \mathcal{B}$ é um teorema de T. De fato, a seguinte sequência atesta esse fato:

1. $(\mathcal{B} \to ((\mathcal{B} \to \mathcal{B}) \to \mathcal{B})) \to ((\mathcal{B} \to (\mathcal{B} \to \mathcal{B})) \to (\mathcal{B} \to \mathcal{B}))$	Axioma (ii)
2. $\mathcal{B} \to ((\mathcal{B} \to \mathcal{B}) \to \mathcal{B})$	Axioma (i)
3. $(\mathcal{B} \to (\mathcal{B} \to \mathcal{B})) \to (\mathcal{B} \to \mathcal{B})$	1, 2 e Modus Ponens
4. $\mathcal{B} \to (\mathcal{B} \to \mathcal{B})$	Axioma (i)
5. $\mathcal{B} \to \mathcal{B}$	3, 4 e Modus Ponens

Lema 6.4 *Sejam $\mathcal{B}$ e $\mathcal{C}$ proposições. No cálculo proposicional as seguintes proposições são teoremas:*

(a) $\neg\neg\mathcal{B} \to \mathcal{B}$

(b) $\mathcal{B} \to \neg\neg\mathcal{B}$

(c) $\neg\mathcal{B} \to (\mathcal{B} \to \mathcal{C})$

(d) $(\neg\mathcal{C} \to \neg\mathcal{B}) \to (\mathcal{B} \to \mathcal{C})$

(e) $(\mathcal{B} \to \mathcal{C}) \to (\neg\mathcal{C} \to \neg\mathcal{B})$

(f) $\mathcal{B} \to (\neg\mathcal{C} \to \neg(\mathcal{B} \to \mathcal{C}))$

(g) $(\mathcal{B} \to \mathcal{C}) \to ((\neg\mathcal{B} \to \mathcal{C}) \to \mathcal{C})$

Demonstração:

(a) Pelo Teorema da Dedução para o Cálculo Proposicional, basta mostrar que $T \cup \{\neg\neg\mathcal{B}\} \vdash_L \mathcal{B}$

1. $\neg\neg\mathcal{B}$	Hipótese
2. $\neg\neg\mathcal{B} \to (\neg\mathcal{B} \to \neg\neg\mathcal{B})$	Axioma (i)
3. $(\neg\mathcal{B} \to \neg\neg\mathcal{B}) \to ((\neg\mathcal{B} \to \neg\mathcal{B}) \to \mathcal{B})$	Axioma (iii)
4. $\neg\mathcal{B} \to \neg\mathcal{B}$	Observação acima
5. $\mathcal{B}$	1-4 e Modus Ponens

(b) Pelo Teorema da Dedução para o Cálculo Proposicional, basta mostrar que $T \cup \{\mathcal{B}\} \vdash_L \neg\neg\mathcal{B}$

1. $\mathcal{B}$	Hipótese
2. $(\neg\neg\neg\mathcal{B} \to \neg\mathcal{B}) \to ((\neg\neg\neg\mathcal{B} \to \mathcal{B}) \to \neg\neg\mathcal{B})$	Axioma (iii)
3. $\neg\neg\neg\mathcal{B} \to \neg\mathcal{B}$	Item (a)
4. $(\neg\neg\neg\mathcal{B} \to \mathcal{B}) \to \neg\neg\mathcal{B}$	2, 3 e Modus Ponens
5. $\mathcal{B} \to (\neg\neg\neg\mathcal{B} \to \mathcal{B})$	Axioma (i)
6. $\neg\neg\mathcal{B}$	1, 5, 4 e Modus Ponens

(c) Pelo Teorema da Dedução para o Cálculo Proposicional, basta mostrar que $T \cup \{\neg\mathcal{B}, \mathcal{B}\} \vdash_L \mathcal{C}$

1. $\mathcal{B}$	Hipótese
2. $\neg\mathcal{B}$	Hipótese
3. $\mathcal{B} \to (\neg\mathcal{C} \to \mathcal{B})$	Axioma (i)
4. $\neg\mathcal{B} \to (\neg\mathcal{C} \to \neg\mathcal{B})$	Axioma (i)
5. $\neg\mathcal{C} \to \mathcal{B}$	1, 3 e Modus Ponens
6. $\neg\mathcal{C} \to \neg\mathcal{B}$	2, 4 e Modus Ponens
7. $(\neg\mathcal{C} \to \neg\mathcal{B}) \to ((\neg\mathcal{C} \to \mathcal{B}) \to \mathcal{C})$	Axioma (iii)
8. $\mathcal{C}$	6, 7, 5 e Modus Ponens

(d) Pelo Teorema da Dedução para o Cálculo Proposicional, basta mostrar que $T \cup \{\neg\mathcal{C} \to \neg\mathcal{B}, \mathcal{B}\} \vdash \mathcal{C}$

1. $\neg\mathcal{C} \to \neg\mathcal{B}$	Hipótese
2. $\mathcal{B}$	Hipótese
3. $(\neg\mathcal{C} \to \neg\mathcal{B}) \to ((\neg\mathcal{C} \to \mathcal{B}) \to \mathcal{C})$	Axioma (iii)
4. $\mathcal{B} \to (\neg\mathcal{C} \to \mathcal{B})$	Axioma (i)
5. $(\neg\mathcal{C} \to \mathcal{B}) \to \mathcal{C}$	1, 3 e Modus Ponens
6. $\neg\mathcal{C} \to \mathcal{B}$	2, 4 e Modus Ponens
8. $\mathcal{C}$	5, 6 e Modus Ponens

(e) Pelo Teorema da Dedução para o Cálculo Proposicional, basta mostrar que $T \cup \{\mathcal{B} \to \mathcal{C}, \neg\mathcal{C}\} \vdash \neg\mathcal{B}$

1. $\mathcal{B} \to \mathcal{C}$	Hipótese
2. $\neg\mathcal{C}$	Hipótese
3. $\neg\neg\mathcal{B} \to \mathcal{B}$	Item (a)
4. $\mathcal{C} \to \neg\neg\mathcal{C}$	Item (b)
5. $\neg\neg\mathcal{B} \to \neg\neg\mathcal{C}$	Teorema 6.3 em 3, 1 e 4, respectivamente
6. $(\neg\neg\mathcal{B} \to \neg\neg\mathcal{C}) \to (\neg\mathcal{C} \to \neg\mathcal{B})$	Item (d)
7. $\neg\mathcal{B}$	5, 6, 2 e Modus Ponens

(f) Pelo Teorema da Dedução para o Cálculo Proposicional, basta mostrar que

$T \cup \{\mathcal{B}, \neg\mathcal{C}\} \vdash \neg(\mathcal{B} \to \mathcal{C})$

1. $\mathcal{B}$	Hipótese
2. $\neg\mathcal{C}$	Hipótese
3. $\mathcal{B} \to ((\mathcal{B} \to \mathcal{C}) \to \mathcal{C})$	Por Modus Ponens e duas aplicações do Teorema 6.3
4. $((\mathcal{B} \to \mathcal{C}) \to \mathcal{C}) \to (\neg\mathcal{C} \to \neg(\mathcal{B} \to \mathcal{C}))$	Item (e)
5. $\neg\mathcal{C} \to \neg(\mathcal{B} \to \mathcal{C})$	1, 3, 4 e Modus Ponens
6. $\neg(\mathcal{B} \to \mathcal{C})$	2, 5 e Modus Ponens

(g) Pelo Teorema da Dedução para o Cálculo Proposicional, basta mostrar que $T \cup \{\mathcal{B} \to \mathcal{C}, \neg\mathcal{B} \to \mathcal{C}\} \vdash_L \mathcal{C}$

1. $\mathcal{B} \to \mathcal{C}$	Hipótese
2. $\neg\mathcal{B} \to \mathcal{C}$	Hipótese
3. $(\mathcal{B} \to \mathcal{C}) \to (\neg\mathcal{C} \to \neg\mathcal{B})$	Item (e)
4. $\neg\mathcal{C} \to \neg\mathcal{B}$	1, 3 e Modus Ponens
5. $(\neg\mathcal{B} \to \mathcal{C}) \to (\neg\mathcal{C} \to \neg\neg\mathcal{B})$	Item (e)
6. $\neg\mathcal{C} \to \neg\neg\mathcal{B}$	2, 5 e Modus Ponens
7. $(\neg\mathcal{C} \to \neg\neg\mathcal{B}) \to ((\neg\mathcal{C} \to \neg\mathcal{B}) \to \mathcal{C})$	Axioma (iii)
8. $(\neg\mathcal{C} \to \neg\mathcal{B}) \to \mathcal{C}$	6, 7 e Modus Ponens
9. $\mathcal{C}$	4, 8 e Modus Ponens

□

Vejamos um exemplo que ilustra a ideia usada no próximo resultado. Seja $\mathcal{B}$ a proposição $\neg(\neg B_1 \to B_2)$. Então a tabela-verdade de $\mathcal{B}$ é a seguinte:

B_1	B_2	$\neg(\neg B_1 \to B_2)$
V	V	F
V	F	F
F	V	F
F	F	V

O Lema 6.5 afirma, respectivamente para a atribuição correspondente a cada linha da tabela-verdade acima, que vale: $T \cup \{B_1, B_2\} \vdash_L \neg\neg(\neg B_1 \to B_2)$, $T \cup \{B_1, \neg B_2\} \vdash_L \neg\neg(\neg B_1 \to B_2)$, $T \cup \{\neg B_1, B_2\} \vdash_L \neg\neg(\neg B_1 \to B_2)$ e $T \cup \{\neg B_1, \neg B_2\} \vdash_L \neg(\neg B_1 \to B_2)$.

Para simplificar a notação, para uma sequência $\mathcal{A}_1,...,\mathcal{A}_n$ de proposições de T, denotaremos por $\{\mathcal{A}_1,...,\mathcal{A}_n\}$ o conjunto $T \cup \{\mathcal{A}_1,...,\mathcal{A}_n\}$ dentro do ambiente de prova.

Lema 6.5 *Sejam $\mathcal{B}$ uma proposição e $B_1,...,B_k$ todas as letras proposicionais que ocorrem em $\mathcal{B}$. Para cada atribuição verdade para $B_1,...,B_k$, defina B'_j como sendo B_j caso B_j assuma valor T; caso contrário, defina B'_j como sendo $\neg B_j$. Por fim, defina $\mathcal{B}'$ como sendo $\mathcal{B}$ caso $\mathcal{B}$ assuma valor T; caso contrário, defina $\mathcal{B}'$ como sendo $\neg\mathcal{B}$. Nestas condições vale que $\{B'_1,...,B'_k\} \vdash_L \mathcal{B}'$.*

Demonstração: Faremos esta prova por indução no número n de ocorrências de conectivos lógicos na proposição $\mathcal{B}$. Para o caso base, se $n = 0$ então $\mathcal{B}$ é formada por uma única letra proposicional, digamos, B_1. Neste caso só temos duas atribuições possíveis para B_1 e é imediato que $\{B_1\} \vdash_L B_1$ e $\{\neg B_1\} \vdash_L \neg B_1$.

Suponha agora que o resultado seja válido para qualquer proposição com número de ocorrência de conectivos lógicos igual a $j < n$.

Caso 1. Existe uma proposição $\mathcal{C}$ tal que $\mathcal{B}$ é a proposição $\neg\mathcal{C}$. Note que $\mathcal{C}$ possui o número de ocorrência dos conectivos lógicos menor que n, e portanto, pela hipótese de indução, o resultado vale para $\mathcal{C}$. Temos agora dois sub-casos:

(a) $\mathcal{C}$ assume valor V. Para as atribuições-verdade em que $\mathcal{C}$ vale V temos que $\mathcal{B}$ vale F. Então $\mathcal{C}'$ é $\mathcal{C}$ e $\mathcal{B}'$ é $\neg\mathcal{B}$. Por hipótese de indução temos que $\{B'_1,...,B'_k\} \vdash_L \mathcal{C}$. Assim, por Modus Ponens e pelo Teorema 6.4 (b) segue que $\{B'_1,...,B'_k\} \vdash_L \neg\neg\mathcal{C}$. E como $\neg\neg\mathcal{C}$ é $\mathcal{B}'$, segue o resultado.

(b) $\mathcal{C}$ assume valor F. Neste caso, $\mathcal{C}'$ é $\neg\mathcal{C}$ (que é $\mathcal{B}$) e $\mathcal{B}$ vale V, logo $\mathcal{B}'$ é $\mathcal{B}$. Com isso obtemos que $\mathcal{C}'$ é $\mathcal{B}'$. Por hipótese de indução vale $\{B'_1,...,B'_k\} \vdash_L \mathcal{C}'$, e portanto vale $\{B'_1,...,B'_k\} \vdash_L \mathcal{B}'$, como queríamos.

Caso 2. Existem proposições $\mathcal{C}$ e $\mathcal{D}$ tais que $\mathcal{B}$ é a proposição $\mathcal{C} \to \mathcal{D}$. Como $\mathcal{C}$ e $\mathcal{D}$ possuem uma quantidade de conectivos lógicos menor que n, segue pela hipótese de indução que $\{B'_1,...,B'_k\} \vdash_L \mathcal{C}'$ e $\{B'_1,...,B'_k\} \vdash_L \mathcal{D}'$. Neste caso, a tabela-verdade do símbolo $\to$ nos dá 3 casos possíveis:

(a) $\mathcal{C}$ assume valor F. Então $\mathcal{B}$ assume valor V e, neste caso $\mathcal{C}'$ é $\neg\mathcal{C}$ e $\mathcal{B}'$ é $\mathcal{B}$. Por hipótese de indução segue que $\{B'_1,...,B'_k\} \vdash_L \neg\mathcal{C}$. Do Teorema 6.4 ($c$) e Modus Ponens segue que $\{B'_1,...,B'_k\} \vdash_L \mathcal{C} \to \mathcal{D}$, isto é,$\{B'_1,...,B'_k\} \vdash_L \mathcal{B}$. Como estamos no caso em que $\mathcal{B}'$ é $\mathcal{B}$, segue o resultado.

(b) $\mathcal{C}$ e $\mathcal{D}$ assumem valor V. Então $\mathcal{B}$ assume valor V, logo $\mathcal{D}'$ é $\mathcal{D}$ e $\mathcal{B}'$ é $\mathcal{B}$. Por hipótese de indução segue que $\{B'_1,...,B'_k\} \vdash_L \mathcal{D}$. Do axioma ($i$) e por Modus Ponens segue que $\{B'_1,...,B'_k\} \vdash_L \mathcal{C} \to \mathcal{D}$, e como $\mathcal{B}'$ é $\mathcal{B}$, segue o resultado desejado.

(c) $\mathcal{C}$ assume valor V e $\mathcal{D}$ assume valor F. Então $\mathcal{B}$ assume o valor F, e assim $\mathcal{B}'$ é $\neg\mathcal{B}$, $\mathcal{C}'$ é $\mathcal{C}$ e $\mathcal{D}'$ é $\neg\mathcal{D}$. Por hipótese de indução segue que $\{B_1',...,B_k'\} \vdash_L \mathcal{C}$ e $\{B_1',...,B_k'\} \vdash_L \neg\mathcal{D}$. Pelo Teorema 6.4 (f) e Modus Ponens inferimos $\{B_1',...,B_k'\} \vdash_L \neg(\mathcal{C} \to \mathcal{D})$ e como $\neg(\mathcal{C} \to \mathcal{D})$ é $\mathcal{B}'$, segue o resultado desejado.

Caso 3. Existem proposições $\mathcal{C}$ e $\mathcal{D}$ tais que $\mathcal{B}$ é a proposição $\mathcal{C} \wedge \mathcal{D}$.

(a) $\mathcal{C}$ e $\mathcal{D}$ assumem valores V. Por hipótese de indução temos $\{B_1',...,B_k'\} \vdash_L \mathcal{C}$ e $\{B_1',...,B_k'\} \vdash_L \mathcal{D}$. Assim por Modus Ponens inferimos, via axioma (ix), que vale $\{B_1',...,B_k'\} \vdash_L \mathcal{C} \wedge \mathcal{D}$.

(b) $\mathcal{D}$ ou $\mathcal{C}$ assumem valores F. Neste caso temos que $\mathcal{B}'$ é $\neg(\mathcal{C} \wedge \mathcal{D})$. Afirmamos que basta mostrar $\{B_1',...,B_k'\} \vdash_L \mathcal{C} \to \neg\mathcal{D}$. De fato, por (iv) e (vii) temos, respectivamente, que $T \vdash_L (\mathcal{C} \wedge \mathcal{D}) \leftrightarrow \neg(\mathcal{C} \to \neg\mathcal{D})$ e $T \vdash_L ((\mathcal{C} \wedge \mathcal{D}) \leftrightarrow \neg(\mathcal{C} \to \neg\mathcal{D})) \to ((\mathcal{C} \wedge \mathcal{D}) \to \neg(\mathcal{C} \to \neg\mathcal{D}))$. Destes dois resultados inferimos, por Modus Ponens, que $T \vdash_L (\mathcal{C} \wedge \mathcal{D}) \to \neg(\mathcal{C} \to \neg\mathcal{D})$. O item (e) do Lema 6.4 nos dá $T \vdash_L ((\mathcal{C} \wedge \mathcal{D}) \to \neg(\mathcal{C} \to \neg\mathcal{D})) \to (\neg\neg(\mathcal{C} \to \neg\mathcal{D}) \to \neg(\mathcal{C} \wedge \mathcal{D}))$ e por Modus Ponens inferimos $T \vdash_L \neg\neg(\mathcal{C} \to \neg\mathcal{D}) \to \neg(\mathcal{C} \wedge \mathcal{D})$. Do Teorema 6.4 (b) temos que $T \vdash_L (\mathcal{C} \to \neg\mathcal{D}) \to \neg\neg(\mathcal{C} \to \neg\mathcal{D})$, e destes dois últimos resultados inferimos, via Modus Ponens, $T \vdash_L (\mathcal{C} \to \neg\mathcal{D}) \to \neg(\mathcal{C} \wedge \mathcal{D})$. Temos agora duas opções:

  (a) $\mathcal{D}$ assume valor F. Neste caso a hipótese de indução nos dá $\{B_1',...,B_k'\} \vdash_L \neg\mathcal{D}$. Do axioma (i) segue que $\{B_1',...,B_k'\} \vdash_L \mathcal{C} \to \neg\mathcal{D}$.

  (b) $\mathcal{D}$ assume valor V (e portanto $\mathcal{C}$ assume valor F). Neste caso a hipótese de indução nos dá $\{B_1',...,B_k'\} \vdash_L \neg\mathcal{C}$. Do Lema 6.4 (c) segue que $\{B_1',...,B_k'\} \vdash_L \mathcal{C} \to \neg\mathcal{D}$.

Caso 4. Existem proposições $\mathcal{C}$ e $\mathcal{D}$ tais que $\mathcal{B}$ é a proposição $\mathcal{C} \vee \mathcal{D}$.

(a) $\mathcal{C}$ ou $\mathcal{D}$ assumem valor V. Neste caso temos que $\mathcal{B}' = \mathcal{B}$. O axioma (v) nos dá que $(\mathcal{C} \vee \mathcal{D}) \leftrightarrow (\neg\mathcal{C} \to \mathcal{D})$ é um teorema de T. Assim, como $\mathcal{B}'$ é a proposição $\mathcal{C} \vee \mathcal{D}$, basta mostrarmos que $B_1^{'},\ldots,B_k^{'}\} \vdash_L \neg\mathcal{C} \to \mathcal{D}$, e inferimos $\mathcal{B}'$ pelo axioma (vii), como fizemos no item anterior.

Caso $\mathcal{D}$ assuma valor V, pela hipótese de indução obtemos $\{B_1',...,B_k'\} \vdash_L \mathcal{D}$. Pelo axioma do tipo (i) temos que a proposição $\mathcal{D} \to (\neg\mathcal{C} \to \mathcal{D})$ é um teorema de T, e portanto, $\{B_1^{'},\ldots,B_k^{'}\} \vdash_L \neg\mathcal{C} \to \mathcal{D}$.

Caso $\mathcal{C}$ assuma valor V, por hipótese de indução obtemos $\{B_1',...,B_k'\} \vdash_L \mathcal{C}$. Pelos itens (b) e (c) do Lema 6.4 temos, respectivamente que as proposições

$\mathcal{C} \to \neg\neg\mathcal{C}$ e $\neg\neg\mathcal{C} \to (\neg\mathcal{C} \to \mathcal{D})$ são teoremas de T. Assim, por Modus Ponens, $\{B_1^{'}, \ldots, B_k^{'}\} \vdash_L \neg\mathcal{C} \to \mathcal{D}$

(b) $\mathcal{C}$ e $\mathcal{D}$ assumem valor F. Por hipótese de indução vale $\{B_1', ..., B_k'\} \vdash_L \neg\mathcal{C}$ e $\{B_1', ..., B_k'\} \vdash_L \neg\mathcal{D}$. E neste caso $\mathcal{B}$ assume valor F, logo $\mathcal{B}'$ é a proposição $\neg(\mathcal{C} \vee \mathcal{D})$. Pela equivalência $(\mathcal{C} \vee \mathcal{D}) \leftrightarrow (\neg\mathcal{C} \to \mathcal{D})$ dada pelo axioma (v) e pelo axioma (vii) inferimos $(\mathcal{C} \vee \mathcal{D}) \to (\neg\mathcal{C} \to \mathcal{D})$. E pela contrapositiva dada pelo item (e) do Lema 6.4 inferimos $\neg(\neg\mathcal{C} \to \mathcal{D}) \to \neg(\mathcal{C} \vee \mathcal{D})$. Assim, basta mostrar que $\{B_1', ..., B_k'\} \vdash_L \neg(\neg\mathcal{C} \to \mathcal{D})$. Isto, por sua vez, se deve ao fato de que vale $\{B_1', ..., B_k'\} \vdash_L \neg\mathcal{C}$ e $\{B_1', ..., B_k'\} \vdash_L \neg\mathcal{D}$, e concluímos portanto, , usando o item (f) do Lema 6.4, o desejado.

Caso 5. Existem proposições $\mathcal{C}$ e $\mathcal{D}$ tais que $\mathcal{B}$ é a proposição $\mathcal{C} \leftrightarrow \mathcal{D}$.

(a) $\mathcal{C}$ e $\mathcal{D}$ assumem valores-verdade iguais. Note que, neste caso, $\mathcal{B}' = \mathcal{B}$.

No caso em que ambas assumem valor V temos que $\{B_1', ..., B_k'\} \vdash_L \mathcal{C}$ e $\{B_1', ..., B_k'\} \vdash_L \mathcal{D}$. Pelo axioma (i) valem $\mathcal{C} \to (\mathcal{D} \to \mathcal{C})$ e $\mathcal{D} \to (\mathcal{C} \to \mathcal{D})$. Por fim, inferimos $\{B_1', ..., B_k'\} \vdash_L \mathcal{D} \to \mathcal{C}$ e $\{B_1', ..., B_k'\} \vdash_L \mathcal{C} \to \mathcal{D}$. Pelo axioma lógico (ix) e Modus Ponens inferimos $\{B_1', ..., B_k'\} \vdash_L (\mathcal{C} \to \mathcal{D}) \wedge (\mathcal{D} \to \mathcal{C})$. Logo do axioma lógico $(viii)$ inferimos $\{B_1', ..., B_k'\} \vdash_L \mathcal{C} \leftrightarrow \mathcal{D}$, e como $\mathcal{C} \leftrightarrow \mathcal{D} = \mathcal{B} = \mathcal{B}'$, segue o resultado.

O caso em que ambas assumem valor F é inteiramente análogo, usando o item (c) do Lema 6.4 e obtendo válidas em T as proposições $\neg\mathcal{C} \to (\mathcal{C} \to \mathcal{D})$ e $\neg\mathcal{D} \to (\mathcal{D} \to \mathcal{C})$.

(b) $\mathcal{C}$ e $\mathcal{D}$ assumem valores-verdade diferentes. Então $\mathcal{B}'$ é igual a $\neg(\mathcal{C} \leftrightarrow \mathcal{D})$. Dos axioma dos tipos (vi) e (vii) segue que $T \vdash_L (\mathcal{C} \leftrightarrow \mathcal{D}) \to (\mathcal{C} \to \mathcal{D})$ e $T \vdash_L (\mathcal{C} \leftrightarrow \mathcal{D}) \to (\mathcal{D} \to \mathcal{C})$. Do item (e) do Lema 6.4 segue, respectivamente, que $T \vdash_L \neg(\mathcal{C} \to \mathcal{D}) \to \neg(\mathcal{C} \leftrightarrow \mathcal{D})$ e $T \vdash_L \neg(\mathcal{D} \to \mathcal{C}) \to \neg(\mathcal{C} \leftrightarrow \mathcal{D})$. Usaremos isto nos dois subcasos possíveis.

(i) $\mathcal{C}$ assume valor F e $\mathcal{D}$ assume valor V. Por hipótese de indução temos que $\{B_1', ..., B_k'\} \vdash_L \neg\mathcal{C}$ e $\{B_1', ..., B_k'\} \vdash_L \mathcal{D}$. Pelo item (f) do Lema 6.4 segue que $T \vdash_L \mathcal{D} \to (\neg\mathcal{C} \to \neg(\mathcal{D} \to \mathcal{C}))$. Disto e de $T \vdash_L \neg(\mathcal{D} \to \mathcal{C}) \to \neg(\mathcal{C} \leftrightarrow \mathcal{D})$ inferimos, por Modus Ponens, que $\{B_1', ..., B_k'\} \vdash_L \neg(\mathcal{C} \leftrightarrow \mathcal{D})$, como desejado.

(ii) $\mathcal{C}$ assume valor V e $\mathcal{D}$ assume valor F. Por hipótese de indução temos que $\{B_1', ..., B_k'\} \vdash_L \mathcal{C}$ e $\{B_1', ..., B_k'\} \vdash_L \neg\mathcal{D}$. Pelo item (f) do Lema 6.4 segue que $T \vdash_L \mathcal{C} \to (\neg\mathcal{D} \to \neg(\mathcal{C} \to \mathcal{D}))$. Disto e de $T \vdash_L \neg(\mathcal{C} \to \mathcal{D}) \to \neg(\mathcal{C} \leftrightarrow \mathcal{D})$

inferimos, por Modus Ponens, que $\{B_1',...,B_k'\} \vdash_L \neg(\mathcal{C} \leftrightarrow \mathcal{D})$, como desejado. □

Teorema 6.6 (Completude do cálculo proposicional) *Se $\mathcal{B}$ é uma tautologia do cálculo proposicional T então $\mathcal{B}$ é um teorema de T.*

Demonstração: Seja $\mathcal{B}$ uma tautologia de T e sejam $B_1,...,B_k$ todas as letras proposicionais que ocorrem em $\mathcal{B}$. Para qualquer atribuição-verdade para $B_1,...,B_k$ temos que o valor-verdade de $\mathcal{B}$ é V, já que $\mathcal{B}$ é uma tautologia. Assim, pelo Lema 6.5 vale $\{B_1',...,B_k'\} \vdash_L \mathcal{B}$. Quando B_k assume valor V vale que $\{B_1',...,B_{k-1}',B_k\} \vdash_L \mathcal{B}$, e quando B_k' assume valor F vale que $\{B_1',...,B_{k-1}',\neg B_k\} \vdash_L \mathcal{B}$. Assim, pelo Teorema da Dedução para o Cálculo Proposicional segue que $\{B_1',...,B_{k-1}'\} \vdash_L B_k \rightarrow \mathcal{B}$ e $\{B_1',...,B_{k-1}'\} \vdash_L \neg B_k \rightarrow \mathcal{B}$. Logo, pelo Teorema 6.4 (g) e por Modus Ponens segue que $\{B_1',...,B_{k-1}'\} \vdash_L \mathcal{B}$. Refazendo este processo para cada $i < k$ temos que $\emptyset \vdash_L \mathcal{B}$, e em particular segue que $\mathcal{B}$ é um teorema de T. □

Teorema 6.7 *Toda sentença de uma linguagem de primeira ordem $\mathcal{L}$ que é fecho universal de uma tautologia de $\mathcal{L}$ pode ser provada usando apenas Modus Ponens e fechos universais de instâncias das seguintes tautologias:*

1. $\varphi \rightarrow (\psi \rightarrow \phi)$
2. $(\varphi \rightarrow (\psi \rightarrow \phi)) \rightarrow ((\varphi \rightarrow \psi) \rightarrow (\varphi \rightarrow \phi))$
3. $(\neg\varphi \rightarrow \neg\psi) \rightarrow ((\neg\varphi \rightarrow \psi) \rightarrow \varphi)$
4. $(\varphi \wedge \psi) \leftrightarrow \neg(\varphi \rightarrow \neg\psi)$
5. $(\varphi \vee \psi) \leftrightarrow (\neg\varphi \rightarrow \psi)$
6. $(\varphi \leftrightarrow \psi) \rightarrow (\varphi \rightarrow \psi)$
7. $(\varphi \leftrightarrow \psi) \rightarrow (\psi \rightarrow \varphi)$
8. $((\varphi \rightarrow \psi) \wedge (\psi \rightarrow \varphi)) \rightarrow (\varphi \leftrightarrow \psi)$
9. $\varphi \rightarrow (\psi \rightarrow (\varphi \wedge \psi))$

Demonstração: Seja σ uma tautologia de $\mathcal{L}$. Fixada T uma teoria para L, a partir da tautologia σ podemos obter uma tautologia (do cálculo proposicional) $\mathcal{B}$ de T fazendo a substituição de todas as fórmulas básicas que ocorrem em σ, digamos, $\varphi_1,...,\varphi_k$, por letras proposicionais quaisquer, digamos, $B_1,...,B_k$, tomando o cuidado de substituir as mesmas fórmulas básicas por letras proposicionais iguais. Para a tautologia $\mathcal{B}$ de T podemos aplicar o Teorema 6.6 e obter uma prova $\mathcal{A}_1,...,\mathcal{A}_n$ em T para $\mathcal{B}$. Vamos agora desfazer a substituição feita no início. Em cada $\mathcal{A}_j$, substitua-a as ocorrências de B_i por φ_i, e para cada letra proposicional que ocorrer e for diferente de todas as B_i's, substitua por uma sentença qualquer. Como tal sequência foi obtida a partir de uma prova para $\mathcal{B}$ em T, segue que tal sequência é uma prova para σ. $\square$

REFERÊNCIAS BIBLIOGRÁFICAS

[1] G. S. Boolos, *The Logic of Provability*, Cambridge University Press, Cambridge, 1994.

[2] W. A. Carnielli, M. Rathjen, *Combinatória e indemonstrabilidade, ou o 13. trabalho de Hércules*,. Matemática Universitária (1991).

[3] R. A. S. Fajardo, *Lógica Matemática*, Edusp, São Paulo, 2017.

[4] R E. Grandy, *Advanced Logic for Applications*, D. Reidel Publishing Company, Dordrecht and Boston, 1977.

[5] K. Kunen, *The Foundations of Mathematics*, London, 2009.

[6] E. Mendelson, *Introduction to Mathematical Logic*, New York, Chapman and Hall/CRC, 2015.

[7] J. Paris, L. Harrington, *A mathematical incompleteness in Peano arithmetic*, Handbook of Mathematical Logic. North-Holland Pub. Co. **90** (1977), 1133-1142.

[8] P. Smith, *An Introduction to Gödel's Theorems*, Cambridge University Press., Cambridge, 2013.

[9] R. Zach, *Hilbert's Program Then and Now*, Handbook of the Philosophy of Science **5** (2006), 411-447.