Lógica Matemática

Rogério Augusto dos Santos Fajardo

Prefácio

A matemática não é uma ciência, propriamente, mas, sim, uma linguagem. Seus objetos de estudo não são reais, concretos, palpáveis, mas são abstratos, padrões estabelecidos pela mente humana que permeiam todas as ciências. Em certo sentido, portanto, a matemática pode ser vista como uma forma de falar sobre esses objetos abstratos de maneira clara, para podermos entendê-los, desenvolvê-los e utilizá-los melhor. As ciências que se baseiam em grande parte na matemática são chamadas de *ciências exatas*. Isso porque chegou-se ao consenso de que quanto mais uma ciência nela for alicerçada nela, menor é o risco de apresentar conclusões erradas. Tal prerrogativa impõe a essa linguagem uma enorme responsabilidade: a de não apresentar erros. Não pode admitir imprecisões, falta de clareza ou ambiguidades. Por esse motivo, filósofos e matemáticos começaram a perceber – especialmente no início do século XX – que a linguagem que usamos no cotidiano não era adequada para tratar de matemática, e que era necessário formalizar a linguagem da matemática de maneira rigorosa. Foi nesse contexto que surgiu a lógica matemática.

O objetivo deste livro é introduzir ao estudante de matemática – seja em um curso de licenciatura ou em um curso de bacharelado – os fundamentos da lógica de primeira ordem, mostrando como essa pode ser utilizada para formalizar a matemática, tornando mais precisas as definições, notações e demonstrações que nela aparecem.

Dentro dessa proposta, e procurando ser um texto autocontido – na expectativa de atender a um público maior que o de estudantes de matemática – foram incluídos capítulos sobre teoria dos conjuntos. Primeiro a teoria *ingênua* dos conjuntos, sem formalização rigorosa (Capítulo 3), e mais tarde, no Apêndice A, já tendo sido desenvolvido todo o aparato lógico, a teoria *axiomática* dos conjuntos. Para convencer o leitor da suficiência da lógica e da teoria dos conjuntos no processo de fundamentação da matemática,

foi necessário incluir, no Apêndice A, de forma resumida, a construção dos conjuntos numéricos.

Apenas introduzir as definições e resultados técnicos da lógica, sem passar por pelo menos uma breve discussão histórica e filosófica sobre o propósito desses conceitos, torna a aprendizagem insossa e sem sentido. Por isso temos o Capítulo 1, com um pouco dessa discussão, que já se iniciou no primeiro parágrafo deste prefácio.

O Capítulo 2 apresenta a lógica proposicional. Embora muito pouco do que está nesse capítulo é usado nos subsequentes, e de ser possível falar de lógica de primeira ordem sem falar de lógica proposicional, por motivos didáticos mantivemos a tradição de iniciar os estudos de lógica com a proposicional. Complementando esse assunto, acrescentamos o Apêndice B, sobre álgebras de Boole, como um tópico opcional que enriquece o conhecimento sobre lógica proposicional e lógica, de forma geral.

O principal tema deste livro, a lógica de primeira ordem, é apresentado nos capítulos 4 a 6 em seus três pilares em capítulos separados: a linguagem (conjunto de símbolos e regras para compor esses símbolos), a semântica (significado da linguagem) e axiomática (processo de derivar uma afirmação a partir de outras, isto é, provar teoremas).

Os principais teoremas metamatemáticos – isto é, aqueles resultados que dizem respeito à própria lógica, apesar de também poderem ser provados *dentro* da lógica, como em uma regressão infinita (que será melhor discutida no Capítulo 1) – são enunciados e provados no Capítulo 7. A saber: teoremas da correção e completude, teorema da dedução, teorema da compacidade, teorema de Löweinheim-Skolem e os teoremas de incompletude de Gödel.

Não há pré-requisito formal para ler este livro, já que todos os conceitos usados são definidos e explicados dentro do texto. Porém, é aconselhável que o leitor tenha alguma experiência em demonstrações matemáticas informais, adquiridas em disciplinas como álgebra, álgebra linear e análise real. Caso contrário, deverá estar preparado para a dificuldade crescente que esse livro apresenta, especialmente a partir do Capítulo 5.

Conteúdo

Capítulo 1

Conceitos fundamentais da lógica

Neste capítulo apresentamos algumas discussões filosóficas e referências históricas sobre o surgimento e desenvolvimento da lógica matemática, introduzindo alguns conceitos importantes que serão desenvolvidos no decorrer desta obra. Tais discussões pretendem motivar o leitor e prepará-lo para as definições técnicas que se seguirão, de modo que essas se tornem mais intuitivas e claras.

Para quem deseja conhecer mais sobre a história da lógica e dos fundamentos da matemática indicamos [7], [14] e [31]. Uma visão lúdica do assunto encontra-se em [5], que escreve a história da lógica em quadrinhos. Nessas referências são descritos os questionamentos de diversos matemáticos e filósofos que contribuíram com o surgimento e desenvolvimento da lógica.

1.1 O que é lógica?

A Enciclopédia Barsa ([6]) nos dá a seguinte definição de lógica: "Ciência que estuda as leis do raciocínio e as condições de verdade em vários domínios do conhecimento".

Aristóteles, na Grécia Antiga, foi um dos pioneiros do desenvolvimento da lógica, apresentando regras para que um raciocínio esteja encadeado corretamente, chegando a conclusões verdadeiras a partir de premissas verdadeiras.

No século XIX, alguns matemáticos e filósofos – dentre eles George Boole (1815–1864), Augustus De Morgan (1806–1871), Gottlob Frege (1848–1925),

Bertrand Russell (1872–1970) e Alfred North Whitehead (1861–1947) – começaram a usar a lógica para fundamentação da matemática. Perceberam que, para esse propósito, era necessário desenvolver uma simbologia própria para a linguagem lógica, para evitar os paradoxos e imprecisões provenientes da linguagem natural começaram a desenvolver *lógica simbólica*, formada por uma linguagem estrita e universal, livre de contexto.

Entendemos por *linguagem* um conjunto de símbolos (geralmente visuais ou sonoros) que, dependendo da maneira como são dispostos em sequência, apresentam significados distintos. Por exemplo, um idioma pode ser visto como duas linguagens: uma em que os símbolos usados são sons (a linguagem *falada*) e outra em que os símbolos são visuais (a linguagem *escrita*). Foquemo-nos na língua escrita. Temos nela um conjunto de símbolos (as letras do alfabeto, os sinais de pontuação, os acentos gráficos, e até os espaços usados para separar as palavras) e algumas regras para juntar esses símbolos formando *palavras*, assim como algumas regras para juntar as palavras para formar *frases*. Nem todo agrupamento de letras forma uma palavra existente, assim como nem todo agrupamento de palavras forma uma frase bem estruturada.

Se alguém domina a língua escrita de um determinado idioma, é capaz de compreender quando um agrupamento de letras forma uma palavra, e quando um agrupamento de palavras forma uma frase gramaticalmente correta. Mas isso não será suficiente para qualquer forma de comunicação se não houver nessas frases outro fator essencial na liguagem: o *significado*. Quem domina um idioma não apenas reconhece as frases bem estruturadas, mas sabe transpor esse conjunto de sinais ao mundo real (ou a um mundo fictício, como em um conto de fadas), concedendo às palavras uma interpretação nesse mundo, e permitindo que a linguagem seja utilizada para que cada um possa transmitir a outros sua própria percepção do universo.

Percebemos, então, que toda linguagem é constituída de dois elementos. A *sintaxe* consiste no conjunto de símbolos usados e nas regras de formação de palavras e frases a partir desses símbolos. A *semântica* de uma linguagem é a forma como esses símbolos, palavras e frases adquirem um significado, uma interpretação em algum universo definido.

Estabelecer uma linguagem adequada e bem estruturada é fundamental para resolvermos e entendermos problemas dos mais variados objetos de estudo. O filósofo Wittgeinstein acreditava que diversos problemas da filosofia só existiam devido a falhas na linguagem utilizada, e que, portanto, eles seriam resolvidos à medida que aperfeiçoássemos a linguagem (vide [24]).

Foi partindo desse princípio que Wittgeinstein ajudou a desenvolver a lógica matemática, como uma linguagem rigorosa e livre de ambiguidades.

Exemplos clássicos de como uma linguagem imprecisa pode trazer problemas inerentes a ela são os *paradoxos*, que são afirmações que apresentam, em si, contradições aparentemente insolúveis. Vejamos, por exemplo, os paradoxos de Zenão de Eléia (490–430a.c.), que afirmava não haver movimento:

1. A flecha que voa nunca sai do lugar, pois, em cada instante de tempo ocupa uma só posição no espaço. Logo, ela está imóvel em todo o tempo.

2. O corredor Aquiles nunca alcança a tartaruga, quando postos a correr simultaneamente, com a tartaruga à frente. Pois, cada vez que Aquiles alcança a posição onde a tartaruga estava anteriormente, essa última, por sua vez, já avança um pouco, de modo que nunca será possível alcançá-la.

3. Entre dois pontos há infinitos pontos. Ninguém pode atravessar infinitos pontos. Logo, não há movimento.

Os argumentos de Zenão eram, na época, difíceis de serem rebatidos, por mais absurda que fosse sua conclusão. Quando um argumento parece correto, e sua conclusão é claramente falsa, mesmo partindo de premissas corretas, temos um *sofisma*. É necessário rever nossa linguagem e processo de argumentação se quisermos eliminar esses erros de raciocínio. No caso dos paradoxos de Zenão, o sofisma é oriundo da dificuldade de conceituar a infinitude. Sendo o infinito um dos primeiros conceitos matemáticos totalmente abstratos, nota-se a necessidade de uma linguagem aperfeiçoada para tratar esses conceitos de maneira precisa.

A lógica surgiu basicamente com dois propósitos: o de formalizar as "leis do pensamento" (essa expressão foi utilizada por outro pioneiro da lógica: George Boole), que utilizamos constantemente para argumentar e chegar a conclusões corretas a partir de premissas dadas, e o de estabelecer uma linguagem mais apropriada para a matemática e a filosofia, para evitar as armadilhas dos paradoxos e dos sofismas.

Para alcançar esse propósito, a formação de "palavras" e "frases" na lógica deve seguir regras objetivas, para que possamos limitar a linguagem e ter *controle* sobre ela. Isto é, para que possamos estudar propriedades gerais sobre as sentenças lógicas, o que é muito difícil de se conseguir na linguagem

natural. Dizemos, então, que a lógica possui uma *sintaxe controlada*, livre de contexto.

O significado de uma sentença lógica depende de uma *interpretação*. No caso da lógica proposicional, essa interpretação é dada pela valoração, uma função que atribui a cada sentença o valor verdadeiro ou falso (veja Seção 2.2). No caso da lógica de primeira ordem, essa é dada por um modelo e uma valoração das variáveis, como será visto no Capítulo 5. A interpretação da linguagem é chamada de *semântica*.

1.2 A lógica e a linguagem natural

Por que precisamos criar uma linguagem nova para formalizar a matemática e outras formas de raciocínio? Ou, por outro lado, por que não poderíamos substituir a linguagem usada no dia-a-dia pela linguagem lógica, se essa é mais rigorosa?

Para responder a essas perguntas e entendermos melhor a diferença entre a linguagem lógica e a linguagem natural, recorremos a um dos fundadores da lógica moderna. Gottlob Frege comparava a linguagem natural ao olho humano e a lógica ao microscópio, conforme a seguinte explanação, extraída de [23]:

> "Creio que posso tornar mais clara a relação entre minha conceitografia e a linguagem comum comparando-a à que existe entre o microscópio e o olho. Este, pela extensão de sua aplicabilidade, pela agilidade com que é capaz de adaptar-se às diferentes circunstâncias, leva grande vantagem sobre o microscópio. Considerado como aparelho ótico, o olho exibe decerto muitas imperfeições que habitualmente permanecem despercebidas, em virtude da ligação íntima que tem com a vida mental. No entanto, tão logo os fins científicos imponham exigências rigorosas quanto à exatidão das discriminações, o olho revelar-se-á insuficiente. O microscópio, pelo contrário, conforma-se a esses fins de maneira mais perfeita, mas, precisamente por isso, é inutilizável para todos os demais."

A extensão de visão do olho humano é bem maior que a do microscópio, mas esse enxerga pequenos detalhes não visíveis aos olhos humanos. A visão do microscópio é mais detalhada, porém mais limitada.

A lógica – justamente por possuir uma sintaxe controlada e livre de contexto – tem um poder expressivo muito inferior à linguagem natural. Ela é insuficiente para descrevermos sentimentos e outros pensamentos mais complexos, e por esse motivo não pode substituir a linguagem cotidiana.

Por outro lado, quando estudamos assuntos mais restritos, com menos complexidade, porém com maior exigência de rigor – como é o caso da matemática – a lógica faz-se necessária.

A linguagem natural ganha em expressividade, e a lógica ganha em rigor. A linguagem natural é útil para a visão panorâmica, e a lógica é útil para a visão detalhada.

À medida que queremos aproximar a lógica da linguagem natural, ganhando um pouco da expressividade dela sem perder o rigor daquela, pagamos o preço da complicação. Da mesma forma como uma imagem digitalizada no computador tenta aproximar uma cena real através de pequeníssimos quadradinhos coloridos, e fica tão mais dispendiosa para a memória do computador quanto exigimos maior resolução, também a lógica torna-se substancialmente mais complicada à medida que tentamos aproximá-la da linguagem natural, mantendo o rigor de uma linguagem lógica. É o caso das lógicas não-clássicas, descritas na Seção 1.6. Especialmente a lógica intuicionista e a lógica fuzzy foram elaboradas para se aproximarem da linguagem natural, e por isso mesmo são mais complexas que a lógica de primeira ordem.

Mesmo não sendo possível, na comunicação cotidiana, substituir a linguagem natural pela linguagem lógica, a compreensão da última fortalecerá o domínio da primeira. Quem estudou lógica será capaz de perceber alguns padrões onde é possível aplicar o rigor matemático, em fragmentos da linguagem. Não será frequente aplicarmos a lógica na linguagem natural para tirarmos conclusões logicamente corretas, de caráter incontestável, como, na concepção aristotélica da lógica formal, mas poderá nos prevenir de tirar conclusões erradas, conforme disse Bertrand Russel, no seguinte texto extraído de [21], página 93:

> A lógica era, antigamente, a arte de tirar conclusões; agora, tornou-se a arte de abster-se de deduções, pois parece que as conclusões a que somos inclinados a chegar com naturalidade quase nunca são válidas. Concluo, portanto, que a lógica dever ser ministrada nas escolas com o propósito de ensinarem as pessoas a não raciocinar. Porque, se raciocinarem, certamente o farão de forma equivocada.

1.3 Linguagem e metalinguagem

No início de *Uma breve história do tempo* ([10]), o físico inglês Stephen Hawking nos conta a seguinte história:

> Um famoso cientista – alguns dizem que foi Bertrand Russell –, fazendo uma conferência sobre astronomia, descreveu como a Terra gira em torno do Sol e como o Sol, por sua vez, gira em torno do centro de uma vasta coleção de estrelas chamada galáxia. No final da conferência, uma senhora baixinha e idosa levantou-se ao fundo da sala e falou: "O que o senhor acaba de nos dizer é tolice. O mundo, na verdade, é um objeto achatado, apoiado nas costas de uma tartaruga gigante." O cientista sorriu com superioridade antes de replicar: "E sobre o que se apóia a tartaruga?". "Você é muito esperto, rapaz, muito esperto" – disse a velhinha –, "mas existem tartarugas marinhas por toda a extensão embaixo dela."

A concepção *nom-sense* de uma "torre infinita de tartarugas" para apoiar a Terra ilustra bem o problema da regressão infinita, na formalização da lógica, conforme descreveremos a seguir.

A lógica é uma linguagem utilizada para descrever e demonstrar com rigor os fatos matemáticos. Ora, mas a lógica é, em si, parte da matemática [1]. E como qualquer outra parte da matemática, há resultados e teoremas sobre ela. Mas se a linguagem da matemática é a própria lógica, qual linguagem utilizaremos quando construímos a lógica?

A princípio, utilizamos a linguagem natural, mas de forma controlada, para que, após definida a linguagem lógica, possamos transferir o que foi feito para a linguagem lógica. Assim, trabalhamos com a lógica em dois níveis: aquela sobre a qual estamos provando teoremas e fazendo definições, e aquela que utilizamos para escrevê-los. A essa linguagem que usamos para escrever sobre a linguagem chamamos de *metalinguagem*.

Por exemplo, um teorema sobre números naturais, escrito na linguagem da lógica, é um teorema matemático. O teorema de Gödel, que diz que em

[1] O lógico e matemático Charles Dogdson, conhecido pelo pseudônimo Lewis Carrol, criou uma situação em seu livro *Alice no país dos espelhos* bem similar a essa. Alice viu o rei vermelho dormindo, e foi alertada a não acordá-lo, pois ele estaria sonhando com ela. Portanto, se ela o acordasse, Alice deixaria de existir. Mas sabemos que a história toda narrava um sonho de Alice. Ou seja, Alice sonhava com o rei, que sonhava com Alice, que sonhava com o rei... Nessa situação hipotética, se um acordasse ambos desapareceriam.

certos tipos de sistemas lógicos sempre existe uma sentença que não pode ser provada nem verdadeira nem falsa, é um resultado que fala diretamente da lógica, e por isso é um teorema *metamatemático*.

1.4 Demonstração matemática

Uma demonstração matemática se assemelha a uma argumentação na linguagem natural. Quando queremos convencer alguém de alguma opinião, começamos procurando afirmações com as quais nosso interlocutor já previamente concorda, ou por serem consideradas óbvias, ou porque conhecemos alguns pontos de vista do interlocutor. Em seguida, propomos outra afirmação e mostramos que essa é consequência daquelas. Portanto, se alguém acredita naquelas afirmações deve, também, aceitar a última. A partir desse ponto podemos incluir essa nova afirmação entre aquelas que são aceitas como verdadeira pelo nosso interlocutor. Continuamos, dessa forma, encadeando frases até chegarmos à afirmação que defendemos.

Na prática, no entanto, uma argumentação não é tão simples assim. Não é possível determinar com precisão se uma frase é consequência de outras ou não. Nem mesmo é possível estabelecer o que é óbvio ou senso comum, e o que não é.

Na matemática, por justamente servir de base para as chamadas ciências exatas, esperamos uma certeza nos resultados que a linguagem natural não é capaz de proporcionar. Há e sempre haverá problemas em aberto, mas uma vez provado um teorema matemático, em que cada passo da demonstração foi cuidadosamente verificado, não deverá haver dúvidas sobre sua validade.

O conceito de demonstração matemática evoluiu muito ao longo do tempo. Houve época em que a matemática era retórica e não possuía uma simbologia própria. Euclides, quando escreveu os *Elementos* (veja [11]), estabeleceu um novo padrão de demonstrações matemáticas, introduzindo os conceitos de *axiomas* e *postulados*. Uma axioma era, na definição daquela época, *uma verdade evidente em si mesma*. Ou seja, corresponde ao *óbvio* na argumentação. Os postulados também tinham um significado semelhante, mas eram específicos para a geometria – enquanto os axiomas dissertavam sobre grandezas matemáticas, em geral – e "menos óbvios". Correspondem ao que chamamos, na argumentação, de *senso comum*.

Escrito aproximadamente no ano 300 a.c., os *Elementos* se tornaram a grande referência do rigor matemático até meados do século XIX, quando

veio o desenvolvimento da lógica moderna e, com ela, alguns conceitos foram revistos. David Hilbert reformulou os axiomas e postulados de Euclides, introduzindo a ideia de *conceitos primitivos*. Enquanto Euclides tentou definir conceitos como ponto, curva e reta, Hilbert considerou esses e outros como conceitos primitivos, que dispensam definição. Os axiomas e postulados deixaram de ser considerados "evidentes em si mesmos", e passaram a ser apenas afirmações que *assumimos* como verdadeiras.

A grande inovação que Hilbert fez sobre as demonstrações matemáticas foi torná-las independentes de qualquer interpretação intuitiva do significado das expressões matemáticas. Sobre os conceitos primitivos, como ponto, reta e plano, Hilbert dizia que esses poderiam significar qualquer coisa, como *mesas, cadeiras e canecas de cerveja*. Seja qual for o significado que você atribuir a esses conceitos, esse não interfere na análise da validade de uma demonstração. É claro que a intuição é essencial para o processo de desenvolvimento da matemática, mas verificar se uma demonstração está correta não pode depender dela. Ou seja, *é possível provar um teorema conhecendo apenas a sintaxe da lógica, e não a semântica*. Sem a semântica, um teorema não tem valor algum. Mas verificar a prova de um teorema sem depender da semântica contribuiu com a credibilidade do resultado.

O uso da lógica simbólica foi outro passo importante na evolução do conceito moderno de demonstração matemática. A sintaxe controlada da lógica permite definirmos precisamente quando uma afirmação é consequência de outras, através de regras que possam ser verificadas computacionalmente. Essas são as chamadas *regras de inferência*.

Portanto, na matemática moderna, uma demonstração é uma sequência de fórmulas matemáticas, em uma linguagem lógica apropriada, em que cada fórmula ou é um axioma ou é obtida a partir de fórmulas anteriores através de uma regra de inferência. Um *teorema* é qualquer uma dessas fórmulas que ocorrem em uma demonstração.

Com exceção do *Principia Mathematica*, de Russell e Whitehead ([22]), nenhum matemático escreve demonstrações completas, no sentido do parágrafo anterior, usando estritamente a linguagem simbólica. Porém, é importante ter alguma noção de que *os argumentos apresentados podem ser formalizados na linguagem lógica*, se tivermos tempo e paciência suficientes.

Um teorema matemático depende, dessa forma, dos axiomas e regras de inferência estabelecidos, bem como da própria linguagem lógica. Nisso ainda há grandes discussões filosóficas sobre quais axiomas devemos assumir e qual lógica utilizamos. Por isso não podemos considerar axiomas como

verdades absolutas, mas apenas como hipóteses que assumimos verdadeiras. Uma demonstração bem feita não gera contestações sobre sua validade, mas poderá haver contestações filosóficas sobre o sistema de axiomas adotado.

Vamos comparar a explicação acima com o que acontece na linguagem natural. Um debate racional deve deixar claro quais são os pressupostos assumidos pelos debatedores. Você pode assumir como "axioma", em uma argumentação, tudo que você sabe que faz parte dos princípios morais ou políticos de seu interlocutor, mas não pode assumir como axioma seus próprios princípios, se sabe que o seu interlocutor não as tem. O conjunto de princípios e a ideologia de cada um correspondem ao sistema de axiomas. Provar teoremas a partir de um sistema de axiomas faz parte da matemática, discutir o sistema de axiomas faz parte da filosofia.

Concluímos a descrição das três componentes de uma lógica: a linguagem, a semântica e o sistema de axiomas. A linguagem é o conjunto de símbolos utilizados e as regras que determinam quando agrupamentos desses símbolos são fórmulas bem formadas. A semântica é a interpretação que fazemos desses símbolos, e o sistema de axiomas é o conjunto de axiomas e regras de inferência que definem as demonstrações nessa lógica.

Nos Capítulos 4, 5 e 6 mostramos essas três componentes no caso da lógica de primeira ordem.

Conforme vimos, pela explicação de Hilbert sobre conceitos primitivos, o sistema de axiomas, assim como a linguagem, está associada à sintaxe da linguagem. Porém, o sistema de axiomas deve ser elaborado de modo a manter coerência com a semântica. As propriedades de *correção* e *completude* de um sistema de axiomas – que serão mostradas no Capítulo 7, para o caso da lógica de primeira ordem – asseguram que o sistema prova exatamente as fórmulas que são verdadeiras de acordo com a semântica, e são requisitos fundamentais para uma boa axiomatização.

No Apêndice A mostramos a força expressiva da lógica de primeira ordem, que, através da teoria dos conjuntos, é capaz de formalizar toda a matemática, reduzindo seus teoremas a teoremas lógicos.

1.5 O paradoxo do mentiroso

A lógica formal aristotélica estabelecia dois princípios fundamentais para a análise da veracidade de uma sentença. O *princípio do terceiro excluído* assegura que uma sentença deve ser verdadeira ou falsa. Em outras palavras,

ou ela própria é verdadeira ou sua negação. O *princípio da não-contradição* atesta que uma sentença não pode ser simultaneamente verdadeira e falsa. Ou seja, uma sentença e sua negação não podem ser ambas verdadeiras. Esses princípios são válidos em todas as chamadas *lógicas clássicas*, incluindo a lógica proposicional e a lógica de primeira ordem, que são temas deste livro e são utilizadas pela maioria dos matemáticos para formalizar a matemática.

À luz desses princípios, imagine que queiramos analisar se a frase seguinte, escrita na linguagem natural, é verdadeira ou falsa.

Eu estou mentindo.

Ora, se a frase é verdadeira, então é falsa, pois ela própria atesta isso. Por outro lado, se dissermos que a frase é falsa, o que isso significa? Que não é verdade o que a frase diz, ou seja, significa que não é uma mentira. Então a frase é verdadeira.

Portanto vimos que, se a frase for verdadeira, ela será falsa, e, se for falsa, será verdadeira. Então ou será simultaneamente verdadeira e falsa, ou não será nem verdadeira nem falsa, entrando em conflito ou com o princípio da não-contradição ou com o princípio do terceiro excluído. Esse é o *paradoxo do mentiroso* . Pior do que uma mera contradição, em que simplesmente descobrimos que uma sentença é falsa, nesse tipo de paradoxo não é possível sequer determinar se ela é verdadeira ou falsa.

Há muitas variações do paradoxo do mentiroso. Uma semelhante ao que enunciamos:

Esta afirmação é falsa.

Em todos os paradoxos desta categoria, ocorre a situação de *auto-referência*, em que uma frase nega a si própria. Algumas situações ligeiramente diferentes também costumam ser chamadas de paradoxais, e estão associadas a auto-referência, mas não são autênticos paradoxos. Como a seguinte frase:

Tudo que eu digo é mentira.

Nesta frase, apesar da clara auto-referência que caracteriza o paradoxo do mentiroso, ainda *pode ser* que consigamos decidir se ela é verdadeira ou falsa. Claro que, se ela for verdadeira, então ela será falsa, pois está inclusa nas "coisas que eu digo". Porém, se for falsa, ao contrário do que ocorre com

os exemplos anteriores, não podemos concluir que ela seja verdadeira. Se eu já disse antes alguma verdade, então a frase acima é simplesmente falsa.

Outro paradoxo clássico é o *paradoxo do barbeiro de Servilha*.

> *Havia em Servilha um barbeiro que só cortava o cabelo de todas as pessoas que não cortavam o próprio cabelo.*

Pergunta: o barbeiro de Servilha cortava o próprio cabelo? Se sim, então ele não podia cortar, pois ele *só* cortava o cabelo de quem não cortava o próprio cabelo. Se não cortava, ele deveria, pois cortava o cabelo de *todas* as pessoas que não cortavam o próprio cabelo.

Diferente dos outros casos, não mostramos que a frase é tanto verdadeira quanto falsa, ou nem verdadeira nem falsa. De fato, mostramos que a frase é falsa, e que um barbeiro assim, na verdade, *não existe*.

No dia-a-dia nos deparamos frequentemente com frases auto-contraditórias que lembram o paradoxo do mentiroso. Eis alguns exemplos clássicos:

> *Nunca diga nunca.*
>
> *Toda regra tem exceção.*
>
> *Não se deixe influenciar pela opinião de outros.*

Mas chegou um momento em que, mais que um trocadilho na linguagem natural, o paradoxo do mentiroso começou a se tornar uma ameaça real para o pensamento matemático. Digamos que alguém queira definir um número da seguinte maneira:

> *O menor número natural que não pode ser definido com menos de vinte palavras.*

Não há dúvida quanto à boa definição do número acima. Como temos uma quantidade finita de palavras, com menos de vinte delas só conseguimos descrever uma quantidade limitada de números naturais. Então é possível escolhermos o menor dos números que não podem ser descritos dessa maneira. Chamemo-lo de n. A definição de n usa apenas catorze palavras, mas isso é um absurdo, pois n não pode ser definido com menos de vinte palavras.

Esse paradoxo – conhecido como *Paradoxo de Richard* – expõe o perigo de usar a linguagem natural para formalizar a matemática. Por isso precisamos

de uma linguagem *de sintaxe controlada*: para evitar situações como a auto-referência, que podem levar a matemática a uma contradição.

Mas nem a linguagem rígida da lógica tem protegido a matemática do perigo da auto-referência. Usando um paradoxo semelhante ao do barbeiro de Servilha, Russell derrubou a tentativa de Frege de formalizar a matemática através da lógica e teoria dos conjuntos. Na teoria de Frege, um conjunto seria definido por uma sentença lógica que descreve as propriedades que caracterizam seus elementos. Por exemplo, o conjunto dos números primos seria definido como "o conjunto dos números naturais que possuem exatamente dois divisores inteiros positivos". Essa frase pode ser escrita na linguagem lógica e define, portanto, um conjunto matemático. Mas Russell observou que, seguindo essa teoria, podemos definir o seguinte conjunto:

> O conjunto de todos os conjuntos que não pertencem a si mesmos.

Se X é esse conjunto, podemos levantar a seguinte questão: X pertence a si mesmo? Se sim, então, pela definição, X não pertence a si mesmo. Se não pertence a si mesmo, a definição de X garante que ele pertence a X. Assim como acontece com o barbeiro de Servilha, a existência de tal conjunto leva a uma contradição.

Para sanar esse problema, Russell criou a teoria dos tipos, na qual os objetos matemáticos são classificados por uma hierarquia infinita. Os objetos de tipo 0 são os indivíduos – como os números naturais – que não possuem, eles próprios, elementos. Os objetos de tipo 1 são conjuntos de objetos do tipo 0. Os de tipo 2 possuem como elementos apenas os objetos de tipo 1, e assim por diante. Seguinte essa linha, Russell e Whitehead formalizaram toda a matemática básica ao escreverem o *Principia Mathematica* ([22]), uma obra de mais de 2000 páginas onde mais de 300 são utilizadas apenas para provar que $1 + 1 = 2$.

No entanto, o problema da auto-referência também afeta a axiomatização de Russell e Whitehead. O jovem austríaco Kurt Gödel, aos 24 anos, em sua tese de doutorado (veja [8]), mostrou que se o sistema de Russell se for consistente, ele é *incompleto*, ou seja, algumas proposições não podem ser provadas nem refutadas pelo sistema [2].

[2]Não confundir o conceito de incompletude dos teoremas de Gödel com a completude a qual nos referimos agora há pouco, sobre a compatibilidade da sintaxe e da semântica.

O argumento usado por Gödel foi mais uma variação do paradoxo do mentiroso. Usando a técnica da aritmetização da linguagem, Gödel mostrou que mesmo na linguagem simbólica controlada do *Principia* é possível escrever uma fórmula que equivale ao seguinte:

Eu não posso ser provada.

Chamemos tal fórmula de A. Suponha que o sistema prove que A é verdadeira. Ora, então haveria uma demonstração para A. Logo, provamos que "A fórmula A pode ser provada". Mas essa é justamente a negação de A. Por outro lado, se provarmos a negação de A, isso significa que de fato A pode ser provada, então existe uma demonstração para A. Ou seja, se provarmos A, provamos a negação de A, e se provarmos a negação de A, provamos A. Portanto, ou provamos tanto A quanto sua negação – tornando o sistema inconsistente – ou não provamos nem A nem sua negação – tornando o sistema incompleto.

O segundo teorema de Gödel tem consequências ainda piores para as tentativas de Russell e Hilbert de formalizar a matemática de modo completo e livre de contradições. Gödel mostra que, se o sistema for consistente, ele não poderá provar a própria consistência. De fato, pelo comentário do parágrafo anterior, vemos que, se o sistema for consistente, não poderá provar A, pois, neste caso, provaria também sua negação. Logo, se provarmos a consistência do sistema, em particular provamos que A não pode ser provada. Mas isso é justamente o que diz a fórmula A, que, portanto, acaba de ser provada, levando o sistema a uma inconsistência.

Gödel mostrou que a falha no sistema do *Principia* não era exatamente um erro desse, mas um fato inevitável, que ocorre em qualquer tentativa de sistematizar a matemática, satisfazendo algumas condições mínimas que os lógicos buscavam.

Apesar de parecer uma ingênua "brincadeira" com palavras, não é exagero dizer que o paradoxo do mentiroso causou um significativo alvoroço na matemática. Há muita literatura de divulgação científica sobre o assunto. Raymond Smullyam, em seus livros ([26], [27] e [28]), cria vários passatempos e enigmas matemáticos baseados nesse tipo de paradoxo, que ele chama de "enigmas gödelianos". Outro livro, que é um grande clássico sobre o assunto, é o de Hofstadter ([12]), que traça um paralelo entre as obras do lógico-matemático Gödel, do artista plástico Escher e do compositor Bach – todas caracterizadas por frequentes auto-referências.

Os teoremas de Gödel serão temas da Seção 7.5.

1.6 Um passeio pelas diferentes lógicas

Existem muitos tipos de lógica, cada uma delas apresentando suas aplicações teóricas e práticas. Listaremos, a seguir, as principais lógicas existentes, com uma breve descrição do que elas significam e para que são usadas.

- **Lógica proposicional** (ou **cálculo proposicional**): A lógica proposicional é o mais elementar exemplo de lógica simbólica. Sua semântica tem como base os princípios do terceiro excluído e da não-contradição, sendo, assim, a primeira referência de *lógica clássica*.

  A linguagem da lógica proposicional é formada pelas fórmulas atômicas (representadas geralmente por letras minúsculas), parênteses e conectivos ("e", "ou", "não", "se... então" etc.), e não possui quantificadores ("para todo" e "existe"). Mas essa simplicidade faz com que ela não tenha força expressiva para formalizar a matemática.

- **Lógica de primeira ordem** (ou **cálculo dos predicados**): É a lógica usada para formalizar a matemática e, por esse, motivo, o tema principal deste livro. Sua sintaxe também apresenta os conectivos da lógica proposicional, mas acrescenta os quantificadores ("para todo" e "existe") e as variáveis, além de outros símbolos específicos, que dependem do assunto que a linguagem aborda (por exemplo, $+$ e $\cdot$ na linguagem da aritmética e $\in$ na linguagem da teoria dos conjuntos).

  A presença dos quantificadores torna substancialmente mais difícil a construção da sintaxe e da semântica, em relação à lógica proposicional, mas ganha muito em expressividade.

- **Lógica de segunda ordem**: Assemelha-se à lógica de primeira ordem, mas possui quantificadores sobre classes de indivíduos, e não apenas sobre indivíduos. Por exemplo, um sistema de lógica de primeira ordem sobre aritmética dos números naturais permite construirmos sentenças do tipo "Para todo número natural temos..." ou "Existe um número natural tal que...", mas não permite sentenças do tipo "Para todo **conjunto** de números naturais temos..." ou "Existe um **conjunto** de números naturais tal que...". Esse tipo de sentença existe na lógica de segunda ordem.

  Porém, alguns teoremas importantes que valem na lógica de primeira ordem não valem na lógica de segunda ordem, o que apresenta uma

grande desvantagem para a última. Além disso, a teoria dos conjuntos consegue "driblar" essa limitação da lógica de primeira ordem na formalização da matemática.

- **Teoria dos tipos**: Criada por Bertrand Russell, em seu *Principia Mathematica*, é uma extrapolação da ideia da lógica de segunda ordem. Na teoria dos tipos, quantificamos os indivíduos, as classes de indivíduos, as classes de classes de indivíduos, e assim por diante, como se fosse uma *lógica de ordem infinita* [3]. Para fazer isso, o processo não é muito diferente da lógica de primeira ordem: apenas classificamos as variáveis por *tipos* (variáveis de primeiro tipo, variáveis de segundo tipo, e assim por diante). Além do trabalho original de Russell e Whitehead ([22]), o leitor poderá conferir a formalização da teoria dos tipos na tese de Gödel ([8]).

- **Lógica modal**: A lógica modal usa a *semântica dos mundos possíveis*. É uma extensão da lógica proposicional, acrescendo-lhe dois operadores: "necessariamente" e "possivelmente". O valor lógico – verdadeiro ou falso – de uma sentença depende de qual dos "mundos possíveis" ela está sendo analisada. Dizemos que uma sentença é "necessariamente verdadeira" em um mundo se ela é verdadeira em todos os mundos *acessíveis* àquele. Dizemos que uma sentença é "possivelmente verdadeira" em um mundo se é verdadeira em pelo menos um mundo acessível a esse

  Os operadores modais são semelhantes aos quantificadores, mas a semântica de Kripke (dos mundos possíveis) oferece uma interpretação diferente da dos quantificadores, pois se baseia em uma relação de acessibilidade entre os mundos.

- **Lógica descritiva**: A lógica descritiva pode ser considerada como um fragmento da lógica de primeira ordem, uma vez que toda sentença escrita na linguagem da lógica descritiva pode ser traduzida, de uma maneira relativamente simples, para uma sentença de mesmo significado na lógica de primeira ordem. Por outro lado, com uma sintaxe mais simples e sem uso de variáveis, tornou-se uma ferramenta útil em ciências da computação.

[3] Seguindo esse pensamento, podemos dizer que a lógica proposicional é uma *lógica de ordem zero*.

- **Lógica paraconsistente**: As lógicas clássicas – aquelas que atendem aos princípios do terceiro excluído e da não-contradição – são bastante intolerantes em relação às contradições. Se uma teoria incluir premissas contraditórias, isto é, deduzir uma sentença e sua negação a partir dos axiomas, dela poderá se deduzir qualquer sentença, através dos princípios da lógica clássica, tornando-o inútil. Por isso existe a preocupação – como veremos no Capítulo 7 – em provarmos a consistência (não-contradição) de um sistema lógico.

  Por outro lado, a lógica paraconsistente – criada pelo filósofo e matemático brasileiro Newton da Costa – permite contradições, tornando possível que uma sentença e sua negação sejam simultaneamente aceitas como verdadeiras.

  Dentre as diversas aplicações mencionadas pelo professor Newton ressaltamos a robótica: um programa de inteligência artificial deve saber como agir em caso de receber informações contraditórias, sem entrar em colapso e sem descartar totalmente as contradições.

- **Lógica intuicionista**: A implicação da lógica clássica é contra-intuitiva, pois não traduz a relação de causa-efeito que aparece na linguagem natural. Na lógica intuicionista a definição da implicação é um dos principais pontos que a diferencia da lógica proposicional, mas há outras diferenças, como dupla negação não se anular e não haver provas por absurdo. Parte dos matemáticos – os *construcionistas* – adota essa lógica para formalizar a matemática, entendendo que o modo moderno predominante de sistematizar a matemática a afastou da realidade e das aplicações práticas.

  Enquanto a lógica paraconsistente permite considerar que tanto uma fórmula quanto sua negação como verdadeiras, a lógica intuicionista é *paracompleta*, pois ela nega o princípio do terceiro excluído, permitindo que uma fórmula e sua negação sejam ambas falsas.

- **Lógica fuzzy** (ou **lógica difusa**): Enquanto na lógica clássica cada afirmação recebe apenas o valor de verdadeiro ou falso, a lógica *fuzzy* permite valorar uma fórmula com qualquer valor real no intervalo $[0, 1]$. Permitindo "verdades parciais", se aproxima de alguns problemas reais, que necessitam lidar com incertezas. Pode ser interpretada do ponto de vista estatístico, onde a valoração das fórmulas representam a probabilidade de um evento ocorrer.

Capítulo 2

Lógica proposicional

A lógica proposicional estende a lógica aristotélica, acrescentando-lhe uma linguagem simbólica que proporciona maior precisão e expressividade. Assim como a lógica formal, a proposicional relaciona os juízos de verdadeiro ou falso entre várias proposições, independente do significado de cada uma delas. É a lógica mais conhecida entre não-matemáticos, servindo frequentemente de temas para concursos públicos e sendo, ocasionalmente, ensinada no ensino médio.

Este capítulo requer pouco conhecimento prévio de matemática. Apenas noções intuitivas e superficiais de conjuntos, funções e sequências são requeridas.

A ideia de "conjuntos de símbolos", recorrente neste capítulo, será tratada de maneira informal. Se alguém quiser formalizar a lógica proposicional dentro da teoria axiomática dos conjuntos deve fazer algo semelhante à aritmetização da linguagem, como na Seção 7.5, usando os axiomas de ZFC (vide Apêndice A).

Este livro não tratará da abordagem axiomática da lógica proposicional, pois a tabela-verdade oferece um método mais simples e eficaz para verificar se uma fórmula da lógica proposicional é verdadeira ou não. Indicamos [30] para esse assunto.

Sugerimos [25] como uma leitura complementar sobre a lógica proposicional, com destaque ao método do *tableaux* para verificação de tautologias.

2.1 A linguagem da lógica proposicional

Chamamos de *alfabeto* de uma linguagem o conjunto dos símbolos que a compõem. O alfabeto da lógica proposicional é constituída pelos seguintes símbolos:

Variáveis proposicionais: Também chamadas de *fórmulas atômicas*, são os elementos "indivisíveis" da lógica, e as representamos pelas letras minúsculas, geralmente a partir da letra p:

$$p, q, r, s, \ldots$$

Quando precisamos usar muitas fórmulas atômicas, e as letras tornam-se insuficientes, costumamos usar a letra p indexada por um número natural:

$$p_0, p_1, p_2, \ldots$$

Conectivos lógicos: São os símbolos que nos permitem construir novas fórmulas a partir de outras.

$\neg$	negação (não)
$\wedge$	conjunção (e)
$\vee$	disjunção (ou)
$\rightarrow$	implicação (se ... então)
$\leftrightarrow$	equivalência (se, e somente se)

Delimitadores: São os parênteses, que servem para evitar ambiguidades na linguagem:

(	parêntese esquerdo
)	parêntese direito

Agora que conhecemos o alfabeto da linguagem da lógica proposicional, precisamos conhecer sua *gramática*, isto é, as regras que determinam quando uma sequência de símbolos do alfabeto formam expressões com significados. As sequências que são formadas de acordo com essas regras são chamadas de *fórmulas*[1]. Costumamos representar as fórmulas por letras maiúsculas, eventualmente indexadas com números naturais.

[1] No inglês, costuma-se usar a expressão *well-formed formula* (fórmula bem formada).

Regras de formação das fórmulas:

1. Variáveis proposicionais são fórmulas;
2. Se A é uma fórmula, $(\neg A)$ é uma fórmula;
3. Se A e B são fórmulas, $(A \wedge B)$, $(A \vee B)$, $(A \rightarrow B)$ e $(A \leftrightarrow B)$ também são fórmulas;
4. Não há outras fórmulas além das obtidas pelo uso das regras 1 a 3.

Vejamos um exemplo de como funcionam essas regras. Pela regra número 1, p é uma fórmula. Pela regra número 2, $(\neg p)$ é uma fórmula. Mas, novamente pela regra número 1, sabemos que q é uma fórmula. Logo, a regra número 3 garante que $(q \wedge (\neg p))$ também é uma fórmula. E então $(p \rightarrow (q \wedge (\neg p)))$ é uma fórmula, que pode ser lida como: "se p é verdadeiro, então q e não p são verdadeiro", ou "se p é verdadeiro, então q é verdadeiro e p é falso".

Usando as regras 1 a 3 sucessivamente, podemos continuar com o procedimento do exemplo anterior, criando fórmulas tão complexas quanto precisarmos. A regra número 4 nos assegura que todas as fórmulas podem ser construídas passo-a-passo pelas regras anteriores. Formalizando essa ideia, enunciamos o princípio da *indução na complexidade de fórmulas*.

Teorema 2.1 (Indução na complexidade da fórmula)**.** *Suponha que uma propriedade vale para toda fórmula atômica e que, se vale para as fórmulas A e B, também vale para $(\neg A)$, $(A \wedge B)$, $(A \vee B)$, $(A \rightarrow B)$ e $(A \leftrightarrow B)$. Então essa propriedade vale para todas fórmulas da linguagem da lógica proposicional.*

A definição de fórmula pode ser melhorada usando teoria dos conjuntos elementar, de maneira semelhante ao que fazemos quando definimos o conjunto dos números naturais em ZFC (vide Apêndice A. Para fazer isso, consideramos um conjunto enumerável correspondente aos símbolos do alfabeto e X o conjunto de todas as sequências finitas de símbolos. Seja Z o conjunto de todos os subconjuntos Y de X tais que:

1. As variáveis proposicionais pertencem a Y;
2. Se A pertence a Y, então $(\neg A)$ pertence a Y;

3. Se A e B pertencem a Y, então $(A \wedge B)$, $(A \vee B)$, $(A \rightarrow B)$ e $(A \leftrightarrow B)$ pertencem a Y.

Tomando F a intersecção de Z (vide Capítulo 3) temos que F satisfaz as condições acima (isto é, pertence à família Z) e é o menor conjunto (na ordem da inclusão) que pertence a Z. Isto é, se $Y \in Z$ então $F \subset Y$. Segue facilmente, daí, o teorema da indução na complexidade da fórmula (fica como exercício ao leitor, após a leitura do Capítulo 3).

Utilizando a indução na complexidade das fórmulas, podemos provar o seguinte teorema, que garante não haver ambiguidade na formação das fórmulas.

Teorema 2.2 (Unicidade da representação das fórmulas)**.** *Para toda fórmula A, uma, e apenas uma, das afirmações abaixo é verdadeira:*

- *A é uma fórmula atômica;*
- *Existe uma única fórmula B tal que A é a fórmula $(\neg B)$;*
- *Existem únicas fórmulas B e C tais que A é a fórmula $(B \wedge C)$;*
- *Existem únicas fórmulas B e C tais que A é a fórmula $(B \vee C)$;*
- *Existem únicas fórmulas B e C tais que A é a fórmula $(B \rightarrow C)$;*
- *Existem únicas fórmulas B e C tais que A é a fórmula $(B \leftrightarrow C)$.*

Deixamos a demonstração do teorema acima como exercício ao leitor. Sugerimos que se faça a prova, por indução na complexidade, das seguintes propriedades, sobre a "contagem de parênteses" em uma fórmula:

- O número de parênteses esquerdos em uma fórmula é sempre igual ao número de parênteses direitos;
- Dada qualquer ocorrência de um conectivo na fórmula, o número de parênteses esquerdos que se localizam *à esquerda* desse conectivo é estritamente maior que o número de parênteses direitos que estão à sua esquerda.
- Em uma fórmula do tipo $(*A)$ ou $(A * B)$, onde A e B são fórmulas e $*$ é um conectivo, o número de parênteses esquerdos que estão à esquerda de $*$ é exatamente um a mais que o número de parênteses direitos à esquerda de $*$.

- Existe apenas uma ocorrência de conectivo, na fórmula, que satisfaz a condição anterior.

Subfórmulas: As fórmulas intermediárias, usadas no processo de construção de uma fórmula através das regras 1 a 3, são chamadas de *subfórmulas* da fórmula em questão. Por exemplo, p, q, $(\neg p)$, e $(q \wedge (\neg p))$ são subfórmulas de $(p \rightarrow (q \wedge (\neg p)))$. Formalmente, introduzimos a seguinte definição, que é recursiva e só é possível graças ao princípio da indução na complexidade das fórmulas:

Definição 2.3 (Subfórmulas)**.** As *subfórmulas* da fórmula $(\neg A)$ são a fórmula A e as subfórmulas de A. As subfórmulas das fórmula $(A \wedge B)$, $(A \vee B)$, $(A \rightarrow B)$ e $(A \leftrightarrow B)$ são as fórmulas A, B e as subfórmulas de A e de B.

A cada fórmula iremos associar um número natural que chamaremos de *grau de complexidade* da fórmula.

Definição 2.4 (Grau de complexidade da fórmula)**.** Para cada fórmula da lógica proposicional determinamos um número natural conforme as seguintes regras:

1. Uma fórmula atômica tem grau de complexidade 0;

2. Se A tem grau de complexidade n, a fórmula $(\neg A)$ tem grau de complexidade $n + 1$;

3. Se A e B têm graus de complexidade n e m, respectivamente, então $(A \wedge B)$, $(A \vee B)$, $(A \rightarrow B)$ e $(A \leftrightarrow B)$ têm grau de complexidade $max\{n, m\} + 1$, onde $max\{n, m\}$ é o maior valor entre n e m.

Por exemplo, a fórmula p tem grau de complexidade 0, por ser atômica, e a fórmula $\neg p$ tem grau de complexidade 1. Pela regra número 3, a fórmula $((\neg p) \wedge q)$ tem grau de complexidade 2: um a mais que o maior valor entre os graus de complexidade de $\neg p$ (que é 1) e de q (que é 0).

A Definição 2.4 permite, *a priori*, que o grau de complexidade seja multivalorado, ou não tenha valor algum. Em nenhum momento, na definição, escrevemos "*o grau de complexidade da fórmula é n*", mas escrevemos "*a fórmula tem grau de complexidade n*". Poderia ocorrer de uma fórmula ter, simultaneamente, mais de um valor natural, ou mesmo nenhum. Precisamos

usar o princípio da indução na complexidade da fórmula para provarmos que, de fato, o grau de complexidade é unicamente determinado.

Essa discussão faz-se necessária porque por várias vezes utilizamos definições por recorrência sem explicar de maneira rigorosa. O parágrafo anterior nos dá uma ideia de como formalizarmos definições recursivas, que serão formalizadas no Apêndice A, Teorema A.20.

Omissão de parênteses: O uso de parênteses é essencial para que o teorema da unicidade de representação das fórmulas seja verdadeiro, evitando ambiguidades na linguagem. Porém, às vezes escrevemos as fórmulas de maneira simplificada, omitindo o excesso de parênteses, sem comprometer a clareza, conforme as regras seguintes:

1. Omitimos os parênteses extremos de uma fórmula, lembrando de "recolocá-los" na sequência da formação das fórmulas (por exemplo, escrevemos $p \wedge (q \vee r)$ em vez de $(p \wedge (q \vee r))$).

2. Em sequências apenas de disjunções ou apenas de conjunções omitimos os parênteses consecutivos, usando a notação $A \wedge B \wedge C$ no lugar de $(A \wedge B) \wedge C$ ou de $A \wedge (B \wedge C)$. Da mesma forma, utilizamos a notação $A \vee B \vee C$ no lugar de $(A \vee B) \vee C$ ou de $A \vee (B \vee C)$. Vale também a alteração análoga em sequências maiores. Por exemplo, escrevemos $A \wedge B \wedge C \wedge D$ no lugar de $((A \wedge B) \wedge C) \wedge D$.

3. Em fórmulas e subfórmulas da forma $\neg(\neg A)$ escrevemos simplesmente $\neg\neg A$.

4. Omitimos parênteses em subfórmulas da forma $(\neg A)$, escrevendo, simplesmente, $\neg A$. Assim, fica convencionado que $\neg p \wedge q$ significa $(\neg p) \wedge q$ e **não** significa $\neg(p \wedge q)$.

Convém que se faça algumas observações a respeito das regras acima. Em primeiro lugar, lembramos que se trata de regras **informais**, usadas para simplificar a notação, como uma abreviatura. Para efeitos formais e onde exigir resultados metamatemáticos mais rigorosos, não devemos considerar essas simplificações.

A segunda "regra" de omissão de parênteses fere o princípio da unicidade de representação, já que $p \wedge q \wedge r$ pode significar tanto $(p \wedge q) \wedge r$ quanto $p \wedge (q \wedge r)$, que são fórmulas diferentes. No entanto, como percebemos intuitivamente

e confirmaremos na próxima seção, em termos semânticos não há diferença entre uma fórmula e outra.

A quarta regra não é usada unanimemente, por isso deve ser usada com prudência. Podemos compará-la com as aulas das chamadas "expressões numéricas", que aprendemos no ensino fundamental, em que somos ensinados a fazer primeiro a operação de multiplicação. Da mesma forma, mediante essa regra de omissão de parênteses damos preferência ao conectivo de negação em relação aos conectivos binários.

2.2 Valoração

Na seção anterior tratamos da parte sintática da lógica proposicional. A semântica será dada pela valoração, que atribui, a cada fórmula, um valor de verdadeiro ou falso. Usaremos a noção intuitiva de função, que será tratada com mais rigor no Capítulo 3 e no Apêndice A.

Chamamos de *linguagem da lógica proposicional* o conjunto das fórmulas da lógica proposicional.

Definição 2.5 (Valoração)**.** Seja **L** a linguagem da lógica proposicional. Uma *valoração* é uma função V de **L** em $\{0, 1\}$ que satisfaz as seguintes condições:

- $V(\neg A) = 1$ se, e somente se, $V(A) = 0$
- $V(A \wedge B) = 1$ se, e somente se, $V(A) = 1$ e $V(B) = 1$.
- $V(A \vee B) = 1$ se, e somente se, $V(A) = 1$ ou $V(B) = 1$.
- $V(A \rightarrow B) = 1$ se, e somente se, $V(A) = 0$ ou $V(B) = 1$.
- $V(A \leftrightarrow B) = 1$ se, e somente se, $V(A) = V(B)$.

Dizemos que uma fórmula A é *verdadeira* para a valoração V se $V(A) = 1$. Se $V(A) = 0$ dizemos que A é *falsa* para a valoração V.

Na definição acima, 0 significa *falso* e 1 significa *verdadeiro*.

O seguinte teorema mostra que uma valoração depende exclusivamente de seus valores nas fórmulas atômicas. Esse resultado é essencial para o método da tabela-verdade.

Teorema 2.6. *Seja v uma função cujo domínio é o conjunto das fórmulas atômicas, e cujo contra-domínio é $\{0,1\}$. Então existe uma única valoração V tal que $V(p) = v(p)$, para qualquer fórmula atômica p.*

Demonstração: Definiremos V recursivamente sobre o grau de complexidade das fórmulas. Se A é uma fórmula de grau 0, então A é uma fórmula atômica, e definimos $V(A) = v(A)$. Seja $n > 0$ e suponha que temos definido $V(A)$ para toda fórmula A de grau menor que n. Seja C uma fórmula de grau n e vamos definir $V(C)$. Se C é da forma $\neg A$, então A tem grau menor que n e, portanto, $V(A)$ está definida. Definimos, então, $V(C) = 1 - V(A)$. Se C é da forma $A \wedge B$, temos que A e B têm grau menor que n, e definimos $V(C) = 1$ se $V(A)$ e $V(B)$ são ambos iguais a 1, e 0 caso contrário. Assim, analogamente, definimos $V(C)$ de acordo com as condições da valoração, para os casos de C ser da forma $A \vee B$, $A \rightarrow B$ ou $A \leftrightarrow B$. Pelo teorema da unicidade de representação, sabemos que C tem uma e apenas uma dessas formas, o que faz com que essa definição seja boa. Provamos facilmente, por indução em n, que V é uma valoração e está bem definida em todas as fórmulas. ■

O próximo teorema diz que o valor de uma fórmula depende exclusivamente do valor das suas subfórmulas atômicas.

Teorema 2.7. *Sejam V e V' duas valorações. Seja A uma fórmula tal que $V(p) = V'(p)$, para toda variável proposicional p que é subfórmula de A. Então $V(A) = V'(A)$.*

Demonstração: Provemos por indução no grau de complexidade de A. Se A tem complexidade 0, então A é uma fórmula atômica p, e o teorema é imediato, nesse caso. Suponha que o teorema é verdadeiro para as fórmulas de grau de complexidade menor do que n, onde $n \geq 1$. Seja A uma fórmula de grau de complexidade n. Em particular, como $n \geq 1$, A não é atômica. Logo, possui uma das formas $\neg B$, $B \wedge C$, $B \vee C$, $B \rightarrow C$ ou $B \leftrightarrow C$. Se A é da forma $B \wedge C$, temos que B e C têm graus de complexidade menores do que n. Sejam V e V' satisfazendo as hipóteses do teorema para A. Como as subfórmulas atômicas de B e de C são também subfórmulas de A, temos que $V(p) = V'(p)$, para toda subfórmula atômica p de B ou de C. Logo, por hipótese indutiva, $V(B) = V'(B)$ e $V(C) = V'(C)$, de onde deduzimos que $V(A) = V'(A)$. Os outros casos são análogos. ■

Definição 2.8 (Tautologia)**.** Dizemos que uma fórmula é uma *tautologia* se for verdadeira para qualquer valoração.

As tautologias mais simples que conhecemos são $p \vee \neg p$ e $p \to p$. Não precisa estudar lógica nem ver como está o tempo para saber que as frases "Está chovendo ou não está chovendo" e "Se está chovendo então está chovendo" são sempre verdadeiras.

A situação oposta à da tautologia é o que ocorre com a fórmula $p \wedge \neg p$. Não importa qual valoração tomamos, $p \wedge \neg p$ será sempre falsa. Chamamos tal tipo de fórmula de *contradição*.

Definição 2.9 (Contradição)**.** Dizemos que uma fórmula é uma *contradição* se for falsa para qualquer valoração.

Finalmente definimos o que são fórmulas equivalentes:

Definição 2.10 (Equivalência)**.** Dizemos que duas fórmulas A e B são *equivalentes* se $V(A) = V(B)$, para toda valoração V.

A seguir, enunciamos uma série de resultados fáceis de verificar.

Teorema 2.11. *Para todas fórmulas A e B valem:*

(a) *A é uma tautologia se, e somente se, $\neg A$ é uma contradição;*

(b) *A é uma contradição se, e somente se, $\neg A$ é uma tautologia;*

(c) *A e B são equivalentes se, e somente se, $A \leftrightarrow B$ é uma tautologia;*

(d) *Se A é uma tautologia e p é uma fórmula atômica, então, se substituirmos todas as ocorrências de p, em A, pela fórmula B, a fórmula obtida será uma tautologia;*

(e) *Se A e $A \to B$ são tautologias então B é uma tautologia.*

Para exemplificar o item (d), considere a fórmula $p \to p$. Essa é, claramente, uma tautologia. Agora troquemos as duas ocorrências de p pela fórmula $(p \wedge q)$. Teremos a fórmula $(p \wedge q) \to (p \wedge q)$ é uma tautologia.

O item (e) é uma forma de apresentarmos a regra de inferência *modus ponens*, conforme veremos na Seção 6.2.

2.3 Tabela-verdade

Vimos que, para analisarmos os possíveis valores de uma fórmula, precisamos analisar todas as possibilidades de valores das fórmulas atômicas que a constituem, e os valores das subfórmulas através das regras dos conectivos. Para condensar esse processo em um método mecânico e eficiente criou-se a *tabela-verdade*.

O primeiro passo para montar a tabela-verdade de uma fórmula é destrinchá-la nas subfórmulas. Depois montamos uma coluna para cada subfórmula, colocando as mais elementares à esquerda, e as mais complexas à direita, partindo das fórmulas atômicas até a fórmula toda. Em seguida, montamos uma linha para cada possível valoração das fórmulas atômicas que ocorrem na fórmula – indicando V (ou 1) para verdadeira e F (ou 0) para falsa – e usamos as regras dos conectivos para completar a tabela. Como exemplo, construamos as tabelas-verdade para as fórmulas com apenas um conectivo lógico.

Tabela-verdade para a negação:

p	$\neg p$
V	F
F	V

Tabela-verdade para a conjunção:

p	q	$p \wedge q$
V	V	V
V	F	F
F	V	F
F	F	F

Tabela-verdade para a disjunção:

p	q	$p \vee q$
V	V	V
V	F	V
F	V	V
F	F	F

Tabela-verdade para a implicação:

p	q	$p \rightarrow q$
V	V	V
V	F	F
F	V	V
F	F	V

Tabela-verdade para a equivalência:

p	q	$p \leftrightarrow q$
V	V	V
V	F	F
F	V	F
F	F	V

As colunas da tabela-verdade representam as fórmulas e subfórmulas, enquanto as linhas representam as valorações, que atribuem a cada fórmula atômica um valor de verdadeiro ou falso.

O próximo exemplo será um pouco mais complexo. Considere a fórmula $(\neg p) \vee q$. As suas subfórmulas são: p, q e $\neg p$. A tabela-verdade para essa fórmula fica:

p	q	$\neg p$	$(\neg p) \vee q$
V	V	F	V
V	F	F	F
F	V	V	V
F	F	V	V

Expliquemos a primeira linha da tabela-verdade acima, caso ainda haja alguma dúvida sobre ela. Suponhamos que p e q sejam verdadeiras, isto é, tomemos uma valoração em que atribui a p e q os valores de verdadeiro. Então, como p é verdadeira, pela regra da negação temos que $\neg p$ é falsa. Como $\neg p$ é falso e q é verdadeira, a regra da disjunção nos diz que $(\neg p) \vee q$ é verdadeira. E assim construímos a primeira linha, e, seguindo o mesmo raciocínio, construímos as outras três.

Observe que a tabela-verdade de $(\neg p) \vee q$ é idêntica à de $p \rightarrow q$, se preservarmos a ordem das linhas e desconsiderarmos as colunas intermediárias

entre as fórmulas atômicas e a fórmula completa (neste caso, a coluna da subfórmula $\neg p$). Isso ocorre porque as duas fórmulas são equivalentes e, portanto, todas as valorações resultam no mesmo resultado final (a saber, o valor falso na segunda linha e verdadeiro nas demais).

Nas tautologias, a última coluna marca sempre verdadeiro, como o exemplo a seguir, da fórmua $(p \wedge q) \rightarrow p$.

p	q	$p \wedge q$	$(p \wedge q) \rightarrow p$
V	V	V	V
V	F	F	V
F	V	F	V
F	F	F	V

Nota-se que, cada vez que adicionamos uma nova fórmula atômica à fórmula, dobramos o número de linhas da tabela-verdade. Por exemplo, a tabela-verdade para a fórmula $(p \vee q) \rightarrow r$ é:

p	q	r	$p \vee q$	$(p \vee q) \rightarrow r$
V	V	V	V	V
V	V	F	V	F
V	F	V	V	V
V	F	F	V	F
F	V	V	V	V
F	V	F	V	F
F	F	V	F	V
F	F	F	F	V

Portanto, a tabela-verdade de uma fórmula contendo n fórmulas atômicas diferentes, terá 2^n linhas. Isso nos dará, ao todo, 2^{2^n} possíveis tabelas-verdade de fórmulas com n fórmulas atômicas.

Vamos dar um exemplo de como aplicar esses exemplos em um problema prático. Analisemos o seguinte problema:

> João não dorme quando José toca piano ou Joaquim toca violão. Se João estiver dormindo, podemos saber se José está tocando piano?

Esse problema é bem simples e pode ser resolvido facilmente sem uso de tabela-verdade. Se José estivesse tocando piano, pela hipótese do problema sabemos que João não estaria dormindo. Então fica fácil concluir que José

não podia estar tocando piano, quando João dormia. Mas vejamos como resolver esse problema através de uma tabela-verdade. Em primeiro lugar precisamos definir quais são as frases principais do problema e substituí-las por fórmulas atômicas. Teremos o seguinte;

p: José está tocando piano.

q: Joaquim está tocando violão.

r: João está dormindo.

A hipótese do problema afirma que a seguinte frase é verdadeira, se a reescrevermos de forma apropriada:

> Se José está tocando piano ou Joaquim está tocando violão, então João não está dormindo.

Escrevendo a frase nessa forma, que tem o mesmo sentido daquela apresentada no problema, fica fácil identificá-la com a seguinte fórmula da lógica proposicional:

$$(p \vee q) \rightarrow (\neg r).$$

A tabela-verdade da fórmula acima fica

p	q	r	$\neg r$	$p \vee q$	$(p \vee q) \rightarrow (\neg r)$
V	V	**V**	F	V	F
V	V	F	V	V	**V**
V	F	**V**	F	V	F
V	F	F	V	V	**V**
F	V	**V**	F	V	F
F	V	F	V	V	**V**
F	F	**V**	F	F	**V**
F	F	F	V	F	**V**

Ressaltamos em negrito os casos em que r é verdadeiro (ou seja, quando João está dormindo) e em que $(p \vee q) \rightarrow (\neg r)$ é verdadeiro. Pelo problema, só sobrou a sétima linha como a única possível. Daí concluímos que p e q são falsos, ou seja, José não está tocando piano e Joaquim não está tocando violão.

Aparentemente complicamos um problema bem mais simples. Embora a tabela-verdade seja uma ferramenta objetiva para resolvermos problemas de

lógica proposicional, ela não deve inibir nossa intuição e raciocínio dedutivo. Muitas vezes não é necessário montar toda a tabela verdade. No problema em questão, por exemplo, podemos eliminar as linhas em que r é falsa, pois o enunciado já nos diz que João está dormindo. Um pouco de bom senso nos poupa de trabalho desnecessário.

2.4 Diagramas de Venn-Euler

Os diagramas de Venn-Euler ilustram a relação existente entre lógica e teoria dos conjuntos, associando os conectivos lógicos às operações conjuntísticas.

Para estabelecer essa relação, consideramos um conjunto-universo formado por todas as valorações da lógica proposicional. Identificamos, nesse universo, cada fórmula como o conjunto das valorações que a tornam verdadeira. Nos *diagramas de Venn-Euler*, os pontos correspondem às valorações, e as regiões desenhadas representam as fórmulas.

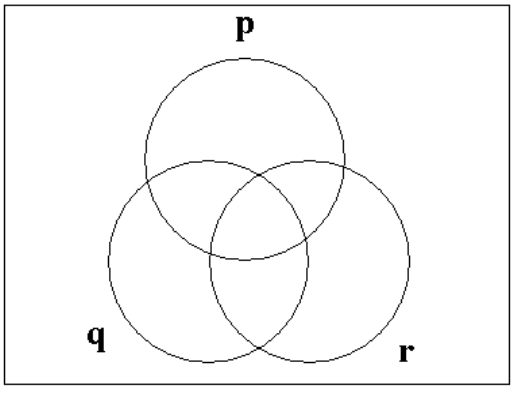

Figura 2.1: Representação das fórmulas atômicas p, q e r.

Se representamos três fórmulas atômicas em um diagrama, precisamos

que esses conjuntos sejam *independentes*, o que significa que toda combinação que formamos tomando cada um desses conjuntos ou seu complemento tem intersecção não-vazia. A definição precisa desse conceito será dada na linguagem de álgebras de Boole, no Apêndice B. Mas a Figura 2.1 exemplifica bem o que queremos. Repare que os três círculos que representam as fórmulas atômicas delimitam um total de oito regiões do diagrama. No caso geral, um diagrama contendo n fórmulas atômicas precisa ter 2^n regiões.

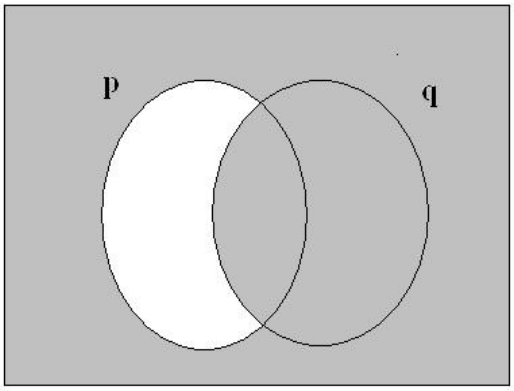

Figura 2.2: Representação da fórmula $p \to q$ (ou de $(\neg p) \vee q$)

Para representar uma fórmula no diagrama, sombreamos as regiões correspondentes às valorações que tornam tal fórmula verdadeira. A Figura 2.2 representa a fórmula $p \to q$ – que é equivalente a $(\neg p) \vee q$ – em um diagrama constituído de duas fórmulas atômicas.

Pelo mesmo diagrama fica fácil visualizar que a negação de $p \to q$ (ou seja, o complemento da área sombreada) é equivalente a $p \wedge (\neg q)$ – o conjunto dos pontos que estão em p e não estão em q.

Observamos que o conectivo de negação é representado, nos diagramas de Venn-Euler, pelo *complemento* de conjunto. De fato, o conjunto das valorações que tornam $\neg p$ verdadeira é o conjunto das valorações que tornam p

falsa. O conectivo da disjunção (ou) é representado pela união e a conjunção (e) pela intersecção.

Para tornar a ideia desses diagramas ainda mais intuitiva, imaginemos o seguinte: as valorações (ou pontos do diagrama) representam os indivíduos, as fórmulas (regiões do diagrama) são características que determinam grupos de indivíduos.

Por exemplo, se pensarmos no universo como o conjunto dos animais, a fórmula atômica p pode representar a característica "é mamífero", e q pode representar "ter asas". A fórmula $p \wedge q$ corresponde ao conjunto dos animais que são mamíferos *e* têm asas. Os morcegos estariam "dentro" dessa fórmula, ao passo que cavalos e pardais ficariam de fora. Esses no entanto, se enquadrariam na fórmula $p \vee q$, que corresponde ao conjunto dos animais que são mamíferos *ou* tem asas.

2.5 Recíproca e contrapositiva

Um erro comum – que ocorre tanto no estudo da matemática quanto no uso da linguagem cotidiana – é confundir as fórmulas $p \to q$ e $q \to p$. Vamos imaginar que alguém diga: "Se eu for viajar, então eu vou comprar um carro novo." Suponhamos que o autor da frase decida não viajar. Poderemos, então, concluir que ele não comprará o carro? De jeito nenhum! Ele garantiu que compraria o carro caso tivesse decidido viajar. Mas nada afirmou na hipótese de ter desistido da viagem.

Lembremos da semântica da fórmula $p \to q$. Tal fórmula só será falsa se p for verdadeira e q for falsa. Assim, o cidadão do exemplo só terá mentido se ele viajar e não comprar o carro que prometera.

Observe que essa estrutura é muito diferente da frase: "Se eu comprar um carro novo, então eu vou viajar". Diferente da frase anterior, essa só será falsa no caso do indivíduo comprar o carro e não viajar. Essa frase é chamada de *recíproca* da primeira, e tem valor lógico diferente dessa. As duas frases não são equivalentes.

Agora suponhamos que nosso amigo do primeiro exemplo diga, após alguns dias: "não vou comprar um carro". O que poderemos concluir, supondo que ele seja totalmente sincero e não mude de ideia? Certamente ele decidiu não viajar, porque, se tivesse viajado, teria comprado o carro. Logo, a afirmação "se eu viajar, então eu vou compar um carro novo" equivale à seguinte: "Se eu não comprar um carro novo, então não vou viajar". Essa

afirmação é chamada de *contrapositiva* da primeira, e ambas são logicamente equivalentes.

Recíproca e Contrapositiva: Considere uma fórmula da forma $A \to B$. A fórmula $B \to A$ é chamada de *recíproca* da fórmula $A \to B$, e a fórmula $\neg B \to \neg A$ é chamada de *contrapositiva* de $A \to B$.

Através da tabela-verdade podemos provar o seguinte resultado:

Proposição: Uma fórmula e sua contrapositiva são equivalentes.

Observação sobre a implicação lógica: Na linguagem natural, a estrutura "se... então" tem um sentido diferente do que na lógica clássica. Quando usamos essa estrutura, na linguagem natural, há uma relação de causa e efeito. Por exemplo: a frase "se chover, então o rio transbordará" indica que o transbordamento do rio seria uma consequencia da chuva. Na linguagem lógica, a implicação não necessariamente traduz essa ideia.

A frase "Se a lua é verde, então o sol é quadrado" é verdadeira? Na linguagem natural, essa frase não tem sentido, primeiro porque não há relação entre a cor da lua e o formato do sol, e segundo porque a hipótese e a tese da implicação são ambas absurdas. Mas, logicamente, a frase é verdadeira, porque é da forma $p \to q$, onde p significa "a lua é verde" e q significa "o sol é quadrado". Como ambas as fórmulas atômicas são falsas, a tabela-verdade nos diz que a fórmula é verdadeira, o que não coincide com o uso intuitivo da linguagem natural, que só utiliza a implicação quando existe uma relação de causa-efeito.

Se negarmos a frase "Se a lua é verde, então o sol é quadrado", sob o ponto de vista da lógica proposicional, obteremos algo equivalente a "A lua é verde **e** o sol não é quadrado", o que é claramente falso, pois a lua não é verde. Formalmente, podemos expressar isso da seguinte maneira (deixamos a verificação a cargo do leitor):

As fórmulas $\neg(p \to q)$ e $p \wedge \neg q$ são equivalentes.

2.6 Falácias e silogismos formais

Aproveitando essa discussão sobre implicação lógica, discutiremos aqui algumas relações entre a lógica simbólica e a argumentação na linguagem natural.

Conforme discutimos na Seção 1.4, uma demonstração matemática se assemelha a uma argumentação na linguagem natural. Se a demonstração está correta e parte de hipóteses (ou axiomas) verdadeiras, a conclusão provada será verdadeira (embora, na matemática, há uma longa discussão sobre o que significa ser "verdadeira").

Quando argumentamos na linguagem natural, partimos de *premissas*, que pressupomos ser verdadeiras, para tentar mostrar, logicamente, que a tese que queremos defender é verdadeira. Um *argumento válido* – também chamado de *silogismo* – é aquele que, quando aplicado a premissas verdadeiras, necessariamente leva a conclusões verdadeiras. Naturalmente, podemos argumentar corretamente partindo de premissas falsas, o que pode levar a conclusões falsas. Analisar a validade de um argumento é diferente de analisar a veracidade das premissas ou da conclusão.

Assim como em demonstrações matemáticas podem ocorrer erros que passam despercebidos ao autor, em argumentações podem ocorrer falhas de raciocínio, sejam elas acidentais ou intencionais. Um argumento que parece válido, mas não é, podendo levar a conclusões falsas a partir de premissas verdadeiras, é chamado de *falácia* ou *sofisma*.

Alguns tipos especiais de falácias e de silogismos estão diretamente ligadas à lógica proposicional, ou à antiga lógica formal. Essas são as chamadas *falácias e silogismos formais*.

Apresentamos, aqui, duas falácias e dois silogismos que estão diretamente ligados aos conceitos de recíproca e contrapositiva, apresentados na seção anterior.

> **Afirmando o antecedente:** É o silogismo que de A e de $A \to B$ conclui B.

O silogismo *afirmando o antecedente* corresponde à regra *modus ponens*. Exemplo: *Todo homem é mortal. Sócrates é homem. Logo, Sócrates é mortal.*

> **Afirmando o consequente:** É a falácia que de B e de $A \to B$ conclui A.

Trata-se do erro comum de confundir uma implicação com a sua recíproca. Exemplo: *Se beber, não dirija. Eu não dirijo, logo, devo beber.*

> **Negando o consequente:** É o silogismo que de de $A \to B$ e de $\neg B$ conclui $\neg A$.

Esse silogismo – muito utilizado em provas por absurdo (e no seu correspondente na linguagem natural, que é o sarcasmo) – é o uso correto da contrapositiva, e também é chamado de *modus tollens*. Exemplo: *todo número racional ao quadrado é diferente de 2. Logo, raiz de 2 é irracional.* Aplicando ao exemplo anterior, o seguinte argumento é correto: *Se beber, não dirija. Preciso dirigir. Logo, não devo beber.*

> **Negando o antecedente:** É a falácia que de de $A \to B$ e de $\neg A$ conclui $\neg B$.

Essa é outra forma de se manifestar a tradicional confusão entre uma implicação e sua recíproca. Exemplo: *Penso, logo existo. Lagartixas não pensam, logo, lagartixas não existem.*

Essas falácias aqui listadas são as que estão mais relacionadas à compreensão equivocada da lógica proposicional. Há muitas outras além dessas. Alguns exemplos: argumentação circular, apelo à ignorância, apelo à emoção, apelo ao novo, argumento de autoridade, *ad hominem*, descida escorregadia, espantalho, analogia imprópria, falso dilema, generalização apressada e muitas outras. Em [18] há um capítulo interessante chamado *enciclopédia das falácias*, com uma lista de nada menos que 35 falácias.

2.7 Leis de De Morgan

Já vimos a equivalência entre $\neg(p \to q)$ e $p \wedge (\neg q)$. Somadas a ela, as leis de De Morgan – que são propriedades gerais das álgebras de Boole, melhores discutidas no Apêndice B – permitem substituirmos qualquer fórmula por outra equivalente que só possua negação em frente às fórmulas atômicas. A demonstração dessas leis é simples e deixamos como exercício (faça pela tabela-verdade ou pela definição):

> **Leis de De Morgan:** As fórmulas $\neg(p \wedge q) \leftrightarrow ((\neg p) \vee (\neg q))$ e $\neg(p \vee q) \leftrightarrow ((\neg p) \wedge (\neg q))$ são tautologias.

Para explicar essas equivalências, pensemos no seguinte exemplo: se um vendedor lhe promete um carro *silencioso e veloz*, ele terá descumprido a promessa se o veículo que ele lhe vender *não for silencioso ou não for veloz*.

Como a lógica proposicional satisfaz todos os axiomas de álgebras de Boole, trocando igualdade por equivalência (vide Apêndice B), também podemos observar que os outros axiomas são verdadeiros. Por exemplo, a distributividade de conjuntos também vale para lógica proposicional. Ou seja, $A \wedge (B \vee C)$ é equivalente a $(A \wedge B) \vee (A \wedge C)$, assim como $A \vee (B \wedge C)$ é equivalente a $(A \vee B) \wedge (A \vee C)$.

Distributividade: As fórmulas $(A \wedge (B \vee C)) \leftrightarrow ((A \wedge B) \vee (A \wedge C))$ e $(A \vee (B \wedge C)) \leftrightarrow ((A \vee B) \wedge (A \vee C))$ são tautologias.

Temos ainda a propriedade associativa, que justifica a omissão de parênteses em sequências de fórmulas contendo só conjunções ou só disjunções.

Associatividade: As fórmulas $((A \wedge B) \wedge C)) \leftrightarrow (A \wedge (B \wedge C))$ e $((A \vee B) \vee C)) \leftrightarrow (A \vee (B \vee C))$ são tautologias.

2.8 Redefinindo conectivos

Para estudarmos resultados teóricos sobre a linguagem da lógica proposicional, às vezes convém utilizarmos uma quantidade reduzida de conectivos lógicos, se esses forem suficientes para expressar todas as fórmulas.

Por exemplo, no lugar de uma fórmula do tipo $A \rightarrow B$, podemos considerar a fórmula $(\neg A) \vee B$. Repare que ambas as fórmulas só serão falsas no caso de A ser verdadeira e B ser falsa. Ou seja, elas são equivalentes. Você pode verificar isso através da tabela-verdade ou intuitivamente. Considere a frase: "se eu comprar um carro então eu vou viajar". Em que situação terei eu descumprido com a promessa? No caso de eu comprar um carro e não viajar. Ou seja, a minha afirmação equivale à seguinte: "ou eu viajo, ou eu não compro um carro"[2].

Reduzir o conectivo bicondicional (equivalência) aos outros conectivos é simples. A fórmula $A \leftrightarrow B$ é claramente equivalente a $(A \rightarrow B) \wedge (B \rightarrow A)$. Pela observação anterior podemos eliminar também a implicação, transformando a fórmula em

$$((\neg A) \vee B) \wedge ((\neg B) \vee A).$$

[2]Observe a presença da leis de De Morgan nessas observações.

Finalmente, as leis de De Morgan nos permitem escrever a conjunção a partir da disjunção, ou vice-versa, com o auxílio da negação. Assim, $A \wedge B$ é equivalente a $\neg((\neg A) \vee (\neg B))$, e $A \vee B$ é equivalente a $\neg((\neg A) \wedge (\neg B))$ (observe que, além das leis de De Morgan, usamos a equivalência entre A e $\neg\neg A$).

Enfim, provamos que, apenas com a negação e a disjunção, ou apenas com a negação e a conjunção, conseguimos expressar toda a lógica proposicional, substituindo algumas fórmulas por outras equivalentes.

> **Teorema:** Para toda fórmula A da lógica proposicional existe uma fórmula B equivalente a A cujos únicos conectivos são $\vee$ e $\neg$.

A tabela seguinte mostra como redefinimos todos os conectivos em termos desses dois:

$A \wedge B$	$\neg((\neg A) \vee (\neg B))$
$A \to B$	$(\neg A) \vee B$
$A \leftrightarrow B$	$\neg(\neg((\neg A) \vee B) \vee \neg((\neg B) \vee A)))$

Como foi dito anteriormente, poderíamos ter usado a conjunção, no lugar da disjunção. Todavia, a disjunção apresenta a vantagem de expressar com mais facilidade a implicação.

Poderíamos, também, ter usado $\neg$ e $\to$, como símbolos primitivos, pois $A \vee B$ é equivalente a $(\neg A) \to B$. Fica como exercício ao leitor verificar que não é possível definir o conectivo $\neg$ a partir de $\vee$ e $\to$, ou de $\wedge$ e $\to$, ou ainda de $\wedge$ e $\vee$, bem como não é possível definir o operador $\vee$ a partir de $\neg$ e $\leftrightarrow$.

No final do capítulo, apresentaremos ao leitor um exercício tirado de [25] que mostrará ser possível definirmos um novo conectivo lógico (binário) tal que todos os outros possam ser definidos a partir desse único conectivo.

2.9 Forma disjuntiva normal

Essa discussão sobre como definir um conectivo a partir de outros desperta uma pergunta natural: será que todos os possíveis conectivos podem ser definidos a partir do que temos? Em outras palavras, queremos inverter o processo da tabela-verdade: dada uma tabela procuramos uma fórmula para ela (isto é, escolhemos como deve ser a última coluna da tabela-verdade).

Por exemplo, queremos encontrar uma fórmula A que resulte na seguinte tabela-verdade:

p	q	r	A
V	V	V	V
V	V	F	F
V	F	V	F
V	F	F	V
F	V	V	V
F	V	F	F
F	F	V	F
F	F	F	F

Observe que há três linhas da tabela-verdade (a primeira, quarta e quinta) em que A está marcada como verdadeira. Nas demais, A é marcada como falsa.

A primeira linha diz que, se a valoração marcar como verdadeiras todas as fórmulas atômicas p, q e r, então A deverá ser verdadeira. Ou seja, se $p \wedge q \wedge r$ for verdadeira, a fórmula A será verdadeira.

A quarta linha nos diz que se p for assinalada como verdadeira, e q e r como falsas, então também teremos A verdadeira. Ou seja, $p \wedge \neg q \wedge \neg r$ também deverá implicar A.

Pela quinta linha verificamos que $\neg p \wedge q \wedge r$ implicam em A verdadeira.

Como são essas as únicas linhas que tornam A verdadeira, para que isso ocorra é necessário e suficiente que uma dessas fórmulas seja verdadeira: $p \wedge q \wedge r$, $p \wedge \neg q \wedge \neg r$ ou $\neg p \wedge q \wedge r$.

Com isso mostramos que a fórmula A procurada pode ser

$$(p \wedge q \wedge r) \vee (p \wedge \neg q \wedge \neg r) \vee (\neg p \wedge q \wedge r)$$

ou equivalente a essa. O leitor é convidado a fazer a tabela-verdade para confirmar.

Nota-se que esse processo para encontrar essa fórmula não foi aleatório, mas um método que se aplica a qualquer tabela-verdade, seguindo os seguintes passos:

1. Marcamos todas as linhas da tabela-verdade em que a fórmula procurada está assinalada como verdadeira;

2. Para cada uma dessas linhas, montamos uma fórmula formada pela conjunção das fórmulas atômicas (quando essa é assinalada, naquela linha, como verdadeira) ou de sua negação (caso seja assinalada como falsa);

3. Tomamos a disjunção das fórmulas obtidas, quando houver mais de uma.

Um caso deve ser tratado separadamente: quando todas as linhas marcam o valor "falso". Nessa situação basta tomarmos a fórmula $p \wedge \neg p$, que, como vimos anteriormente, também será representada simplesmente por $\bot$, o símbolo usado para as contradições, na lógica proposicional.

Há, pelo menos, três vantagens no que acabamos de mostrar. Primeiro, mostramos que para toda tabela-verdade possível existe uma fórmula que se "encaixa" perfeitamente nela. Segundo, mostramos que toda fórmula é equivalente a uma fórmula que obedece uma estrutura determinada, relativamente simples. Terceiro, essa forma em que podemos escrever as fórmulas é muito mais fácil para visualizar e montar a tabela-verdade.

Essa forma de escrevermos fórmulas proposicionais – como disjunção de conjunções de fórmulas atômicas ou de sua negação – é chamada de *forma disjuntiva normal* , conforme a definição seguinte:

Definição 2.12 (Forma disjuntiva normal)**.** Dizemos que uma fórmula é *disjuntiva normal* (ou, está na *forma disjuntiva normal*) se é da forma $A_1 \vee \ldots \vee A_n$, onde cada A_i é da forma $B_1 \wedge \ldots \wedge B_m$, onde cada B_i é uma fórmula atômica ou sua negação.

Convém notar que podemos ter um caso "degenerado" da definição da forma disjuntiva normal, em que $n = 1$, em $A_1 \vee \ldots \vee A_n$. Ou seja, fórmulas como $p \wedge \neg q$ também se enquadram na definição de forma disjuntiva normal, ainda que não possuem disjunção. Do mesma modo, m pode ser 1, em $B_1 \wedge \ldots \wedge B_m$, não sendo necessário que haja conjunções na fórmula. Assim, uma fórmula atômica (ou sua negação) são os casos mais simples de fórmulas na forma disjuntiva normal.

Vimos que é possível contruir uma fórmula na forma disjuntiva normal para qualquer tabela-verdade. Esse resultado mostra que não precisamos de mais conectivos na lógica proposicional além dos que já temos, isto é, todos os outros possíveis conectivos podem ser definidos a partir dos usuais. Para formalizá-lo de maneira precisa, lembrando que cada linha da tabela-verdade

corresponde a uma valoração das fórmulas atômicas, enunciamos o próximo teorema.

Teorema 2.13. *Sejam $p_1, \ldots, p_n$ fórmulas atômicas e seja X um conjunto de funções de $\{p_1, \ldots, p_n\}$ em $\{0, 1\}$. Então existe uma fórmula A na forma disjuntiva normal tal que A é verdadeira para uma valoração V se, e somente se, a restrição de V a essas fórmulas atômicas pertence a X. Isto é, se existe f em X tal que $f(p_i) = V(p_i)$, para todo i entre 1 e n.*

Demonstração: Se X for vazio, tomemos A a fórmula $p \wedge \neg p$. Suponhamos X não-vazio e escrevamos $X = \{f_1, \ldots, f_m\}$. Para cada $j \in \{1, \ldots m\}$ definimos $A_j = B_j^1 \wedge \ldots \wedge B_j^n$, onde cada B_j^i é p_i, se $f_j(p_i) = 1$, e $\neg p_i$, se $f_j(p_i) = 0$. Defina A como a fórmula $A_1 \vee \ldots \vee A_m$.

Suponhamos que $V(A) = 1$, para uma valoração V. Isso significa que $V(A_j) = 1$, para algum j, o que implica que $V(B_j^i) = 1$, para todo $i \in \{1, \ldots, n\}$. Quando $f_j(p_i) = 1$, temos que B_j^i é p_i e, portanto, $V(p_i) = 1$. Quando $f_j(p_i) = 0$, temos que B_j^i é $\neg p_i$ e, portanto, $V(p_i) = 0$.

Reciprocamente, se $V(p_i) = f_j(p_i)$, para algum $j \in \{1, \ldots, m\}$ e todo $i \in \{1, \ldots, n\}$, temos, pelo mesmo argumento, $V(B_j^i) = 1$ e, portanto, $V(A) = 1$, como queríamos provar. ■

Observe que a demonstração acima formaliza o processo que descrevemos anteriormente para obtermos uma fórmula disjuntiva normal a partir da tabela-verdade. As funções pertencentes a X representam as linhas em que a fórmula é marcada como verdadeira.

Como conseguimos uma fórmula disjuntiva normal para cada tabela-verdade, então, dada uma fórmula qualquer, conseguimos uma outra, na forma disjuntiva normal, que possui a mesma tabela-verdade. Ou seja, do Teorema 2.13 segue facilmente o seguinte corolário.

Corolário 2.14. *Toda fórmula proposicional é equivalente a alguma fórmula na forma disjuntiva normal.*

Demonstração: Seja B uma fórmula e tome F o conjunto das subfórmulas atômicas de B. Defina

$$X = \{V|_F : V \text{ é valoração e } V(B) = 1\},$$

lembrando que $V|_F$ denota a função de F em $\{0, 1\}$ dada pela restrição de V a F, Pelo Teorema 2.13 existe uma fórmula A na forma disjuntiva normal tal que, para toda valoração V temos $V(A) = 1$ se, e somente se, $V|_F \in X$.

Seja V uma valoração. Vamos mostrar que $V(A) = V(B)$. Para isso, mostraremos que $V(B) = 1$ se, e somente se, $V(A) = 1$. Suponha que $V(B) = 1$. Temos, por definição de X, que $V|_F \in X$. Logo, $V(A) = 1$, por definição de A. Reciprocamente, suponha que $V(A) = 1$. Temos $V|_F$. Isso significa que existe uma valoração V' tal que $V'(B) = 1$ e $V'|_F = V|_F$. Como F é o conjunto das subfórmulas atômicas de B, do Teorema 2.7 segue que $V(B) = V'(B) = 1$. ■

Exercícios

1. Construa a tabela-verdade de cada uma das fórmulas abaixo, e verifique se cada uma é tautologia, contradição ou contigência (isto é, nem tautologia nem contradição). Tente se convencer do resultado antes de montar a tabela.

(a) $p \to (q \to (p \wedge q))$

(b) $((p \to q) \wedge (q \wedge r)) \to (p \to r)$

(c) $(p \to q) \to (q \to p)$

(d) $(p \wedge q) \vee r$

(e) $p \wedge (q \vee r)$

(f) $(p \vee \neg q) \to r$

(g) $p \wedge (\neg q \leftrightarrow \neg r)$

(h) $(p \vee (q \wedge r)) \leftrightarrow ((\neg q \vee \neg r) \to p)$

(i) $p \vee (q \wedge (p \vee (\neg q \wedge r)))$

(j) $((p \to q) \wedge (q \wedge r)) \leftrightarrow (p \to r)$

2. Novamente, verifique se cada uma das fórmulas abaixo é tautologia, contradição ou contigência. Mas, desta vez, use a definição de valoração.

(a) $p \to (q \wedge ((r \vee s \vee t) \to q))$

(b) $p \to (q \to (r \to (s \to (t \to p))))$

(c) $(p \to (q \leftrightarrow \neg q)) \wedge (\neg p \to (r \wedge s \wedge t \wedge (\neg r \vee \neg t)))$

(d) $((r \vee s) \to (q \wedge (r \to \neg(s \vee t)))) \to (p \to p)$

(e) $p \leftrightarrow (\neg p \wedge ((q \wedge (r \to s)) \to (q \vee t)))$

(f) $p \leftrightarrow (\neg p \vee ((q \wedge (r \leftrightarrow \neg s)) \to (q \vee t)))$

(g) $p \to (q \to (r \to (s \to (t \to \neg p))))$

(h) $(p \vee \neg p) \wedge (q \to q) \wedge (r \to (s \vee r)) \wedge ((t \wedge \neg q) \to t)$

(i) $((p \wedge q \wedge \neg r) \vee (s \wedge \neg t)) \leftrightarrow ((\neg p \vee \neg q \vee r) \wedge (\neg s \vee t))$

(j) $(p \to q) \to ((r \to s) \to (t \to p))$

3. Para cada fórmula dos exercício 1 e 2, calcule o seu grau de complexidade.

4. Mostre que as fórmulas abaixo são tautologias:

(a) $(\neg\neg p) \leftrightarrow p$

(b) $(\neg(p \wedge q)) \leftrightarrow (\neg p \vee \neg q)$

(c) $(\neg(p \vee q)) \leftrightarrow (\neg p \wedge \neg q)$

(d) $(\neg(p \to q)) \leftrightarrow (p \wedge (\neg q))$

(e) $(\neg(p \leftrightarrow q)) \leftrightarrow ((p \wedge \neg q) \vee (\neg p \wedge q))$

5. Usando o exercício anterior, escreva as negações das fórmulas abaixo, de forma que o conectivo da negação só apareça diante das fórmulas atômicas.

(a) $(p \wedge q) \to r$

(b) $p \to (p \wedge q)$

(c) $p \leftrightarrow (q \vee r)$

(d) $p \vee (q \wedge (r \vee s))$

(e) $p \to (q \to r)$

(f) $\neg p \to (q \vee r)$

(g) $(p \vee q) \to (r \wedge s)$

(h) $p \vee (q \to r)$

(i) $(p \to q) \to r$

(j) $(p \to q) \to (r \to s)$

6. Baseando-se no exercício 5, escreva a negação das seguintes frases:

(a) Se eu prestar vestibular, eu vou prestar para Medicina.

(b) Se eu fizer faculdade, eu vou cursar Matemática ou Física.

(c) Eu só vou comprar um carro novo se for promovido.

(d) Se chover ou fizer frio, eu vou ficar em casa ou vou para o cinema.

(e) Se fizer sol e não houver trovoadas eu vou para o parque ou para a praia.

(f) Se chover, eu vou ficar em casa para estudar ou ler um livro.

(g) Se eu estudar física, eu não vou estudar história, a menos que eu também estude português.

(h) Eu não ouço Beethoven quando leio Kafka, a menos que esteja chovendo e eu esteja deprimido.

(i) Eu sempre ouço Mozart ou Bach quando leio Agatha Christie, exceto quando estou cansado.

(j) Eu sempre ouço música quando leio um livro de ficção, mas nunca ouço música quando estou estudando, exceto, às vezes, quando eu estou estudando matemática ou quando estudo física em um dia chuvoso.

7. Reescreva as fórmulas do exercício 5 na forma disjuntiva normal.

8. Para cada fórmula abaixo encontre uma equivalente que seja tão simples quanto possível (poucos conectivos e baixo grau de complexidade).

(a) $p \to (q \to p)$

(b) $p \to ((q \vee p) \to \neg p)$

(c) $(p \vee q) \to (p \to q)$

(d) $p \wedge (q \vee (p \wedge \neg q))$

(e) $(p \vee q) \wedge (\neg p \vee q)$

(f) $p \leftrightarrow ((p \vee q) \wedge \neg q)$

9. Defina os demais conectivos usuais a partir de $\neg$ e $\to$

10. Considere um conectivo binário $\circ$ definido pela seguinte tabela-verdade (exercício adaptado de [25]):

p	q	$p \circ q$
V	V	F
V	F	F
F	V	F
F	F	V

(a) Defina $\circ$ a partir dos conectivos usuais;

(b) Mostre que a partir de $\circ$ é possível definir qualquer conectivo.

11. Prove que não é possível definir o conectivo $\neg$ a partir dos outros conectivos da linguagem.

12. Prove que a partir de $\neg$ e $\leftrightarrow$ não é possível definir o conectivo $\wedge$.

Sugestão: Por indução na complexidade das fórmulas construídas com esses conectivos, mostre que toda tabela-verdade tem uma quantidade par de linhas que assinalam a fórmula como verdadeira.

13. Diga quais dos argumentos são ou não válidos. Identifique o uso das falácias "afirmando o consequente" e "negando o antecedente".

(a) Ouvir *rock* me dá dor-de-cabeça. Quando estou com dor-de-cabeça não estudo. Hoje não estudei. Portanto, ouvi *rock*.

(b) Ouvir *rock* me deixa alegre. Eu só estudo quando estou alegre. Hoje eu ouvi *rock*. Portanto, vou estudar.

(c) Eu só fico tranquilo quando ouço música clássica. Eu nunca estudo quando eu não estou tranquilo. Hoje eu estudei. Logo, eu ouvi música clássica.

14. Problema retirado de [29]:

Nenhum gato fantasiado de garça é antissocial.
Nenhum gato sem rabo brinca com gorilas.
Gatos com bigodes sempre se fantasiam de garça.
Nenhum gato sociável tem garras rombudas.
Nenhum gato tem rabo, a menos que tenha bigodes.
Portanto:
Nenhum gato com garras rombudas brinca com gorilas.
A dedução é logicamente correta?

Capítulo 3

Teoria intuitiva dos conjuntos

O estudo de lógica de primeira ordem requer algum conhecimento elementar de teoria dos conjuntos, que iremos prover neste capítulo. A abordagem é ingênua – isto é, utiliza a linguagem natural e trata os conjuntos de modo intuitivo, não axiomático – e pretende fixar notações e definições que o leitor possivelmente já conhece. A teoria axiomática dos conjuntos será vista resumidamente no Apêndice A.

Há uma circularidade – como descrevemos na Seção 1.3 – entre lógica de primeira ordem e da teoria dos conjuntos, uma vez que uma depende de noções da outra em seu processo de formalização. Mesmo na lógica proposicional, vimos serem necessárias pelo menos noções intuitivas de aritmética – incluindo indução e recursão – e de conjuntos (tratamos, por exemplo, valorações como funções). Por outro lado, fundamentar a teoria dos conjuntos exige uma axiomatização que se baseia em lógica.

Para sairmos deste círculo vicioso temos algumas opções. A primeira delas é desenvolver a teoria dos conjuntos com um mínimo de conhecimento de lógica, trabalhando com os axiomas na metalinguagem – como é feito em [9] – para posteriormente formalizar a mesma teoria dos conjuntos usando a lógica. A segunda opção é introduzir a lógica usando apenas noções elementares e intuitivas de teoria dos conjuntos e, então, com a lógica formalizada, construímos a teoria axiomática dos conjuntos. A terceira opção é introduzir apenas a linguagem da lógica de primeira ordem (e, eventualmente, o sistema de axiomas) para desenvolvermos a teoria axiomática dos conjuntos – como em [17] – antes de definirmos a semântica da lógica de primeira ordem.

Optamos, neste livro, pela segunda opção. Este capítulo é requisito para o estudo de álgebras de Boole e da semântica da lógica de primeira ordem,

temas do Apêndice B e Capítulos 5 e 7.

3.1 Noções de conjuntos

Qualquer tentativa de definir conjuntos seria circular, pois usaria, inevitavelmente, algum termo que é quase sinônimo de conjunto, como agrupamento, coleção ou reunião. Assumimos que todos entendem a concepção intuitiva de conjuntos. Falaremos sobre algumas propriedades que caracterizam o conceito matemático de conjuntos e fixaremos algumas notações.

Não tentaremos aqui explicar o que é conjunto, pois isso inevitavelmente incorreria numa definição circular, em que utilizaríamos algum termo sinônimo de conjunto, como agrupamento, coleção ou reunião. Assumindo que essa noção intuitiva todos possuem, e na tentativa de definir implicitamente o termo, enunciamos um dos axiomas da teoria de Zermelo e Fraenkel.

> **Axioma da extensão:** Dois conjuntos são iguais se, e somente se, eles possuem os mesmos elementos.

Podemos inferir desse axioma que descrever todos os elementos de um conjunto é suficiente para defini-lo. Por esse motivo, uma das formas comuns de representar um conjunto é escrevendo todos seus elementos entre chaves, separados por vírgulas, como no seguinte exemplo:

$$\{1, 2, 3, 5, 8\}$$

Os elementos do conjunto acima, são, portanto, 1, 2, 3, 5 e 8. O axioma da extensão nos diz, ainda, que não importa a ordem em que escrevemos os elementos dos conjuntos, nem contamos as repetições. Vale, por exemplo, a igualdade

$$\{1, 2, 3, 5, 8\} = \{2, 1, 1, 5, 3, 8\},$$

pois todo elemento do conjunto à esquerda é igual a algum elemento do conjunto à direita, e vice-versa.

Quando um conjunto é infinito, não podemos escrever todos seus elementos. Uma solução informal para esse caso é o uso da reticências para que o leitor tente "adivinhar" quem são os outros elementos dos conjuntos, como na seguinte descrição do conjunto dos números pares:

$$\{0, 2, 4, 6, \ldots\}$$

Esse tipo de notação é comum quando o contexto não nos deixa dúvida sobre seu significado, mas está longe de ser uma notação rigorosa, por possibilitar ambiguidades. Em casos de conjuntos infinitos ou muito grandes é preferível utilizar outro método para representar conjuntos, que é descrevendo uma propriedade comum e exclusiva a todos os seus elementos, como no próximo exemplo.

> O conjunto de todos os números naturais que são divisíveis por 2

Na teoria axiomática precisamos, através dos demais axiomas, justificar a existência de cada conjunto que definimos. Na teoria ingênua, ou intuitiva, definimos um conjunto simplesmente descrevendo seus elementos. Mas, conforme vimos na Seção 1.5, formalizar a teoria dos conjuntos desse modo – como tentou Frege – gera o paradoxo de Russell, induzindo a contradição.

Símbolo de pertinência: O símbolo $\in$ (leia-se "*pertence*") é o símbolo primitivo da teoria dos conjuntos. Se x é um elemento de um conjunto A, escrevemos $x \in A$ (leia-se "x *pertence a* A"). Se x não é um elemento de A, escrevemos tal fato como $x \notin A$ ("x *não pertence a* A"). Por exemplo, $1 \in \{1, 2, 3, 5, 8\}$, mas $4 \notin \{1, 2, 3, 5, 8\}$.

O símbolo de pertinência nos leva a uma outra forma de representar conjuntos. Se A é um conjunto e $P(x)$ é uma propriedade sobre os elementos x de A, escrevemos *o conjunto dos elementos de* A *que satisfazem a propriedade* P como

$$\{x \in A : P(x)\}$$

Por exemplo, o conjunto dos números naturais menores que 5 pode ser descrito como

$$\{x \in \mathbb{N} : x < 5\}$$

Um dos axiomas de Zermelo e Fraenkel – o axioma da separação – garante a existência de conjuntos dessa forma. Mas não podemos esquecer de indicar o *domínio*, isto é, um conjunto previamente fixado (na notação acima é o conjunto A e no exemplo, $\mathbb{N}$) do qual *separamos* os elementos com a propriedade desejada. Ou seja, não devemos escrever algo como $\{x : P(x)\}$, sem especificar *onde está* x, pois esse tipo de definição – como concebia Frege – permite o surgimento do paradoxo de Russell, levando o sistema a uma contradição.

Conjuntos de conjuntos: Contrariando um erro comum difundido no ensino de matemática, o símbolo de pertinência pode ser usado entre conjuntos. Afinal, *os elementos de um conjunto podem, eles próprios, serem conjuntos*. Considere, por exemplo, $\{1\}$, $\{1,2\}$ e $\{1,2,3\}$. Podemos definir A tendo esses três conjuntos como elementos. Isto é,

$$A = \{\{1\},\{1,2\},\{1,2,3\}\}.$$

Nesse caso está correto escrever $\{1\} \in A$, como também é correto escrever $1 \notin A$. De fato, o número 1, em si, não está na lista dos elementos de A, mas o conjunto $\{1\}$ – que é diferente do número 1 – está.

Conjunto vazio: Um conjunto que não tem elementos é chamado de *conjunto vazio* e será denotado por $\emptyset$. O axioma da extensão nos garante que o conjunto vazio é único.

Símbolo de inclusão: Sejam A e B dois conjuntos. Dizemos que A *está contido* em B – ou A é um *subconjunto* de B – se todo elemento de A pertence a B.

Denotamos por $A \subset B$ quando A está contido em B. O símbolo $\subset$ é chamado de *símbolo de inclusão de conjuntos*.

Dizemos que A *está contido propriamente em* B – ou A *é um subconjunto próprio de* B – se $A \subset B$ e $A \neq B$. Isto é, se todo elemento de A pertence a B, mas existe pelo menos um elemento de B que não pertence a A.

Com o símbolo de inclusão, podemos reescrever o axioma da extensão da seguinte forma:

> **Afirmação:** Dois conjuntos A e B são iguais se, e somente se, $A \subset B$ e $B \subset A$.

Façamos a negação lógica da frase que define a inclusão. Negar que "todo elemento de A pertence a B" significa que "existe pelo menos um elemento de A que não pertence a B". Isso nunca ocorre se A for o conjunto vazio, pois este último não possui elemento algum. Concluímos, então – pelo chamado *argumento de vacuidade* – que o conjunto vazio está contido em qualquer conjunto.

> **Afirmação:** Para todo conjunto A temos $\emptyset \subset A$.

Prestemos atenção na diferença entre o significado da pertinência e da inclusão, especialmente quando trabalhamos com conjuntos de conjuntos. Um conjunto A pertence a um conjunto B se A é um dos elementos de B. Por outro lado, A está contido em B se todos elementos de A são elementos de B. Por exemplo, se $A = \{1, 2\}$ e $B = \{1, 2, 3\}$, podemos dizer que A está contido em B, isto é,

$$\{1, 2\} \subset \{1, 2, 3\},$$

pois os elementos de A são 1 e 2, sendo que ambos também são elementos de B. Mas o conjunto A, em si, não é igual a 1, ou a 2, ou a 3. Logo

$$\{1, 2\} \notin \{1, 2, 3\}$$

Mas se tomarmos B como o conjunto $\{\{1\}, \{1, 2\}, \{1, 2, 3\}\}$, o conjunto $A = \{1, 2\}$ é um dos elementos do conjunto B. Ou seja,

$$\{1, 2\} \in \{\{1\}, \{1, 2\}, \{1, 2, 3\}\}$$

Por outro lado, o número 1 pertence a A e não pertence B. Logo, usando $\not\subset$ para a negação da inclusão, temos

$$\{1, 2\} \not\subset \{\{1\}, \{1, 2\}, \{1, 2, 3\}\}$$

União, intersecção e subtração de conjuntos: Dados dois conjuntos A e B definimos a *união* de A e B – que será denotada por $A \cup B$ – como o conjunto de todos os elementos que pertencem a A *ou* pertencem a B. Definimos a *intersecção* de A e B – que denotaremos por $A \cap B$ – como o conjunto de todos os elementos que pertencem a A *e* pertencem a B.

A *subtração* de A e B será denotada por $A \setminus B$ e é o conjunto de todos os elementos de A que não pertencem a B.

As operações de união, intersecção e subtração de conjuntos correspondem aos operadores de disjunção, conjunção e negação, respectivamente, da lógica proposicional, conforme foi explicado na Seção 2.4. As álgebras de Boole esclarecem de forma mais aprofundada a relação entre os operadores lógicos e os operadores conjuntísticos.

Ainda há duas notações importantes que precisamos definir: a de união e intersecção de uma família de conjuntos. Se $\mathcal{F}$ é um conjunto, definimos a *união* de $\mathcal{F}$ como

$$\bigcup \mathcal{F} = \{x : \text{existe } X \in \mathcal{F} \text{ tal que } x \in X\}$$

e, se $\mathcal{F} \neq \emptyset$, definimos a *intersecção* de $\mathcal{F}$ como

$$\bigcap \mathcal{F} = \{x : x \in X \text{ para todo } X \in \mathcal{F}\}$$

O termo *família de conjuntos* é redundante e tem propósito didático. Na teoria axiomática dos conjuntos, tudo é conjunto. Em particular, todos são famílias de conjuntos.

Se tomarmos a família de conjuntos como sendo o conjunto vazio, a união é obviamente ele próprio. Mas se aplicarmos a definição de intersecção de família de conjuntos ao vazio, veremos que qualquer conjunto se enquadra como elemento dessa intersecção. Como não existe conjunto de todos os conjuntos (é uma consequência do paradoxo de Russell), tampouco existe intersecção de uma família vazia. Portanto, deixamos registrado que, enquanto união de família de conjuntos se aplica a qualquer conjunto, a intersecção se aplica a todos menos o vazio.

A união de uma família de conjuntos segue do axioma da união, e a intersecção é consequência do axioma da separação, conforme está mostrado no Apêndice A.

Se, por um lado, a união de dois conjuntos representa a disjunção, e a intersecção, a conjunção, por outro lado, observamos, pelas definições anteriores, que a união de uma família de conjuntos representa o quantificador existencial "existe" (veja Seção 4.1), e a intersecção, o quantificador universal "para todo".

3.2 Relações

As definições de relação e função serão utilizadas na semântica da lógica de primeira ordem e nas álgebras de Boole. No Apêndice A formalizamos os conceitos aqui apresentados a partir dos axiomas de teoria dos conjuntos.

Definição 3.1 (Produto cartesiano)**.** Se A e B são conjuntos, definimos o *produto cartesiano* de A e B como o conjunto dos pares ordenados (x, y) tais que $x \in A$ e $y \in B$.

Relembramos o conceito de *par ordenado*. A proposição seguinte é um teorema de ZFC, mas como, aqui, não entramos no assunto da construção do par ordenado, nem na axiomática de Zermelo e Fraenkel, podemos considerá-la como uma definição implícita de par ordenado. Provaremos formalmente a proposição seguinte na Seção A.2.

Proposição 3.2 (Par ordenado)**.** Dois pares ordenados (x, y) e (x', y') são iguais se, e somente se, $x = x'$ e $y = y'$.

Notemos, nesse ponto, a diferença entre par ordenado e par não-ordenado. Um conjunto é determinado unicamente pelos seus elementos. Isto é, dois conjuntos são iguais se, e somente se, eles têm os mesmos elementos. Não conta, portanto, nem a ordem ou repetição deles. Assim, os conjuntos $\{1, 2\}$ e $\{2, 1\}$ são iguais, assim como os conjuntos $\{1, 2, 3\}$ e $\{2, 1, 1, 3\}$. Por outro lado, quando utilizamos a notação de *par ordenado*, estamos considerando a ordem. Ou seja, o par $(1, 2)$ é diferente do par $(2, 1)$.

A definição de par ordenado pode ser estendida a qualquer quantidade de elementos, lembrando que, em sequências ordenadas, a ordem e a repetição dos elementos importam. Assim, se n é um número natural maior que 1, definimos uma *n-upla* como uma sequência de n elementos, separados por vírgulas e delimitados por parênteses. Por exemplo, $(1, 3, 2, 1, 4)$ é uma 5-upla que é diferente da 4-upla $(1, 2, 3, 4)$.

Com isso, podemos estender a definição de produto cartesiano de n conjuntos. A definição abaixo é bastante comum, quando fazemos vários produtos cartesianos do mesmo conjunto.

Definição 3.3. Sejam $n > 1$ um número natural e A um conjunto. Denotamos por A^n o conjunto das n-uplas de elementos de A.

Agora podemos definir relação. As mais utilizadas são as relações binárias, que discutiremos daqui a pouco.

Definição 3.4 (Relação)**.** Uma *relação* entre dois conjuntos A e B é um subconjunto de $A \times B$. Uma *relação* n-ária em A é um subconjunto de A^n. Uma *relação binária* é uma relação 2-ária.

Um exemplo de relação binária em $\mathbb{N}$: o conjunto R formado por todos os pares (x, y) pertencentes a $\mathbb{N}^2$ tais que y é divisível por x.

Adotaremos algumas notações.

> **Notação:** Se R é uma relação binária em um conjunto X, denotamos $(x, y) \in R$ por xRy.
>
> Se R é uma relação n-ária em um conjunto X, denotamos $(x_1, \ldots, x_n) \in R$ por $R(x_1, \ldots, x_n)$.

No exemplo da relação de divisibilidade, em vez da letra R costuma-se usar o símbolo $|$, de modo que $x|y$ significa "y é divisível por x". Os símbolos de desigualdade $<$ e $\leq$ são exemplos conhecidos dessa notação. Não é comum escrevermos $(x, y) \in <$, quando x é menor do que y, mas, sim, $x < y$.

3.3 Funções

Dedicamos esta seção a um tipo especial de relação:

Definição 3.5 (Função)**.** Uma *função de A em B* é uma relação $f \subset A \times B$ tal que, para cada $x \in A$, existe um único $y \in B$ tal que $(x, y) \in f$.

Se $x \in A$, denotamos por $f(x)$ o único elemento y de B tal que $(x, y) \in f$.

Dizemos que A é o *domínio* da função f. O conjunto $\{f(x) : x \in B\}$ é chamado de *imagem* de f.

Não entraremos aqui na definição de contra-domínio da função porque essa exige uma discussão mais aprofundada, uma vez que, pela definição aqui feita de função, não é possível "recuperar" o conjunto B (que seria o contra-domínio de f).

Definição 3.6. Uma função f é dita *injetora* se $f(x) \neq f(y)$, sempre que $x \neq y$. Dizemos que f é *sobrejetora* em relação a B se B é a imagem de f. Uma *bijeção* – ou *função bijetora* – de A em B é uma função injetora que possui domínio A e imagem B.

Com isso introduzimos o conceito de *conjuntos equipotentes*.

Definição 3.7. Dizemos que um conjunto A é *equipotente* a um conjunto B se existe uma bijeção de A em B. Dizemos que um conjunto A é *enumerável* se é equipotente a $\mathbb{N}$.

Usando a definição seguinte veremos que, se A é equipotente a B, então B é equipotente a A. Com isso, costumamos dizer que A e B *são equipotentes* quando A é equipotente a B ou, equivalentemente, B é equipotente a A.

Definição 3.8. Se f é uma função de domínio A e imagem B, e g é uma função de domínio B e imagem C, definimos a *composição de f em g* – denotada por $g \circ f$ – o conjunto dos pares (a, c) tais que existe $b \in B$ tal que $(a, b) \in f$ e $(b, c) \in g$.

Se f é uma função bijetora de A em B, definimos a *função inversa* de f como o conjunto dos pares (b, a) tais que $(a, b) \in f$. Denotamos tal função por f^{-1}.

Na definição acima falta mostrar que a composição de funções e a inversa de uma função bijetora são, de fato, funções. Deixamos ao leitor essa demonstração. Também deixamos como exercício ao leitor, no final deste capítulo, mostrar que a inversa de uma função bijetora é bijetora, de onde segue que, se A é equipotente a B, então B é equipotente a A.

Quando o domínio de uma função é o conjunto dos números naturais, chamamos tal função de *sequência*, e introduzimos uma notação específica para ela.

Definição 3.9. Uma *sequência* é uma função cujo domínio é o conjunto dos números naturais ou um subconjunto dele. Se $S \subset \mathbb{N}$ e f é uma função de domínio S, podemos escrevemos f na forma $(x_n)_{n \in S}$, onde $f(n) = x_n$.

Agora falamos sobre outro tipo especial de função, também utilizado no estudo de álgebras de Boole e de lógica de primeira ordem.

Definição 3.10 (Operação)**.** Uma *operação n-ária* em um conjunto A é uma função de A^n em A.

Se F é uma operação n-ária, denotamos $F((x_1, \ldots, x_n))$ por $F(x_1, \ldots, x_n)$. Se $n = 2$, chamamos tal operação de *binária*, e denotamos $F(x, y)$ por xFy.

Temos, como exemplo, as operações de soma e multiplicação no conjunto $\mathbb{N}$ (o conjunto dos números naturais). E como bem sabemos, costumamos escrever $x + y$ em vez de $+(x, y)$ ou $+((x, y))$.

Notemos que uma operação n-ária em A pode ser vista como um tipo especial de relação $(n + 1)$-ária.

3.4 Relações de ordem

Voltemos a falar de relações binárias, definindo mais dois tipos importantes de relações.

Definição 3.11 (Ordem)**.** Uma *ordem* em um conjunto X é uma relação binária R em X que satisfaz as seguintes propriedades, para todos $x, y, z \in X$:

- Reflexividade: xRx;

- Anti-simetria: se xRy e yRx então $x = y$;
- Transitividade: se xRy e yRz então xRz.

Costuma-se uma relação de ordem por $\leq$. Ou por $<$ quando nos referimos a uma *ordem estrita*, em que trocamos a reflexividade pela *anti-reflexividade* (xRx é falso para todo x) e anti-simetria pela *assimetria* (xRy implica não valer yRx).

Observem que, pela definição, não necessariamente todo par de elementos é *comparável*. Isto é, podem existir dois elementos x e y em X tais que não vale nem $x \leq y$ nem $y \leq x$. Alguns livros chamam essa definição de ordem de *ordem parcial*. Quando $x \leq y$ ou $y \leq x$, para todos $x, y \in X$, dizemos $\leq$ é uma *ordem linear*, também chamada de *ordem total*. A relação de ordem no conjunto dos números reais é uma ordem linear. A relação de inclusão, numa família de conjuntos, é uma relação de ordem. Na maioria das vezes (pois depende do domínio que tomamos), a inclusão é uma ordem parcial que não é linear.

3.5 Relações de equivalência

A próxima definição é semelhante à da ordem – exceto pelo fato de trocarmos anti-simetria por simetria – mas apresenta características matemáticas bem diferentes.

Definição 3.12 (Relação de equivalência)**.** Dizemos que uma relação $R \subset X \times X$ é uma *relação de equivalência em* X se satisfaz as seguintes propriedades, para todos $x, y, z \in X$:

- Reflexividade: xRx;
- Simetria: se xRy então yRx;
- Transitividade: se xRy e yRz então xRz.

Definição 3.13 (Classes de equivalência)**.** Sejam X um conjunto e R uma relação de equivalência em X. Para cada $x \in X$ definimos

$$[x]_R = \{y \in R : xRy\},$$

também chamado de *classe de equivalência de* x. Definimos

$$X/R = \{[x]_R : x \in X\}$$

o *conjunto das classes de equivalência em* X, que também é chamado de *quociente de* X *pela relação* R.

As classes de equivalência dividem o conjunto X em "grupos disjuntos", do mesmo modo como uma escola divide seus alunos em classes, de modo que todos alunos pertencem a alguma classe e nenhum aluno pertence a duas classes diferentes. Essa definição de classes poderia ser usada para qualquer tipo de relação, mas precisamos das propriedades de simetria, reflexividade e transitividade para que a divisão em classes tenha essa propriedade de "particionar" o conjunto em classes disjuntas, conforme mostra o próximo teorema.

Teorema 3.14. *Seja* R *uma relação de equivalência em um conjunto* X*. As seguintes afirmações são verdadeiras:*

(a) $\bigcup(X/R) = X$*;*

(b) $\emptyset \notin X/R$*;*

(c) *Para todos* $Y, Z \in X/R$*, se* $Y \neq Z$ *então* $Y \cap Z = \emptyset$*;*

(d) *Se* $x \in Y$ *e* $Y \in X/R$*, para todo* $y \in X$ *temos que* xRy *se, e somente se,* $y \in Y$*.*

Demonstração: Usaremos a notação $[x]$ para o conjunto $\{y \in X : xRy\}$.

Dado $x \in X$, temos que $x \in [x]$, uma vez que, pela propriedade reflexiva, xRx. Isso prova (a) e (b).

Para provarmos (c), assumimos que Y e Z são dois elementos de X/R que não são disjuntos e mostraremos que $Y = Z$. Sejam $x \in Y \cap Z$ e $y_0, z_0 \in X$ tais que $Y = [y_0]$ e $Z = [z_0]$. Dado $y \in Y$, temos, por definição, que y_0Ry. Logo, pela simetria, yRy_0. Mas como $x \in Y$, temos y_0Rx. Pela transitividade temos yRx. Mas, como $x \in Z$, temos z_0Rx e, pela simetria, xRz_0. Logo, a transitividade nos dá yRz_0 e, novamente pela simetria, z_0Ry, o que prova que $y \in Z$. Isso conclui que $Y \subset Z$ e um argumento análogo mostra que $Z \subset Y$, provando que $Y = Z$.

Mostremos a parte (d). Se $Y \in X/R$, existe $y_0 \in X$ tal que $Y = [y_0]$. Como $x \in Y$, temos que y_0Rx e, portanto, xRy_0. Se yRx, por transitividade

e simetria temos yRy_0 e y_0Ry. Logo, $y \in Y$. Por outro lado, se $y \in Y$, temos y_0Ry e, portanto, xRy, concluindo a prova do teorema. ■

Exercícios

1. Usando o axioma da extensão, prove que $\emptyset$ e $\{\emptyset\}$ são conjuntos diferentes.

2. Para cada par de conjuntos abaixo, decida qual(is) dos símbolos $\in$ e $\subset$ tornam a fórmula verdadeira. Lembre-se que a resposta também pode ser ambos os símbolos ou nenhum deles. Justifique cada resposta.

(a) $\{\emptyset\} \ldots \{\emptyset, \{\emptyset\}\}$

(b) $\{\emptyset\} \ldots \{\{\emptyset\}\}$

(c) $\{1, 2, 3\} \ldots \{\{1\}, \{2\}, \{3\}\}$

(d) $\{1, 2, 3\} \ldots \{\{1\}, \{1, 2\}, \{1, 2, 3\}\}$

(e) $\{1, 2\} \ldots \{1, \{1\}, 2, \{2\}, \{3\}\}$

(f) $\{\{1\}, \{2\}\} \ldots \{\{1, 2\}\}$

3. Seja x o conjunto $\{\emptyset, \{\emptyset\}, \emptyset, \{\emptyset, \{\emptyset\}\}\}$

(a) Quantos elementos tem o conjunto x?

(b) Descreva todos os subconjuntos de x.

(c) Descreva, utilizando chaves e vírgula, o conjunto de todos os subconjuntos de x.

(d) Quantos elementos o conjunto dos subconjuntos de x possui?

4. Prove que $x \subset x$, para todo x.

5. Prove que $x \in y$ se, e somente se, $\{x\} \subset y$.

6. Prove que a inversa de uma função bijetora é uma função bijetora, e a composição de funções bijetoras é bijetora.

7. Seja X um conjunto e sejam x_0 e y_0 dois elementos distintos de X. Considere a seguinte relação em X:

$$R = \{(x, y) \in X \times X : x = y\} \cup \{(x_0, y_0), (y_0, x_0)\}$$

(a) Prove que R é uma relação de equivalência em X.

(b) Descreva os elementos de X/R.

8. Considere C um conjunto não-vazio de conjuntos não-vazios tal que, para todos x e y pertencentes a C, se $x \neq y$ então $x \cap y = \emptyset$. Seja $X = \bigcup C$. Defina uma relação R como o conjunto dos pares $(x, y) \in X^2$ para os quais existe $z \in C$ tal que $x \in z$ e $y \in z$.

(a) Prove que R é uma relação de equivalência em X.

(b) Mostre que $C = X/R$.

(c) Prove que duas relações de equivalência diferentes possuem classes de equivalências diferentes.

9. Como fica uma relação de equivalência sobre $\emptyset$? Ela satisfaz o Teorema 3.14?

10. Seja $\mathcal{F}$ uma família não-vazia de conjuntos e considere a relação R formada pelo conjunto dos pares ordenados (A, B) em $\mathcal{F}^2$ tais que A é equipotente a B. Mostre que R é uma relação de equivalência.

Capítulo 4

Lógica de primeira ordem – linguagem

A lógica de primeira ordem apresenta algumas vantagens que justificam ser ela o principal objeto de estudo deste livro e da maioria dos cursos avançados de lógica: é intuitiva, mantendo uma boa proximidade da linguagem natural, é expressiva o suficiente para formalizar toda a matemática e possui algumas propriedades bastante importantes, como os teoremas da completude, compacidade e Löweinheim-Skolem, que serão mostrados no Capítulo 7.

Conforme explicado na Seção 1.4, a lógica de primeira ordem se divide em três partes: a linguagem, que trata dos símbolos utilizados e da regra de formação de fórmulas, a semântica, que interpreta a linguagem, dando-lhe um significado, e a axiomatização, ou sistema de axiomas, que dita as regras para demonstrações de teoremas.

Diferentemente da lógica proposicional, a linguagem da lógica de primeira ordem não é única. Há alguns símbolos comuns a todas as linguagens e outros específicos. Por exemplo, na teoria dos conjuntos utilizamos o símbolo $\in$, enquanto na aritmética usamos os símbolos $+$, $\cdot$, 0 e 1. Por isso, quando tratamos de lógica de primeira ordem, precisamos estabelecer a linguagem à qual estamos nos referindo.

Numa linguagem da lógica de primeira ordem – que também costumamos chamar de *linguagem de primeira ordem* – destacaremos os seguintes aspectos: o alfabeto (os símbolos utilizados), os termos (sequências finitas de símbolos que representam indivíduos do universo a que se refere a linguagem) e as fórmulas (sequências finitas de símbolos que representam asserções sobre os indivíduos).

Neste livro trataremos apenas de linguagens finitárias e enumeráveis. Isto é, as fórmulas são formadas por uma quantidade finita de símbolos e a quantidade de símbolos é enumerável (consequentemente, existe uma quantidade enumerável de fórmulas). As linguagens não-enumeráveis têm importância teórica, mas apresentam pouca utilidade prática para a formalização da matemática, pois não nos permite representar graficamente cada símbolo, de maneira unicamente determinada.

4.1 O alfabeto

O alfabeto de uma linguagem de primeira ordem é constituído dos seguintes símbolos:

Variáveis: representadas pelas letras minúsculas: $x, y, z, \ldots$. Eventualmente, são indexadas pelos números naturais: $x_1, x_2, x_3, \ldots$.

Conectivos: $\neg$ (negação – "não"), $\rightarrow$ (condicional – "se... então"), $\wedge$ (conjunção – "e"), $\vee$ (disjunção – "ou"), $\leftrightarrow$ (bicondicional – "se, e somente se").

Quantificadores: $\forall$ (quantificador universal – "para todo"), $\exists$ (quantificador existencial – "existe").

Delimitadores: são os parênteses esquerdo e direito: **(** e **)**, e a vírgula: **,**.

Símbolo de igualdade: $=$

Símbolos relacionais: Para cada número natural n há uma lista (eventualmente vazia) de símbolos relacionais n-ários, geralmente representados por letras maiúsculas e que podem ser indexadas pelos números naturais.

Símbolos funcionais: Para cada número natural n há uma lista (eventualmente vazia) de símbolos funcionais n-ários, geralmente representados por letras maiúsculas e que podem ser indexadas pelos números naturais.

Constantes: Uma lista (pode ser vazia) de símbolos. Geralmente usamos as letras minúsculas do início do alfabeto $(a, b, c, \ldots)$, eventualmente indexadas com números naturais $(a_1, a_2, \ldots)$.

Enquanto os demais símbolos são comuns a qualquer linguagem de primeira ordem, os símbolos relacionais e funcionais e as constantes são específicos da linguagem em que estamos trabalhando. Fixaremos duas linguagens como exemplo: a linguagem **N** tratará dos conjuntos numéricos (o universo são os números), e a linguagem **P** tratará das relações familiares (o universo são as pessoas).

Embora trataremos posteriormente da semântica, já podemos antecipar algumas ideias para que o leitor consiga acompanhar intuitivamente a construção da linguagem. Para interpretar as fórmulas, precisamos estabelecer um conjunto-universo, também chamado de *domínio*. Os símbolos funcionais n-ários correspondem a operações n-árias no universo. Os símbolos relacionais n-ários serão interpretados como relações n-árias sobre o universo. As constantes serão elementos do universo. Um *modelo* para a linguagem será formado por um conjunto não-vazio (chamado de *domínio* ou *universo*), uma operação n-ária para cada símbolo funcional n-ário da linguagem, uma relação n-ária para cada símbolo relacional n-ário e um elemento do domínio para cada constante da linguagem.

Na linguagem dos números temos dois símbolos funcionais binários ($+$ e $\cdot$), duas constantes (0 e 1) e um símbolo relacional binário ($\leq$). Um modelo para a linguagem poderá ser um dos conjuntos numéricos que conhecemos – os naturais, os inteiros, os racionais, os reais ou os complexos – com as operações usuais. Mas, como podemos ver no Apêndice B, pode ser, também, uma álgebra de Boole.

Na linguagem **P** das pessoas podemos estabelecer os símbolos funcionais unários Pai, Mãe, os símbolos relacionais unários Homem, Mulher, o símbolo relacional binário Irmãos e as constantes João e Maria.

4.2 Termos

Lembremos um pouco da gramática da língua portuguesa. Uma frase é formada por uma ou mais *orações*. Para formarmos uma oração precisamos de um verbo que relaciona o *sujeito* e o *objeto* da oração. Esses podem ser substantivos ou expressões que substituem, ou complementam, substantivos. Quando alguém escreve, por exemplo, "o cachorro do primo de José mordeu o nariz do sobrinho do meu vizinho", temos, nessa oração, um verbo ("mordeu"), que corresponde a um símbolo relacional, um sujeito ("o cachorro do primo de José") e um objeto ("o nariz do sobrinho do meu vizinho"). Esses

correspondem aos termos de uma linguagem de primeira ordem. Notemos que, enquanto a oração se refere a um *fato* (passível de ser julgada como falso ou verdadeiro), o sujeito e objeto se referem a seres do universo. Notemos, também, que cada uma dessas expressões é centrada em uma palavra. O sujeito da oração é centrada no nome próprio "José", que corresponde a uma constante na linguagem lógica. As expressões "primo de" e "cachorro do" correspondem a símbolos funcionais, que associam um objeto a outro, na frase. O pronome "meu" torna implícito o pronome "eu", no objeto da oração, que corresponde a uma variável da linguagem, pois, apenas lendo a frase, não podemos saber a quem se refere pronomes como "eu", "ele" ou "ela". Interpretar a frase dependerá do contexto, que, quando virmos a semântica da lógica da primeira ordem, corresponderá à *valoração* das variáveis.

Assim, os termos são formados por aplicações sucessivas de símbolos funcionais sobre as variáveis e constantes. Formalmente, são sequências finitas de símbolos do alfabeto que seguem as seguintes regras:

1. As variáveis são termos;

2. As constantes são termos;

3. Se $t_1, \ldots, t_n$ são termos e F é um símbolo funcional n-ário, então $F(t_1, \ldots, t_n)$ é um termo;

4. Todos os termos têm uma das formas acima.

Como veremos nas abreviaturas, símbolos funcionais binários costumam, na prática, seguir uma sintaxe diferente. Escrevemos $(t_1 F t_2)$ no lugar de $F(t_1, t_2)$. Por exemplo, escrevemos $(x + y)$ em vez de $+(x, y)$.

Exemplos de termos na linguagem $\mathbf{N}$: $(0 + x)$, $1 + (y \cdot (0 + 1))$. Exemplos de termos na linguagem $\mathbf{P}$: Pai(João), Pai(Mãe(Maria)), Mãe(x).

Continuando a comparação entre lógica de primeira ordem e gramática da linguagem natural, os termos mais simples – que são as variáveis e constantes – correspondem aos sujeitos e objetos constituídos por uma única palavra. Assim, as constantes representam os substantivos (ou melhor ainda, os substantivos próprios), pois indicam objetos (ou pessoas, ou seres de qualquer espécie, dependendo de qual é o domínio da linguagem) bem definidos. As variáveis podem ser comparadas aos pronomes, que representam objetos indefinidos (*ele*, *ela*, *alguém*, *isto*, *aquilo*).

4.3 Fórmulas

Fórmulas são sequências finitas de símbolos do alfabeto que seguem as seguintes regras:

1. Se t e s são termos, $(t = s)$ é uma fórmula;

2. Se $t_1, \ldots, t_n$ são termos e R é um símbolo relacional n-ário, $R(t_1, \ldots, t_n)$ é uma fórmula;

3. Se A e B são fórmulas, $(\neg A)$, $(A \to B)$, $(A \wedge B)$, $(A \vee B)$ e $(A \leftrightarrow B)$ são fórmulas;

4. Se A é fórmula e x é uma variável, então $(\forall x A)$ e $(\exists x A)$ são fórmulas;

5. Todas as fórmulas têm uma das formas acima.

Como acontece com os termos, a sintaxe dos símbolos relacionais binários também pode seguir uma regra diferente: se t_1 e t_2 são termos e R é um símbolo relacional binário, escrevemos $(t_1 R t_2)$ no lugar de $R(t_1, t_2)$. Por exemplo, escrevemos $x \leq y$ em vez de $\leq (x, y)$.

Fazendo novamente a analogia entre lógica de primeira ordem e gramática da língua portuguesa, as fórmulas correspondem às *frases*, que fazem alguma asserção (verdadeira ou não) a respeito dos elementos do universo. Os símbolos relacionais e o símbolo de igualdade correspondem aos *verbos* (ou às *locuções verbais*) e as fórmulas atômicas são as *orações*. Por exemplo, a frase *o pai de João é irmão da mãe de Maria* pode ser representado, na linguagem **P**, pela fórmula Irmãos (Pai(João),Mãe(Maria)).

Se quisermos dizer que "todas as pessoas possuem alguma irmã" (independente disso ser verdade ou não) podemos escrever

$$\forall x(\exists y(\textsc{Irmãos}(x, y) \wedge \textsc{Mulher}(y))).$$

Exercício: tente "axiomatizar" a linguagem **P**. Ou seja, escreva o maior número possível de fórmulas que são verdadeiras nessa linguagem, exceto aquelas que são consequências do que você já escreveu (não explicamos ainda o que significa *ser verdadeiro* nem *ser consequência*, mas trabalhemos intuitivamente).

Na linguagem dos números, os "verbos" são $\leq$ e $=$. Um exemplo de fórmula: $x \leq (y + 1)$. Se queremos dizer que não existe raiz de 2, podemos escrever

$$\forall x(\neg((x \cdot x) = (1 + 1)))$$

As fórmulas dos tipos 1 e 2 da definição de fórmulas são as únicas que não possuem conectivo proposicional nem quantificador, e são chamadas de *fórmulas atômicas*.

4.4 Omissão de parênteses

Como acontece com a lógica proposicional, omitimos o excesso de parênteses quando a ausência deles não prejudica a compreensão da fórmula nem causa ambiguidades. Seguem abaixo algumas regras que utilizamos para omitir parênteses:

- Omitimos os parênteses externos de uma fórmula, recolocando quando a usamos para compor outras fórmulas. Por exemplo, escrevemos $A \wedge B$ no lugar de $(A \wedge B)$, mas recolocamos os parênteses quando escrevemos, por exemplo, $\forall x(A \wedge B)$.

- Em sequências de conjunções e em sequências de disjunções, omitimos o uso sucessivo de parênteses. Isto é, escrevemos $A \wedge B \wedge C$ no lugar de $(A \wedge B) \wedge C$ ou de $A \wedge (B \wedge C)$, o mesmo valendo para o conectivo $\vee$.

- Eventualmente, quando não houver riscos de más interpretações, omitimos os parênteses externos em subfórmulas do tipo $\forall xA$, $\exists xA$ e $\neg A$. Por exemplo, escrevemos $\neg\forall x\exists yA$, em vez de $\neg(\forall x(\exists yA))$.

Há uma notação alternativa que dispensa o uso de parênteses e das vírgulas sem causar ambiguidade. Trata-se da *notação prefixada*, em que os símbolos – mesmo os conectivos binários – são colocados sempre à frente dos seus parâmetros. Nessa notação adotamos as seguintes regras: se $t_1, \ldots, t_n$ são termos e F é um símbolo funcional n-ário, $Ft_1 \ldots t_n$ é um termo; se $t_1, \ldots, t_n$ são termos e R é um símbolo relacional n-ário, $Rt_1 \ldots t_n$ é uma fórmula; se t e s são termos, $= st$ é uma fórmula; se A e B são fórmulas e x é uma variável, $\exists xA$, $\forall xA$, $\neg A$, $\wedge AB$, $\vee AB$, $\rightarrow AB$ e $\leftrightarrow AB$ são fórmulas.

Apesar dessa notação apresentar grandes vantagens teóricas pela ausência de delimitadores, a compreensão de fórmulas torna-se bem menos intuitiva. Se tomarmos, por exemplo, a fórmula "Não existe raiz de 2" – $\forall x \neg(x \cdot x = 1 + 1)$ – , na notação prefixada seria

$$\forall x \neg = \cdot xx + 11$$

4.5 Abreviaturas

Assim como fizemos na lógica proposicional, podemos incluir novos símbolos na linguagem da lógica de primeira ordem, enxergando-os como abreviaturas da linguagem que já conhecemos, ou podemos reduzir a quantidade de *símbolos primitivos* e definir os demais a partir desses.

Por exemplo, na linguagem **P**, podemos definir uma relação binária que signifique "*x é tio de y*". Assim, se t e s são termos, definimos a relação $\textsc{Tio}(t, s)$ como

$$\textsc{Homem}(t) \wedge (\textsc{Irmãos}(t,\textsc{Pai}(s)) \vee \textsc{Irmãos}\ (t,\textsc{Mãe}(s)))$$

Na linguagem **N** podemos adicionar um símbolo relacional binário $<$ de modo que $t < s$ seja abreviatura de $(\neg(t = s)) \wedge (t \leq s))$.

Algumas abreviaturas são comuns a todas as linguagens de primeira ordem. Listamos abaixo algumas delas:

- **Diferente:** $t \neq s$ é abreviatura de $\neg(t = s)$;
- **Não existe:** $\nexists x A$ é abreviatura de $\neg\exists x A$;

Existem outras abreviaturas, como "existe um único", que, para definirmos, precisamos antes falar sobre substituição de variáveis.

Podemos reduzir a quantidade de símbolos do alfabeto básico, redefinindo uns a partir de outros. Por exemplo, dizer que "existe x que satisfaça uma propriedade P" é o mesmo que dizer que "não é verdade que todo x não satisfaz a propriedade P". Dessa forma, podemos eliminar o quantificador existencial e definí-lo a partir do quantificador universal. Os conectivos proposicionais são redefinidos assim com fizemos na lógica proposicional. Escolheremos redefinir todos os conectivos e quantificadores a partir de $\forall$, $\neg$ e $\wedge$, mas isso pode ser mudado conforme a necessidade.

- $A \vee B$ é abreviatura de $\neg((\neg A) \wedge (\neg B))$;
- $A \to B$ é abreviatura de $(\neg A) \vee B$;
- $A \leftrightarrow B$ é abreviatura de $(A \to B) \wedge (B \to A)$;
- $\exists x A$ é abreviatura de $\neg \forall x \neg A$.

Também trataremos a notação (tFs) como uma abreviatura de $F(t, s)$, quando F é um símbolo funcional binário, e (tRs) como abreviatura de $R(t, s)$ quando R é um símbolo relacional binário.

Para resultados teóricos, metamatemáticos – isto é, resultados matemáticos *sobre* a lógica de primeira ordem – é vantajoso possuirmos o mínimo possível de símbolos. Mas, para expressarmos de maneira clara e sucinta tudo que queremos, quanto mais símbolos, melhor. Tratando alguns símbolos como abreviaturas a partir de outros, usufruímos de ambos os benefícios.

4.6 Unicidade da representação

Usando as abreviaturas da seção anterior – isto é, não iremos considerar $\exists$, $\vee$, $\to$, $\leftrightarrow$ como símbolos primitivos da linguagem – vamos enunciar os teoremas que asseguram que uso de parênteses evita ambiguidades da linguagem.

Teorema 4.1 (Unicidade da representação dos termos)**.** *Se t é um termo de uma linguagem $\boldsymbol{L}$, então uma, e apenas uma, das asserções abaixo é verdadeira:*

- *t é uma variável;*
- *t é uma constante;*
- *t é da forma $F(t_1, \ldots, t_n)$, onde $t_1, \ldots, t_n$ são termos e F é um símbolo funcional n-ário.*

Além disso, se t é da forma $F(t_1, \ldots, t_n)$ e, ao mesmo tempo, é da forma $G(s_1, \ldots, s_m)$, então temos o seguinte:

- *$n = m$;*
- *F e G são o mesmo símbolo funcional;*

- *t_i é o mesmo termo que s_i, para todo $i \leq n$.*

Na notação acima, chamamos atenção ao uso das *metavariáveis*. Por exemplo, F e G estão sendo usadas como variáveis na metalinguagem para representar símbolos funcionais genéricos.

Para entender melhor a unicidade de representação, suponhamos que não utilizássemos os delimitadores nem a notação pré-fixada ou pós-fixada. Pelas regras de formação (eliminando os parênteses) $0 + x \cdot 1$ é um termo da linguagem **N**. Porém, podemos entender esse termo de duas maneiras: é uma sequência de símbolos da forma t+s, onde t é o termo 0 e s é o termo $x \cdot 1$; ou é uma sequência da forma $t \cdot s$, onde t é o termo $0 + x$ e s é o termo 1. Essa ambiguidade poderia trazer graves consequências a toda a estrutura da linguagem e à definição da semântica.

Agora vamos falar da unicidade da representação das fórmulas.

Teorema 4.2 (Unicidade da representação das fórmulas)**.** *Seja A uma fórmula de uma linguagem $\boldsymbol{L}$. Então A satisfaz uma, e apenas uma, das condições abaixo.*

- *A é uma fórmula atômica da forma $R(t_1, \ldots, t_n)$, onde R é um símbolo relacional n-ário e $t_1, \ldots, t_n$ são termos;*
- *A é uma fórmula atômica da forma $(t_1 = t_2)$ onde t_1 e t_2 são termos;*
- *A é da forma $\neg B$, onde B é uma fórmula;*
- *A é da forma $B \wedge C$, onde B e C são fórmulas;*
- *A é da forma $\forall x B$, onde B é uma fórmula e x uma variável.*

Além disso, valem as seguintes afirmações:

- *Se A é da forma $R(t_1, \ldots, t_n)$ e da forma $R'(s_1, \ldots, s_m)$, então $n = m$, R e R' são o mesmo símbolo e t_i e s_i são o mesmo termo, para todo i entre 1 e n;*
- *Se A é da forma $(t_1 = t_2)$ e da forma $(s_1 = s_2)$ então t_1 e s_1 são o mesmo termo, bem como t_2 e s_2;*
- *Se A é da forma $\neg B$ e da forma $\neg B'$, onde B e B' são fórmulas, então B e B' são a mesma fórmula;*

- *Se A é da forma $B \wedge C$ e da forma $B' \wedge C'$, onde B, B', C e C' são fórmulas, então B e B' são a mesma fórmula e C e C' são a mesma fórmula;*

- *Se A é da forma $\forall u B$ e da forma $\forall v B'$, onde B e B' são fórmulas e u e v são variáveis, então B e B' são a mesma fórmula e u e v a mesma variável.*

Mais uma vez precisamos falar sobre a diferença entre linguagem e metalinguagem, para explicar satisfatoriamente o enunciado acima. Quando escrevemos "*para toda variável u*", a expressão *para toda* corresponde ao quantificador universal escrito na língua portuguesa, e pertence à metalinguagem. Ou seja, à linguagem usada para explicar a linguagem de primeira ordem. Da mesma forma, a letra u está sendo usada na linguagem natural para representar genericamente uma variável qualquer da linguagem de primeira ordem. Portanto, u é uma *variável da metalinguagem*, à qual também chamamos de *metavariável*.

Esse tipo de sutileza entre linguagem e metalinguagem não deve passar despercebido pelo leitor. O uso de metavariáveis será muito frequente nos capítulos que se seguem, e muitas vezes usaremos a mesma letra x para representar variáveis e metavariáveis. O contexto dirá quando se trata de uma variável ou de uma metavariável. Se estiver quantificado na metalinguagem, é uma metavariável.

A demonstração da unicidade de representação das fórmulas segue direto da unicidade dos termos, no caso das fórmulas atômicas, e semelhante ao caso da lógica proposicional, para fórmulas não atômicas.

4.7 Indução na complexidade de termos e fórmulas

Novamente, usando as abreviaturas, para efeitos teóricos consideraremos que uma linguagem de primeira ordem possui os seguintes símbolos do alfabeto: as variáveis, os parênteses, a vírgula, o símbolo de igualdade, o quantificador $\forall$, os conectivos $\wedge$ e $\neg$, e os símbolos específicos da linguagem (símbolos funcionais, símbolos relacionais e constantes). O quantificador existencial e os conectivos $\rightarrow$, $\vee$ e $\leftrightarrow$ serão tratados como abreviaturas, e não como símbolos primitivos.

Os seguintes teoremas seguem dos itens 4 e 5 das regras de formação de termos e fórmulas, respectivamente.

Teorema 4.3 (Indução na complexidade do termo)**.** *Seja* Γ *um conjunto de termos de uma linguagem de primeira ordem* $\boldsymbol{L}$ *e suponha que*

- *todas as variáveis pertencem a* Γ*;*
- *todas as constantes da linguagem* $\boldsymbol{L}$ *pertencem a* Γ*;*
- *se* $t_1, \ldots, t_n$ *pertencem a* Γ *e* F *é um símbolo funcional* n*-ário da linguagem* $\boldsymbol{L}$*, então* $F(t_1, \ldots, t_n)$ *pertence a* Γ*.*

Então Γ *é o conjunto de todos os termos da linguagem.*

Uma propriedade referente aos termos da linguagem pode ser identificado com o conjunto dos termos que satisfazem essa propriedade. Assim, o Teorema 4.3 pode ser reformulado da seguinte forma: se uma propriedade vale para as variáveis e constantes e, valendo para os termos $t_1, \ldots t_n$, vale também para o termo $F(t_1, \ldots, t_n)$, onde F é um símbolo funcional n-ário, então essa propriedade vale para todos os termos.

Teorema 4.4 (Indução na complexidade da fórmula)**.** *Seja* Γ *um conjunto de fórmulas de uma linguagem de primeira ordem* $\boldsymbol{L}$ *e suponha que*

- *as fórmulas atômicas de* $\boldsymbol{L}$ *pertencem a* Γ*;*
- *se* A *pertence a* Γ *então* $\neg A$ *pertence a* Γ*;*
- *se* A *e* B *pertencem a* Γ *então* $A \wedge B$ *pertence a* Γ*;*
- *se* A *pertence a* Γ *e* x *é uma variável, então* $\forall x A$ *pertence a* Γ*.*

Então Γ *é o conjunto de todas as fórmulas da linguagem.*

O princípio de indução na complexidade dos termos e fórmulas, juntamente com a unicidade da representação, permitem que o conceito de grau de complexidade de termos e fórmulas esteja bem definido.

Definição 4.5 (Grau de complexidade de termos)**.** *Definimos o grau de complexidade de um termo* t *do seguinte modo:*

Se t *é uma variável ou constante, então* t *tem grau de complexidade* 0*;*

Se t *é da forma* $F(t_1, \ldots, t_m)$*, onde* F *é um símbolo funcional* m*-ário, então* t *tem grau de complexidade* $n+1$*, onde* n *é o máximo dos graus de complexidade de* $t_1, \ldots, t_m$*.*

Definição 4.6 (Grau de complexidade de fórmulas)**.** *Definimos o grau de complexidade de uma fórmula A do seguinte modo:*

Se A é uma fórmula atômica, A tem grau de complexidade 0;

Se A é da forma $\neg B$ ou $\forall x B$, então A tem complexidade $n+1$, onde n é a complexidade de B.

Se A é da forma $B \wedge C$, então A tem complexidade $n+1$, onde n é o máximo entre a complexidade de B e de C.

Cabem aqui algumas observações importantes. Primeiro, essas definições não estão devidamente formalizadas. A rigor, teríamos que usar uma forma do Teorema da Recursão, como feito no Apêndice A. Mas podemos explicar melhor as definições acima do seguinte modo: admitamos, a princípio, a possibilidade de uma mesma fórmula (ou termo) possuir vários graus de complexidade ao mesmo tempo, ou nenhum. Depois provamos, por indução na complexidade da fórmula (ou termo), que todas as fórmulas (e termos) possuem um único grau de complexidade. Também é necessário usar a unicidade da representação, para mostrarmos que o grau de complexidade está unicamente determinado. Deixamos os detalhes ao leitor.

Segunda observação: essa definição de grau de complexidade considera como quantificador primitivo apenas o $\forall$, e como conectivos primitivos apenas $\neg$ e $\wedge$. Eventualmente, convém mudarmos essa definição conforme a aplicação que queremos. Podemos considerar, por exemplo, $\exists$ e $\vee$ como símbolos primitivos, no lugar de $\forall$ e $\wedge$.

Por último, lembramos que, a rigor, *indução na complexidade da fórmula* (ou termo) é diferente de *indução no grau da complexidade da fórmula*. A primeira usa diretamente os Teoremas 4.3 e 4.4. A segunda usa o princípio de indução finita, para números naturais, e o fato de que o grau de complexidade está bem definido.

4.8 Subtermos e subfórmulas

A definição de subtermos e de subfórmulas é semelhante à definição de subfórmulas na lógica proposicional. Notemos que essas definições são *recursivas*, e para formalizá-las melhor é necessário o uso da indução na complexidade de termos e fórmulas.

Definição 4.7 (Subtermos)**.** Seja t um termo. Definimos os *subtermos* de t da seguinte forma:

- Se t é uma variável ou uma constante, então t é o único subtermo de si mesmo;
- Se t é da forma $F(t_1, \ldots, t_n)$, então os subtermos de t são t e os subtermos de $t_1, \ldots, t_n$.

Dizemos que s é *subtermo próprio* de t se s é subtermo de t e não é t.

Definição 4.8 (Subfórmulas)**.** *Seja A uma fórmula. Definimos as* subfórmulas *de A da seguinte forma:*

- *Se A é uma fórmula atômica então A é a única subfórmula de si mesma;*
- *Se A é da forma $\neg B$ ou da forma $\forall x B$ então as subfórmulas de A são A e as subfórmulas de B;*
- *Se A é da forma $B \wedge C$ então as subfórmulas de A são A, as subfórmulas de B e as subfórmulas de C.*

Dizemos que B é subfórmula própria *de A se B é subfórmula de A e é diferente de A.*

4.9 Variáveis livres

Uma ocorrência de uma variável é *livre* em uma fórmula A se não ocorre no escopo de um quantificador. Ou seja, uma ocorrência de uma variável x é livre em A se não ocorre dentro de uma subfórmula da forma $\forall x B$. Quando uma ocorrência de uma variável não é livre, dizemos que é uma ocorrência *ligada*.

Sempre que nos referimos a uma *ocorrência* de uma variável, estamos nos referindo a uma ocorrência do símbolo em uma subfórmula atômica, não considerando as variáveis apresentadas ao lado do quantificador (como a variável x em $\forall x(y = y)$).

Definição 4.9. Se t e s são termos e x é uma variável, definimos $[t]^s_x$ o termo obtido substituindo a variável x pelo termo s. Formalmente, definimos recursivamente do seguinte modo:

- $[x]^s_x$ é o termo s;

- se c é uma constante, $[c]_x^s$ é o termo c;
- se v é uma variável diferente de x, $[v]_x^s$ é o termo v;
- se t é da forma $F(t_1, \ldots, t_n)$, então $[t]_x^s$ é o termo $F([t_1]_x^s, \ldots, [t_n]_x^s)$.

Definição 4.10. Se A é uma fórmula, x é uma variável e t é um termo, definimos $[A]_x^t$ a fórmula obtida substituindo todas as ocorrências livres da variável x pelo termo t. Formalmente, definimos do seguinte modo:

- Se A é da forma $R(t_1, \ldots, t_n)$ então $[A]_x^t$ é a fórmula $R([t_1]_x^t, \ldots, [t_n]_x^t)$;
- Se A é da forma $(t_1 = t_2)$ então $[A]_x^t$ é a fórmula $([t_1]_x^t = [t_2]_x^t)$;
- Se A é da forma $\neg B$ então $[A]_x^t$ é a fórmula $\neg[B]_x^t$;
- Se A é da forma $B \wedge C$ então $[A]_x^t$ é a fórmula $[B]_x^t \wedge [C]_x^t$;
- Se A é da forma $\forall v B$, onde v é uma variável diferente de x, então $[A]_x^t$ é a fórmula $\forall v [B]_x^t$;
- Se A é da forma $\forall x B$ então $[A]_x^t$ é a própria fórmula A.

Para facilitar a notação, em caso de sucessivas substituições evitamos a repetição dos colchetes. Assim, denotamos por $[A]_{x_1 \ldots x_n}^{t_1 \ldots t_n}$ a fórmula obtida pela substituição em A de todas as ocorrências livres das variáveis $x_1, \ldots, x_n$ pelos termos $t_1, \ldots, t_n$, respectivamente. Por exemplo, em vez de escrevermos $[[A]_{x_1}^{t_1}]_{x_2}^{t_2}$ escrevemos simplesmente $[A]_{x_1 x_2}^{t_1 t_2}$.

Com essa notação podemos introduzir a definição de sentença e o símbolo $\exists!$ (*existe um único*).

Definição 4.11. Chamamos de *sentença* uma fórmula sem variável livre. Isto é, A é uma sentença se A e $[A]_x^t$ são a mesma fórmula, para quaisquer variável x e termo t.

Definição 4.12. Se x é uma variável e A é uma fórmula, definimos $\exists! x A$ como abreviatura para a fórmula

$$(\exists x A) \wedge (\forall y((A \wedge [A]_x^y) \rightarrow (x = y)),$$

onde y é a primeira variável que não ocorre em A.

Para entendermos a definição acima, a primeira parte da conjunção diz que existe x satisfazendo A. A segunda parte diz que esse x é único, isto é, se houver outra variável y para a qual A também é verdadeira substituindo x por y, então $x = y$. Para evitarmos problemas de compatibilidade, tomamos y que não ocorre em A. Escrevemos "a primeira" apenas para que a definição seja unicamente determinada.

Exercícios

1. Usando as linguagens **P** e **N** deste capítulo, sem usar abreviaturas, "traduza" as frases abaixo para a lógica de primeira ordem.

(a) Todo número par maior do que dois pode ser escrito como soma de dois números primos.

(b) Ele é primo de Maria.

(c) x possui exatamente três divisores.

(d) João é filho único.

(e) Todo número positivo admite raiz quadrada.

(f) Maria possui uma única irmã e nenhum irmão.

(g) x e y são primos entre si.

(h) João é meio-irmão de Maria.

(i) z é o máximo divisor comum de x e y.

(j) Maria possui uma avó que tem quatro filhos(as).

2. Exiba as subfórmulas de cada uma das fórmulas que você encontrou no exercício 1.

3. Traduza as fórmulas abaixo para a linguagem natural, da forma mais simplificada que você conseguir.

(a) $\exists x(((\textsc{Pai}(\textsc{Joao})=\textsc{Pai}(x))\wedge((x=\textsc{Pai}(\textsc{Maria}))\vee(x=\textsc{Mae}(\textsc{Maria}))))\vee((\textsc{Mae}(\textsc{Joao})=\textsc{Mae}(x))\wedge((x=\textsc{Pai}(\textsc{Maria}))\vee(x=\textsc{Mae}(\textsc{Maria})))))$

(b) $\exists x\exists y((\neg(x=y))\wedge(\textsc{Joao}=\textsc{Pai}(x))\wedge(\textsc{Joao}=\textsc{Pai}(y))\wedge\forall z((\textsc{Joao}=\textsc{Pai}(z))\rightarrow((z=x)\vee(z=y))))$

(c) $\forall x(((\textsc{Mae}(\textsc{Pai}(\textsc{Maria}))=\textsc{Mae}(\textsc{Pai}(x)))\vee(\textsc{Mae}(\textsc{Pai}(\textsc{Maria}))=\textsc{Mae}(\textsc{Mae}(x))))\rightarrow \mathrm{M}(x))$

4. Para cada uma das frases abaixo, verifique se é possível escrevê-la na linguagem **N**. Se sim, escreva-a, introduzindo, se necessário, novos símbolos definíveis a partir dos símbolos primitivos. Se não, dê uma sugestão para estender a linguagem de modo que possamos escrevê-la. Diga, em cada frase, qual é o domínio (conjunto-universo) a que se refere a linguagem.

(a) Existem infinitos números primos.

(b) Todo subconjunto dos números naturais possui um elemento mínimo.

(c) Se uma propriedade vale para o número 0 e, valendo para um número natural, vale também para seu sucessor, então essa propriedade vale para todos os números naturais.

(d) x possui exatamente três divisores.

(e) O módulo de x é menor do que 5.

(f) x é um número racional.

(g) x é um quadrado perfeito.

(h) Não existem números reais não-nulos x, y, z tais que $x^3 + y^3 = z^3$.

(i) Não existem números reais não-nulos x, y, z e um natural $n > 2$ tais que $x^n + y^n = z^n$.

(j) Todo número par maior do que 2 pode ser escrito como soma de dois ou mais números primos.

5. Defina uma linguagem de primeira ordem apropriada – introduzindo constantes, símbolos funcionais e relacionais – para cada uma das frases abaixo, e traduza-as para a linguagem que você criou. Ressalte qual é o conjunto universo da linguagem que você está utilizando (preste atenção, pois, em alguns casos, o universo pode ser formado por mais de uma categoria de objetos).

(a) Todo homem é mortal, exceto Sócrates.

(b) Todo mundo é amigo de alguém.

(c) Alguém é amigo de todo mundo.

(d) Todas as pessoas conhecem alguém que conhece alguém que conhece alguém que conhece Stephen Hawking.

(e) Todas as pessoas que foram para Marte sabem voar.

(f) Para todo $\varepsilon > 0$ existe $\delta > 0$ tal que para todos x e y pertencentes ao domínio de f, se $|x - y| < \delta$ então $|f(x) - f(y)| < \varepsilon$.

(g) x é o menor número real que é maior ou igual a todos os elementos do conjunto S.

(h) Dados dois pontos distintos existe uma única reta que passa por esses dois pontos.

(i) Dados uma reta e um ponto fora dessa reta, existe uma única reta que passa por esse ponto e é paralela à reta dada.

(j) Existem animais que têm pelo e botam ovos, e todos os pássaros botam ovos.

6. Lembrando que $\neg\forall x A$ é equivalente a $\exists x \neg A$, e $\neg\exists x A$ é equivalente a $\forall x \neg A$, passe as frases do exercício 5 para a negação, **usando o símbolo de negação apenas na frente de subfórmulas atômicas**. Escreva as respostas na linguagem natural e na linguagem de primeira ordem.

7. Identifique as ocorrências livres e não-livres das fórmulas abaixo. Conte quantas variáveis livres cada fórmula possui.

(a) $(\exists x((1+y)=x)) \wedge \forall y(y<x)$.

(b) $\forall y \forall z((y \cdot z = x) \rightarrow ((y \neq z) \wedge ((y=1) \vee (z=1))))$.

(c) $(\exists x(x \cdot x = 2)) \rightarrow (x+1=0)$.

(d) $\forall x \exists y(z<1)$.

(e) $(\exists x((1+y)=x)) \wedge (\forall y(y<x))$.

(f) $\forall x(((x<6) \wedge (0<x)) \rightarrow \exists y(x \cdot y = z))$.

(g) $(\forall y \exists z(x+y=z)) \rightarrow (x=0)$.

(h) $(x<y+1) \rightarrow \forall x \exists y(x \neq y)$.

(i) $\forall x((x=0) \vee (0<x)) \wedge \exists y(y \cdot (1+1) = x)$.

(j) $\forall x(x>(1+1) \rightarrow y<(x+x))$.

8. Escreva a fórmula $[A]_x^{1+1}$ tomando A cada uma das fórmulas do exercício 7.

9. Considere A a fórmula do item (f) do exercício 7. Suponha que estamos trabalhando no universo dos números naturais e que temos todos os números naturais como constantes. Para quais constantes c a sentença $[A]_z^c$ é verdadeira? Justifique.

10. Identifique, no exercício 7, as fórmulas de uma variável livre, e mostre a qual subconjunto do conjunto dos números naturais cada uma delas se refere.

Capítulo 5

Lógica de primeira ordem – semântica

Neste capítulo aprenderemos a interpretar o significado das fórmulas da linguagem de primeira ordem. No Capítulo 4 já apresentamos uma ideia intuitiva sobre como fazer isso. Precisamos, primeiro, estabelecer o universo a que se refere a linguagem. Depois, interpretamos as constantes como elementos do universo, os símbolos relacionais como relações nesse mesmo universo, e os símbolos funcionais como funções. A estrutura formada por todas essas componentes é chamada de *modelo* para uma linguagem de primeira ordem, e veremos como determinar se uma sentença é verdadeira ou falsa em um dado modelo.

Para ilustrar o que é um modelo, antes de entrarmos na definição técnica, consideremos, na linguagem da aritmética, a sentença $\exists x(x \cdot x = 1 + 1)$. Se considerarmos essa sentença no modelo dos números racionais, o universo – também chamado de *domínio* – é o conjunto dos números racionais. A constante 1, vista como um símbolo da linguagem, será interpretada como o número racional 1, na metalinguagem. Os símbolos $+$ e $\cdot$ serão interpretados, respectivamente, como a soma e o produto de números racionais. Nesse modelo, a sentença em questão é falsa, pois sabemos que a raiz quadrada de dois é irracional. Mas no modelo dos números reais a sentença é verdadeira.

Apesar da parecerem complicadas, as definições que se seguem neste capítulo estão muito próximas da nossa concepção intuitiva e até mesmo da linguagem natural. Compreender essa proximidade entre o uso intuitivo dos símbolos lógicos e a definição rigorosa é fundamental no estudo de lógica.

5.1 Modelos

Seja L uma linguagem de primeira ordem. Um *modelo* $\mathcal{M}$ para a linguagem L é uma estrutura constituída das seguintes componentes:

- Um conjunto não-vazio D, que chamaremos de *domínio*, ou *universo*, de $\mathcal{M}$;
- Para cada símbolo relacional n-ário R, uma relação n-ária $R^{\mathcal{M}}$ em D (isto é, $R^{\mathcal{M}}$ é um subconjunto de D^n);
- Para cada constante c um elemento $c^{\mathcal{M}}$ de D;
- Para cada símbolo funcional n-ário F, uma função $F^{\mathcal{M}}$ de D^n em D.

Formalmente, um modelo é uma quádrupla ordenada $(D, (R_i)_{i\in I}, (F_j)_{j\in J}, (c_k)_{k\in K})$, onde R_i, F_j e c_k são as interpretações dos símbolos relacionais, símbolos funcionais e constantes, respectivamente.

5.2 Interpretação de termos

Os termos de uma linguagem representam elementos do domínio. A interpretação de termos será uma função que determinará a qual objeto do domínio se refere o termo. Essa interpretação dependerá de três fatores. Primeiro, é claro, da linguagem, que dirá quais são os símbolos utilizados na formação dos termos. Em segundo lugar, a interpretação depende do modelo, que interpretará as constantes e os símbolos funcionais. Porém, as variáveis, como o nome sugere, não têm uma interpretação fixa que depende apenas do modelo. Para completarmos o terceiro fator que irá determinar a interpretação dos termos precisamos estabelecer uma *valoração* para as variáveis.

Definição 5.1. Se $\mathcal{M}$ é um modelo cujo domínio é D, uma *valoração para o modelo* $\mathcal{M}$ é uma função σ que associa a cada variável um elemento de D.

A valoração estabelece o valor, no domínio, apenas das variáveis. Precisamos estender a função da valoração para todos os termos, pois, conforme foi explicado no Capítulo 4, os termos representam objetos do domínio. A interpretação dos termos depende unicamente da valoração e do modelo. A primeira determina os elementos do domínio associados às variáveis. O segundo estabelece a interpretação das constantes e dos símbolos funcionais.

Definição 5.2. Dados um modelo $\mathcal{M}$ e uma valoração σ, a *interpretação de termos sob a valoração* σ é uma função σ^* que estende a função σ a todos os termos, conforme as seguintes condições:

- Se x é variável, $\sigma^*(x) = \sigma(x)$;
- Se c é uma constante, $\sigma^*(c) = c^{\mathcal{M}}$;
- Se F é um símbolo funcional n-ário e $t_1, \ldots, t_n$ são termos, então $\sigma^*(F(t_1, \ldots, t_n)) = F^{\mathcal{M}}(\sigma^*(t_1), \ldots, \sigma^*(t_n))$.

5.3 Definição de verdade

Sejam $\mathcal{M}$ um modelo, σ uma valoração para o modelo $\mathcal{M}$ e A uma fórmula. Denotamos por $(\mathcal{M}, \sigma) \models A$ quando A *é verdadeira no modelo* $\mathcal{M}$ *para uma valoração* σ, que definimos recursivamente do seguinte modo:

- Para quaisquer termos t_1 e t_2, $(\mathcal{M}, \sigma) \models (t_1 = t_2)$ se, e somente se, $\sigma^*(t_1) = \sigma^*(t_2)$;
- Se R é um símbolo relacional n-ário e $t_1, \ldots, t_n$ são termos, então $(\mathcal{M}, \sigma) \models R(t_1, \ldots, t_n)$ se, e somente se, $(\sigma^*(t_1), \ldots, \sigma^*(t_n)) \in R^{\mathcal{M}}$;
- $(\mathcal{M}, \sigma) \models \neg A$ se, e somente se, não ocorre $(\mathcal{M}, \sigma) \models A$;
- $(\mathcal{M}, \sigma) \models A \vee B$ se, e somente se, $(\mathcal{M}, \sigma) \models A$ ou $(\mathcal{M}, \sigma) \models B$;
- $(\mathcal{M}, \sigma) \models \forall x A$ se, e somente se, $(\mathcal{M}, \theta) \models A$, para toda valoração θ que satisfaz $\theta(v) = \sigma(v)$, para toda variável v que não é x.

Usando as abreviaturas e a definição acima, podemos deduzir as seguintes propriedades, que deixamos como exercício ao leitor:

- $(\mathcal{M}, \sigma) \models A \wedge B$ se, e somente se, $(\mathcal{M}, \sigma) \models A$ e $(\mathcal{M}, \sigma) \models B$;
- $(\mathcal{M}, \sigma) \models A \rightarrow B$ se, e somente se, $(\mathcal{M}, \sigma) \models B$ ou não ocorre $(\mathcal{M}, \sigma) \models A$;
- $(\mathcal{M}, \sigma) \models \exists x A$ se, e somente se, existe uma valoração θ tal que $(\mathcal{M}, \theta) \models A$ e $\theta(v) = \sigma(v)$, para toda variável v que não é x.

Denotamos por $\mathcal{M} \models A$ (que significa que A *é verdadeira* no modelo $\mathcal{M}$, ou, também, $\mathcal{M}$ *satisfaz* a fórmula A) quando $(\mathcal{M}, \sigma) \models A$ vale para toda valoração σ.

Expliquemos um pouco mais sobre a definição de satisfatibilidade para fórmulas que começam com o quantificador $\forall$. Novamente precisamos discutir sobre a diferença entre linguagem e metalinguagem. É comum, em cursos com demonstrações matemáticas informais, dizermos coisas como "*tome x igual a* 2". Porém, quando estamos formalizando a lógica de primeira ordem, x é visto como um símbolo, apenas. Não pode ser igual a 2, a 3, ou a qualquer outro número. O que muda é a valoração, de modo que o correto seria dizer "*tome uma valoração que atribui a x o valor* 2". Ou seja, *se na linguagem quantificamos uma variável, na metalinguagem quantificamos as valorações sobre a variável*. Portanto, dizer que a fórmula $\forall x A$ é verdadeira em um modelo mediante uma valoração σ, significa dizer que A é verdadeira nesse modelo, *mesmo modificando o valor de σ na variável x*. Mas não garante que A continue verdadeira quando alteramos a valoração σ em outras variáveis além de x.

Observe que, cada vez que quantificamos uma variável, dentro do escopo daquele quantificador temos a liberdade de mudar a valoração naquela variável específica. Por exemplo, se quisermos verificar se a fórmula $\forall x(x + y = 0)$ é verdadeira em um modelo mediante uma valoração σ, precisamos testar todas as alterações de σ na variável x, mantendo, porém, o valor de σ em y. Em particular, a validade da fórmula A só depende da valoração nas variáveis livres.

Formalizamos esse argumento através do seguinte teorema:

Teorema 5.3. *Sejam $\mathcal{M}$ um modelo para uma linguagem L, A uma fórmula de L e σ e θ duas valorações para o modelo $\mathcal{M}$ tais que $\sigma(v) = \theta(v)$, para toda variável v que ocorre livre em A. Então $(\mathcal{M}, \sigma) \models A$ se, e somente se, $(\mathcal{M}, \theta) \models A$.*

Demonstração: Fixados o modelo $\mathcal{M}$ e a linguagem L, provaremos o teorema por indução na complexidade de A.

É trivial mostrar que o teorema é verdadeiro quando A é uma fórmula atômica, e também é trivial mostrar que, se vale para A e B, também vale para $\neg A$ e $A \vee B$.

Suponhamos que vale a hipótese indutiva para A. Ou seja, para todas as valorações σ e θ tais $\sigma(v) = \theta(v)$, quando v ocorre livre em A, temos

que $(\mathcal{M}, \sigma) \models A$ se, e somente se, $(\mathcal{M}, \theta) \models A$. Provaremos que o mesmo resultado vale para as fórmulas do tipo $\forall x A$.

Suponha que $(\mathcal{M}, \sigma) \models \forall x A$ e que θ é uma valoração tal que $\theta(v) = \sigma(v)$, para todas as variáveis que ocorrem livres em $\forall x A$. Vamos mostrar que

$$(\mathcal{M}, \theta) \models \forall x A \tag{1}$$

Para isso, considere θ' uma valoração que coincide com θ em todas as variáveis diferentes de x. Precisamos mostrar que

$$(\mathcal{M}, \theta') \models A \tag{2}$$

Considere σ' uma valoração tal que $\sigma'(x) = \theta'(x)$ e $\sigma'(v) = \sigma(v)$, para toda variável v diferente de x. De (1) segue que

$$(\mathcal{M}, \sigma') \models A \tag{3}$$

Observamos que $\sigma'(x) = \theta'(x)$, pela definição de σ', e que

$$\sigma'(v) = \sigma(v) = \theta(v) = \theta'(v),$$

para toda variável v que ocorre livre e $\forall x A$ (lembrando que x *não* ocorre livre em $\forall x A$). Portanto, de (3) e da hipótese indutiva concluímos (1).

A recíproca, isto é, se $(\mathcal{M}, \theta) \models \forall x A$ então $(\mathcal{M}, \sigma) \models \forall x A$, é análoga. ■

Em particular, se a fórmula A é uma sentença – isto é, não possui variáveis livres – então a satisfatibilidade de A em um modelo $\mathcal{M}$ não depende da valoração. Ou seja, se a fórmula for verdadeira mediante uma valoração será verdadeira em qualquer outra. Segue, portanto, do teorema, o seguinte corolário:

Corolário 5.4. *Se A é uma sentença e $\mathcal{M}$ é um modelo, então $\mathcal{M} \models A$ ou $\mathcal{M} \models \neg A$.*

Demonstração: Suponha que não vale $\mathcal{M} \models A$. Isto é, existe uma valoração σ tal que $(\mathcal{M}, \sigma) \models \neg A$. Pelo Teorema 5.3, como A – e, consequentemente, $\neg A$ – não possui variáveis livres, temos que $(\mathcal{M}, \theta) \models \neg A$, para toda valoração θ. Portanto, $\mathcal{M} \models \neg A$. A recíproca é análoga. ■

Exemplo: Considere **L** a linguagem da aritmética, com dois símbolos funcionais binários $+$ e $\cdot$, as constantes 0 e 1 e o símbolo relacional binário $\leq$. Definimos $\mathcal{M} = (D, 0^{\mathcal{M}}, 1^{\mathcal{M}}, +^{\mathcal{M}}, \cdot^{\mathcal{M}}, \leq^{\mathcal{M}})$ um modelo para **L** onde:

$D = \{1, 2, 3\}$;

$0^{\mathcal{M}} = 1$;

$1^{\mathcal{M}} = 2$;

$+^{\mathcal{M}} = \{(1,1,1), (1,2,2), (1,3,3), (2,1,2), (2,2,3), (2,3,1), (3,1,3), (3,2,1), (3,3,2)\}$;

$\cdot^{\mathcal{M}} = \{(1,1,1), (1,2,1), (1,3,1), (2,1,1), (2,2,2), (2,3,3), (3,1,1), (3,2,3), (3,3,2)\}$;

$\leq^{\mathcal{M}} = \{(1,1), (1,2), (1,3), (2,2), (2,3), (3,3)\}$.

Mais uma vez percebamos a diferença entre linguagem e metalinguagem. Quando escrevemos uma fórmula de **L** tratamos 0 e 1 como *símbolos*, não como *objetos matemáticos*. Já os números 1, 2 e 3 na definição de D se referem aos objetos matemáticos que representamos, *na metalinguagem*, por 1, 2 e 3. Esse modelo interpreta o símbolo 0 como o número 1, e o símbolo 1 como o número 2.

Lembramos que um operador binário pode ser visto como uma relação ternária. Portanto, na nossa definição da operação $+^{\mathcal{M}}$, que, obviamente, não coincide com a interpretação usual da soma, temos $1 +^{\mathcal{M}} 1 = 1$, $1 +^{\mathcal{M}} 2 = 2$, e assim por diante.

Quem já cursou álgebra poderá reconhecer que esse modelo nada mais é que o corpo $\mathcal{Z}_3$, isto é, os números inteiros módulo 3, em que identificamos os números com seus respectivos restos na divisão por 3. Assim, 2+2 é igual a 4, que é igual a 1 módulo 3. Novamente, chamamos a atenção para o fato que o 0 está sendo representado pelo 1, o 1 pelo 2 e o 2 (isto é, 1+1), pelo 3.

Fixe σ uma valoração tal que $\sigma(x) = 1$ e $\sigma(y) = 2$.

Considere σ^* a interpretação de termos da linguagem **L** no modelo $\mathcal{M}$ mediante a valoração σ.

Vamos considerar a fórmula $x + y = 1$. Para verificarmos se essa fórmula é verdadeira no modelo $\mathcal{M}$ mediante a valoração σ, precisamos saber quais são as interpretações dos termos $x + y$ e do termo 1. Temos, por definição, que $\sigma^*(1) = 1^{\mathcal{M}}$, que é 2 (lembramos que a interpretação das constantes já é determinada pelo modelo, e não depende da valoração). Por outro lado,

$$\sigma^*(x + y) = \sigma^*(x) +^{\mathcal{M}} \sigma^*(y) = 1 +^{\mathcal{M}} 2 = 2$$

Portanto, $\sigma^*(x+y)$ e $\sigma^*(1)$ são ambos iguais a 2, concluindo que $(\mathcal{M},\sigma) \models x+y=1$.

Notemos que os números usados dentro do escopo de σ^* são símbolos da linguagem. Já os valores (a imagem) de σ^* são objetos do domínio do modelo e, portanto, pertencem à metalinguagem.

Agora verifiquemos a veracidade da fórmula $\forall x((x+y)=1)$. Para sabermos se ela é verdadeira em $\mathcal{M}$ mediante a valoração σ, precisamos testar a fórmula $(x+y)=1$ mediante todas as possíveis alterações de σ na variável x. Ou seja, precisamos saber se para toda valoração θ tal que $\theta(y)=2$ (podemos alterar σ *apenas* na variável x), temos $(\mathcal{M},\theta) \models x+y=1$. Mas isso não é verdade se tomarmos $\theta(x)=2$ (veja que $2 +^{\mathcal{M}} 2 = 3$, e $1^{\mathcal{M}} = 2$, logo $2 +^{\mathcal{M}} 2 \neq 1^{\mathcal{M}}$). Portanto,

$$(\mathcal{M},\sigma) \models \neg\forall x(x+y=1)$$

Exercícios

Nos exercícios 1 a 5 consideraremos **L** a linguagem dos corpos e conjuntos numéricos. A saber, **L** é constituído pelas constantes 0 e 1, os símbolos funcionais $+$ e $\cdot$ e o símbolo relacional $\leq$.

Chamaremos de *axiomas de corpo* o seguinte conjunto de sentenças da linguagem **L**:

1. $0 \neq 1$;
2. $\forall x(x+0=x)$;
3. $\forall x(x\cdot 1=x)$;
4. $\forall x\forall y(x+y=y+x)$;
5. $\forall x\forall y(x\cdot y=y\cdot x)$;
6. $\forall x\forall y\forall z((x+y)+z=x+(y+z))$;
7. $\forall x\forall y\forall z((x\cdot y)\cdot z=x\cdot(y\cdot z))$;
8. $\forall x\exists y(x+y=0)$;
9. $\forall x((x\neq 0)\rightarrow\exists y(x\cdot y=1))$;
10. $\forall x\forall y\forall z(x\cdot(y+z)=(x\cdot y)+(x\cdot z))$.

1. Considere $\mathcal{M}$ o seguinte modelo do exemplo proposto após o Corolário 5.4. Mostre que $\mathcal{M}$ satisfaz todos os axiomas de corpo.

2. Considere $\mathcal{M}$ o modelo do exercício anterior e σ uma valoração satisfazendo

$\sigma(x) = 1$

$\sigma(y) = 2$

$\sigma(z) = 3$

Verifique quais das seguintes fórmulas abaixo são verdadeiras no modelo $\mathcal{M}$ mediante a valoração σ (entenda $t < s$ como abreviatura de $(t \leq s) \wedge \neg(t = s)$).

(a) $x + y = 0$;

(b) $\forall y((y \neq 0) \rightarrow (y \cdot x = y))$;

(c) $\forall x(x \cdot 0 = 0)$;

(d) $\exists x((y \neq x) \wedge (y \leq x))$;

(e) $\forall y \exists x((y \neq x) \wedge (y \leq x))$;

(f) $y \leq 1$;

(g) $(y \leq x) \rightarrow (x \leq y)$;

(h) $((x \leq y) \wedge (y \leq z)) \rightarrow (x \leq z)$;

(i) $((0 < y) \wedge (0 < z)) \rightarrow (0 < y \cdot z)$

(j) $\forall x((x + y = 0) \rightarrow ((0 < x) \leftrightarrow \neg(0 < y)))$

3. Para cada fórmula A contendo variáveis livres do exercício anterior, considere o *fecho universal* de A a sentença $\forall x \forall y \forall z A$. Verifique se essas sentenças são verdadeiras no modelo $\mathcal{M}$ do exercício 1.

4. Seja Γ o conjunto dos axiomas de corpo. Para cada sentença A abaixo construa um modelo (se existir) que satisfaça $\Gamma \cup \{A\}$ e outro (se existir) que satisfaça $\Gamma \cup \{\neg A\}$. Justifique.

(a) $1 + 1 = 0$;

(b) $\forall x(x \cdot 0 = 0)$;

(c) $\forall x \forall y \forall z(((x \leq y) \wedge (y \leq z)) \rightarrow (x = z))$;

(d) $\exists x(x \cdot x = 1 + 1)$;

(e) $\forall x \exists y((y \leq x) \rightarrow (x \leq y))$;

(f) $\exists x \exists y((x \neq 0) \wedge (y \neq 0) \wedge (x \cdot y = 0))$;

(g) $\forall x((\neg(x \leq 0)) \rightarrow \exists y(y \cdot y) = x)$;

(h) $1 + 1 = 1$;

(i) $\forall x \forall y \exists z(x + z = y)$;

(j) $\exists x(x + 1 = x)$.

5. Considere $\mathcal{M}$ um modelo para $\mathbf{L}$ definido da seguinte forma:

$D = \mathcal{P}(\mathbb{N})$ (o conjunto das partes dos números naturais);

$0^{\mathcal{M}} = \emptyset$;

$1^{\mathcal{M}} = \mathbb{N}$;

$\leq^{\mathcal{M}} = \{(X, Y) \in D^2 : X \subseteq Y\}$;

$+^{\mathcal{M}} = \{(X, Y, Z) \in D^3 : X \cup Y = Z\}$;

$\cdot^{\mathcal{M}} = \{(X, Y, Z) \in D^3 : X \cap Y = Z\}$.

Prove que $\mathcal{M}$ satisfaz os axiomas de álgebras de Boole (vide Definição B.1) e verifique quais dos axiomas de corpo são verdadeiros em $\mathcal{M}$ e quais não são.

6. Considere $\mathcal{M}$ um modelo cujo domínio é conjunto dos números naturais, e cujas interpretações dos símbolos 0, 1, + e $\cdot$ são as usuais. Diga para quais valorações as seguintes fórmulas são verdadeiras em $\mathcal{M}$. Justifique usando a definição de semântica.

(a) $\forall x((\exists z(x \cdot z = y)) \rightarrow \exists z((1 + 1) \cdot z = x)))$

(b) $(\exists x(x + x = y)) \rightarrow (\exists y(y + x = y))$

7. Seja $\mathbf{L}$ uma linguagem com uma constante e, um símbolo funcional binário $\circ$, e um símbolo relacional binário $\leq$. Tome $\mathcal{M}$ o seguinte modelo para $\mathbf{L}$, cujo dominio é D:

$D = \{1, 2\}$;

$e^{\mathcal{M}} = 1$;

$\circ^{\mathcal{M}} = \{(1, 1, 1), (1, 2, 2), (2, 1, 2), (2, 2, 1)\}$;

$\leq^{\mathcal{M}} = \{(1, 1), (2, 2), (2, 1)\}$.

Considere, ainda, σ uma valoração tal que $\sigma(x) = 1$, $\sigma(y) = 2$ e $\sigma(z) = 2$. Usando a definição de semântica, e justificando sua resposta com todos os detalhes, verifique se as seguintes fórmulas são verdadeiras no modelo $\mathcal{M}$ mediante a valoração σ.

(a) $(y \leq x) \rightarrow \forall x(x \circ z = z)$;

(b) $\forall x \exists y(x \circ y = e)$;

(c) $\forall y(y \leq x \circ y) \wedge \exists x(\neg(x \circ y = z))$.

8. Sendo $\mathbf{L}$ a linguagem do exercício anterior, considere Γ o conjunto das seguintes sentenças.

- $\forall x((x \circ e = x) \wedge (e \circ x = x))$;
- $\forall x \exists y(x \circ y = e)$;
- $\forall x \forall y \forall z(x \circ (y \circ z) = (x \circ y) \circ z)$.

Seja A a sentença

$$\forall x(x \circ x = e)$$

Mostre que a sentença A é independente de Γ, construindo um modelo para $\Gamma \cup \{A\}$ e outro para $\Gamma \cup \{\neg A\}$

Capítulo 6

Lógica de primeira ordem – axiomatização

A terceira e última parte para completar a definição da lógica de primeira ordem é o sistema de axiomas. Neste capítulo aprenderemos o que é uma demonstração matemática, de acordo com o mais alto padrão de rigor requerido pela matemática moderna.

6.1 O programa de Hilbert

A linguagem e a axiomatização da lógica de primeira ordem seguem alguns princípios estabelecidos por David Hilbert (conhecidos como *programa de Hilbert*), para a formalização da matemática. Alguns deles são os seguintes:

- A linguagem da lógica é composta por uma quantidade enumerável de símbolos;
- As fórmulas são sequências finitas de símbolos;
- As demonstrações são sequências finitas de fórmulas;
- Há um algoritmo que, em finitos passos, determina se uma sequência de símbolos é uma fórmula ou não;
- Há um algoritmo que, em finitos passos, determina se uma sequência de fórmulas é uma demonstração ou não.

O programa de Hilbert incluía, também, os dois seguintes objetivos: o sistema deveria ser completo (provar qualquer sentença ou sua negação) e consistente (não possuir contradições), e tais fatos deveriam ser provados usando o próprio sistema. No entanto, Gödel mostrou que, em qualquer sistema lógico, essas últimas metas propostas por Hilbert não podem ser atingidas, conforme mostraremos na Seção 7.5. Para todos os demais princípios do programa de Hilbert a lógica de primeira ordem – juntamente com a teoria dos conjuntos de Zermelo e Fraenkel – é suficiente, na formalização da matemática moderna.

Quanto às demonstrações, podemos detalhar um pouco mais como deve ser uma demonstração axiomática através das seguintes condições:

- Há um conjunto de fórmulas que são chamadas de *axiomas*;
- Há um conjunto finito de relações (n-árias) no conjunto de fórmulas, e essas relações são chamadas de *regras de inferência*.
- Há um algoritmo que, em finitos passos, determina se uma fórmula é um axioma ou não;
- Há um algoritmo que, em finitos passos, determina se uma dada n-upla de fórmulas $(A_1, \ldots, A_n)$ pertence ou não a uma regra de inferência.
- Uma sequência finita de fórmulas é uma demonstração se, e somente se, cada fórmula A nessa sequência é um axioma ou existem fórmulas $A_1 \ldots, A_{n-1}$ anteriores a A, nessa sequência, tais que $(A_1, \ldots, A_{n-1}, A)$ pertence a alguma regra de inferência.

Ou seja, *demonstração matemática* é uma sequência de fórmulas onde cada uma ou é um axioma ou é obtida das fórmulas anteriores através de uma regra de inferência. Um *teorema* é qualquer fórmula que aparece em alguma demonstração. Em particular, os axiomas são teoremas.

6.2 Sistema de axiomas para a lógica de primeira ordem

O sistema de axiomas da lógica de primeira ordem é composto por cinco axiomas e duas regras de inferência. Na verdade, são cinco *esquemas de axiomas*, pois cada um representa uma lista infinita de axiomas.

Os axiomas apresentados aqui são os *axiomas lógicos*, que valem em qualquer teoria que utiliza a lógica de primeira ordem. Esses axiomas traduzem os argumentos comuns que utilizamos em demonstrações matemáticas.

Lembramos que é virtualmente impossível fazer uma demonstração completa, nos padrões que apresentaremos neste capítulo. Na prática, utilizamos os argumentos usuais que estamos acostumados em cursos como análise real ou álgebra. Mas conhecer o processo formal de demonstração lógica nos dá um ponto de apoio, evitando as armadilhas da linguagem cotidiana. Isto é, devemos, em cada momento, tomar o cuidado de saber como formalizaríamos cada trecho de uma argumentação matemática, caso fosse necessário.

Antes de descrevermos os axiomas e regras de inferências, introduziremos algumas definições.

Definição 6.1. Seja ϕ uma fórmula da lógica proposicional e sejam $p_1, \ldots, p_n$ todas as fórmulas atômicas que aparecem em ϕ. Dizemos que uma fórmula A de uma linguagem de primeira ordem $\mathbf{L}$ é uma *instância de* ϕ se existem fórmulas $A_1, \ldots, A_n$ da linguagem $\mathbf{L}$ tais que A é obtida substituindo cada fórmula atômica p_i por A_i.

As instâncias de tautologia são, portanto, aquelas fórmula obtidas a partir de uma tautologia substituindo uniformemente cada proposição por uma fórmula de primeira ordem. Por exemplo, $(\forall x(x = y)) \to (\forall x(x = y))$ é uma instância de $p \to p$, substituindo p por $(\forall x(x = y))$, e, portanto, será verdadeira, não importando se a fórmula $\forall x(x = y)$ é verdadeira ou não.

Definição 6.2. Sejam A uma fórmula, x uma variável e t um termo. Dizemos que uma ocorrência de x é *livre para um termo t em A* se não está no escopo de qualquer variável que ocorre em t. Isto é, se essa ocorrência de x não está em uma subfórmula B da forma $\forall vC$, onde v é uma variável que ocorre em t.

Ou seja, uma ocorrência de uma variável x em A não é livre para t se a substituição de x por t em A adiciona alguma variável ligada. Por exemplo, na fórmula $\exists y(x = 0)$, x não ocorre livre para y, ou para qualquer termo que contenha a variável y. Em particular, uma ocorrência de x em A é livre para x se, e somente se, é uma ocorrência livre em A.

Com essas definições, podemos introduzir os axiomas. Lembramos que cada item abaixo consiste, na realidade, em um *esquema de axiomas*, isto é, um conjunto infinito de axiomas, definido por uma regra bem precisa, de

modo que, se tomarmos qualquer fórmula de uma linguagem de primeira ordem, conseguimos facilmente descobrir se essa fórmula é um axioma ou não.

A1 As instâncias de tautologia são axiomas.

A2 Se A e B são fórmulas e x é uma variável que não ocorre livre em A, então $(\forall x(A \to B)) \to (A \to \forall x B)$ é um axioma.

A3 Se A é uma fórmula, t é um termo, e x é uma variável tal que todas as ocorrências livres de x em A são livres para t, então $(\forall x A) \to [A]_x^t$ é um axioma.

A4 $x = x$ é um axioma, para qualquer variável x;

A5 Se x e y são variáveis, e A e B são fórmulas tais que B é obtida através da substituição de uma ocorrência de x por y em A, desde que essa ocorrência seja livre para x e y, então $(x = y) \to (A \to B)$ é um axioma.

As regras de inferência são duas:

Modus Ponens: Se A e $A \to B$ são teoremas então B é teorema.

Generalização: Se A é um teorema e x é uma variável, então $\forall x A$ é teorema.

Dizemos que uma substituição de uma variável x por um termo t (que, eventualmente, pode ser também uma variável) em uma fórmula A é *boa* se essa ocorrência de x em A é livre para t e para o próprio x. Os axiomas A3 e A5 "só permitem" substituições boas. Para entendermos melhor esse conceito, considere um modelo que possui mais de um elemento. Nesse modelo podemos verificar que vale a fórmula

$$\forall x \exists y(\neg(x = y))$$

Suponha que não tivéssemos colocado nenhuma restrição sobre a substituição de variável. O esquema A3, substituindo x por y, nos daria o seguinte axioma:

$$(\forall x \exists y(\neg(x = y))) \to \exists y(\neg(y = y))$$

que, naturalmente, é falso em um modelo com dois ou mais elementos (porque o antecedente é verdadeiro e o consequente é falso).

Definição 6.3. Uma fórmula A é um *teorema* da lógica de primeira ordem se existe uma sequência de fórmulas $(A_i)_{0\leq i\leq n}$ tal que A_n é a fórmula A e, para cada $i \leq n$, vale uma das condições abaixo:

- A_i é um axioma;
- Existem $j < i$ e uma variável x tal que A_i é a fórmula $\forall x A_j$;
- Existem $j, k < i$ tais que A_k é a fórmula $A_j \to A_i$.

Exemplos de axiomas: Na linguagem da aritmética, considere a fórmula

$$(x < y) \to ((\exists y(y = 0)) \vee (x < y))$$

Se substituirmos todas as ocorrências da subfórmula $(x < y)$ por p, e a subfórmula $(\exists y(y = 0))$ por q, obtemos a fórmula proposicional $p \to (q \vee p)$, que é uma tautologia. Portanto, a fórmula acima é um axioma do esquema A1 (instância de tautologia).

Aplicando a regra da generalização nessa fórmula obtemos o seguinte teorema:

$$\forall y((x < y) \to ((\exists y(y = 0)) \vee (x < y)))$$

Porém, tal fórmula, apesar de ser um teorema, *não é um axioma*, pois não é instância de tautologia (apenas a subfórmula dentro do quantificador o é) nem se encaixa em nenhum outro esquema de axiomas.

Vejamos um exemplo de um axioma do tipo A2. Considere a fórmula

$$\forall x((y = 0) \to (x + y = x)) \to ((y = 0) \to \forall x(x + y = x))$$

Tomando $y = 0$ no lugar de A e $x + y = x$ no lugar de B, como a variável x não ocorre livre em $y = 0$, percebemos que essa fórmula é um axioma do tipo A2.

Se trocássemos $y = 0$ pela fórmula $\exists x(x = y)$ ainda teríamos um axioma do tipo A2, pois x não ocorre livre em $\exists x(x = y)$. Mas se trocássemos $y = 0$ por $x = y$, então não seria um axioma.

Vamos tentar entender o esquema de axiomas A2. Suponhamos que conseguimos provar que, para todo x, a fórmula A implica a fórmula B. Obviamente, isso não implica que se A for verdadeiro para *um* valor de x então B o será para todo x. Porém, se a fórmula A não depende de x, então a veracidade de A certamente nos garante a veracidade de B para todo x.

O esquema de axiomas A3 também requer um certo cuidado com a substituição de variáveis. Ele é bem intuitivo: se provamos que uma fórmula A é verdadeira para todo x, então, em particular, será verdadeira para qualquer termo que colocamos no lugar de x. Vejamos um exemplo de um axioma do tipo A3:

$$(\forall x(x + 0 = x)) \rightarrow (1 + 0 = 1)$$

Mas, como discutimos anteriormente, precisamos observar se a substituição da variável por outro termo é boa. Considere a seguinte fórmula:

$$(\forall x \exists y(x + y = 1)) \rightarrow (\exists y(y + y) = 1)$$

A princípio, essa fórmula parece um axioma do tipo A3, substituindo as ocorrências livres de x por y em $\exists y(x + y = 1)$. Porém, a substituição de x por y não é boa, pois "prendemos" a variável y no escopo do quantificador existencial. Ou seja, x não é livre para y em A.

Reparem que, de fato, tal fórmula não é verdadeira no modelo dos números inteiros.

O esquema A4 é óbvio e dispensa comentários. Agora vamos entender o esquema A5.

Se $x = y$, então podemos substituir qualquer ocorrência livre de x por y em qualquer lugar de uma fórmula A. Diferente do esquema A3, a substituição não é em todas as ocorrências livres da variável x, mas apenas em uma (e, aplicando iteradamente o esquema, em quantas ocorrências quisermos). A seguinte fórmula é, portanto, um exemplo de axioma do tipo A5.

$$(x = y) \rightarrow ((x + x = 0) \rightarrow (x + y = 0))$$

Já a fórmula seguinte *não* é um axioma do tipo A5, porque a substituição é feita em uma ocorrência em que x não é livre e, portanto, não é uma substituição boa:

$$(x = y) \rightarrow (\exists x(x + x = 0) \rightarrow \exists x(x + y = 0))$$

De modo semelhante, a seguinte fórmula também não é axioma do tipo A5, pois a substituição de x por y não é boa:

$$(x = y) \rightarrow (\exists y(x + x = 0) \rightarrow \exists y(x + y = 0))$$

No Capítulo 7 provaremos que os axiomas são, de fato, verdadeiros em todos os modelos. Provaremos, também, que todas as fórmulas que são verdadeiras em todos os modelos podem ser provadas a partir dos axiomas e das regras de inferência.

6.3 Principais esquemas de teoremas

Encontrar um caminho para demonstrar um teorema a partir da pequena lista de axiomas apresentada na seção anterior não é uma tarefa fácil. Como poderemos perceber logo no primeiro teorema desta seção, mesmo resultados que temos como triviais são difíceis de provar. Porém, cada vez que provamos um teorema, podemos colocá-lo diretamente dentro de uma outra demonstração, sem precisarmos prová-lo novamente. Melhor ainda se provarmos *esquemas de teoremas*, que, como os esquemas de axiomas, são enunciados na metalinguagem em funções de fórmulas arbitrárias (por exemplo, se A e B são teoremas, então $A \wedge B$ é um teorema). Por esse tipo de resultado ser enunciado e demonstrado na metalinguagem, o chamamos de *metateoremas*. Na prática, eles funcionam como novos axiomas e regras de inferências que deduzimos, e, a partir de então, podemos utilizá-los nas próximas demonstrações.

Portanto, encontrar uma demonstração torna-se paulatinamente mais fácil à medida que provamos os "primeiros" teoremas e metateoremas, e as demonstrações se tornam mais próximas das argumentações que estamos acostumados a fazer na metalinguagem. Isso porque os argumentos lógicos que costumamos usar intuitivamente nas demonstrações feitas na "matemática comum", sem a linguagem lógica, começam a incorporar a lista de metateoremas que podemos usar sem precisar redemonstrar. Dessa forma, tudo que conseguimos provar com rigor na linguagem natural, também conseguiremos provar na linguagem lógica.

O propósito desta seção é provar axiomaticamente uma quantidade razoável de teoremas e metateoremas, de modo que as demonstrações axiomáticas se tornem mais factíveis – pelo menos nos níveis mais elementares – , e não apenas uma possibilidade teórica.

Vamos começar por um teorema bem simples: $(x = y) \to (y = x)$. Escreveremos as fórmulas que compõem a demonstração explicando, entre colchetes, após cada fórmula, como a obtivemos.

1. $(x = y) \to ((x = x) \to (y = x))$ [Do esquema A5, tomando $x = x$ no lugar de A e $y = x$ no lugar de B]

2. $(x = x) \to (((x = y) \to ((x = x) \to (y = x))) \to ((x = y) \to (y = x)))$ [Do esquema $A1$, tomando a tautologia $p \to ((q \to (p \to r)) \to (q \to r))$, substituindo p por $x = x$, q por $x = y$ e r por $y = x$]

3. $x = x$ [Esquema A4]

4. $((x = y) \to ((x = x) \to (y = x))) \to ((x = y) \to (y = x))$ [modus ponens aplicado a 2 e 3, tomando como A a fórmula $x = x$ e como B a fórmula $((x = y) \to ((x = x) \to (y = x))) \to ((x = y) \to (y = x))$]

5. $(x = y) \to (y = x)$ [Modus Ponens aplicado a 1 e 4, tomando $(x = y) \to ((x = x) \to (y = x))$ no lugar de A e $(x = y) \to (y = x)$ no lugar de B]

O próximo grupo de metateoremas que mostraremos são novas regras de inferência obtidas a partir do modus pones e das instâncias de tautologias. Começamos derivando a regra de inferência que é a contrapositiva do modus ponens, e corresponde ao silogismo lógico *negando o consequente*. Como todos metateoremas desse grupo têm demonstrações bem parecidas e simples, deixaremos a maioria das demonstrações como exercício ao leitor.

Lembramos que estamos seguindo aquelas regras de omissão de parênteses, quando não houver comprometimento com o significado. Eliminamos os parênteses externos e em sequências de operadores unários ($\neg$, $\forall$ e $\exists$).

Teorema 6.4 (Modus Tollens)**.** *Se $A \to B$ e $\neg B$ são teoremas então $\neg A$ é um teorema.*

Demonstração: Pela tabela-verdade podemos verificar que a seguinte fórmula é uma instância de tautologia, onde A e B são fórmulas quaisquer:

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

Se $A \to B$ é um teorema, da fórmula acima e de modus ponens concluímos que a seguinte fórmula é um teorema:

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

Aplicando modus ponens novamente – assumindo que $\neg B$ é um teorema – concluímos $\neg A$. ■

Teorema 6.5. *Se A e B são teoremas então $A \wedge B$ é teorema.*

Demonstração: Como no Teorema 6.4, basta aplicarmos duas vezes modus ponens à seguinte instância de tautologia:

$$A \to (B \to (A \wedge B))$$

■

Os próximos oito teoremas seguem o mesmo método e deixaremos as provas como exercícios.

Teorema 6.6. *Se $A \to B$ e $B \to C$ são teoremas então $A \to C$ é um teorema.*

Teorema 6.7. *Se $A \to (B \to C)$ e B são teoremas, então $A \to C$ é um teorema.*

Teorema 6.8. *Se $A \to B$ e $B \to A$ são teoremas então $A \leftrightarrow B$ é um teorema.*

Teorema 6.9. *Se $A \to (B \to C)$ e $A \to (C \to D)$ são teoremas então $A \to (B \to D)$ é um teorema.*

Teorema 6.10. *Se $A \to B$ e $A \to C$ são teoremas então $A \to (B \wedge C)$ é um teorema.*

Teorema 6.11. *Se $A \to (B \to C)$ é um teorema então $(A \wedge B) \to C$ é um teorema.*

Teorema 6.12. *Uma fórmula da forma $A \to B$ é um teorema se, e somente se, $(\neg B) \to (\neg A)$ é um teorema.*

Teorema 6.13. *Se $A \to B$ e $(\neg A) \to B$ são teoremas então B é um teorema.*

Os dois teoremas seguintes generalizam o esquema de axiomas A5, sobre substituição de termos iguais em uma fórmula.

Teorema 6.14. *Se t e s são termos, e B é obtido a partir de A através de uma substituição de t por s, em uma ocorrência que não está no escopo de nenhuma ocorrência de uma variável que ocorre em t ou em s, então $(t = s) \to (A \to B)$ é um teorema.*

Demonstração Sejam x e y duas variáveis que não aparecem nas fórmulas A e B nem nos termos t e s. Considere C a fórmula obtida pela substituição do termo t pela variável x na fórmula A, na mesma ocorrência em que t é substituído por s, em B. Da mesma forma, considere D a fórmula em que substituímos essa mesma ocorrência de s em B pela variável y.

Como x e y não ocorrem em A nem em B, reparemos que $[C]_x^t$ é a fórmula A, e $[D]_y^s$ é a fórmula B. Pela hipótese, temos que x e y não estão no escopo de nenhuma variável que ocorre em t ou s. Portanto, as substituições em $[C]_x^t$ e $[D]_y^s$ são boas. Como escolhemos x e y que não aparecem nas fórmulas A e B, temos que D é obtido a partir de uma substituição boa de x por y em C. Portanto, o esquema A5 nos fornece o seguinte axioma:

$$(x = y) \to (C \to D)$$

Pela regra da generalização

$$\forall x((x = y) \to (C \to D))$$

Usando as observações acima notamos que a seguinte fórmula é uma instância de A3:

$$\forall x((x = y) \to (C \to D)) \to ((t = y) \to (A \to D))$$

Por modus ponens, das duas últimas fórmulas obtemos

$$(t = y) \to (A \to D)$$

Novamente pela generalização:

$$\forall y((t = y) \to (A \to D))$$

Por A3:

$$\forall y((t = y) \to (A \to D)) \to ((t = s) \to (A \to B))$$

Usando modus ponens mais uma vez obtemos o teorema que queríamos:

$$(t = s) \to (A \to B)$$

■

Na hipótese do Teorema 6.14 também dizemos que a substituição de t por s é *boa*.

Teorema 6.15. *Se t e s são termos, e B é obtido a partir de A através de duas ou mais substituições boas de t por s, então $(t = s) \to (A \to B)$ é um teorema.*

Demonstração Se B é obtido a partir de n substituições de t por s em A, considere uma sequência de fórmulas $A_0, \ldots, A_n$ em que A_0 é a fórmula A, A_n é a fórmula B, e cada fórmula é obtida a partir de uma substituição de t por s na fórmula anterior. O metateorema 6.14 nos dá, para cada $i < n$, o seguinte teorema:

$$(1) \qquad (t = s) \to (A_i \to A_{i+1})$$

Mostraremos, por indução em i, que para todo $i < n$ vale o teorema

$$(2) \qquad (t = s) \to (A_0 \to A_{i+1})$$

Para $i = 0$ a expressão (2) é um caso particular de (1). Suponha que temos mostrado o seguinte teorema:

$$(3) \qquad (t = s) \to (A_0 \to A_i)$$

De (3) e (1) e da nova regra de inferência 6.9 obtemos (2). Tomando $i = n-1$ obtemos

$$(t = s) \to (A_0 \to A_n)$$

■

Teorema 6.16. *Se A é um teorema, t é um termo, e x é uma variável livre para t, em A, então $[A]^t_x$ é um teorema.*

Demonstração: Pela regra da generalização, $\forall x A$ é um teorema. De $A3$ temos que $(\forall x A) \to [A]^t_x$ é um teorema. De Modus Ponens concluímos que $[A]^t_x$ é um teorema. ■

Mostraremos, agora, as propriedades reflexiva, simétrica e transitiva da igualdade entre termos.

Teorema 6.17. *Se t é um termo, então $t = t$ é um teorema.*

Demonstração: Segue de A4 e 6.16. ■

Teorema 6.18. *Se t e s são termos, então $(t = s) \to (s = t)$ é um teorema.*

Demonstração: Provamos, no exemplo, que $(x = y) \to (y = x)$ é um teorema. Aplicando duas vezes 6.16 provamos o que queríamos. ■

Teorema 6.19. *Se t, s e u são termos, então $((t = s) \wedge (s = u)) \to (t = u)$ é um teorema.*

Demonstração: Mostraremos a sequência de fórmulas da demonstração, enumerando as fórmulas à esquerda e indicando, à direita, os axiomas, regras de inferência, metateoremas e fórmulas anteriores utilizados. Abreviamos as regras de generalização e modus ponens como G e MP, respectivamente, e omitimos detalhes nas indicações dos esquemas de axiomas. Cabe ao leitor (nesta e nas próximas demonstrações) completar os detalhes, como verificar as instâncias de tautologia e se as substituições são boas.

1. $(x = y) \to (y = x)$ [6.18]
2. $(y = x) \to ((y = z) \to (x = z))$ [A5]
3. $(x = y) \to ((y = z) \to (x = z))$ [6.6, 1 e 2]
4. $((x = y) \to ((y = z) \to (x = z))) \to (((x = y) \wedge (y = z)) \to (x = z))$ [A1]
5. $((x = y) \wedge (y = z)) \to (x = z)$ [MP, 4 e 3]
6. $((t = y) \wedge (y = z)) \to (t = z)$ [6.16, 5]
7. $((t = s) \wedge (s = z)) \to (t = z)$ [6.16, 6]
8. $((t = s) \wedge (s = u)) \to (t = u)$ [6.16, 7]

■

Os próximos teoremas nos ajudarão a trabalhar melhor com o quantificador universal.

Teorema 6.20. *Se A e B são fórmulas e x é uma variável, então $\forall x(A \to B) \to ((\forall x A) \to (\forall x B))$ é um teorema.*

Demonstração

1. $(\forall x A) \to A$ [A3]
2. $((\forall x A) \to A) \to ((A \to B) \to ((\forall x A) \to B))$ [A1]
3. $(A \to B) \to ((\forall x A) \to B)$ [MP, 1 e 2]
4. $(\forall x(A \to B)) \to (A \to B)$ [A3]
5. $(\forall x(A \to B)) \to ((\forall x A) \to B)$ [6.6, 4 e 3]
6. $\forall x((\forall x(A \to B)) \to ((\forall x A) \to B))$ [G e 5]
7. $(\forall x((\forall x(A \to B)) \to ((\forall x A) \to B))) \to ((\forall x(A \to B)) \to (\forall x((\forall x A) \to B)))$ [A2]
8. $(\forall x(A \to B)) \to (\forall x((\forall x A) \to B))$ [MP, 6 e 7]
9. $(\forall x((\forall x A) \to B)) \to ((\forall x A) \to (\forall x B))$ [A2]
10. $(\forall x(A \to B)) \to ((\forall x A) \to (\forall x B))$ [6.6, 8 e 9]

■

Teorema 6.21. *Se $A \to B$ e $\forall x A$ são teoremas, então $\forall x B$ é teorema.*

Demonstração:

1. $A \to B$ [hipótese]
2. $\forall x A$ [hipótese]
3. $\forall x(A \to B)$ [G e 1]
4. $(\forall x(A \to B)) \to ((\forall x A) \to (\forall x B))$ [6.20]
5. $(\forall x A) \to (\forall x B)$ [MP, 3 e 4]
6. $\forall x B$ [MP, 2 e 5]

■

Teorema 6.22. *Se A e B são fórmulas e x é uma variável, então $\forall x(A \wedge B) \to ((\forall x A) \wedge (\forall x B))$ é um teorema.*

Demonstração:

1. $(A \wedge B) \rightarrow A$ [A1]
2. $\forall x((A \wedge B) \rightarrow A)$ [G e 1]
3. $(\forall x((A \wedge B) \rightarrow A)) \rightarrow ((\forall x(A \wedge B)) \rightarrow (\forall xA))$ [6.20]
4. $(\forall x(A \wedge B)) \rightarrow (\forall xA)$ [MP, 2 e 3]
5. $(\forall x(A \wedge B)) \rightarrow (\forall xB)$ [Repita os passos anteriores]
6. $(\forall x(A \wedge B)) \rightarrow ((\forall xA) \wedge (\forall xB))$ [6.10, 4 e 5]

■

Teorema 6.23. *Se A e B são fórmulas e x é uma variável, então $\forall x(A \wedge B) \leftrightarrow ((\forall xA) \wedge (\forall xB))$ é um teorema.*

Demonstração:

1. $A \rightarrow (B \rightarrow (A \wedge B))$ [A1]
2. $\forall x(A \rightarrow (B \rightarrow (A \wedge B)))$ [G e 1]
3. $(\forall x(A \rightarrow (B \rightarrow (A \wedge B)))) \rightarrow ((\forall xA) \rightarrow (\forall x(B \rightarrow (A \wedge B))))$ [6.20]
4. $(\forall xA) \rightarrow (\forall x(B \rightarrow (A \wedge B)))$ [MP, 2 e 3]
5. $(\forall x(B \rightarrow (A \wedge B))) \rightarrow ((\forall xB) \rightarrow (\forall x(A \wedge B)))$ [6.20]
6. $(\forall xA) \rightarrow ((\forall xB) \rightarrow (\forall x(A \wedge B)))$ [6.6, 4 e 5]
7. $((\forall xA) \wedge (\forall xB)) \rightarrow (\forall x(A \wedge B))$ [6.11 e 6]
8. $(\forall x(A \wedge B)) \rightarrow ((\forall xA) \wedge (\forall xB))$ [6.22]
9. $\forall x(A \wedge B) \leftrightarrow ((\forall xA) \wedge (\forall xB))$ [6.8, 7 e 8]

■

Teorema 6.24. *Se $A \leftrightarrow B$ é um teorema e x é uma variável, então $(\forall xA) \leftrightarrow (\forall xB)$ é um teorema.*

Demonstração:

1. $A \leftrightarrow B$ [Hipótese]
2. $(A \leftrightarrow B) \rightarrow (A \rightarrow B)$ [A1]
3. $A \rightarrow B$ [MP, 1 e 2]
4. $\forall x(A \rightarrow B)$ [G e 3]
5. $(\forall x(A \rightarrow B)) \rightarrow ((\forall xA) \rightarrow (\forall xB))$ [6.20]
6. $(\forall xA) \rightarrow (\forall xB)$ [MP, 4 e 5]
7. $(\forall xB) \rightarrow (\forall xA)$ [Analogamente aos passos 1 a 6]
8. $(\forall xA) \leftrightarrow (\forall xB)$ [6.8, 6 e 7]

■

Terminamos nossa lista com alguns teoremas sobre o quantificador existencial.

Teorema 6.25. *Se A é uma fórmula e x é uma variável, então $A \rightarrow (\exists xA)$ é um teorema.*

Demonstração: Lembramos que a fórmula acima é uma abreviatura de $A \rightarrow (\neg\forall x\neg A)$. Façamos a prova:

1. $(\forall x\neg A) \rightarrow (\neg A)$ [A3]
2. $(\neg\neg A) \rightarrow (\neg\forall x\neg A)$ [6.12]
3. $A \rightarrow (\neg\neg A)$ [A1]
4. $A \rightarrow (\neg\forall x\neg A)$ [6.6, 3 e 2]

■

Teorema 6.26. *Se A é uma fórmula e x é uma variável, então $(\forall xA) \rightarrow (\exists xA)$ é um teorema.*

Demonstração:

1. $(\forall x A) \to A$ [A3]
2. $A \to (\exists x A)$ [6.25]
3. $(\forall x A) \to (\exists x A)$ [6.6, 1 e 2]

■

Teorema 6.27. *Se x e y são variáveis, $\forall x \exists y (x = y)$ é um teorema.*

Demonstração:

1. $(\forall y(\neg(x = y))) \to (\neg(x = x))$ [A3]
2. $((\forall y(\neg(x = y))) \to (\neg(x = x))) \to ((x = x) \to \neg\forall y \neg(x = y))$ [A1]
3. $(x = x) \to \neg\forall y \neg(x = y)$ [MP, 1 e 2]
4. $x = x$ [A4]
5. $\neg\forall y \neg(x = y)]$ [MP, 4 e 3]
6. $\exists y(x = y))$ [definição de $\exists$]
7. $\forall x \exists y (x = y)$ [G e 6]

■

6.4 Fórmulas equivalentes

Continuamos a apresentar alguns metateoremas cruciais para as demonstrações formais. Desta vez, mostraremos teoremas da forma $A \leftrightarrow B$, que serão úteis para a próxima seção, sobre forma normal prenexa.

Definição 6.28. Dizemos uma fórmula A é *equivalente* a uma fórmula B se $A \leftrightarrow B$ é um teorema da lógica de primeira ordem.

Observe que "ser equivalente a" é uma relação simétrica, isto é, se A é equivalente a B então B é equivalente a A. De fato, $A \leftrightarrow B$ é teorema se, e somente se, $B \leftrightarrow A$ é teorema. Por isso poderemos falar, a partir de agora, que A e B *são equivalentes*, quando A é equivalente a B. Também é imediato ver que é uma relação reflexiva – toda fórmula é equivalente a si mesma – e, usando algumas tautologias, provamos facilmente a transitividade da equivalência, que enunciamos no próximo lema.

Lema 6.29. *Se A é uma fórmula equivalente a B e B é equivalente a C, então A e C são equivalentes.*

O lema seguinte é consequência imediata da definição do conectivo $\leftrightarrow$ e do Teorema 6.4. É uma formalização de um argumento muito comum: provamos a equivalência entre duas afirmações provando cada uma das implicações.

Lema 6.30. *Duas fórmulas A e B são equivalentes se, e somente se, as fórmulas $A \to B$ e $B \to A$ são teoremas da lógica de primeira ordem.*

Usando o Teorema 6.24 podemos derivar uma nova regra de inferência: fórmulas equivalentes podem ser substituídas uma por outra em qualquer momento.

Teorema 6.31. *Suponha que D seja uma fórmula obtida a partir de uma fórmula C substituindo uma ou mais ocorrências de uma subfórmula A (em C) por uma fórmula B. Nesse caso, se A é equivalente a B então C é equivalente a D.*

Demonstração: Mostraremos que o teorema vale quando substituímos *uma* ocorrência de A. Para mais de uma substituição, procedemos como no Teorema 6.15, fazendo uma substituição por vez.

Se $A \leftrightarrow B$ é um teorema, então, por 6.24, $(\forall x A) \leftrightarrow (\forall x B)$ é um teorema, para qualquer variável x. Da mesma forma, se F é uma fórmula, como $(A \leftrightarrow B) \to ((A \wedge F) \leftrightarrow (B \wedge F))$ é uma tautologia, usando modus ponens concluímos que $(A \wedge F) \leftrightarrow (B \wedge F)$ é um teorema. Analogamente, à medida que compomos C e D a partir de A e B usando os conectivos lógicos e o quantificador universal (tratando o existencial como uma abreviatura), provamos que $C \leftrightarrow D$ é um teorema.

No final deste capítulo apresentamos, em um exercício, sugestões para formalizarmos melhor essa demonstração, usando indução. ■

Teorema 6.32. *Se x é uma variável que não ocorre livre em A, então A é equivalente a $\forall x A$.*

Demonstração: Do axioma A3 temos que $(\forall x A) \to A$ é um teorema. Pelo Lema 6.30, precisamos provar que $A \to (\forall x A)$. De fato, temos:

1. $A \to A$ [A1]
2. $\forall x(A \to A)$ [1 e G]
3. $(\forall x(A \to A)) \to (A \to \forall x A)$ [A2]
4. $A \to \forall x A$ [MP, 3 e 2]

■

Teorema 6.33. *Se y é uma variável que não ocorre livre em A, então $\forall x A$ é equivalente a $\forall y[A]^y_x$ e $\exists x A$ é equivalente a $\exists y[A]^y_x$.*

Demonstração: De A3 e generalização temos $\forall y((\forall x A) \to [A]^y_x)$. Como y não ocorre livre em A (e, portanto, em $\forall x A$), por A2 e *modus ponens* temos $(\forall x A) \to (\forall y[A]^y_x)$.

Notamos que, como y não ocorre livre em A, temos que $[[A]^y_x]^x_y$ é a fórmula A. Também observamos que x não ocorre livre em $[A]^y_x$, visto que as ocorrências livres de x em A foram substituídas por y (estamos assumindo que x e y são, de fato, variáveis diferentes, pois, caso contrário, o teorema é trivial). Assim, repetindo o argumento anterior, considerando $[A]^y_x$ no lugar de A e trocando as variáveis x e y, concluímos que $(\forall y[A]^y_x) \to (\forall x A)$. Pelo Lema 6.30 isso conclui a primeira parte do teorema. A segunda parte, sobre os quantificadores existenciais, segue da primeira, usando a definição de $\exists$. ■

Teorema 6.34. *Se x é uma variável que não ocorre livre em B, então $(\forall x A) \wedge B$ é equivalente a $\forall x(A \wedge B)$.*

Demonstração: Pelo Teorema 6.32, B é equivalente a $\forall x B$. Logo, pelo Teorema 6.31, a fórmula $(\forall x A) \wedge B$ é equivalente a $(\forall x A) \wedge (\forall x B)$, que, por 6.23 é equivalente a $\forall x(A \wedge B)$. Do Lema 6.29 concluímos o teorema. ■

Teorema 6.35. *Se x e y são variáveis tais que x não ocorre livre em B e y não ocorre livre em A, então $(\forall x A) \wedge (\forall y B)$ é equivalente a $\forall x \forall y(A \wedge B)$.*

Demonstração: Por 6.34 sabemos que $(\forall x A) \wedge (\forall y B)$ é equivalente a $\forall x(A \wedge \forall y B)$. Por sua vez, essa equivale a $\forall x((\forall y B) \wedge A)$, por 6.31, dada a equivalência entre $A \wedge \forall y B$ e $(\forall y B) \wedge A$. Mas, usando a hipótese de que y não ocorre livre em A, de 6.34 segue que $(\forall y B) \wedge A$ é equivalente a $\forall y(B \wedge A)$ e, portanto, a $\forall y(A \wedge B)$. Usando novamente o Teorema 6.31 concluímos que $\forall x((\forall y B) \wedge A)$ equivale a $\forall x \forall y(A \wedge B)$. Portanto, segue do Lema 6.29 a equivalência desejada. ■

Teorema 6.36. *Se x é uma variável que não ocorre livre em A, então $A \to \forall x B$ é equivalente a $\forall x(A \to B)$.*

Demonstração: A implicação $(\forall x(A \to B)) \to (A \to \forall x B)$ é um axioma do tipo A2. Pelo Lema 6.30 basta provarmos que

$$(A \to \forall x B) \to \forall x(A \to B)$$

é teorema. Observe que x não ocorre livre em A, por hipótese, nem em $\forall x B$, uma vez que todas as ocorrências de x nessa fórmula são ligadas. Logo, de 6.32 segue que $A \to \forall x B$ é equivalente a $\forall x(A \to \forall x B)$. Mas por A3 e generalização sabemos que $\forall x(\forall x B \to B)$ é um teorema. Logo, podemos facilmente provar, usando uma instância de tautologia adequada (exercício ao leitor), que $A \to \forall x B$ é equivalente a

$$\forall x(A \to \forall x B) \wedge \forall x(\forall x B \to B).$$

Mas essa, por sua vez, usando 6.23, equivale a

$$\forall x((A \to \forall x B) \wedge (\forall x B \to B)).$$

A seguinte fórmula é a generalização de uma instância de tautologia:

$$\forall x(((A \to \forall x B) \wedge (\forall x B \to B)) \to (A \to B)).$$

Assim, pelos Teorema 6.20 e usando *modus ponens* concluímos que

$$\forall x(((A \to \forall x B) \wedge (\forall x B \to B))) \to \forall x(A \to B).$$

Portanto, aplicando o Teorema 6.31 chegamos ao teorema que buscávamos:

$$(A \to \forall x B) \to \forall x(A \to B).$$

■

Teorema 6.37. *Se x é uma variável que não ocorre livre em B, então $(\exists x A) \wedge B$ é equivalente a $\exists x(A \wedge B)$.*

Demonstração: Usando a definição do quantificador existencial e algumas equivalências entre os conectivos proposicionais, podemos verificar que $(\exists x A) \wedge B$ equivale a $\neg(B \rightarrow \forall x \neg A)$. Por 6.36 e pela hipótese de x não ocorrer livre em B temos que $(B \rightarrow \forall x \neg A)$ equivale a $\forall x(B \rightarrow \neg A)$, que, por sua vez, é equivalente a $\forall x \neg(A \wedge B)$. Logo, $\neg(B \rightarrow \forall x \neg A)$ equivale a $\neg \forall x \neg(A \wedge B)$, que é a fórmula $\exists x(A \wedge B)$. Usando a transitividade da equivalência entre fórmulas (Lema 6.29) concluímos o teorema. ■

Teorema 6.38. *Se x e y são variáveis tais que x não ocorre livre em B e y não ocorre livre em A, então $(\exists x A) \wedge (\exists y B)$ é equivalente a $\exists x \exists y(A \wedge B)$.*

Demonstração: Aplique duas vezes o Teorema 6.37, analogamente ao que foi feito na demonstração do Teorema 6.36. Deixamos os detalhes para o leitor. ■

Teorema 6.39. *Se x e y são variáveis tais que x não ocorre livre em B e y não ocorre livre em A, então $(\forall x A) \wedge (\exists y B)$ é equivalente a $\forall x \exists y(A \wedge B)$.*

Demonstração: Análoga aos Teoremas 6.36 e 6.38. ■

6.5 Forma normal prenexa

Fórmulas equivalentes podem ser tratadas, em certo sentido, como *a mesma fórmula*. Tal ideia será formalizada no Apêndice B, e pode ser aplicada tanto para fórmulas da lógica proposicional quanto para fórmulas de uma linguagem de primeira ordem. Podemos considerar, intuitivamente, que fórmulas diferentes mas equivalentes são *a mesma fórmula escrita de maneiras diferentes*. Ou seja, em *formas* diferentes. Para resultados teóricos convém, portanto, encontrarmos formas padrões para representar as fórmulas. No caso da lógica proposicional, vimos a forma disjuntiva normal. Na lógica de primeira ordem, a forma padrão das fórmulas será colocando todos os quantificadores na frente. Considerando a linguagem possuindo apenas o quantificador $\forall$ e os conectivos $\neg$ e $\wedge$ como símbolos primitivos – dentre os quantificadores e conectivos – e considerando que toda dupla negação pode ser eliminado na fórmula, mantendo a equivalência com a original (veja Teorema 6.31), a seguinte definição formaliza esse conceito.

Definição 6.40. *[Forma Normal Prenexa]* Dizemos que uma fórmula A está na *forma normal prenexa* se toda subfórmula de A da forma $B \wedge C$ não possui quantificador.

Por exemplo, uma fórmula do tipo $\forall x \exists y A$ está na forma normal prenexa. Já as fórmulas $(\forall x A) \wedge (\forall y B)$ e $(\forall x A) \rightarrow B$ não estão. O que os teoremas da Seção 6.4 mostram são vários casos em que podemos "passar para a frente" os quantificadores de uma fórmula, tanto os universais quanto os existenciais. Usaremos aqueles resultados para provarmos o seguinte teorema:

Teorema 6.41. *Toda fórmula de uma linguagem de primeira ordem é equivalente a uma fórmula que está na forma normal prenexa.*

Demonstração: Procederemos por indução no grau de complexidade da fórmula. Fixemos uma linguagem de primeira ordem. Fórmulas atômicas não possuem quantificadores e já estão, portanto, na forma normal prenexa. Seja $n > 0$ um número natural. Assumamos, por indução, que, toda fórmula de complexidade menor do que n é equivalente a alguma fórmula na forma normal prenexa. Seja C uma fórmula de grau n. Vamos provar que C é equivalente a alguma fórmula na forma normal prenexa.

Se C é da forma $\forall x A$, então, por hipótese indutiva, A é equivalente a alguma fórmula A' que está na forma prenexa. Como subfórmulas da forma $A_1 \wedge A_2$ de $\forall x A'$ também são subfórmulas de A, tem-se que $\forall x A'$ também está na forma normal prenexa, e, pelo Teorema 6.31, é equivalente a C. O mesmo argumento se aplica quando C é da forma $\neg A$.

Assumimos, então, que C é da forma $A \wedge B$. Usando a hipótese indutiva e o Teorema 6.31 podemos assumir, sem perda de generalidade, que A e B estão na forma prenexa. Vamos dividir a demonstração em alguns casos.

Caso 1: B não possui quantificadores.

Vamos proceder por indução no número de quantificadores em A. Explicando melhor, provaremos uma afirmação à parte que diz o seguinte: se A está na forma prenexa e B não possui quantificadores, então $A \wedge B$ é equivalente a uma fórmula na forma prenexa.

Assumimos que A não é da forma $\neg\neg A'$. De fato, se for dessa forma, substituímos A por A', procedendo igualmente com A' caso ela própria inicie

com dupla negação [1]. Assumimos, também, que A possui quantificadores, pois, caso contrário, a fórmula $A \wedge B$ já está na forma prenexa.

Como A está na forma prenexa, o fato de possuir quantificador descarta a possibilidade de ser da forma $A_1 \wedge A_2$, ou mesmo $\neg(A_1 \wedge A_2)$. Só resta dois casos: ou A é da forma $\forall x A'$ ou da forma $\exists x A'$ (lembrando que $\exists x$ é abreviatura de $\neg\forall x\neg$). Consideremos, primeiro, o caso em que A é da forma $\forall x A'$.

Tome y uma variável que não ocorre livre nem em A nem em B. Pelos Teoremas 6.33 e 6.31, A é equivalente a $\forall y[A']^y_x$ e $A \wedge B$ é equivalente a $(\forall y[A']^y_x) \wedge B$. Como y não ocorre livre em B, por 6.34 essa última é equivalente a $\forall y([A']^y_x \wedge B)$. Mas $[A']^y_x$ tem um quantificador a menos do que A. Logo, por hipótese indutiva, existe uma fórmula D na forma prenexa equivalente a $[A']^y_x \wedge B$. Portanto, $A \wedge B$ é equivalente a $\forall y D$, que está na forma normal prenexa.

Se A é da forma $\exists x A'$ a prova é análoga ao caso $\forall x A'$, usando o Teorema 6.37 no lugar de 6.34.

A partir de agora podemos assumir que tanto A quanto B começam com um quantificador.

> **Caso 2:** C é da forma $(\forall u A') \wedge (\forall v B')$, onde u e v são variáveis não necessariamente distintas.

Sejam x e y variáveis que não ocorrem nem em A' nem em B'. Por 6.32 e 6.31 a fórmula C é equivalente a

$$(\forall x[A']^x_u) \wedge (\forall y[B']^y_v),$$

que, pelo Teorema 6.35 é equivalente a

$$\forall x \forall y([A']^x_u \wedge [B']^y_v).$$

Notemos que A e B estarem na forma prenexa implica que A' e B' também estão, e a troca de variáveis não altera esse fato.

Isso conclui a prova para o caso 2. Restam ainda mais dois: quando C tem o formato $(\exists u A') \wedge (\exists v B')$ ou $(\forall u A') \wedge (\exists v B')$. As demonstrações para esses casos, no entanto, são a mesma que para o caso 2, usando os teoremas 6.38 e 6.39 no lugar de 6.36.

■

[1] Os mais preciosistas, que não se agradaram com essa explicação, podem provar por indução na complexidade das fórmulas que toda fórmula é equivalente a alguma fórmula que não tenha dupla negação.

Excercícios

1. Verifique se cada uma das fórmulas abaixo é um teorema da lógica de primeira ordem ou não. Se for teorema, prove a partir dos axiomas e regras de inferência, deixando claro qual axioma você está usando, em cada passo. Se não for teorema, exiba um modelo que satisfaça sua negação.

(a) $\forall x \exists y(\neg(y = x)) \to \exists y(\neg(y = 0))$;

(b) $\forall x \exists y(\neg(x = y))$;

(c) $\forall x \exists y(y < x) \to \exists y(y < y)$;

(d) $\forall x((0 < x) \to (0 < x + x)) \to ((0 < x) \to \forall x(0 < x + x))$;

(e) $\forall x \forall y((x + 1 = 0) \to ((y = 1) \to (x + 1 = 0)))$;

(f) $(x = y) \to ((\exists y(x = 0)) \to (\exists y(y = 0))$;

(g) $(x + y = 0) \to \forall z((x + z = 1) \to (x + y = 0))$;

(h) $(x = 0) \to (x + x \leq 1 \to x + 0 \leq 1)$;

(i) $(x \leq y) \to ((x + 1 \leq 0) \to ((0 \leq 1) \wedge (x \leq y)))$;

(j) $(x = y) \to \forall z((x + z = 0) \to (y + z = 0))$.

(k) $(x = 0) \to (x + 1 = 0 + 1)$;

(l) $(x = 0) \to \forall z(x + z = 0 + z)$.

2. Usando a Definição 6.3, justifique por que podemos incluir teoremas como novos axiomas em demonstrações. Isto é, se existe uma sequência de fórmulas em que cada uma é ou um axioma, ou um teorema, ou obtida a partir das anteriores através de uma regra de inferência, então a última fórmula dessa sequência também é um teorema.

3. Vale a recíproca do Teorema 6.20? Isto é, para todas fórmulas A e B e toda variável x a fórmula

$$((\forall x A) \to (\forall x B)) \to (\forall x(A \to B))$$

é um teorema? Se sim, prove. Se não, dê exemplos de fórmulas A e B e de um modelo que torna a fórmula acima falsa.

4. Refaça as demonstrações dos Teoremas 6.17, 6.18 e 6.19 sem utilizar outros teoremas, mas apenas os cinco esquemas de axiomas e as duas regras de inferência originais.

5. Refaça a demonstração do Teorema 6.31 com mais rigor, usando indução no grau de complexidade de fórmula (dica: chame de m o grau de complexidade de $A \leftrightarrow B$ e use indução no grau de complexidade de $C \leftrightarrow D$).

6. Sejam A um teorema de uma linguagem de primeira ordem e v uma variável que não ocorre em A. Mostre que, se substituirmos todas as ocorrências de uma variável u em A (livres ou não, e inclusive aquelas ao lado de um quantificador) pela variável v, a fórmula obtida também é um teorema.

7. Escreva cada uma das fórmulas abaixo na forma normal prenexa.

(a) $(\forall x \exists y \forall x \forall z \exists w(x + y = z \cdot w)) \wedge (x < y) \wedge (z + w = 0)$;

(b) $\forall x \exists y((y = x) \rightarrow \exists z(z + y = 0))$;

(c) $(\forall x \neg(x < 0)) \vee (\exists x(x + 1 = 0))$;

(d) $\forall x(0 < x \wedge \exists y(x + y = 1))$;

(e) $(\neg(x = 0)) \rightarrow (\forall y \exists z(y \cdot z = x))$.

Capítulo 7

Metamatemática

Já completamos o tripé da descrição da lógica de primeira ordem: descrevemos os símbolos utilizados e as regras de formação de fórmulas a partir dos símbolos (linguagem), descrevemos os significados dessas sequências de símbolos, atribuindo uma noção de verdade e falso para as fórmulas (semântica) e criamos um processo para provarmos fórmulas verdadeiras através de manipulações dos símbolos a partir de regras bem definidas (sistema de axiomas).

Agora aplicaremos a matemática – que será formalizada através da própria lógica de primeira ordem – para mostrarmos resultados *sobre* a lógica. Como esses resultados são provados na metalinguagem, a respeito das linguagens de primeira ordem, costumamos chamar de *metamatemática* a parte da matemática que estuda os teoremas sobre lógica.

Dois dos principais resultados aqui apresentados são os teoremas da correção e completude, que mostram a compatibilidade entre semântica e axiomatização, definidas nos dois capítulos anteriores. De certa forma esses teoremas nos dizem que a axiomatização que criamos cumpre bem seu papel, não provando nada mais (teorema da correção) nem menos (teorema da completude) do que as fórmulas verdadeiras.

Encerraremos o capítulo com um esboço da prova dos famosos teoremas de incompletude de Gödel. Superficialmente falando, o primeiro teorema de incompletude afirma que qualquer sistema de axiomas consistente – isto é, livre de contradições – capaz de formalizar a aritmética possui sentenças que não podem ser provadas nem refutadas. Pelo segundo teorema, tal sistema não pode provar que ele próprio é consistente.

Discutiremos alguns conceitos antes de provarmos esses teoremas.

7.1 Consequência, consistência e independência

Quando se estuda lógica e os fundamentos da matemática, é necessário prestar atenção à diferença dos conceitos de *sentenças consistentes* e *teoremas*. Essa questão surge, inclusive, em algumas questões envolvendo argumentação na linguagem natural. Vamos explicar essa diferença com uma pequena analogia, que servirá, também, para antecipar o enunciado do teorema da completude.

Suponha que alguém é acusado de um crime e é julgado em um tribunal. A discussão sobre a culpa do réu envolverá duas partes – o promotor e o advogado de defesa – e será julgada pelo júri.

Qual é o papel de cada uma dessas partes? O promotor tentará provar a culpa do réu e o advogado tentará provar sua inocência, correto? Errado! De fato, o promotor tentará provar a culpa do réu, mas o advogado, para ter sucesso na sua defesa, *não precisa* provar a inocência do réu. Lembremos que *o ônus da prova cabe ao acusador*, já que, pela lei, *todos são considerados inocentes até que se prove o contrário*. Dessa forma, o júri é instruído a, havendo *dúvida razoável* sobre a culpa do réu, inocentá-lo.

Portanto, ao advogado de defesa cabe, apenas, convencer o júri de que não há provas conclusivas da culpa do seu cliente. Isso não prova que o réu é inocente, mas que o cliente *pode ser inocente*.

O promotor, na tentativa de provar que o réu é culpado, levará ao tribunal várias evidências, e convencerá o júri de que a única explicação possível para os fatos apresentados através das evidências, é o réu ter cometido o referido crime. Uma das estratégias do advogado de defesa (quando esse não consegue refutar as evidências) é apresentar ao júri uma *teoria alternativa* ao crime. Isto é, uma história hipotética segundo a qual seu cliente é inocente e que explica todos os fatos comprovados pelas evidências apontadas pela promotoria. Ele não precisa provar que essa versão dos fatos, por ele apresentada, *é a verdadeira*, mas, sim, que essa versão *é possível*.

Fazendo uma analogia entre a lógica e o tribunal, a *teoria alternativa* corresponde a um *modelo*. Provar que o réu é culpado corresponde a dizer, na terminologia da lógica, que a culpa do réu *é um teorema*. Mostrar que *é possível* que o réu seja inocente significa dizer que a inocência do réu é *consistente* com os fatos apresentados. Isto é, *não podemos provar a culpa do réu a partir das evidências*, ou, equivalentemente, *existe uma explicação plausível para inocência do réu*.

Como acontece com o promotor, em um tribunal, que quer provar a culpa

do réu a partir dos fatos comprovados pelas evidências, também na matemática e na lógica queremos saber quando uma sentença é consequência de um conjunto de fórmulas.

Consideremos um exemplo em álgebra. Existem algumas sentenças que são conhecidas como *axiomas de corpos*, e chamamos de corpo qualquer conjunto (modelo) para os quais essas sentenças são verdadeiras. Agora, tomamos uma sentença qualquer – digamos, $\forall x(x \cdot 0 = 0)$ – e queremos descobrir se essa fórmula é um teorema da teoria dos corpos ou não. Se provarmos essa sentença a partir dos axiomas de corpos (usando os axiomas lógicos e as regras de inferência) saberemos que tal sentença será verdadeira em todo modelo que satisfaz os axiomas de corpos e dizemos que a fórmula $\forall x(x \cdot 0 = 0)$ é *consequência* dos axiomas de corpos.

Se, no entanto, quisermos provar que essa sentença não é consequência dos axiomas de corpos (e, portanto, não é teorema da teoria dos corpos), basta mostrarmos que existe *um* corpo no qual essa sentença não vale. Ou seja, basta exibirmos um modelo que satisfaz todos os axiomas de corpos mas não satisfaz $\forall x(x \cdot 0 = 0)$. Neste caso, dizemos que a negação dessa fórmula é *consistente* com a teoria dos corpos.

Na analogia jurídica, os axiomas de corpos seriam os fatos comprovados pelas evidências e testemunhos, e um modelo que satisfaz todos os axiomas de corpos mas não a sentença $\forall x(x \cdot 0 = 0)$ corresponde à teoria alternativa do crime. Neste caso, em particular, sabemos pelos cursos de álgebra que isso não ocorre: todo corpo satisfaz $\forall x(x \cdot 0 = 0)$, visto que esse é, de fato, um teorema da teoria dos corpos.

Nessa discussão podemos perceber que existem duas noções de consequência. Primeiro: a sentença $\forall x(x \cdot 0 = 0)$ pode ser provada a partir dos axiomas de corpo, utilizando o sistema de axiomas da lógica de primeira ordem. Segundo: todo modelo que satisfaz os axiomas de corpo satisfaz, também, a fórmula $\forall x(x \cdot 0 = 0)$. Se a axiomatização da lógica de primeira ordem funcionar como esperamos, esses dois conceitos precisam ser equivalentes, e é sobre isso que discutiremos a seguir.

Estabelecemos a seguinte notação: se $\mathcal{M}$ é um modelo e Γ é um conjunto de fórmulas da mesma linguagem, denotaremos por $\mathcal{M} \models \Gamma$ quando $\mathcal{M} \models A$, para toda fórmula A pertencente a Γ.

Definição 7.1. Dizemos que A é *consequência semântica* de Γ em uma linguagem L se, para todo modelo $\mathcal{M}$ da linguagem, se $\mathcal{M} \models \Gamma$ então $\mathcal{M} \models A$. Denotamos $\Gamma \models_L A$ quando A for consequência semântica de Γ na lingua-

gem L. Quando estiver claro no contexto qual é a linguagem L, escrevemos apenas $\Gamma \models A$.

O subescrito L é necessário *a priori* na definição, pois precisamos nos certificar de que tomamos um modelo da linguagem fixada. Porém, veremos mais à frente que isso não tem importância. Quando lemos $\Gamma \models A$, consideramos a linguagem que contém todos os símbolos que ocorrem nas fórmulas em Γ e na fórmula A. A sintaxe da linguagem permite distinguirmos o tipo de cada símbolo (funcional, relacional ou constante, e quantos parâmetros possui). Eventuais símbolos adicionais na linguagem não alteram o conceito de consequência semântica. Ou seja, se L é uma linguagem à qual as fórmulas em $\Gamma \cup \{A\}$ pertencem, e L' é uma linguagem que *estende* L – isto é, que contém todos os símbolos de L e mais alguns – então $\Gamma \models_L A$ se, e somente se, $\Gamma \models_{L'} A$. Deixamos a demonstração desse fato como exercício ao leitor (essa demonstração se assemelha à do Lema 7.16).

Observe que uma fórmula ser consequência semântica do conjunto vazio significa ser verdadeira em todo modelo. De fato, pelo usual argumento de vacuidade sempre temos $\mathcal{M} \models \emptyset$, para qualquer modelo $\mathcal{M}$, pois o conjunto vazio não tem nenhuma fórmula que atesta o contrário. Portanto, $\emptyset \models A$ significa que para todo modelo $\mathcal{M}$ vale $\mathcal{M} \models A$.

Uma terceira observação, bastante crucial, diz respeito do papel das valorações na definição de consequência semântica. Destrinchando essa definição, incorporando a definição de validade em um modelo, temos o seguinte: $\Gamma \models A$ se, e somente se, para todo modelo $\mathcal{M}$, se, *para toda valoração* σ temos $(\mathcal{M}, \sigma) \models \Gamma$, então *para toda valoração* θ temos $(\mathcal{M}, \theta) \models A$. Usamos, na frase anterior, propositalmente símbolos diferentes para salientar que a primeira valoração σ pode não ser a mesma que θ. O leitor poderia confundir essa definição com a seguinte, que possui uma sutil diferença: *para todo modelo* $\mathcal{M}$ e *para toda valoração* σ, *se* $(\mathcal{M}, \sigma) \models \Gamma$ *então* $(\mathcal{M}, \sigma) \models A$.

Vamos dar um exemplo para esclarecer a diferença das duas possíveis definições. A fórmula $0 = 1$ é consequência semântica da fórmula $x = 1$ (ou melhor, *do conjunto de fórmulas* $\{x = 1\}$). De fato, se $\mathcal{M} \models x = 1$, isso significa $\sigma(x) = 1^{\mathcal{M}}$ *para toda* valoração σ. Em particular, $1^{\mathcal{M}}$ é o único elemento do domínio de $\mathcal{M}$. Portanto, $\sigma^*(0) = \sigma^*(1)$ para toda valoração σ, o que implica que $\mathcal{M} \models 0 = 1$.

Por outro lado, na "definição alternativa" $0 = 1$ não seria consequência semântica de $x = 1$, pois $(\mathcal{M}, \sigma) \models x = 1$ não implica $(\mathcal{M}, \sigma) \models 0 = 1$. Podemos ter que essa valoração σ, em particular, atribui a x o valor $1^{\mathcal{M}}$, que

pode ser diferente de $0^{\mathcal{M}}$.

Notemos, portanto, que a definição de consequência semântica foi feita de modo a "validar" a regra de inferência da generalização. Isto é, se $\Gamma \models A$, então $\Gamma \models \forall x A$.

A próxima noção de consequência é aquela em que provamos alguma fórmula a partir de outras (por exemplo, quando provamos um teorema de álgebra a partir dos axiomas de corpo), conforme a definição a seguir.

Definição 7.2. Em uma linguagem de primeira ordem L, sejam A uma fórmula e Γ um conjunto de fórmulas. Dizemos que A é *consequência sintática* de Γ (e denotaremos por $\Gamma \vdash A$) se A pode ser provada a partir de Γ. Isto é, se existe uma sequência de fórmulas, $(A_i)_{0 \leq i \leq n}$ tal que A_n é a fórmula A e, para cada $i \leq n$, pelo menos uma das seguintes asserções é verdadeira:

- A_i é um axioma;
- A_i pertence a Γ;
- Existem $j < i$ e uma variável x tal que A_i é a fórmula $\forall x A_j$;
- Existem $j, k < i$ tal que A_k é a fórmula $A_j \to A_i$.

O principal resultado deste capítulo será provar que consequência sintática é equivalente a consequência semântica. Isso significa que nosso sistema de axiomas é *correto* – isto é, só prova afirmações verdadeiras - e *completo* – isto é, prova todas as afirmações verdadeiras.

Definição 7.3. Um conjunto Γ de fórmulas é *consistente* se $\neg(x = x)$ não é consequência sintática de Γ.

Uma fórmula A é *consistente* com um conjunto de fórmulas Γ se $\Gamma \cup \{A\}$ é consistente.

Uma sentença A é *indecidível* em relação a um conjunto de fórmulas Γ se A e $\neg A$ são consistentes com Γ.

Uma fórmula A é *relativamente consistente* com um conjunto de fórmulas Γ se Γ é inconsistente ou $\Gamma \cup \{A\}$ é consistente.

Uma sentença A é *independente* de um conjunto de fórmulas Γ se A e $\neg A$ são relativamente consistentes com Γ.

Notemos que, se um conjunto Γ de fórmulas é inconsistente, não apenas a fórmula $\neg(x = x)$ é consequência sintática de Γ, mas todas as fórmulas

da linguagem. De fato, $(x = x) \to ((\neg(x = x)) \to A)$ é uma instância de tautologia, qualquer que seja a fórmula A. Se $\neg(x = x)$ pode ser provada a partir de Γ, usando o axioma $x = x$ e a regra modus ponens duas vezes provamos A.

Por outro lado, se provarmos alguma fórmula e sua negação a partir de Γ, provamos qualquer outra fórmula, e teremos Γ inconsistente.

Após mostrarmos a equivalência entre consequências sintática e semântica mostraremos que um conjunto Γ de fórmulas é consistente se, e somente se, existe um modelo $\mathcal{M}$ tal que $\mathcal{M} \models \Gamma$.

As definições de consistência relativa e independência se justificam por causa de um dos teoremas de incompletude de Gödel, que afirma que um sistema (em certas condições) não pode provar sua própria consistência. Assim, não conseguimos provar que $\Gamma \cup \{A\}$ é consistente por não sabermos a respeito da consistência do próprio Γ. Mas, se A é relativamente consistente com Γ, sabemos, ao menos, que, se existir alguma inconsistência em $\Gamma \cup \{A\}$, já existia anteriormente em Γ. É o que acontece, por exemplo, com o axioma da escolha em relação à teoria dos conjuntos. Não podemos garantir que a teoria dos conjuntos é consistente, mas existe uma demonstração de que o axioma da escolha é relativamente consistente com os outros axiomas da teoria dos conjuntos de Zermelo e Fraenkel. Portanto, se há alguma inconsistência na teoria dos conjuntos com o axioma da escolha, essa inconsistência já existe mesmo se tirarmos o axioma da escolha. Não é dele "a culpa" por uma eventual contradição que encontremos nos axiomas de ZFC.

Encerramos esta seção mostrando o teorema da compacidade, que, apesar de ser um resultado simples, é um dos mais importantes, no estudo de lógica de primeira ordem, e segue do fato das demonstrações serem finitas.

Teorema 7.4 (Compacidade)**.** *Seja Γ um conjunto de fórmulas e suponha que todo subconjunto finito de Γ é consistente. Então Γ é consistente.*

Demonstração: Suponha que Γ seja inconsistente. Seja $(A_i)_{i \leq n}$ uma demonstração de $\neg(x = x)$. Considere Γ_0 o conjunto das fórmulas A_i tais que $i \leq n$ e $A_i \in \Gamma$. Temos que Γ_0 é finito e $A_i \in \Gamma_0$ sempre que $A_i \in \Gamma$. Logo, $(A_i)_{i \leq n}$ também é uma demonstração de $\neg(x = x)$ a partir de Γ_0, contradizendo que Γ_0 é consistente. ■

Na Seção 7.4 discutiremos uma das mais célebres aplicações do teorema da compacidade. Mas, para isso, precisamos, primeiro, dos teoremas da correção e completude.

7.2 Teorema da correção

A escolha dos axiomas e regras de inferência do sistema de axiomas da lógica de primeira ordem não foi feita por acaso. O sistema deve ser compatível com a semântica, no sentido de que deve provar *apenas* as fórmulas verdadeiras e – o que é mais difícil – ser capaz de provar *qualquer* fórmula verdadeira. Ou seja, *o sistema de axiomas foi definido de modo que os conceitos de consequência semântica e sintática sejam equivalentes*. Como discutimos na Seção 7.1, se provamos uma fórmula A a partir dos axiomas de corpo, esperamos que todo corpo (isto é, um modelo que satisfaz os axiomas de corpo) satisfaça a fórmula A. Reciprocamente, se em todo corpo vale a fórmula A esperamos que exista uma demonstração de A a partir dos axiomas de corpo. Se uma dessas afirmações falhar, há algo errado com a nossa concepção de demonstração e precisamos revê-la. Os teoremas da correção e completude garantem que a axiomatização da lógica funciona como esperado. O da correção mostra que consequência sintática implica consequência semântica, e da completude mostra que consequência semântica implica consequência sintática.

Provaremos, nesta seção, o teorema da correção. Antes, precisamos de alguns lemas, sendo que cada um servirá para provar a satisfatibilidade de um esquema de axiomas em um modelo arbitrário. As demonstrações dos lemas que se seguem apresentam uma certa dificuldade técnica e precisam ser estudadas com bastante calma, pois servirão para compreendermos melhor a semântica da lógica de primeira ordem e o conceito de substituição boa de variáveis.

Lema 7.5. *Sejam x uma variável e A uma fórmula que não possui ocorrência livre de x. Sejam $\mathcal{M}$ um modelo e σ e θ valorações tais que $\sigma(y) = \theta(y)$, para toda variável y diferente de x. Então $(\mathcal{M}, \sigma) \models A$ se, e somente se, $(\mathcal{M}, \theta) \models A$.*

Demonstração: Consequência imediata do Teorema 5.3, pois as duas valorações são iguais para todas as variáveis diferentes de x. Como, por hipótese, x não ocorre livre em A, em particular σ e θ são iguais em todas as variáveis que ocorrem livres em A. ■

Lema 7.6. *Sejam x uma variável, t um termo e A uma fórmula em que toda ocorrência de x é livre para t. Sejam $\mathcal{M}$ um modelo e σ e θ valorações tais*

que $\theta(x) = \sigma^*(t)$ e $\sigma(y) = \theta(y)$, para toda variável y diferente de x. Então $(\mathcal{M}, \theta) \models A$ se, e somente se, $(\mathcal{M}, \sigma) \models [A]^t_x$.

Demonstração: Fixando x, t e $\mathcal{M}$ como no enunciado, mostraremos o lema por indução na complexidade da fórmula A. O lema é trivial para as fórmulas atômicas, pois $\theta(x) = \sigma^*(t)$ implica que $\theta^*(s) = \sigma^*([s]^t_x)$. Como $[\neg A]^t_x = \neg[A]^t_x$ e $[A \wedge B]^t_x = [A]^t_x \wedge [B]^t_x$, também é fácil verificar que, se o lema vale para A e B, vale para $\neg A$ e $A \wedge B$.

Assumindo que o lema é verdadeiro para uma fórmula A, provaremos que é verdadeiro para a fórmula $\forall x A$ e as do tipo $\forall y A$, onde y não é a variável x.

O primeiro caso é imediato do Lema 7.5, uma vez que $[\forall x A]^t_x$ é a própria fórmula $\forall x A$ – pois a substituição só é feita nas ocorrências livres – e as valorações σ e θ coincidem nas variáveis diferentes de x.

Considere y uma variável diferente de x e suponha que o lema é verdadeiro para uma fórmula A. Suponha que $(\mathcal{M}, \theta) \models \forall y A$ e que σ é uma valoração tal que $\sigma(z) = \theta(z)$, para todo z diferente de x, e que $\sigma^*(t) = \theta(x)$. Mostraremos que

$$(\mathcal{M}, \sigma) \models \forall y [A]^t_x, \tag{1}$$

quando as hipóteses do lema forem satisfeitas.

Analisemos o caso em que y ocorre no termo t. Se x não ocorre livre em A, a fórmula $\forall y [A]^t_x$ é a própria fórmula $\forall y A$ e (1) segue da hipótese e da definição de satisfatibilidade para o quantificador universal. Se x ocorre livre em A, então essa ocorrência não é livre para t em $\forall y A$, visto que x está no escopo de y e y ocorre em t. Assim, por contradizer as hipóteses do lema, esse se torna automaticamente verdadeiro para $\forall y A$.

Podemos, portanto, assumir que y não ocorre no termo t.

Seja σ_0 uma valoração tal que $\sigma_0(z) = \sigma(z)$, para toda variável z diferente de y. Defina $\theta_0(y) = \sigma_0(y)$ e $\theta_0(z) = \theta(z)$, para todo z diferente de y. Em particular, $\theta_0(x) = \theta(x) = \sigma^*(t)$. Como y não ocorre em t, $\sigma^*(t) = \sigma^*_0(t)$. Por outro lado, temos $(\mathcal{M}, \theta_0) \models A$. Portanto, pela hipótese indutiva, $(\mathcal{M}, \sigma_0) \models [A]^t_x$, provando que $(\mathcal{M}, \sigma) \models \forall y [A]^t_x$.

Agora assumimos que $(\mathcal{M}, \sigma) \models \forall y [A]^t_x$ e provaremos que $(\mathcal{M}, \theta) \models \forall y A$. Seja θ_0 uma valoração tal que $\theta_0(z) = \theta(z)$, para toda variável z diferente de y. Defina uma valoração σ_0 tal que $\sigma_0(y) = \theta_0(y)$ e $\sigma_0(z) = \theta(z)$, para as demais variáveis z diferentes de y. Analogamente ao que foi provado na recíproca,

temos que $(\mathcal{M}, \sigma_0) \models [A]^t_x$ e, pela hipótese de indução, $(\mathcal{M}, \theta_0) \models A$, de onde concluímos que $(\mathcal{M}, \theta) \models \forall y A$. ■

Lema 7.7. *Sejam x e y variáveis e A e B fórmulas tais que B é obtida a partir de uma substituição de x por y em uma ocorrência em A livre para x e y. Sejam $\mathcal{M}$ um modelo e σ e uma valoração tais que $\sigma(x) = \sigma(y)$. Então $(\mathcal{M}, \sigma) \models A$ se, e somente se, $(\mathcal{M}, \sigma) \models B$.*

Demonstração: Fixados o modelo $\mathcal{M}$ e as variáveis x e y, provaremos o lema por indução na complexidade de A.

Se s é um termo obtido pela substituição de uma variável x por y em um termo t, e σ uma valoração tal que $\sigma(x) = \sigma(y)$, é fácil provar, por indução na complexidade dos termos, que $\sigma^*(s) = \sigma^*(t)$. Disso segue que o lema é verdadeiro para fórmulas atômicas. O passo indutivo também é trivial para os conectivos $\neg$ e $\wedge$.

Suponha que a hipótese indutiva vale para uma fórmula A. Mostraremos que o lema é verdadeiro para as fórmulas do tipo $\forall z A$. Se z é a variável x ou y o lema é verdadeiro, visto que todas as ocorrências das variáveis em A estão no escopo de z. Assumimos, portanto, que z não é a variável x nem a variável y, e supomos que $(\mathcal{M}, \sigma) \models \forall z A$. Mostraremos que $(\mathcal{M}, \sigma) \models C$, onde C é obtida a partir de uma substituição boa de x por y em $\forall z A$.

Está claro que C é da forma $\forall z B$, onde B é obtida a partir de uma substituição boa de x por y em A. Seja θ uma valoração tal que $\theta(v) = \sigma(v)$, para toda variável v diferente de z. Temos que $(\mathcal{M}, \theta) \models A$. Como x e y são diferentes de v, temos que $\theta(x) = \sigma(x) = \sigma(y) = \theta(y)$. Portanto, pela hipótese indutiva, $(\mathcal{M}, \sigma) \models B$, como queríamos. A recíproca é análoga. ■

Teorema 7.8 (da Correção)**.** *Sejam $\boldsymbol{L}$ uma linguagem de primeira ordem, Γ um conjunto de fórmulas de $\boldsymbol{L}$ e A uma fórmula de $\boldsymbol{L}$. Se $\Gamma \vdash A$ então $\Gamma \models A$.*

Demonstração: Provaremos, inicialmente, que todos os axiomas são verdadeiros em qualquer modelo. Isso claramente vale para as instâncias de tautologia e fórmulas do tipo $x = x$. Analisaremos os axiomas dos esquemas A2, A3 e A5.

Suponha que existem um modelo $\mathcal{M}$, uma variável x, uma fórmula B e uma fórmula A que não possui x como variável livre tais que $\mathcal{M}$ não satisfaz

$(\forall x(A \to B)) \to (A \to (\forall xB))$. Isso significa que existe uma valoração σ tal que

$$(\mathcal{M}, \sigma) \models (\forall x(A \to B)) \wedge A \wedge \neg\forall xB.$$

Como $(\mathcal{M}, \sigma) \models \neg\forall xB$, existe uma valoração θ tal que $\theta(y) = \sigma(y)$, para toda variável y diferente de x, e $(\mathcal{M}, \theta) \models \neg B$. Como x não ocorre livre em A, pelo Lema 7.5 temos que $(\mathcal{M}, \theta) \models A$. Mas, como θ coincide com σ em todas as variáveis diferentes de x e $(\mathcal{M}, \sigma) \models \forall x(A \to B)$, temos $(\mathcal{M}, \theta) \models A \to B$, contradizendo que A e $\neg B$ são verdadeiros nesse modelo.

Agora consideremos um axioma do esquema A3. Sejam A uma fórmula, t um termo e x uma variável que não possui ocorrência em A no escopo de alguma variável que ocorre em t. Sejam $\mathcal{M}$ um modelo e σ uma valoração. Suponhamos, por absurdo, que $\mathcal{M}$ não satisfaz $(\forall xA) \to [A]^t_x$ mediante a valoração σ. Isso significa que

$$(\mathcal{M}, \sigma) \models (\forall xA) \wedge \neg[A]^t_x. \tag{1}$$

Seja θ a valoração tal que $\theta(x) = \sigma^*(t)$ e $\theta(y) = \sigma(y)$, para toda variável y diferente de x. Temos que $(\mathcal{M}, \theta) \models A$, o que, pelo Lema 7.6, implica que $(\mathcal{M}, \sigma) \models [A]^t_x$, contradizendo (1).

A validade dos axiomas do esquema A5 segue facilmente do Lema 7.7.

Uma vez provada a validade dos axiomas, concluímos a demonstração do teorema da correção por indução no comprimento das demonstrações do teorema. Isto é, suponhamos que o teorema é verdadeiro para as fórmulas que possuem demonstrações com até n fórmulas. Sejam A um teorema e $(A_i)_{0 \leq i \leq n}$ uma sequência de fórmulas como na Definição 7.2. Seja $\mathcal{M}$ um modelo que satisfaz todas as fórmulas que pertencem a Γ. Pela hipótese de indução todas as fórmulas A_i, para $i < n$ são válidas em $\mathcal{M}$. Para provarmos que $\mathcal{M}$ satisfaz A_n – que é a fórmula A – consideraremos os quatro casos da Definição 7.2.

- Se A_n pertence a Γ então $\mathcal{M} \models A_n$, pela hipótese.
- Se A_n é um axioma, provamos que $\mathcal{M} \models A_n$.
- Se existem $i < n$ e x variável tais que A_n é a fórmula $\forall xA_i$ então, pela hipótese indutiva, $\mathcal{M} \models A_i$. Isso significa que, para toda valoração σ temos $(\mathcal{M}, \sigma) \models A_i$. Logo, $\mathcal{M} \models \forall xA_i$.
- Se existem $i, j < n$ tais que A_j é a fórmula $A_i \to A_n$, como $\mathcal{M} \models A_i$ e $\mathcal{M} \models A_j$, temos $\mathcal{M} \models A_n$.

■

Corolário 7.9. *Sejam Γ um conjunto de fórmulas de uma linguagem de primeira ordem e $\mathcal{M}$ um modelo para a mesma linguagem tal que $\mathcal{M} \models \Gamma$. Então Γ é consistente.*

Demonstração: Se Γ é inconsistente, $\Gamma \vdash \neg(x = x)$ e, pelo Teorema 7.8, $\Gamma \models \neg(x = x)$. Quando $\mathcal{M} \models \Gamma$ isso implica que $\mathcal{M} \models \neg(x = x)$, contradizendo que $\mathcal{M} \models x = x$. ■

7.3 Teorema da completude

Mostraremos nesta seção um dos resultados mais importantes da lógica de primeira ordem: toda fórmula verdadeira pode ser provada. Ou seja, nosso sistema de axiomas não apenas é *correto*, provando apenas fórmulas verdadeiras, como também é *completo*, provando *todas* as fórmulas verdadeiras. Antes desenvolveremos uma série de resultados, começando com o teorema da dedução.

Teorema 7.10 (da Dedução)**.** *Sejam L uma linguagem, Γ um conjunto de fórmulas, A uma sentença e B uma fórmula. Então $\Gamma \cup \{A\} \vdash B$ se, e somente se, $\Gamma \vdash A \to B$.*

Demonstração: Provaremos que $\Gamma \cup \{A\} \vdash B$ implica $\Gamma \vdash A \to B$. A outra implicação segue imediatamente da regra modus ponens.

Primeiro mostraremos que podemos assumir, sem perda de generalidade, que Γ é um conjunto de sentenças. Para isso, definimos o *fecho universal* de uma fórmula F a fórmula $\forall x_1 \ldots \forall x_n F$, onde $x_1, \ldots, x_n$ são as variáveis livres de F. Pelo esquema de axiomas A3 e por modus ponens, se o fecho universal de F pertence a Γ então F é consequência sintática de Γ. Por outro lado, se F pertence a Γ, pela regra da generalização temos que o fecho universal de F é consequência sintática de Γ. Assim, se tomarmos Γ' o conjunto dos fechos universais das fórmulas que pertencem a Γ, uma fórmula é consequência sintática de Γ' se, e somente se, o é de Γ. Portanto, tomando Γ' no lugar de Γ, assumimos que todas as fórmulas de Γ não possuem variáveis livres.

Fixados L e Γ, provaremos o teorema por indução no comprimento da demonstração. Isto é, nossa hipótese indutiva diz que, para toda sentença A' e fórmula B', e todo $m < n$, se existe uma sequência de fórmulas $(A'_i)_{i \leq m}$ que é

uma demonstração de B' a partir de $\Gamma \cup \{A'\}$, então existe uma demonstração de $A' \to B'$ a partir de Γ.

Suponha que B é uma fórmula, A uma sentença e $(A_i)_{i \leq n}$ uma demonstração de B a partir de $\Gamma \cup \{A\}$. Temos três possibilidades. No primeiro caso, B é um axioma ou um elemento de $\Gamma \cup \{A\}$. Se B é um axioma ou pertence a Γ, como $B \to (A \to B)$ é uma instância de tautologia, por modus ponens deduzimos $A \to B$ a partir de Γ. Se B é a própria fórmula A, então $A \to B$ é a fórmula $A \to A$, que é uma instância de tautologia.

No segundo caso, B é obtida a partir de modus ponens. Isso significa que existem $i, j < n$ tais que A_i é a fórmula $A_j \to B$. Pela hipótese indutiva, $\Gamma \vdash A \to A_j$ e $\Gamma \vdash A \to (A_j \to B)$. Por outro lado, a seguinte fórmula é uma instância de tautologia:

$$(A \to A_j) \to ((A \to (A_j \to B)) \to (A \to B)).$$

Logo, usando modus ponens duas vezes, obtemos $\Gamma \vdash A \to B$.

No terceiro caso assumimos que B é obtida a partir da regra da generalização. Sejam $i < n$ e x variável tal que B é a fórmula $\forall x A_i$. Pela hipótese indutiva temos $\Gamma \vdash A \to A_i$. Pela regra da generalização temos $\Gamma \vdash \forall x(A \to A_i)$. Como A não possui variáveis livres, pelo esquema $A2$ e por modus ponens temos $\Gamma \vdash A \to (\forall x A_i)$, como queríamos. ■

Corolário 7.11. *Se Γ é um conjunto consistente de sentenças de uma linguagem de primeira ordem e A é uma sentença dessa linguagem, então $\Gamma \cup \{A\}$ ou $\Gamma \cup \{\neg A\}$ é consistente.*

Demonstração: Se $\Gamma \cup \{A\}$ e $\Gamma \cup \{\neg A\}$ são ambos inconsistentes, então $\Gamma \cup \{A\} \vdash \neg(x = x)$ e $\Gamma \cup \{\neg A\} \vdash \neg(x = x)$. Pelo Teorema 7.10 temos $\Gamma \vdash A \to (\neg(x = x))$ e $\Gamma \vdash (\neg A) \to (\neg(x = x))$. Logo, pelo Teorema 6.13, temos $\Gamma \vdash \neg(x = x)$. Portanto, Γ é inconsistente. ■

Corolário 7.12. *Se Γ é um conjunto consistente de sentenças de uma linguagem de primeira ordem e A é uma sentença dessa linguagem, então $\Gamma \cup \{A\}$ é consistente se, e somente se, $\neg A$ não é consequência sintática de Γ.*

Demonstração: Se $\Gamma \cup \{A\}$ é consistente então é trivial que $\neg A$ não pode ser consequência sintática de Γ. Suponha que $\Gamma \cup \{A\}$ é inconsistente. Isto é, $\Gamma \cup \{A\} \vdash \neg(x = x)$. Pelo teorema da dedução $\Gamma \vdash A \to (\neg(x = x))$. Pelo teorema 6.12 temos que $\Gamma \vdash (x = x) \to \neg A$. Usando o axioma A4 e modus ponens concluímos que $\Gamma \vdash \neg A$. ■

Definição 7.13. Dizemos que um conjunto Δ de sentenças de uma linguagem de primeira ordem $\mathbf{L}$ é *maximalmente consistente* se é consistente e, para todo conjunto Λ de sentenças de $\mathbf{L}$, se Λ é consistente e $\Delta \subseteq \Lambda$ então $\Delta = \Lambda$.

Lema 7.14. *Seja Δ um conjunto maximalmente consistente de sentenças de uma linguagem de primeira ordem.*

(a) *Para toda sentença A da linguagem L, ou $A \in \Delta$ ou $\neg A \in \Delta$, e não ambos.*

(b) *Duas sentenças A e B pertencem a Δ se, e somente se, $A \wedge B$ pertence a Δ.*

(c) *Para toda sentença A da linguagem L, temos $\Delta \vdash A$ se, e somente se, $A \in \Delta$.*

Demonstração: Pelo Corolário 7.11 temos que $\Delta \cup \{A\}$ ou $\Delta \cup \{\neg A\}$ é consistente. Como Δ não está contido propriamente em nenhum conjunto consistente, então ou A ou $\neg A$ pertence a Δ. Porém, como $A \to ((\neg A) \to (\neg(x = x)))$ é uma instância de tautologia, se A e $\neg A$ pertencessem a Δ teríamos Δ inconsistente. Provamos a parte (a) do lema.

Se $A \in \Delta$ obviamente temos $\Delta \vdash A$. Reciprocamente, se $\Delta \vdash A$ e $A \notin \Delta$, pela parte (a) temos $\neg A \in \Delta$. Repetindo o argumento do parágrafo acima disso segue que Δ é inconsistente. Provamos, assim, a parte (c) do teorema. A parte (b) segue imediatamente de (c). ■

Lema 7.15. *Se Γ é um conjunto consistente de sentenças de uma linguagem $\boldsymbol{L}$, existe um conjunto maximalmente consistente de sentenças de $\boldsymbol{L}$ que contém o conjunto Γ.*

Demonstração: Seja $(A_n)_{n\in\mathbb{N}}$ uma enumeração de todas as sentenças da linguagem $\mathbf{L}$ [1].

Definimos $\Delta_0 = \Gamma$. Uma vez definido Δ_n, definimos $\Delta_{n+1} = \Delta_n \cup \{A_n\}$, se $\Delta_n \cup \{A_n\}$ é consistente, e $\Delta_{n+1} = \Delta_n \cup \{\neg A_n\}$, caso contrário. Por indução e pelo Corolário 7.11 temos que Δ_n é consistente, para todo n. Seja Δ a união de Δ_n, para $n \in \mathbb{N}$. Isto é, Δ é o conjunto de todas as fórmulas

[1] A existência dessa enumeração será melhor justificada na Seção 7.5, quando falarmos da numeração de Gödel

que pertencem a Δ_n, para *algum* n. Pelo teorema da compacidade, Δ é consistente. Mostraremos que Δ é maximalmente consistente.

Suponhamos que existe Δ' um conjunto consistente de sentenças de $\mathbf{L}$ tal que $\Delta \subseteq \Delta'$ e existe uma sentença $A \in \Delta'$ que não pertence a Δ. Como A é alguma sentença A_n, temos, então, que $\neg A \in \Delta$ e, portanto, $\neg A \in \Delta'$, contradizendo que Δ' é consistente. ■

O teorema da completude será um corolário do teorema de Henkin, que prova que todo conjunto consistente de sentenças é validado por algum modelo. A ideia central da prova de Henkin é adicionar à linguagem constantes que "testemunham" a validade de sentenças existenciais. O domínio do modelo que construímos para Γ é o conjunto dessas constantes, quocientado por uma relação de equivalência adequada. A interpretação dos símbolos relacionais e funcionais será definida a partir de um conjunto maximalmente consistente que estende Γ.

Lema 7.16. *Seja Γ um conjunto consistente de sentenças de uma linguagem de primeira ordem $\boldsymbol{L}$. Sejam A uma fórmula de $\boldsymbol{L}$ com uma variável livre x e c uma constante da linguagem que não ocorre em A nem em qualquer fórmula que pertence a Γ. Então o conjunto $\Gamma \cup \{(\exists x A) \to [A]^c_x\}$ é consistente.*

Demonstração: Suponha que o conjunto $\Gamma \cup \{(\exists x A) \to [A]^c_x\}$ não é consistente. Pelo Corolário 7.12 temos que $\Gamma \vdash \neg((\exists x A) \to [A]^c_x)$. Logo, $\Gamma \vdash (\exists x(A)) \wedge (\neg[A]^c_x)$. Em particular, $\Gamma \vdash \exists x A$ e $\Gamma \vdash \neg[A]^c_x$.

Tome y uma variável que não ocorre em nenhuma fórmula utilizada na demonstração de $\neg[A]^c_x$. Seja $(A_i)_{i\leq n}$ uma demonstração de $\neg[A]^c_x$. Considere B_i a fórmula obtida pela substituição de todas as ocorrências de c por y, em A_i. Notemos que $(B_i)_{i\leq n}$ é uma demonstração de $\neg[A]^y_x$. De fato, se A_i é um elemento de Γ, por hipótese A_i não possui ocorrência de c e, portanto, B_i é igual a A_i. Se A_i é um axioma, como y não ocorre em A_i, então B_i também é um axioma (verifique isso para cada esquema de axiomas). Se A_i é obtida a partir de modus ponens ou generalização, também é fácil verificar que B_i é obtida a partir de $(B_j)_{j<i}$.

Concluímos que $\Gamma \vdash \neg[A]^y_x$. Pela regra da generalização temos $\Gamma \vdash \forall y(\neg[A]^y_x)$. Observamos que nenhuma ocorrência de y em $[A]^y_x$ está no escopo de x ou de y, uma vez que as primeiras substituições de x por y só foram feitas nas ocorrências livres de x. Logo, $[[A]^y_x]^x_y]$ é a fórmula A. Portanto, usando o esquema de axiomas A3 e modus ponens, concluímos que $\Gamma \vdash \neg A$. Pela

regra da generalização temos que $\Gamma \vdash \forall x(\neg A)$. Mas $\forall x(\neg A)$ é equivalente a $\neg\exists xA$, contradizendo a consistência de Γ, já que $\Gamma \vdash \exists xA$.

■

Teorema 7.17 (Henkin)**.** *Se Γ é um conjunto consistente de sentenças de uma linguagem de primeira ordem $\boldsymbol{L}$, existe um modelo $\mathcal{M}$ da linguagem $\boldsymbol{L}$ tal que $\mathcal{M} \models \Gamma$.*

Demonstração: Considere **L'** a linguagem **L** acrescida de uma quantidade infinita enumerável de constantes, que serão indicadas por $c_0, c_1, \ldots, c_n, \ldots$. Seja $(A_n)_{n\in\mathbb{N}}$ uma enumeração de todas as sentenças da linguagem estendida **L'** que são da forma $\exists xA$.

Repetindo o argumento apresentado na demonstração do Lema 7.16, verificamos que Γ também é um conjunto consistente de fórmulas da linguagem **L'**.

Definimos $\Gamma_0 = \Gamma$. Assumimos que temos definido Γ_n definimos

$$\Gamma_{n+1} = \Gamma_n \cup \{(\exists xA) \to [A]_x^{c_i}\},$$

onde $\exists xA$ é a sentença A_n e i é o menor número natural tal que c_i não ocorre nas fórmulas A_j, para $j \leq n$.

O Lema 7.16 garante que cada Γ_n é consistente. Portanto, pelo teorema da compacidade, o conjunto $\overline{\Gamma} = \bigcup_{n\in\mathbb{N}} \Gamma_n$ é consistente.

Pelo Lema 7.15 existe um conjunto maximalmente consistente Δ de sentenças de **L'** que contém $\overline{\Gamma}$.

Seja S o conjunto das constantes $(c_i)_{i\in\mathbb{N}}$. Em S definimos a relação $\sim$ como $c_i \sim c_j$ se, e somente se, a fórmula $c_i = c_j$ pertence a Δ. O Lema 7.14, parte (c), e os teoremas 6.17, 6.18 e 6.19 garantem que $\sim$ é uma relação de equivalência (veja a Seção 3.5). Seja $D = S/\sim$. Isto é, D é o conjunto das classes de equivalência $[c_i]$, onde $[c_i] = \{c_j : c_j \sim c_i\}$. Pelo Teorema 3.14, $[c_i] = [c_j]$ se, e somente se, $c_i \sim c_j$.

Definiremos um modelo $\mathcal{M}$. O domínio de $\mathcal{M}$ será o conjunto D. Se R é uma relação n-ária da linguagem **L**, definimos a interpretação de R no modelo $\mathcal{M}$ da seguinte forma:

$$([c_{i_1}], \ldots, [c_{i_n}]) \in R^{\mathcal{M}} \text{ se, e somente se, } R(c_{i_1}, \ldots, c_{i_n}) \in \Delta$$

Precisamos verificar que essa definição independe da escolha dos representantes. Isto é, $c_{i_k} \sim c_{j_k}$ implica que $R(c_{i_1}, \ldots, c_{i_n}) \in \Delta$ se, e somente se, $R(c_{j_1}, \ldots, c_{j_n}) \in \Delta$. Mas essa afirmação é verdadeira, pelo Teorema 6.15.

Seja F um símbolo funcional n-ário. Vamos definir $F^{\mathcal{M}}([c_{i_1}], \ldots, [c_{i_n}])$. Mostramos no Teorema 6.27 que $\forall x \exists y (y = x)$ é um teorema da lógica de primeira ordem. Usando modus ponens e o esquema A3 para o termo $F(c_{i_1}, \ldots, c_{i_n})$, concluímos que a seguinte sentença é um teorema:

$$\exists y (y = F(c_{i_1}, \ldots, c_{i_n})).$$

Pela construção de Δ, existe uma constante c_i tal que a sentença

$$(\exists y (y = F(c_{i_1}, \ldots, c_{i_n})) \rightarrow (c_i = F(c_{i_1}, \ldots, c_{i_n}))$$

pertence a Δ.

Assim, por modus ponens e pelo Lema 7.14, parte (c), concluímos que $c_i = F(c_{i_1}, \ldots, c_{i_n})$ pertence a Δ. Se existir outra constante c_j tal que $c_j = F(c_{i_1}, \ldots, c_{i_n})$ pertence a Δ, é fácil provar que $c_i = c_j$ pertence a Δ e, portanto, $[c_i] = [c_j]$. Portanto, podemos definir

$$F^{\mathcal{M}}([c_{i_1}], \ldots, [c_{i_n}]) = [c_i].$$

A demonstração de que essa definição independe da escolha dos representantes das classes de equipolência é análoga ao caso dos símbolos relacionais.

Falta interpretarmos as constantes. Definimos $c_n^{\mathcal{M}} = [c_n]$, para as constantes novas. Para as constantes da linguagem $\mathbf{L}$, definimos $c = [c_n]$, onde $c = c_n$ pertence a Δ. Analogamente ao que mostramos para símbolos funcionais, podemos verificar que existe c_n tal que $c = c_n$ pertence a Δ, e também que, se $c = c_n$ e $c = c_m$ ambos pertencem a Δ, então $[c_n] = [c_m]$.

Isso conclui a definição do modelo $\mathcal{M}$. Sejam σ uma valoração e t um termo da linguagem $\mathbf{L}'$ que não possui variáveis. Provaremos, por indução na complexidade do termo, que

(1) $$\sigma^*(t) = [c_k] \text{ se, e somente se } (t = c_k) \in \Delta$$

Se t é constante – seja da linguagem $\mathbf{L}$ ou da linguagem estendida $\mathbf{L}$' – (1) segue imediatamente da definição da interpretação das constantes no modelo. Suponha que (1) seja verdadeira para os termos de grau de complexidade menor do que n, para algum $n \geq 1$. Seja t o termo $F(t_1, \ldots, t_m)$, onde F é um símbolo funcional m-ário e t_j são termos, para $j \in \{1, \ldots, m\}$. Sejam c_{i_j} constantes tais que $\sigma^*(t_j) = [c_{i_j}]$, para cada $j \in \{1, \ldots, m\}$. Como cada t_j tem grau de complexidade menor do que n, pela hipótese indutiva temos que $t_j = c_{i_j}$ pertence a Δ.

Se $[c_k] = \sigma^*(t)$, por definição temos que $F(c_{i_1}, \ldots, c_{i_m}) = c_k$ pertence a Δ. Portanto, como $t_j = c_{i_j}$ também pertencem a Δ, temos $t = c_k$ pertencente a Δ, pois é obtido da substituição de cada c_{i_j} por t_j na fórmula anterior. Reciprocamente, se $t = c_k$ pertence a Δ, temos que $F(c_{i_1}, \ldots, c_{i_m}) = c_k$ pertence a Δ e, portanto, $[c_k] = \sigma^*(t)$,

Agora mostraremos que, para toda sentença A da linguagem **L'**, temos

(2) $$\mathcal{M} \models A \text{ se, e somente se } A \in \Delta$$

Provaremos (2) por indução no grau de complexidade da fórmula A, assumindo como símbolos primitivos $\exists$, $\wedge$ e $\neg$ (normalmente consideramos $\forall$). Observamos que $[A]^t_x$ tem o mesmo grau de complexidade de A.

Fixe σ uma valoração.

Se A é uma fórmula atômica da forma $t = s$, (2) segue de (1). Se A é uma fórmula atômica da forma $R(t_1, \ldots, t_n)$, tomamos constantes c_{i_j} tais que $\sigma^*(t_j) = [c_{i_j}]$, para $j \in \{1, \ldots, n\}$. Por (1) temos que $t_j = c_{i_j}$ pertence a Δ, para todo $j \in \{1, \ldots, n\}$. Assim, temos que A pertence a Δ se, e somente se, $R(c_{i_1}, \ldots, c_{i_n})$ pertence a Δ. Pela definição de $R^{\mathcal{M}}$, isso equivale a dizer que $([c_{i_1}], \ldots, [c_{i_n}]) \in R^{\mathbb{M}}$. Como $\sigma^*(t_j) = [c_{i_j}]$, isso equivale a $(\mathcal{M}, \sigma) \models A$.

Suponha que (2) é verdadeiro para as fórmulas de grau menor que n, para algum $n \geq 1$. Mostraremos que (2) vale para as fórmulas de grau n. Seja A uma fórmula de grau de complexidade n. Se A é da forma $\neg B$ ou $B \wedge C$, a validade de (2) segue da hipótese indutiva e do Lema 7.14.

Suponha que A seja da forma $\exists x B$, onde B tem grau de complexidade $n - 1$. Provemos, primeiro, que se A pertence a Δ então $(\mathcal{M}, \sigma) \models A$. De fato, pela construção de Δ, existe uma constante c_i tal que $(\exists x B) \to [B]^{c_i}_x$ pertence a Δ. Por modus ponens temos que $[B]^{c_i}_x$ pertence a Δ. Pela hipótese de indução, (2) vale para B e $[B]^{c_i}_x$. Logo, $(\mathcal{M}, \sigma) \models [B]^{c_i}_x$. Tomando θ uma valoração tal que $\theta(x) = c_i^{\mathcal{M}}$ e $\theta(v) = \sigma(v)$ nas demais variáveis, pelo Lema 7.6 concluímos que $(\mathcal{M}, \theta) \models B$. Logo, $(\mathcal{M}, \sigma) \models \exists x B$.

Reciprocamente, suponhamos, por absurdo, que $(\mathcal{M}, \sigma) \models \exists x B$ e $\exists x B$ não pertence a Δ. Seja c_i tal que $\sigma(x) = [c_i]$. Pelo Lema 7.6 temos $(\mathcal{M}, \sigma) \models [B]^{c_i}_x$. Como $[B]^{c_i}_x$ não tem variáveis livres, pelo Corolário 5.4 temos que $\mathcal{M} \models [B]^{c_i}_x$. Pela hipótese de indução temos que $[B]^{c_i}_x \in \Delta$.

Como assumimos que $\exists x B$ não pertence a Δ, pelo Lema 7.14, (a), a sentença $\neg \exists x B$ pertence a Δ. Mas essa sentença é equivalente a $\forall x (\neg B)$, e $(\forall x (\neg B)) \to (\neg [B]^{c_i}_x)$ é um axioma do esquema A3. Por modus ponens temos que $\Delta \vdash \neg [B]^{c_i}_x$ e, pelo Lema 7.14, item (c), $\neg [B]^{c_i}_x$ pertence a Δ, contradizendo que Δ é consistente, e concluindo a prova de (2).

Portanto, de (1) concluímos que $\mathcal{M} \models \Delta$. Em particular, $\mathcal{M} \models \Gamma$, pois $\Gamma \subseteq \Delta$. Como nenhuma das constantes $(c_n)_{n\in\mathbb{N}}$ ocorre nas fórmulas de Γ, se considerarmos o modelo $\mathcal{M}$ sem as interpretações dessas constantes, provamos que Γ é verdadeiro em um modelo para a linguagem $\mathbf{L}$. ■

Teorema 7.18 (da Completude)**.** *Sejam $\boldsymbol{L}$ uma linguagem de primeira ordem, Γ um conjunto de fórmulas de $\boldsymbol{L}$ e A uma fórmula de $\boldsymbol{L}$. Se $\Gamma \models A$ então $\Gamma \vdash A$.*

Demonstração: Como fizemos na demonstração do teorema da dedução, podemos assumir que os elementos de Γ e a fórmula A não possuem variáveis livres, substituindo cada uma dessas fórmulas pelo respectivo fecho universal. De fato, é fácil verificar que $\mathcal{M} \models B$ se, e somente se, $\mathcal{M} \models \forall x B$. Assim, se Γ' é o conjunto dos fechos universais das fórmulas de Γ e A' é o fecho universal de A, então $\Gamma \models A$ se, e somente se, $\Gamma' \models A'$. Da mesma forma, como vimos no teorema da dedução, $\Gamma \vdash A$ se, e somente se, $\Gamma' \vdash A'$.

Suponha que não é verdade que $\Gamma \vdash A$. Pelo Corolário 7.12, usando a equivalência entre A e $\neg\neg A$, temos que $\Gamma \cup \{\neg A\}$ é consistente. Pelo teorema de Henkin existe um modelo $\mathcal{M}$ tal que $\mathcal{M} \models \Gamma \cup \{\neg A\}$. Portanto, $\mathcal{M} \models \Gamma$ e não vale $\mathcal{M} \models A$. Logo, A não é consequência semântica de Γ. ■

Na demonstração do teorema de Henkin o domínio do modelo construído para o conjunto Γ é um conjunto de classes de equivalência sobre um conjunto infinito enumerável. Portanto, ou o domínio é finito (que acontece, por exemplo, se Γ contém a fórmula $\forall x \forall y (x = y)$, ou outra semelhante que força a finitude do modelo) ou é infinito enumerável. Esse resultado, que enunciamos a seguir, é conhecido como teorema de Löweinheim-Skolem, no caso particular em que a linguagem é enumerável.

Teorema 7.19 (Löwenheim-Skolem)**.** *Se Γ é um conjunto consistente de sentenças então existe um modelo $\mathcal{M}$ cujo domínio é finito ou enumerável e tal que $\mathcal{M} \models \Gamma$.*

7.4 Aplicação: análise não-standard

Considere uma linguagem de primeira ordem contendo as constantes 0 e 1, os símbolos funcionais binários $+$ e $\cdot$ e um símbolo relacional binário $<$. Seja Γ o conjunto formado pelos axiomas de corpo (vide a seção de exercícios do Capítulo 5) com o acréscimo das seguintes fórmulas:

1. $\neg(x < x)$
2. $x < y \to \neg(y < x)$
3. $(x < y \wedge y < z) \to (x < z)$
4. $(0 < x \wedge 0 < y) \to (0 < x + y \wedge 0 < x \cdot y)$
5. $(x < 0) \vee (x = 0) \vee (0 < x)$

Chamamos as fórmulas pertencentes a Γ de *axiomas de corpo ordenado* , e os modelos que satisfazem Γ são chamados de *corpos ordenados*.

Considere, agora, uma linguagem L de corpo ordenado acrescido de uma constante ε. Defina, recursivamente, termos t_n, para n um número natural positivo, como $t_1 = 1$ e $t_{n+1} = (t_n) + 1$. Ou seja, t_n é o termo (eliminando os parênteses) $1 + 1 + \ldots + 1$, n vezes.

Para cada n inteiro positivo defina a fórmula F_n como $\varepsilon \cdot (t_n) < 1$. Isto é, F_n formaliza, nessa linguagem, a expressão $\varepsilon < \frac{1}{n}$.

Defina $\Gamma_0 = \Gamma \cup \{0 < \varepsilon\}$ e $\Gamma_{n+1} = \Gamma_n \cup \{F_n\}$. Tome $\overline{\Gamma}$ o conjunto $\bigcup_{n\in\mathbb{N}} \Gamma_n$.

Cada Γ_n é consistente. De fato, tomando o conjunto dos números reais, ou dos números racionais, como modelo, interpretando ε como $\frac{1}{2n}$, esse satisfaz todas as fórmulas de Γ_n. Logo, pelo teorema da correção, Γ_n é consistente.

Observe que cada subconjunto finito de $\overline{\Gamma}$ está contido em Γ_n, para algum n. Como cada Γ_n – e, portanto, seus subconjuntos – é consistente, pelo teorema da compacidade concluímos que $\overline{\Gamma}$ é consistente. Portanto, pelo teorema da completude, existe um modelo que satisfaz Γ.

Nesse modelo, ε representa um número estritamente positivo que é menor que $\frac{1}{n}$, para todo n inteiro positivo. Ainda, pelo teorema de Löweinheim-Skolem, podemos tomar esse modelo sendo enumerável. Esse é o modelo (ou melhor, *um* modelo) para a *análise não-standard*, que, diferentemente do conjunto dos números reais, admite infinitos e infinitésimos, oferecendo uma maneira alternativa de estudar cálculo diferencial e integral.

Uma observação importante é que, quando estudamos análise real, aprendemos que corpos ordenados completos são não-enumeráveis e não possuem infinitésimos, pois satisfazem a propriedade arquimediana. Lembramos que a propriedade do supremo, estudada em análise real, quantifica todos os subconjuntos dos reais, o que não pode ser feito diretamente em uma linguagem primeira ordem. Conforme veremos no exercício 7 deste capítulo, essa aplicação do teorema da compacidade e o teorema de Löweinheim-Skolem

provam que de fato não há uma axiomatização direta, em lógica de primeira ordem, para o conjunto dos números reais. Mas o Apêndice A mostra como contornar esse problema, tornando a lógica de primeira ordem suficiente para formalizar toda a matemática, inclusive os números reais.

7.5 Teoremas de incompletude de Gödel

Nesta seção apresentaremos um esboço da demonstração dos teoremas de incompletude de Gödel. O primeiro teorema de incompletude diz que qualquer tentativa de axiomatização da matemática será incompleta, no sentido de sempre haver uma sentença que não pode ser provada nem refutada. O segundo teorema de incompletude – que é um corolário da prova do primeiro teorema – afirma que um sistema consistente capaz de axiomatizar a matemática não pode provar sua própria consistência.

O argumento central de Gödel é criar uma fórmula que diz "eu não posso ser provada", através de uma apurada técnica que representa muito bem o conceito de metamatemática. Gödel usou a aritmética na metalinguagem e conseguiu codificá-la dentro da linguagem, o que lhe permitiu criar essa versão do paradoxo do mentiroso dentro da sintaxe controlada da linguagem lógica.

Não discutiremos, aqui, as interpretações filosóficas dos teoremas de Gödel, assim como não faremos todos os detalhes técnicos das suas provas.

O trabalho original de Gödel – que o leitor pode conferir em [8] ou na coletânea [11] (versões traduzidas em inglês) – não se baseia na lógica de primeira ordem, mas, sim, na teoria dos tipos do *Principia Mathematica* ([22]). Porém, a mesma técnica pode ser usada para qualquer tentativa de axiomatização dentro dos princípios do programa de Hilbert.

Para quem quiser verificar mais detalhes da demonstração de Gödel, além da tese original recomendamos [19].

Funções e relações recursivas: Vamos convencionar que chamaremos de *função de números naturais* uma função que tem como domínio uma potência finita de $\mathbb{N}$ (isto é, $\mathbb{N}^n$, para algum n natural) e contra-domínio $\mathbb{N}$ (isto é, a imagem dessa função está contida em $\mathbb{N}$).

Dizemos que uma função de números naturais é *constante* se a imagem é um conjunto unitário.

Fixaremos a notação $\phi(x_1, \ldots, x_n)$ para designar o valor da função ϕ, de domínio $\mathbb{N}^n$, na n-upla $(x_1, \ldots, x_n)$.

Introduziremos a definição de *função recursiva*.

Definição 7.20. Uma função de números inteiros ϕ é *recursiva* se existe uma sequência de funções $\phi_0, \ldots, \phi_m$ tal que ϕ é a função ϕ_m e, para cada $k \leq m$, ocorre um dos casos abaixo:

- ϕ_k é uma função constante;
- $\phi_k(x) = x + 1$;
- existem $j < k$, $n \in \mathbb{N}$ e $i \leq n$ tais que $dom(\phi_k) = \mathbb{N}^n$, $dom(\phi_j) = \mathbb{N}^{n-1}$ e
$$\phi_k(x_1, \ldots, x_i, \ldots, x_n) = \phi_j(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n);$$
- ϕ_k é uma composição de funções anteriores, isto é, existem $p, p_1, \ldots, p_n < k$ (não necessariamente diferentes) tais que
$$\phi_k(x_1, \ldots, x_n) = \phi_p(\phi_{p_1}(x_1, \ldots, x_n), \ldots, \phi_{p_n}(x_1, \ldots, x_n));$$
- existe $i < k$ e um número natural c tal que $\phi_k(0) = c$ e
$$\phi_k(x + 1) = \phi_i(x, \phi_k(x))$$
- existem $i, j < k$ tais que
$$\phi_k(0, x_2, \ldots, x_n) = \phi_i(x_2, \ldots, x_n)$$
e
$$\phi_k(x + 1, x_2, \ldots, x_n) = \phi_j(x, \phi_k(x, x_2, \ldots, x_n), x_2, \ldots, x_n)$$

Para tentarmos tornar a definição de função recursiva mais intuitiva, observamos que, se sabemos calcular todas as funções recursivas ϕ_i, para $i < k$, não teremos problemas para calcular ϕ_k. Nos dois últimos itens, a "calculabilidade" de ϕ_k é uma aplicação do teorema da recursão finita, que, por sua vez, segue do princípio da indução finita.

Provemos, por exemplo, que a soma é uma função recursiva. Definimos $\phi_0(x) = x + 1$ e $\phi_1(x, y) = \phi_0(y)$. Tomemos ϕ_2 a função identidade, isto é, $\phi_2(x) = x$. Temos que $\phi_2(0) = 0$ e $\phi_2(x + 1) = \phi_1(x, \phi_2(x))$. Logo, ϕ_2 é

uma função recursiva. Defina $\phi_3(x, y) = x + y$. Temos $\phi_3(0, y) = \phi_2(y)$ e $\phi_3(x + 1, y) = \phi_1(x, \phi_3(x, y))$. A sequência $\phi_0, \phi_1, \phi_2, \phi_3$ satisfaz as condições da Definição 7.20 e, portanto, a soma é uma função recursiva. Deixamos a cargo do leitor completar os detalhes e mostrar que a multiplicação e a potência são funções recursivas.

A tese de Church (veja [11] e [3]) mostra que o conceito de funções recursivas, dado por Gödel, coincide com a definição de Turing de funções *computáveis*. Isso significa, intuitivamente, que uma função é recursiva se, e somente se, existe um algoritmo finitário para calcular o valor dessa função, para valores fixados do domínio.

A partir da definição de função recursiva definimos facilmente o significado de *relação recursiva*.

Definição 7.21. Uma relação $R \subseteq \mathbb{N}^n$ é *recursiva* se existe uma função recursiva ϕ tal que $(x_1, \ldots, x_n) \in R$ se, e somente se, $\phi(x_1, \ldots, x_n) = 0$.

Numeração de Gödel: Um dos pontos cruciais da prova de Gödel é a *aritmetização da linguagem*, que consiste em associar fórmulas de uma linguagem de primeira ordem a números naturais, transformando relações metamatemáticas, como a de consequência sintática, em relações de números naturais.

Começamos atribuindo a cada símbolo primitivo da linguagem um número natural positivo, conforme a tabela abaixo.

(	0
)	1
,	2
$\neg$	3
$\wedge$	4
$\forall$	5
$=$	6

Prosseguimos essa sequência atribuindo os valores aos símbolos funcionais, símbolos relacionais e constantes da linguagem específica, além das variáveis. Se a linguagem em questão possuir uma quantidade finita de símbolos específicos, enumeramos primeiro esses símbolos e, depois, as variáveis. Por exemplo, se trabalhamos na linguagem da aritmética, com as constantes 0 e 1, os símbolos funcionais $+$ e $\cdot$ e o símbolo relacional $\leq$, prosseguimos a enumeração acima da seguinte forma:

0	7
1	8
+	9
·	10
$\leq$	11
x_0	12
x_1	13
x_2	14
...	

Se a linguagem possuir uma quantidade infinita enumerável de símbolos funcionais, ou de símbolos relacionais, ou de constantes, alternamos esses com as variáveis. Assim, se tivermos infinitas constantes, associamos essas aos números pares e as variáveis aos números ímpares. De qualquer modo, está claro que, se a linguagem for enumerável – isto é, em cada categoria os símbolos podem ser representado indexando-os com números naturais – é sempre possível estabelecer uma correspondência biunívoca entre os símbolos da linguagem e os números naturais.

Seja A uma sequência finita de símbolos da linguagem (não necessariamente uma fórmula). Sejam $k_1, \ldots, k_n$ os números correspondentes aos símbolos de A, na mesma ordem em que eles ocorrem. Sejam $p_1, \ldots, p_n$ os n primeiros números primos, em ordem crescente. Defina o *número de Gödel* de A como

$$p_1^{k_1} \cdot \ldots \cdot p_n^{k_n+1}$$

Pelo teorema fundamental da aritmética, todo número natural positivo se decompõe de maneira única como produto de potências de números primos. Portanto, a numeração de Gödel nos dá uma correspondência um-a-um entre os números naturais e as sequências finitas (incluindo a vazia) de símbolos. Somar um à última potência foi uma maneira de ajustar essa correspondência biunívoca, embora essa exigência não seja estritamente necessária. O importante é que fórmulas diferentes tenham números de Gödel diferentes.

O mesmo método pode ser aplicado para associarmos números naturais às sequências de fórmulas (ou melhor, *sequências de sequências de símbolos*). Se $(A_i)_{1\leq i\leq n}$ é uma sequência de fórmulas, o número de Gödel de $(A_i)_{1\leq i\leq n}$ é $p_1^{k_1} \cdot \ldots \cdot p_n^{k_n}$, onde $p_1, \ldots, p_n$ são os primeiros n números primos, em ordem crescente, e k_i é o número de Gödel da fórmula A_i, para cada i entre 1 e n.

Introduzimos as seguintes definições:

Definição 7.22. Uma *teoria de primeira ordem* é um par (L, Γ), onde L é uma linguagem de primeira ordem e Γ é um conjunto de fórmulas de L. Um *teorema* de uma teoria (L,Γ) é uma fórmula A da linguagem L tal que $\Gamma \vdash A$. Uma sentença A da linguagem L é *independente* da teoria (L,Γ) se A e $\neg A$ não são teoremas da teoria (L,Γ). Isto é, se A é independente de Γ.

Definição 7.23. Uma teoria de primeira ordem é *consistente* se não existe uma fórmula A tal que A e $\neg A$ são ambos teoremas dessa teoria. Uma teoria é *completa* se, para toda sentença A, uma das sentenças A ou $\neg A$ é um teorema.

Dada uma teoria de primeira ordem (L, Γ), podemos associar os símbolos de L biunivocamente aos números naturais e, a partir daí, estabelecer uma numeração de Gödel para as fórmulas que pertencem a Γ. Assim, via essa numeração, Γ pode ser visto como um subconjunto de $\mathbb{N}$, ou como uma relação 1-ária em $\mathbb{N}$. Gödel mostrou que o fato desse conjunto ser ou não recursivo, de acordo com as definições 7.20 e 7.21, independe da numeração que escolhemos para o alfabeto da linguagem, motivando a seguinte definição:

Definição 7.24. Uma teoria (L, Γ) é *recursiva* se, e somente se, o conjunto dos números de Gödel das fórmulas que pertencem a Γ é uma relação 1-ária recursiva.

De acordo com o conceito de máquina de Turing e a tese de Church, uma teoria é recursiva quando existe um processo finitário – como proclama o programa de Hilbert – para verificar se uma fórmula é um axioma (isto é, pertence a Γ ou não). Em particular, se Γ é vazio, ou o conjunto dos axiomas de Peano, ou os axiomas de ZFC, ou os axiomas de corpo, então Γ é recursivo [2].

Gödel mostrou que se (L, Γ) é uma teoria recursiva e capaz de expressar a aritmética, então conseguimos codificar na linguagem L a relação "*y é o número de Gödel de uma sequência de fórmulas que é uma demonstração da fórmula cujo número de Gödel é x*". Usando o quantificador existencial e a negação criamos, então, uma fórmula de uma variável livre que equivale a "*A fórmula de número x não pode ser demonstrada.*" Usando uma técnica semelhante ao argumento diagonal, usado por Cantor para provar a não-enumerabilidade dos números reais, Gödel mostrou que existe um número

[2]Essa definição só se sustenta porque o conjunto dos axiomas da lógica de primeira ordem é recursivo, e as regras de inferência também são relações recursivas. Por isso basta verificarmos que os axiomas adicionais formam um conjunto recursivo.

natural n tal que a sentença "*a fórmula de número n não pode ser demonstrada*" possui número de Gödel n. Essa é a fórmula "*eu não posso ser demonstrada*", e o argumento final de Gödel muito se assemelha ao paradoxo do mentiroso.

Teorema 7.25 (Primeiro teorema de incompletude de Gödel)**.** *Se* $\boldsymbol{T}$ *é uma teoria de primeira ordem recursiva, consistente e capaz de expressar a aritmética, então* $\boldsymbol{T}$ *é incompleta.*

Esboço da demonstração: Apesar dessa ser a forma mais conhecida do primeiro teorema de incompletude de Gödel, na verdade esse enunciado foi provado posteriormente por Rosser, em 1936 (veja [30] e [20]). A prova original de Gödel assume uma hipótese mais forte do que a consistência de **T**.

Para introduzir esse conceito, precisamos assumir que a linguagem possui as constantes 0 e 1 e o símbolo funcional binário + (ou poderíamos ter apenas a constante 0 e um símbolo funcional unário que significa "sucessor") e introduzimos uma notação para um termo correspondente a um número natural n. Definimos, recursivamente, $t(0)$ como a constante 0 e $t(n+1)$ como o termo $(t(n)+1)$. Dizemos que uma teoria (L, Γ) é ω-*consistente* se não existe uma fórmula A tal que para todo número natural n vale

$$\Gamma \vdash (\exists x A) \wedge \neg [A]_x^{t(n)}.$$

Ou seja, uma teoria para a aritmética é ω-inconsistente se, mesmo provando que existe x para a qual $A(x)$ é verdadeira, a mesma teoria prova que $A(n)$ é falso, sempre que substituímos x por um número natural fixado.

Uma teoria ω-consistente é consistente, mas uma teoria consistente não necessariamente é ω-consistente.

A prova que esboçaremos aqui – chamamos de *esboço* porque omitimos detalhes cruciais e tecnicamente complicadíssimos, de modo que este texto apenas descreve a ideia central e intuitiva da prova – é a de Gödel, assumindo essa hipótese adicional posteriormente omitida por Rosser.

Seja (L, Γ) uma teoria **T** recursiva e ω-consistente. Fixe uma numeração para o alfabeto de L. Assumimos que a linguagem L possui as constantes 0, 1 e o símbolo funcional binário +. Sejam A fórmula de L, S sequência finita de fórmulas de L, n um número natural e t, s, u termos de L. Definimos as seguintes notações:

- $A[t]$ é a fórmula obtida pela substituição de todas as ocorrências livres das variáveis em A pelo termo t.
- Φ_n é a sequência de símbolos do alfabeto de L cujo número de Gödel é n.
- $\overline{D}$ é o conjunto das triplas $(p, m, k) \in \mathbb{N}^3$ tais p é o número de Gödel de uma demonstração de $\Phi_m[t(k)]$ a partir de Γ.
- $A(t, s, u)$ é a fórmula $[[[A]^t_x]^s_y]^u_z$.

A grande dificuldade técnica da demonstração de Gödel está em mostrar que a relação $\overline{D}$ pode ser codificada na linguagem. Essa é a parte que usa a hipótese de que a teoria é recursiva. Omitimos essa demonstração e apenas enunciamos a seguinte afirmação (proposição V de [8]):

Afirmação 1. *A relação $\overline{D}$ é recursiva. Além disso, existe uma fórmula D da linguagem L que possui x, y e z como as únicas variáveis livres e tal que, para todos $(p, m, k) \in \mathbb{N}^3$, temos*

- *Se $(p, m, k) \in \overline{D}$ então $\Gamma \vdash D(t(p), t(m), t(k))$;*
- *Se $(p, m, k) \notin \overline{D}$ então $\Gamma \vdash \neg D(t(p), t(m), t(k))$.*

Ou seja, codificamos na linguagem L uma fórmula que diz "A sequência de fórmulas cujo número de Gödel é x é uma demonstração para a fórmula obtida substituindo as variáveis livres da fórmula de número y por z".

Percebe-se que escrever essa frase é difícil até mesmo na linguagem natural. Todo esse malabarismo sintático serve para conseguirmos uma fórmula que diz "*a fórmula de número n não pode ser provada*", onde n é o número da própria fórmula. Vejamos como fazer isso.

Fixe n o número de Gödel da fórmula $\neg\exists x D$. Considere G a fórmula $\neg\exists x D(x, t(n), t(n))$. Isto é, G diz "a fórmula $\Phi_n[t(n)]$ não pode ser provada". Mas $\Phi_n[t(n)]$ é a fórmula $\neg\exists x D(x, t(n), t(n))$, ou seja, é a própria fórmula G. Portanto, G diz "a fórmula G não pode ser provada".

Descrevamos agora os argumentos informais para provar tanto o primeiro quanto o segundo teorema de Gödel. Mostraremos que G é uma sentença indecidível na teoria $\mathbf{T}$. De fato, se $\mathbf{T}$ prova G, como conseguimos codificar a afirmação "G é um teorema" dentro da própria teoria, prova-se, em $\mathbf{T}$, que "G pode ser provada", o que é justamente a negação de G. Isto é, se

a teoria prova G, prova também $\neg G$, contradizendo que ela é consistente. Reciprocamente, se a $\neg G$ é teorema, isso significa justamente que "G pode ser provada". Pela hipótese de ω-consistência conseguimos encontrar um número (para uma demonstração de G) que testemunha que, de fato, G pode ser provada. Provamos, assim, a sentença G, contradizendo mais uma vez a consistência da teoria.

Para o segundo teorema, o argumento informal é esse: se a teoria prova sua própria consistência, em particular, pelo argumento acima, prova-se, dentro dela, que G não pode ser provada (pois isso, como vimos, por argumentos que podem ser reproduzidos na teoria, implica na sua inconsistência). Mas a afirmação "G não pode ser provada" é justamente a fórmula G. Logo, se $\mathbf{T}$ prova sua própria consistência então prova G e, portanto, é inconsistente.

Formalizemos os argumentos do penúltimo parágrafo, mostrando que G é indecidível em $\mathbf{T}$. Note que G é uma sentença, e portanto mostrar que ela é indecidível é suficiente para concluirmos o teorema.

Suponha que $\Gamma \vdash G$. Tome p o número de Gödel da demonstração de G. Como G é $\Phi_n[t(n)]$, temos $(p, n, n) \in \overline{D}$ e, pela afirmação 1, $\Gamma \vdash D(t(p), t(n), t(n))$. Logo (pela contrapositiva do esquema de axiomas A3), $\Gamma \vdash \exists x D(x, t(n), t(n))$. Mas essa é a fórmula $\neg G$, contradizendo que Γ é consistente.

Reciprocamente, suponha que $\Gamma \vdash \neg G$. Isto é, $\Gamma \vdash \exists x D(x, t(n), t(n))$. Mostraremos que existe um número natural p tal que $(p, n, n) \in \overline{D}$. De fato, se para todo $p \in \mathbb{N}$ tivéssemos $(p, n, n) \notin \overline{D}$, pela afirmação 1 teríamos $\Gamma \vdash \neg D(t(p), t(n), t(n))$, para todo p, contradizendo a hipótese de que a teoria é ω-consistente. Tome, então, $p \in \mathbb{N}$ tal que $(p, n, n) \in \overline{D}$. Pela definição dessa relação temos que a sequência de fórmulas cujo número de Gödel é p é uma demonstração de $\Phi_n[t(n)]$, que é a fórmula G. Concluímos que $\Gamma \vdash G$, contradição.

Concluímos que G e $\neg G$ são sentenças e ambas não são teoremas de $\mathbf{T}$, provando que $\mathbf{T}$ é incompleta. ■

A hipótese da teoria ser recursiva é necessária para o teorema. De fato, se tomarmos L uma linguagem e $\mathcal{M}$ qualquer modelo para a linguagem, definamos Γ o conjunto das sentenças que são verdadeiras em $\mathcal{M}$. De 5.4 e 7.18 segue que (L, Γ) é uma teoria consistente e completa. Portanto, podemos concluir, do primeiro teorema de Gödel, que não existe uma axiomatização finitária para as fórmulas verdadeiras em um modelo que contém os números naturais.

O segundo teorema de incompletude é uma consequência da demonstração do primeiro teorema. Note que a hipótese da teoria ser ω-consistente não é necessária, mesmo na demonstração original de Gödel (vide proposição XI de [8]). De fato, usaremos, na demonstração a seguir, que $\Gamma \vdash G$ implica $\Gamma \vdash \neg G$, e essa implicação foi provada usando apenas a hipótese de consistência.

Teorema 7.26 (Segundo teorema de incompletude de Gödel)**.** *Se $\boldsymbol{T}$ é uma teoria de primeira ordem recursiva, consistente e capaz de expressar a aritmética, então $\boldsymbol{T}$ não pode provar sua própria consistência.*

Esboço da demonstração: Considere G a fórmula construída na demonstração do Teorema 7.25. Provamos que $\Gamma \vdash G$ implica a inconsistência de Γ. Como esse argumento pode ser formalizado dentro da teoria $\mathbf{T}$ (já que codificamos nela a noção de "demonstrável"), temos que, se $\mathbf{T}$ prova sua própria consistência, em particular prova que G não pode ser provada. Ou seja, $\Gamma \vdash \neg\exists x Dem(x, t(n), t(n))$, que é a fórmula G, o que implica que Γ (logo, $\mathbf{T}$) é inconsistente.

Detalhes sobre como fazer essa codificação encontram-se em [8]. ■

Exercícios

1. Prove que, se $\Gamma \subseteq \Delta$ e $\Gamma \vdash A$, então $\Delta \vdash A$.

2. Considere uma linguagem de primeira ordem com um símbolo relacional binário $\leq$ e seja Γ o conjunto dos seguintes axiomas de ordem:

$x \leq x$

$((x \leq y) \wedge (y \leq z)) \rightarrow (x \leq z)$

$((x \leq y) \wedge (y \leq x)) \rightarrow (x = y)$

Mostre que a seguinte sentença é independente de Γ:

$$\forall x \forall y((x \leq y) \vee (y \leq x))$$

3. Mostre que o teorema da dedução não é verdadeiro se substituirmos "sentença" por "fórmula", no enunciado.

4. Considere **L** a linguagem da aritmética. A saber, **L** é constituído pela constante 0, o símbolo funcional unário s (sucessor de) e os símbolos funcionais binários $+$ e $\cdot$.

Considere Γ o conjunto formado pelas seguintes fórmulas de **L**, ditas *axiomas de Peano*:

1. $\neg(s(x) = 0)$ (0 não é sucessor de um número natural);
2. $(s(x) = s(y)) \to (x = y)$ (dois números naturais distintos não têm o mesmo sucessor);
3. $(A^0_x \wedge \forall x(A \to A^{s(x)}_x)) \to \forall x A$, para qualquer fórmula A (Princípio da Indução Finita – note que esse é um *esquema de axiomas*, isto é, uma lista de infinitas fórmulas);
4. $x + 0 = x$;
5. $x + s(y) = s(x + y)$;
6. $x \cdot 0 = 0$;
7. $x \cdot s(y) = (x \cdot y) + x$.

Prove que as seguintes fórmulas são consequências sintáticas de Γ.

(a) $\forall x(\neg(s(x) = x))$.

(b) $s(0) + s(0) = s(s(0))$ (isto é, 1+1=2).

(c) $\forall x(0 \cdot x = 0)$.

5. Considere Γ o conjunto descrito na questão 4. Usando o Teorema da Correção, prove que a fórmula do item (a) da questão anterior **não** é consequência sintática de Γ quando:

(a) Tiramos de Γ a fórmula 1;

(b) Tiramos de Γ a fórmula 2;

(c) Tiramos de Γ as fórmulas do esquema 3 (ou seja, desconsideramos o princípio de indução).

6. Seja $\mathcal{M}$ um modelo para uma linguagem $\mathbf{L}$. Prove que o conjunto Γ das sentenças de $\mathbf{L}$ que são verdadeiras em $\mathcal{M}$ é maximalmente consistente. Conclua que (L, Γ) é uma teoria consistente e completa.

7. Seja $(R, 0, 1, +, \cdot, <)$ um corpo ordenado [3]. Seja S um subconjunto não-vazio de R. Utilizando a notação $x \leq y$ como abreviatura de $x < y \vee x = y$, dizemos que

- $m \in R$ é um *limitante superior* (ou *majorante*) de S se $x \leq m$, para todo $x \in S$;
- S é *limitado* se existe $m \in R$ que é limitante superior de S;
- $s \in R$ é *supremo* de S se é um limitante superior de S e, para todo $m \in R$, se m é um limitante superior de S então $s \leq m$.

Dizemos que R é um *corpo ordenado completo* se todo subconjunto não-vazio e limitado de R admite supremo.

Prove que não existe uma axiomatização de primeira ordem para corpo ordenado completo. Ou seja, não existe um conjunto de sentenças Γ da linguagem dos corpos ordenados tal que todo modelo que satisfaz Γ é um corpo ordenado completo. Faça essa demonstração de dois modos:

(a) Usando o teorema da compacidade. Lembre-se, para isso, da *propriedade arquimediana* dos números reais: para todo real x existe um natural n tal que $x < n$ (em um curso de análise real prova-se que todo corpo ordenado completo satisfaz a propriedade arquimediana).

(b) Usando o teorema de Löweinheim-Skolem e o fato (também provado em análise real) de que o conjunto dos números reais é não-enumerável.

8. Prove que as funções de adição, multiplicação e potenciação são funções recursivas, de acordo com a definição 7.20.

[3] Por um absuso de notação, para facilitar a leitura, eliminamos o sobrescrito R nos símbolos. Ou seja, estamos usando a mesma notação para o símbolo lógico e para sua interpretação.

9. Seja L a linguagem da igualdade. Isto é, L não possui constantes, símbolos funcionais ou símbolos relacionais. Para cada $n \in \mathbb{N}$, considere A_n a fórmula $\exists x_1 \ldots \exists x_n B_n$, onde B_n é a conjunção de todas as fórmulas da forma $\neg(x_i = x_j)$, onde $1 \leq i < j \leq n$. Considere Γ o conjunto $\{A_n : n \in \mathbb{N}\}$.

(a) Prove que, para todo modelo $\mathcal{M}$ para L, $\mathcal{M} \models \Gamma$ se, e somente se, o domínio de $\mathcal{M}$ é infinito.

(b) Prove que, para toda fórmula A de L, vale $\Gamma \vdash A$ se, e somente se, $\mathbb{N} \models A$.

(c) Conclua que (L, Γ) é uma teoria consistente e completa.

Apêndice A

Formalização da matemática em ZFC

Apresentamos neste apêndice resumidamente o sistema de axiomas de Zermelo-Frankel, conhecido como ZFC (a letra "C" se refere ao Axioma da Escolha, do inglês *choice*), e como esse pode ser usado para formalizar toda a matemática que conhecemos, inclusive os teoremas metamatemáticos que constam no Capítulo 7. Esse sistema formaliza a teoria dos conjuntos, descrita intuitivamente no Capítulo 3.

Vimos nos na introdução e nos exercícios do Capítulo 7 algumas axiomatizações para parte da matemática. A saber, os axiomas de corpo e a aritmética de Peano. Todavia, nessas formalizações temos algumas limitações, pois não podemos, na lógica de primeira ordem, quantificar sobre conjuntos, funções e sequências de elementos do universo. Como mostra o Exercício 7 daquele mesmo capítulo, os números reais não podem ser axiomatizados diretamente em lógica de primeira ordem.

A teoria dos conjuntos surge, então, como teoria unificadora, utilizando uma linguagem de primeira ordem. Como os elementos do universo são eles próprios conjuntos, se conseguirmos definir outras entidades matemáticas – tais como funções, pares ordenados, números naturais e números reais – como conjuntos, a lógica de primeira ordem torna-se suficiente para expressar tudo que precisamos para a matemática.

Ao reduzir toda a matemática a um sistema, e sendo esse o mais conciso possível, reduzimos o risco de inconsistência, já que, pelo Segundo Teorema de Gödel, não é possível um sistema consistente provar sua própria consistência, se esse for recursivo e capaz de expressar a aritmética.

O propósito deste apêndice não é prover um curso completo de teoria dos conjuntos. Para esse fim recomendamos [9], [17] e [30], onde o leitor poderá aprender temas importantes como ordinais, cardinais, Lema de Zorn e aritmética transfinita. Este apêndice apenas pretende mostrar que a teoria dos conjuntos – em particular o sistema ZFC – cumpre bem seu papel de sistema unificador, sendo nele possível definirmos os objetos matemáticos básicos, como pares ordenados, produto cartesiano, funções, números naturais e números reais. Outras teorias matemáticas podem ser formalizadas a partir desses objetos, como a geometria euclideana, que pode ser interpretada em $\mathbb{R}^3$.

Convém ressaltar que as demonstrações neste apêndice – quando feitas – estão na linguagem natural. Deixamos como tarefa ao leitor de suma paciência e disposto de bastante tempo livre formalizar essas demonstrações integralmente na lógica de primeira ordem. Sendo essa uma tarefa virtualmente impossível, o leitor poderá indagar qual é a utilidade da lógica para fundamentar a matemática, se, na prática, essa é inviável. Uma resposta a essa pergunta é: com o conhecimento da lógica e de como seria a formalização "utópica" das demonstrações, mesmo quando trabalhamos na linguagem natural e não com todos os detalhes, mantemos em mente uma noção sobre os argumentos utilizados poderem ser formalizados na linguagem lógica. Os axiomas foram apresentados tanto na linguagem natural quanto na linguagem de primeira ordem.

Faremos uma breve discussão sobre o processo de introduzir novos símbolos numa linguagem de primeira ordem. O único símbolo específico da linguagem de ZFC é o símbolo relacional binário $\in$ (pertence). Porém, outros símbolos podem ser definidos para abreviar a linguagem, tais como $\subset$ (relação de inclusão), $\emptyset$ (conjunto vazio), $\cup$ (união), e por aí vai. Mesmo em cursos de álgebra, é comum ouvirmos explicações como essa: "como provamos que o elemento neutro aditivo existe e é único, podemos passar a chamá-lo de 0". Para formalizar essa ideia enunciamos o seguinte teorema:

Teorema A.1. Sejam (Γ, L) e (Γ', L') duas teorias de primeira ordem. Sejam P e A fórmulas da linguagem L e s um símbolo tal que L' é a linguagem L estendida pelo símbolo s.

(a) Suponha que s é uma constante, P possui apenas x como variável livre, $\Gamma \vdash \exists! x P$ e $\Gamma' = \Gamma \cup \{[P]^s_x\}$. Então $\Gamma' \vdash [A]^s_x$ se, e somente se, $\Gamma \vdash A \to B$.

(b) Suponha que s é um símbolo funcional n-ário, as variáveis livres de P são $x, x_1, \ldots, x_n$, $\Gamma \vdash \forall x_1 \ldots \forall x_n \exists! x P$ e $\Gamma' = \Gamma \cup \{P \leftrightarrow s(x_1, \ldots, x_n)\}$. Então $\Gamma' \vdash [A]_x^{s(x_1,\ldots,x_n)}$ se, e somente se, $\Gamma \vdash P \to A$.

(c) Suponha que s é um símbolo relacional n-ário, as variáveis livres de P são $x_1, \ldots, x_n$, $\Gamma' = \Gamma \cup \{P \leftrightarrow s(x_1, \ldots, x_n)\}$ e B é obtida a partir de A substituindo todas as ocorrências das subfórmulas iguais a P pela fórmula $s(x_1, \ldots, x_n)$. Então $\Gamma' \vdash B$ se, e somente se, $\Gamma \vdash A$.

(d) Em todos os itens anteriores, (Γ', L') é uma *extensão conservativa* de (Γ, L). Isto é, para toda fórmula B da linguagem L, $\Gamma' \vdash B$ se, e somente se, $\Gamma \vdash B$.

A demonstração do teorema acima deixaremos como exercício, sugerindo que se faça via semântica, usando os teoremas da correção e completude. Note que, nos três casos, a fórmula P foi usada para definir, em L, o significado do símbolo s da linguagem estendida L'.

Portanto, a partir da próxima seção, todas as definições de novos símbolos podem ser formalizados pelo teorema acima.

A.1 Os axiomas de ZF

Enunciaremos, nesta seção, os nove axiomas de ZF – o axioma da escolha deixaremos para depois – e as primeiras definições e notações sobre conjuntos.

Axioma 1 (da extensão)**.** *Dois conjuntos são iguais se, e somente se, eles têm os mesmos elementos.*

$$\forall x \forall y (x = y \leftrightarrow (\forall z (z \in x \leftrightarrow z \in y)))$$

Nosso primeiro símbolo que adicionamos à teoria dos conjuntos é o de inclusão.

Definição A.2 (Inclusão)**.** Introduzimos um novo símbolo relacional binário $\subset$ definido por:

$$x \subset y \leftrightarrow \forall z (z \in x \to z \in y)$$

Com essa notação o axioma da extensão poderia ser escrito como

$$\forall x \forall y (x = y \leftrightarrow ((x \subset y) \wedge (y \subset x)))$$

Axioma 2 (do vazio)**.** *Existe um conjunto vazio.*

$$\exists x \forall y \neg (y \in x)$$

Teorema A.3. *O conjunto vazio é único*

$$\exists! x \forall y \neg (y \in x)$$

Demonstração: Consequência do axioma da extensão. ■

Definição A.4 (Conjunto vazio)**.** Denotamos o conjunto vazio por $\emptyset$

$$\forall y \neg (y \in \emptyset)$$

Axioma 3 (do par)**.** *Para todos conjuntos x e y existe um conjunto cujos elementos são x e y.*

$$\forall x \forall y \exists z \forall w ((w \in z) \leftrightarrow ((w = x) \vee (w = y)))$$

Pelo axioma da extensão, o conjunto formado pelos elementos x e y é único. Relevando o fato da sintaxe ser um pouco diferente da usual para símbolos funcionais, introduzimos a seguinte definição de um novo símbolo funcional binário:

Definição A.5 (par não-ordenado)**.** Denotamos por $\{x, y\}$ o conjunto formado por x e y.

$$z = \{x, y\} \leftrightarrow \forall w (w \in z \leftrightarrow (w = x \vee w = z))$$

Quando $x = y$ o conjunto $\{x, y\}$ tem, na realidade, apenas um elemento, e denotaremos o conjunto $\{x, x\}$ por $\{x\}$. Quando mostrarmos a existência do conjunto formado exatamente por x, y, z, podemos chamá-lo de $\{x, y, z\}$. Desse modo, podemos estender a definição acima de modo análogo para qualquer quantidade finita de elementos (assim que provarmos que esses conjuntos existem), introduzindo a notação das chaves como símbolos funcionais n-ários, para todo n.

Axioma 4 (da união)**.** *Para todo conjunto x existe o conjunto de todos os conjuntos que pertencem a algum elemento de x.*

$$\forall x \exists y \forall z ((z \in y) \leftrightarrow \exists w ((z \in w) \wedge (w \in x)))$$

Novamente, pelo axioma da extensão, prova-se que a união de um conjunto é única.

Definição A.6 (União)**.** Denotamos por $\bigcup x$ o conjunto formado por todos os elementos dos elementos de x, introduzindo $\bigcup$ como um símbolo funcional unário.

$$(y = \bigcup x) \leftrightarrow \forall z(z \in y \leftrightarrow \exists w(w \in x \wedge y \in w))$$

Teorema A.7. *Para todos x, y, z existe o conjunto $\{x, y, z\}$.*

Demonstração: Pelo axioma do par existem os conjuntos $\{x, y\}$ e $\{z\}$. Novamente pelo axioma do par existe o conjunto $\{\{x, y\}, \{z\}\}$. Pelo axioma da união existe a união desse conjunto. Verifique que essa união é $\{x, y, z\}$. ■

Axioma 5 (das partes)**.** *Para todo conjunto x existe o conjunto dos subconjuntos de x.*

$$\forall x \exists y \forall z((z \in y) \leftrightarrow (z \subset x))$$

Denotaremos esse conjunto de todos os subconjuntos de x por $\mathcal{P}(x)$. A unicidade segue mais uma vez do axioma da extensão.

Axioma 6 (Esquema de axiomas da separação)**.** *Para cada fórmula P em que z não ocorre livre a seguinte fórmula é um axioma:*

$$\forall y \exists z \forall x((x \in z) \leftrightarrow ((x \in y) \wedge P))$$

O conjunto z, como no axioma, será denotado por

$$\{x \in y : P(x)\}$$

Notemos que a única restrição sobre a fórmula P é não conter z como variável livre. Essa restrição é necessária [1] porque utilizamos essa variável no axioma para definir o conjunto $\{x \in y : P(x)\}$. Se permitirmos que a mesma variável que define o conjunto dado pelo axioma da separação também ocorra livre em P, poderíamos tomar P como a fórmula $x \notin z$ e teríamos a seguinte instância do axioma da separação:

[1] Na prática, caso z ocorra livre em P, alteramos a variável usada no enunciado do axioma da separação. Ou seja, a única preocupação que precisamos ter é não utilizar uma variável que ocorre livre em P para nomear o conjunto criado pelo axioma da separação.

$$\forall y \exists z \forall x((x \in z) \leftrightarrow ((x \in y) \wedge (x \notin z)))$$

Se tomássemos, por exemplo, $y = \{\emptyset\}$ e $x = \emptyset$, teríamos $x \in y$ verdadeiro e, portanto, teríamos

$$(x \in z) \leftrightarrow (x \notin z)$$

o que é uma contradição.

Não precisamos impor qualquer outra restrição sobre as variáveis livres em P. Em todas as aplicações do axioma da separação, a variável x ocorre livre em P (por isso utilizamos a notação $P(x)$ para a fórmula P). Mas se x não ocorrer livre em P, isso não causará inconsistência no sistema. Apenas tornará a aplicação do axioma da separação trivial, pois o conjunto z seria vazio ou o próprio y (já que a validade de P, nesse caso, não depende da variável x, que não ocorre livre em P).

Com essa formulação do sistema de Zermelo-Fraenkel o paradoxo de Russell ganha um novo significado, conforme o teorema seguinte.

Teorema A.8 (Paradoxo de Russell)**.** *Não existe conjunto de todos os conjuntos.*

$$\forall x \exists y \neg(y \notin x)$$

Demonstração: Suponha que exista um conjunto y tal que, para todo x, $x \in y$. Pelo axioma da separação para a fórmula $x \notin x$, existe z tal que, para todo x,

$$(x \in z) \leftrightarrow ((x \in y) \wedge (x \notin x))$$

Como $x \in y$ é verdadeiro para todo x temos que

$$(x \in z) \leftrightarrow (x \notin x).$$

Tomando z no lugar de x temos

$$(z \in z) \leftrightarrow (z \notin z),$$

chegando numa contradição. ■

Usando o axioma da separação podemos introduzir a definição de intersecção de dois conjuntos, e do símbolo funcional binário $\cap$. Definimos $x \cap y$ como o conjunto de todos os elementos que pertencem a x e a y ao mesmo

tempo. A unicidade segue do axioma da extensão e a existência do axioma da separação, do seguinte modo:

$$x \cap y = \{z \in x : z \in y\}.$$

Até agora, todos os axiomas que vimos garantem a construção de alguns conjuntos partindo apenas do conjunto vazio. O próximo axioma garante que *todos* os conjuntos são construídos a partir do vazio.

Axioma 7 (da regularidade)**.** *Para todo conjunto x não-vazio existe $y \in x$ tal que $x \cap y = \emptyset$.*

$$\forall x(x \neq \emptyset \rightarrow \exists y(y \in x \wedge x \cap y = \emptyset))$$

O próximo axioma garantirá a existência de um conjunto infinito. Justificaremos melhor a definição seguinte quando falarmos da construção dos números naturais, na Seção A.3.

Definição A.9. Dado um conjunto x, definimos x^+ como $x \cup \{x\}$. Isto é,

$$\forall y(y \in x^+ \leftrightarrow (y \in x \vee y = x))$$

Quando um conjunto possui o vazio como elemento, e é fechado pela operação de sucessor, então dizemos que tal conjunto é *indutivo*, conforme segue a definição.

Definição A.10 (Conjunto indutivo)**.** Dizemos que um conjunto x é *indutivo* se, e somente se, $\emptyset \in x$ e, para todo y, se $y \in x$ então $y^+ \in x$.

Axioma 8 (da infinidade)**.** *Existe um conjunto indutivo.*

$$\exists x(\emptyset \in x \wedge \forall y(y \in x \rightarrow y^+ \in x))$$

Notemos que um conjunto indutivo pode ter mais do que os números naturais, na concepção de Von Neumann. Falaremos mais adiante sobre como definirmos o conjunto dos números naturais.

Terminamos a nossa lista com o axioma da substituição, que, assim como o da separação, é, na verdade, um esquema de axiomas. Há, de fato, uma semelhança entre os dois esquemas, e o da separação poderia ser omitido, pois pode ser provado a partir do axioma da substituição. Mantivemos o primeiro por motivos didáticos.

Axioma 9 (Esquema de axiomas da substituição)**.** *Seja $P(x, y)$ uma fórmula e suponha que, para todo x, y, z temos que $P(x, y)$ e $P(x, z)$ implicam $y = z$. Então, para todo conjunto X, existe o conjunto*

$$\{y : \exists x(x \in X \wedge P(x, y)\}.$$

Formalmente, dada uma fórmula P tal que w não ocorre livre em P, a seguinte fórmula é um axioma:

$$(\forall x \exists! y[P]_x^y) \to \forall z \exists w \forall y(y \in w \leftrightarrow \exists x(x \in z \wedge [P]_x^y))$$

A.2 Produto cartesiano e axioma da escolha

O axioma do par nos permite construir, a partir de dois conjuntos a e b, o par $\{a, b\}$. Porém, nessa definição de par a ordem dos elementos não importa, de modo que $\{a, b\} = \{b, a\}$. Na definição de par ordenado, a igualdade só deverá valer quando a ordem for a mesma.

Definição A.11 (Par ordenado)**.** Dados dois conjuntos a e b, definimos o *par ordenado* (a, b) como o conjunto $\{\{a\}, \{a, b\}\}$. Ou seja,

$$\forall x(x \in (a, b) \leftrightarrow (\forall y(y \in x \leftrightarrow y = a) \vee \forall y(y \in x \leftrightarrow (y = a \vee y = b))))$$

A existência desse conjunto segue do axioma do par, e a unicidade do axioma da extensão.

Notemos que, quando $a = b$, o par ordenado (a, b) é igual ao conjunto $\{\{a\}\}$.

Teorema A.12. *Dois pares ordenados (a, b) e (c, d) são iguais se, e somente se, $a = c$ e $b = d$.*

Demonstração: Um dos lados da equivalência é trivial: se $a = c$ e $b = d$ então os pares ordenados (a, b) e (c, d) são iguais. Mostraremos a outra direção.

Suponha que $(a, b) = (c, d)$. Como $\{a\} \in (a, b)$, temos que $\{a\} \in (c, d)$. Logo $\{a\} = \{c\}$ ou $\{a\} = \{c, d\}$. Em ambos os casos temos que $a = c$, pois $c \in \{a\}$.

Para provarmos que $b = d$, separemos em dois casos. No primeiro caso, supomos que $a = b$, o que implica que $(a, b) = \{\{b\}\}$. Teremos que $\{c, d\} \in$

(a, b) e, portanto, $\{c, d\} = \{b\}$, provando que $b = d$. No segundo caso, supomos que $a \neq b$. Como $\{a, b\} \in (c, d)$ temos $\{a, b\} = \{c\}$ ou $\{a, b\} = \{c, d\}$. Como $\{c\} \subset \{c, d\}$, em ambos os casos o axioma da extensão garante que $b \in \{c, d\}$. Não podemos ter $b = c$, pois provamos que $a = c$ e assumimos que $a \neq b$. Portanto, $b = d$. ■

O próximo teorema nos garante a existência do produto cartesiano de dois conjuntos.

Teorema A.13. *Dados dois conjuntos A e B, existe o conjunto de todos os pares ordenados (a, b) tais que $a \in A$ e $b \in B$.*

Demonstração: Usando os axiomas do par, da união, das partes e da separação, definimos o conjunto

$$X = \{x \in \mathcal{P}(\mathcal{P}(A \cup B)) : \exists a \exists b(a \in A \wedge b \in B \wedge x = (a, b))\}$$

Para verificarmos que X atende as condições do teorema, só resta verificarmos que todo par ordenado (a, b) pertence a $\mathcal{P}(\mathcal{P}(A \cup B))$, para $a \in A$ e $b \in B$.

De fato, $\{\{a\}, \{a, b\}\} \in \mathcal{P}(\mathcal{P}(A \cup B))$ é equivalente a $\{\{a\}, \{a, b\}\} \subset \mathcal{P}(A \cup B)$, que ocorre se, e somente se, $\{a\} \in \mathcal{P}(A \cup B)$ e $\{a, b\} \in \mathcal{P}(A \cup B)$, o que é verdade, pois $\{a\} \subset A \cup B$ e $\{a, b\} \subset A \cup B$. ■

Definição A.14 (Produto cartesiano)**.** Definimos o *produto cartesiano* de dois conjuntos A e B como o conjunto de todos os pares ordenados (a, b) tais que $a \in A$ e $b \in B$. Introduzimos a notação $A \times B$ para esse conjunto. Isto é:

$$(x \in A \times B) \leftrightarrow \exists a \exists b(a \in A \wedge b \in B \wedge x = (a, b))$$

Denotamos $A \times A$ também por A^2.

As definições de função e relação seguem como no Capítulo 3.

Definição A.15 (Função)**.** Dizemos que f é uma *função de A em B* se $f \subset A \times B$ e, para todo $x \in A$, existe um único $y \in B$ tal que $(x, y) \in f$. Denotamos por B^A o conjunto das funções de A em B.

$$f \in B^A \leftrightarrow (f \subset A \times B \wedge \forall x(x \in A \rightarrow \exists! y(x, y) \in f))$$

As notações $f : A \rightarrow B$ e $f(x)$, vistas no Capítulo 3, devem ser evitadas na linguagem lógica rigorosa. Enunciamos, agora, com as definições e novos símbolos introduzidos até aqui, nosso último axioma, que transforma o sistema ZF no sistema ZFC.

Axioma 10 (da escolha)**.** *Para todo conjunto x de conjuntos não-vazios existe uma função $f : x \longrightarrow \bigcup x$ tal que, para todo $y \in x$, $f(y) \in y$.*

$$\forall x((\neg(\emptyset \in x)) \rightarrow \exists f \exists w((f \in w^x) \wedge \forall y \forall z((y,z) \in f \rightarrow (z \in y))))$$

Uma função f de domínio X tal que $f(x) \in x$, para todo $x \in X$, é chamada de *função de escolha* do conjunto (família de conjuntos) X.

A.3 Números naturais e aritmética

Na definição dos números naturais feita por John von Neumann, pensamos em um número natural como o *conjunto dos números naturais menores que ele*. Assim, o 0 é o conjunto dos números naturais menores que 0. Como não existe número natural menor que 0, então 0 será representado pelo conjunto vazio. O número 1 é o conjunto formado pelos números menores que 1. Ou seja, 1 é o conjunto $\{0\}$, que é igual a $\{\emptyset\}$. O número 2 é o conjunto $\{0, 1\}$, ou seja, o conjunto $\{\emptyset, \{\emptyset\}\}$, e assim por diante.

Note que o número 3, que é o conjunto $\{0, 1, 2\}$, pode ser escrito como $\{0, 1\} \cup \{2\}$, assim como $1 = \emptyset \cup \{0\}$ e $2 = \{0\} \cup \{1\}$. Ou seja, o sucessor de um número natural n é o resultado de acrescentarmos o próprio n ao conjunto n. Isto é, $n + 1 = n \cup \{n\}$.

É essa construção que justifica a Definição A.9. Portanto, um conjunto indutivo – como no axioma da infinidade – contém todos os números naturais, mas pode conter mais do que queremos. Para definir o conjunto dos números naturais, é necessário, em certo sentido, *tirarmos o excesso* dos conjuntos indutivos. Para fazermos isso, usamos o axioma da separação para definirmos a intersecção de uma família de conjuntos.

Teorema A.16 (Intersecção de uma família de conjuntos)**.** *Dado um conjunto não-vazio x existe o conjunto formado por todos os conjuntos que pertencem simultaneamente a todos os elementos de x.*

$$\forall x(\exists y(y \in x) \rightarrow \exists y(\forall z((z \in y) \leftrightarrow \forall w((w \in x) \rightarrow (z \in w)))))$$

Denotaremos esse conjunto por $\bigcap x$.

Demonstração: Seja z um elemento de x. Defina o conjunto y como

$$\{v \in z : \forall w((w \in x) \rightarrow (v \in w))\}$$

O axioma da separação garante a existência do conjunto y. Agora verifiquemos que y satisfaz as condições do teorema. Seja $v \in y$. Pela definição de y, para todo $w \in x$ temos $v \in w$. Reciprocamente, se para todo $w \in x$ temos $v \in w$, então, em particular, $v \in z$ e, portanto, $v \in y$. Isso prova que, para todo v, $v \in y$ se, e somente se, $v \in w$, para todo $w \in x$. ■

Como comentamos no final da Seção 3.1, na definição de intersecção precisamos impor a restrição de que a família é não-vazia. A união de uma família vazia é o conjunto vazio. Mas se fizéssemos a intersecção de uma família vazia obteríamos o "conjunto de todos os conjuntos", já que todo conjunto x satisfaz, por vacuidade, a condição "para todo y pertencente ao conjunto vazio, $x \in y$".

Ressalvamos que, a rigor, não podemos utilizar na linguagem o símbolo $\bigcap$ como símbolo funcional, uma vez que ele não pode ser aplicado – na maneira como está definido – para o conjunto vazio. Esse é mais um abuso de notação que precisamos lidar com cuidado.

A partir do axioma da infinidade e do conceito de intersecção de família de conjuntos, construiremos o conjunto dos números naturais, que, na teoria dos conjuntos, costuma ser denotado por ω.

Teorema A.17. *Existe um único conjunto ω que satisfaz as seguintes propriedades:*

(a) *ω é um conjunto indutivo.*

(b) *Se A é um conjunto indutivo então $\omega \subset A$.*

Demonstração: Fixe x um conjunto indutivo – cuja existência é garantida pelo axioma da infinidade – e use os axiomas da parte e da separação para definir

$$\omega = \bigcap \{y \in \mathcal{P}(x) : y \text{ é indutivo}\}$$

Vamos provar que ω é indutivo. Primeiro, provemos que $\emptyset \in \omega$. De fato, se y é um subconjunto de x que é indutivo, então $\emptyset \in y$. Logo $\emptyset$ pertence à intersecção de todos os subconjuntos indutivos de x. Agora, suponha que $z \in \omega$. Isso significa que $z \in y$, para todo y suconjunto indutivo de x. Logo, $z^+ \in y$, para todo $y \subset x$ indutivo. Logo, $x^+ \in A$, provando a parte (a) do teorema.

Agora provemos a parte (b). Seja A um conjunto indutivo. Repetindo o argumento do parágrafo anterior, concluímos que $A \cap x$ é indutivo. Como

$A \cap x \subset x$, temos, pela definição de ω, que todo elemento de ω também pertence a $A \cap x$. Ou seja, $\omega \subset A \cap x$ e, portanto, $\omega \subset A$.

Mostremos a unicidade de ω. Suponha que y é um conjunto que satisfaz os itens (a) e (b) do teorema. Como ambos ω e y são indutivos e satisfazem o item (b), temos $\omega \subset y$ e $y \subset \omega$, provando que $y = \omega$. ■

Definição A.18. Definimos o *conjunto dos números naturais* como o conjunto ω descrito no Teorema A.17.

Deixamos como exercício ao leitor provar que o conjunto ω, com o conjunto vazio interpretando a constante 0 e a operação $x^+ = x \cup \{x\}$ interpretando o símbolo funcional unário s, é um modelo para os três primeiros axiomas de Peano (vide Exercício 4 do Capítulo 7). Em particular, deixamos a cargo do leitor provar o princípio de indução finita, em ω.

Teorema A.19 (Princípio da Indução Finita)**.** *Seja $P(n)$ uma fórmula, onde n aparece como variável livre. Suponha que vale $P(0)$ e que $P(n)$ implica $P(n^+)$. Então $P(n)$ é verdadeira para todo $n \in \omega$.*

A demonstração do teorema acima é simples: usando o axioma da separação definimos o conjunto de todos os elementos n de ω tais que vale $P(n)$. Esse conjunto é indutivo. Logo, pelo Teorema A.17, é igual a ω.

Vamos agora mostrar como definir as operações de adição e multiplicação em ω, mostrando que o sistema ZFC é capaz de exprimir a aritmética. Antes, precisamos enunciar e provar o Teorema da Recursão.

Teorema A.20 (da recursão)**.** *Sejam X um conjunto, x um elemento de X e g uma função de X em X. Então existe uma única função f de ω em ω tal que*

- $f(0) = x$;
- $f(n^+) = g(f(n))$, *para todo* $n \in \omega$.

Demonstração: Usando o axioma da separação, defina o conjunto

$$\mathcal{C} = \{R \in \mathcal{P}(\omega \times X) : (0, x) \in R \wedge \forall n \forall y((n, y) \in R \rightarrow (n^+, g(y)) \in R)\}.$$

Claramente $\omega \times X \in \mathcal{C}$. Logo, $\mathcal{C}$ é não-vazio. Podemos, portanto, definir o conjunto

$$f = \bigcap \mathcal{C}$$

Precisamos provar que f é uma função e que satisfaz a condição para pertencer a $\mathcal{C}$.

Afirmação 1: $f \in \mathcal{C}$

O procedimento da demonstração da afirmação 1 é análogo à demonstração que ω é um conjunto indutivo. Como $(0, x) \in R$, para todo $R \in \mathcal{C}$, então $(0, x) \in f$. Se $(n, y) \in f$, então $(n, y) \in R$, para todo $R \in \mathcal{C}$. Logo, pela hipótese sobre os elementos de $\mathcal{C}$, $(n^+, g(y)) \in R$, para todo $R \in \mathcal{C}$. Logo, $(n^+, g(y)) \in f$, provando que f pertence a $\mathcal{C}$.

Afirmação 2: f é uma função de domínio ω

Vamos provar, por indução, que para todo $n \in \omega$ vale a seguinte fórmula, que iremos denotar por $P(n)$:

$$\exists y((n, y) \in f) \wedge \forall y \forall z(((n, y) \in f \wedge (n, z) \in f) \rightarrow (y = z))$$

Vamos provar $P(0)$. Pela afirmação 1, $(0, x) \in f$. Mostraremos que, se $(0, y) \in f$, então $y = x$. Suponha, por absurdo, que existe $y \neq x$ tal que $(0, y) \in f$. Considere $R = f \setminus \{(0, y)\}$. Vamos verificar que $R \in \mathcal{C}$. De fato, $(0, x) \in R$, pois $(0, x) \in f$ e $x \neq y$. Se $(n, y) \in R$, então $(n, y) \in f$, pois $R \subset f$. Logo, $(n^+, g(y)) \in f$ (pela afirmação 1). Como $n^+ \neq 0$ (axioma 4 de Peano), temos que $(n^+, g(y)) \in f$ é diferente de $(0, y)$ e, portanto, pertence a R.

Portanto, concluímos que $R \in \mathcal{C}$, o que implica que $f \subset R$. Como $R \subset f$, temos $f = R$, absurdo, pois $(0, y) \in f$ e $(0, y) \notin R$.

Vamos agora provar que $P(n)$ implica $P(n^+)$.

Assumindo $P(n)$ como verdadeiro, existe y tal que $(n, y) \in f$. Logo, como $f \in \mathcal{C}$, temos que $(n^+, g(y)) \in f$, provando a "primeira parte" de $P(n^+)$.

Agora supomos, por absurdo, que existe $z \neq g(y)$ tal que $(n^+, z) \in f$. Defina $R = f \setminus \{(n^+, z)\}$. Vamos verificar que $R \in \mathcal{C}$.

Como $n^+ \neq 0$, temos $(0, x) \in R$. Suponha que $(m, v) \in R$. Como $f \in \mathcal{C}$ e $R \subset f$ temos que $(m^+, g(v)) \in f$. Portanto, para mostrarmos que $(m^+, g(v)) \in R$ basta provarmos que $(m^+, g(v)) \neq (n^+, z)$. Dividiremos em dois casos: $m \neq n$ e $m = n$.

Se $m \neq n$, o axioma 3 de Peano nos garante que $m^+ \neq n^+$ e, portanto, $(m^+, g(v)) \neq (n^+, z)$

Suponhamos que $m = n$. Da hipótese indutiva $P(n)$ e da hipótese $(n, y) \in f$ segue que $v = y$. Como assumimos que $z \neq g(y)$, vale $(m^+, g(v) \neq (n^+, z)$.

Concluímos que $R \in \mathcal{C}$ o que novamente contradiz com o fato de R estar contido propriamente em f.

Provamos, por indução, que vale $P(n)$, para todo $n \in \omega$, concluindo a afirmação 2.

Das afirmações 1 e 2 segue imediatamente o teorema. Sendo f uma função de domínio ω e satisfazendo as condições da família de conjuntos $\mathcal{C}$, temos que $(0, x) \in f$, o que significa que $f(0) = x$. Como, para todo n, temos, pela própria definição de função, $(n, f(n)) \in f$, da afirmação 1 segue que $(n^+, g(f(n)) \in f$, o que significa que $f(n^+) = g(f(n))$.

A unicidade da função f pode ser provada por indução. Suponha que existe h satisfazendo as mesmas condições do teorema estabelecidas para f. Temos que $f(0) = h(0)$, pois ambos são iguais a x. Se $f(n) = h(n)$, então $g(f(n)) = g(h(n))$, e ambos são iguais a $f(n^+)$ e $h(n^+)$. Logo, por indução, $f = h$.

■

Usando o teorema da recursão definiremos, para cada número natural m, uma função $s_m : \omega \longrightarrow \omega$ tal que

$$s_m(0) = m$$

$$s_m(n^+) = (s_m(n))^+$$

A soma $m+n$ será definida como $s_m(n)$. Utilizando novamente o teorema da recursão e a definição das funções acima podemos definir, para cada número natural m, uma função $p_m : \omega \longrightarrow \omega$ tal que

$$p_m(0) = 0$$

$$p_m(n^+) = (p_m(n)) + m$$

e definimos $m \cdot n$ como $p_m(n)$.

Essa definição de soma e produto ainda precisa ser melhor justificada, para podermos construí-la axiomaticamente. Façamos isso.

Teorema A.21. *Existe uma função s de ω em ω^ω tal que, para todo $n, m \in \omega$, $s(m)(0) = m$ e $s(m)(n^+) = (s(m)(n))^+$.*

Demonstração: Usando o axioma da separação defina

$$s = \{(m, f) \in \omega \times \omega^\omega : \forall n((f(0) = m) \wedge (f(n^+) = (f(n))^+))\}$$

Pelo teorema da recursão, utilizando-o para a função $g = \{(n, n^+) : n \in \omega\}$, para cada m existe uma única f satisfazendo as condições descritas na definição de s. Logo, s é uma função.

■

Definição A.22. *Definimos a* operação de soma em ω *como a função* $+ : \omega \times \omega \longrightarrow \omega$ *dada por* $+((m, n)) = s(m)(n)$. *Denotamos* $+((m, n))$ *por* $m+n$.

Teorema A.23. *Existe uma função* p *de* ω *em* ω^ω *tal que, para todo* $n, m \in \omega$, $p(m)(0) = 0$ *e* $p(m)(n^+) = p(m)(n) + m$.

Demonstração: Usando o axioma da separação defina

$$p = \{(m, f) \in \omega \times \omega^\omega : \forall n((f(0) = 0) \wedge (f(n^+) = (f(n) + m)))\}$$

Considere $g = \{(i, j) \in \omega \times \omega : i + m = j\}$. Após o leior provar a lei do cancelamento para a soma, é fácil verificar que g é uma função. Tomando essa função g no enunciado do teorema da recursão, mostramos que para cada m existe uma única f tal que $(m, f) \in p$. Logo, p é uma função. ■

Definição A.24. *Definimos a* operação de produto em ω *como a função* $\cdot : \omega \times \omega \longrightarrow \omega$ *dada por* $\cdot((m, n)) = p(m)(n)$. *Denotamos* $\cdot((m, n))$ *por* $m \cdot n$.

Da definição de soma e produto seguem os seguintes axiomas da aritmética de Peano, quando adicionamos os símbolos funcionais binários $+$ e $\cdot$ à linguagem da aritmética:

$$m + 0 = m$$

$$m + n^+ = (m + n)^+$$

$$m \cdot 0 = 0$$

$$m \cdot n^+ = (m \cdot n) + n$$

Como de costume, usaremos a notação xy no lugar de $x \cdot y$.

A.4 Construção do conjunto dos números inteiros

A construção dos números inteiros a partir dos naturais se assemelha muito à construção dos racionais a partir dos inteiros, sendo essa última mais conhecida.

Iremos identificar pares de números naturais que "possuem a mesma diferença". Por exemplo, identificaremos o par $(5, 3)$ com os pares $(4, 2)$, $(6, 4)$ etc. Assim, o número inteiro 2 é o conjunto $\{(2, 0), (3, 1), (4, 2), \ldots\}$ (sendo esses pares ordenados formados por números naturais), enquanto -2 é o conjunto $\{(0, 2), (1, 3), (2, 4), \ldots\}$.

Definimos $R \subset (\omega \times \omega)^2$ como o conjunto dos pares $((a, b), (c, d))$ tais que $a + d = b + c$. Deixamos como exercício ao leitor provar o seguinte fato:

Afirmação: R é uma relação de equivalência

Defina o conjunto dos números inteiros como

$$\mathbb{Z} = (\omega \times \omega)/R$$

Falta definirmos as operações de soma e produto em $\mathbb{Z}$. Para não sobrecarregar o texto, abusaremos a notação utilizando os mesmos símbolos $+$ e $\cdot$ para a soma e produto de números inteiros. Uma definição informal seria

$$[(a, b)] + [(c, d)] = [(a + c, b + d)]$$

$$[(a, b)] \cdot [(c, d)] = [(ac + bd, ad + bc)]$$

Intuitivamente, o par (a, b) representa o número inteiro $a - b$. Pelas propriedades que conhecemos sobre as operações de números inteiros verificamos que $(a-b)+(c-d) = (a+c)-(b+d)$, e $(a-b)\cdot(c-d) = (ac+bd)-(ad+bc)$, justificando a definição acima.

No entanto, precisamos mostrar que tal definição não depende da escolha do representante. Para formalizar esse argumento, definimos a soma e o produto do seguinte modo:

$$S = \{(x, y, z) \in \mathbb{Z}^3 : \exists a \exists b \exists c \exists d((a, b) \in x \wedge (c, d) \in y \wedge (a + c, b + d) \in z\}$$

$$P = \{(x, y, z) \in \mathbb{Z}^3 : \exists a \exists b \exists c \exists d((a, b) \in x \wedge (c, d) \in y \wedge (ac + bd, ad + bc) \in z\}$$

Teorema A.25. *Sejam S e P definidos como acima. Temos que*

(a) *S e P são funções;*

(b) *Para todos a, b, c, d em ω temos que $S([(a,b)],[(c,d)]) = [(a+c, b+d)]$;*

(c) *Para todos a, b, c, d em ω temos que $P([(a,b)],[(c,d)]) = [(ac+bd, ad+bc)]$.*

Demonstração: Para as três partes do teorema precisamos mostrar a independência em relação à escolha dos representantes. Isto é, mostraremos a seguinte afirmação:

> **Afirmação:** Se $(a,b)R(a',b')$ e $(c,d)R(c',d')$ então $(a+c, b+d)R(a'+c', b'+d')$ e $(ac+bd, ad+bc)R(a'c'+b'd', a'd'+b'c')$.

Provaremos a afirmação assumindo as propriedades conhecidas da aritmética: comutatividade, associatividade, lei do cancelamento etc.

Suponha que $(a,b)R(a',b')$ e $(c,d)R(c',d')$. Isso significa que $a+b' = b+a'$ e $c+d' = d+c'$. Logo, $a+b'+c+d' = b+a'+d+c'$, o que significa que $(a+c, b+d)R(a'+c', b'+d')$.

Agora veremos que $(ac+bd, ad+bc)R(a'c'+b'd', a'd'+b'c')$.

Como $a+b' = a'+b$ e $c+d' = c'+d$, temos que, para todos x, y, z, w em ω, vale a seguinte igualdade:

$$(a+b')x+(c+d')y+(a'+b)z+(c'+d)w = (a'+b)x+(c'+d)y+(a+b')z+(c+d')w$$

Tomando $x = c+c'$, $y = a+a'$, $z = d+d'$ e $w = b+b'$, utilizando as propriedades operatórias de números naturais, provamos que $ac+bd+a'd'+b'c' = ad+bc+a'c'+b'd'$ e, portanto, $(ac+bd, ad+bc)R(a'c'+b'd', a'd'+b'c')$. Deixando os detalhes das contas para o leitor completar, concluímos a prova da afirmação.

Para provar que S é uma função de $\mathbb{Z}^2$ em $\mathbb{Z}$, primeiro precisamos mostrar que, para todo $(x,y) \in \mathbb{Z}^2$, existe z tal que $(x,y,z) \in S$. Mas isso é verdade, pois pelo Teorema 3.14, parte (b), x e y são não-vazios. Logo, existem $(a,b) \in x$ e $(c,d) \in y$. Pela parte (a) do mesmo teorema, existe z tal que $(a+c, b+c) \in z$, o que nos dá, pela definição de S, que $(x,y,z) \in S$. O mesmo argumento mostra que, para todo $(x,y) \in \mathbb{Z}^2$, existe z tal que $(x,y,z) \in P$, tomando, desta vez, z contendo $(ac+bd, ad+bc)$.

Isso já prova, quando concluirmos que S e P são funções, as partes (b) e (c) deste teorema.

Agora vejamos a unicidade. Suponha que $(x, y, z) \in S$ e $(x, y, z') \in S$. Pela definição de S, $(x, y, z) \in S$ implica que existem números naturais a, b, c, d tais que $(a, b) \in x$, $(c, d) \in y$ e $(a+c, b+d) \in z$, e $(x, y, z') \in S$ implica que existem números naturais a', b', c', d' tais que $(a', b') \in x$, $(c', d') \in y$ e $(a' + c', b' + d') \in z'$.

Note que não podemos, a princípio, assumir que os números a, b, c, d que testemunham que $(x, y, z) \in S$ são os mesmos que testemunham que $(x, y, z') \in S$.

Porém, como (a, b) e (a', b') ambos pertencem a x, o Teorema 3.14, parte (d), nos garante que $(a, b)R(a', b')$. Da mesma forma temos $(c, d)R(c', d')$. Logo, pela afirmação, $(a+c, b+d)R(a'+c', b'+d')$. Logo, o Teorema 3.14, parte (d), também nos assegura que $(a'+c', b'+d') \in z$. Portanto, $(a'+c', b'+d') \in z \cap z'$, o que implica, pela parte (c) do Teorema 3.14, que $z = z'$, como queríamos provar.

A demonstração de que P é uma função é análoga.

■

Sendo x e y números inteiros, denotamos $S((x, y))$ por $x + y$, e $P((x, y))$ por $x \cdot y$ ou, simplesmente, xy. Realçamos que estamos abusando a notação, ao usar o mesmo símbolo para representar operações em conjuntos diferentes.

Definir função em classes de equivalência através de um representante, para depois mostrar que a definição independe da escolha do representante, é uma prática bastante comum no cotidiano da matemática, com a qual o estudante deve ter se deparado diversas vezes. Aqui foi apresentada a formalização desse processo, que, como podemos notar, não é trivial, apesar de ser bem intuitivo. Reparem que todos os itens do Teorema 3.14 foram utilizados e, na demonstração desse, foram utilizadas todas as três propriedades de relação de equivalência.

A.5 Construção do conjunto dos números racionais

A construção de $\mathbb{Q}$ a partir de $\mathbb{Z}$ é semelhante à construção de $\mathbb{Z}$ a partir de ω.

Primeiro definimos o número inteiro 0 (eventualmente denotado por $0_{\mathbb{Z}}$,

quando houver possibilidade de confusão com o número natural 0) como a classe $[(0,0)]$.

Definimos uma relação R em $\mathbb{Z} \times (\mathbb{Z} \setminus \{0_\mathbb{Z}\})$ como

$$R = \{((a,b),(c,d) \in (\mathbb{Z} \times (\mathbb{Z} \setminus \{0_\mathbb{Z}\}))^2 : ac = bd\}$$

Fica como exercício verificar que R é uma relação de equivalência.

Definimos

$$\mathbb{Q} = (\mathbb{Z} \times (\mathbb{Z} \setminus \{0_\mathbb{Z}\}))/R$$

Obviamente, a classe de equivalência representada pelo par (a,b) corresponde ao número racional representado pela fração $\frac{a}{b}$, e R é a equivalência de frações.

Definimos a soma e o produto de números racionais da seguinte forma:

$$[(a,b)] + [(c,d)] = [(ad + bc, bd)]$$

$$[(a,b)] \cdot [(c,d)] = [(ac, bd)]$$

Deixamos como exercício ao leitor provar que essa definição independe da escolha do representante. Os demais detalhes para a formalização são iguais aos que foram feitos anteriormente, para os números inteiros.

A.6 Construção do conjunto dos números reais

Vimos no Exercício 8 do Capítulo 7 que não é possível axiomatizar o conjunto dos números reais diretamente na lógica de primeira ordem. Porém, dentro do sistema ZFC, que é formalizado em primeira ordem, conseguimos construir um corpo ordenado completo (a grosso modo, o conjunto dos números reais), tornando os teoremas de análise na reta partes de ZFC. Fica claro, também, que

A construção que será feita nesta seção deve-se a Richard Dedekind (1831–1916). Convém ressaltar que essa formulação antecede, historicamente, a própria definição dos conjuntos dos números naturais, e até mesmo a teoria axiomática dos conjuntos. Os temas apresentados neste Capítulo – e no livro, em geral – não estão, de forma alguma, dispostos em ordem cronológica.

Recomendamos [1] para um estudo mais detalhado da construção dos números reais, incluindo outras abordagens, como a das sequências de Cauchy.

Para construirmos os números reais a partir dos racionais, precisamos, antes, introduzir algumas definições sobre a ordem em $\mathbb{Q}$.

Dizemos que um número inteiro x é *positivo* se existe $n \in \omega$ tal que $n \neq 0$ e $(n, 0) \in x$.

Dizemos que um número racional x é *positivo* se existe $(a, b) \in x$ tal que a e b são números inteiros positivos.

Definimos uma relação $<$ em $\mathbb{Q}$ da seguinte forma: $a < b$ se, e somente se, existe um número racional positivo c tal que $a + c = b$.

Dizemos que um subconjunto C de $\mathbb{Q}$ é um *corte* se satisfaz as seguintes propriedades:

- é não-vazio: $\exists x(x \in C)$;
- não contém todos os racionais: $\exists x(x \in \mathbb{Q} \wedge x \notin C)$;
- não tem máximo: $\forall x \exists y(x < y)$;
- é fechado para baixo: $\forall x \forall y((x \in C \wedge y < x) \rightarrow y \in C)$.

Definimos o conjunto dos números reais como:

$$\mathbb{R} = \{C \subset \mathbb{Q} : C \text{ é um corte}\}$$

Intuitivamente, na construção por cortes, pensamos em um número real r. *o conjunto dos racionais menores do que* r. Por exemplo, $\sqrt{2}$ é definido como o conjunto

$$\sqrt{2} = \{x \in \mathbb{Q} : (x < 0) \vee (x \cdot x < 2)\}$$

Dados dois números reais A e B (ou seja, dois cortes contidos em $\mathbb{Q}$) definimos a soma de A e B como:

$$A + B = \{a + b : (a \in A) \wedge (b \in B)\}$$

Para definirmos o produto de A e B, precisamos ter um cuidado extra com os sinais. Se $0 \notin A$ e $0 \notin B$, definimos

$$A \cdot B = \{x \in \mathbb{Q} : \exists a \exists b(a \in A \wedge b \in B \wedge x + (a \cdot b) < 0)\}.$$

A definição de $A \cdot B$ em outros casos será deixada como exercício ao leitor, bem como a tarefa de provar que essas definições estão boas – isto é, são de fato cortes – e que satisfazem os axiomas de corpo ordenado completo, com a ordem da inclusão.

Exercícios

1. Prove as seguintes afirmações:

(a) $\bigcup \emptyset = \emptyset$.

(b) $\bigcup \{\emptyset\} = \emptyset$.

(c) $\bigcup \{\emptyset, \{\emptyset\}\} = \{\emptyset\}$.

(d) $\bigcup \mathcal{P}(x) = x$, para todo x.

(e) $\bigcup n^+ = n$, para todo $n \in \omega$.

(f) $\bigcup \omega = \omega$.

(g) Se $x \subset y$ então $\bigcup x \subset \bigcup y$.

(h) Se $x \subset y$ e ambos são não-vazios, então $\bigcap y \subset \bigcap x$.

2. Prove que os axiomas do vazio e da separação são dispensáveis, podendo ser provados a partir dos outros axiomas de ZFC e dos axiomas lógicos.

3. Encontre uma maneira alternativa de definir par ordenado, de modo que o Teorema A.12 continue verdadeiro para essa nova definição. Justifique.

4. Prove que, em ZFC, não existe o conjunto de todos os conjuntos enumeráveis. **Dica:** Mostre que, se esse conjunto existir, podemos usar os axiomas de ZFC para obter o conjunto de todos os conjuntos, contrariando o Teorema A.8.

5. Prove que, para todo conjunto X, existe o conjunto $\{\{x\} : x \in X\}$.

6. Usando o axioma da regularidade, prove que:

(a) Não existe x tal que $x \in x$;

(b) Não existe x e y tais que $x \in y$ e $y \in x$;

(c) Não existe uma função f de domínio ω tal que $f(n^+) \in f(n)$, para todo $n \in \omega$.

7. Dizemos que um conjunto x é *transitivo* se $z \in y$ e $y \in x$ implicam que $z \in x$, para todos y e z.

(a) Prove que x é transitivo se, e somente, $\bigcup x \subset x$.

(b) Prove que ω é transitivo.

(c) Usando o axioma da regularidade, prove que o conjunto vazio pertence a qualquer conjunto transitivo não-vazio.

8. Para uma determinada teoria consistente $\mathbf{T}$, prove que não existe, em ZFC, o conjunto de todos os modelos para $\mathbf{T}$.

9. Prove que toda teoria consistente possui um modelo que tem, como domínio, um subconjunto de ω.

10. Assumindo que ZFC é consistente, pelo teorema de Löweinheim-Skolem existe um modelo enumerável (isto é, de domínio enumerável) para ZFC. Sabemos que, em ZFC, podemos provar que existem conjuntos não-enumeráveis, como $\mathcal{P}(\omega)$. Como você explica, então, essa aparente contradição: o "conjunto de todos os conjuntos" é enumerável, apesar de conter diversos conjuntos não-enumeráveis?

11. Assumindo que ZFC é consistente, use o segundo teorema de Gödel para provar que a seguinte afirmação é verdadeira mas não pode ser provada em ZFC:

> "Existe um conjunto M e uma relação $R \subset M \times M$ tal que (M, R) é um modelo para a linguagem da teoria dos conjuntos que satisfaz os axiomas de ZFC".

Apêndice B

Álgebras de Boole

As álgebras de Boole nos oferecem uma outra perspectiva para compreendermos a lógica proposicional, e mostrar essa relação entre os dois temas é o objetivo deste apêndice. Para acompanhá-lo, o leitor deve estar familiarizado com o conteúdo dos Capítulos 2 e 3.

Hoje, as álgebras de Boole possuem diversas aplicações na matemática moderna, como em topologia e análise funcional. Trataremos apenas de seus rudimentos, com foco nas álgebras de Lindenbaum, pela sua relevância quanto ao tema deste livro.

Recomendamos [15] para um estudo avançado sobre o assunto.

B.1 Álgebras de Boole

Como acontece nos cursos de álgebra abstrata, definimos uma álgebra de Boole como um conjunto munido de algumas operações satisfazendo determinadas condições, que são os *axiomas de álgebras de Boole*. Usaremos os símbolos $+$, $\cdot$ e $-$ para tais operações, embora notaremos que não há muita semelhança dessas operações com as que conhecemos nos conjuntos numéricos. A operação $+$ corresponde à disjunção, ou à união de conjunto, a operação $\cdot$ corresponde à conjunção, ou à intersecção, e $-$ representa a negação ou o complemento de conjuntos.

Definição B.1. Uma *álgebra de Boole* é uma estrutura $\mathcal{A} = (A, +, \cdot, -, 0, 1)$, onde $+$ e $\cdot$ são operações binárias em A, $-$ é uma operação unária e 0 e 1 são dois elementos distintos de A, que satisfaz, para todo $a, b, c \in A$:

$B1$ $a + (b + c) = (a + b) + c$; (associatividade)

$B1'$ $a \cdot (b \cdot c) = (a \cdot b) \cdot c$;

$B2$ $a + b = b + a$; (comutatividade)

$B2'$ $a \cdot b = b \cdot a$;

$B3$ $a + (a \cdot b) = a$; (absorção)

$B3'$ $a \cdot (a + b) = a$;

$B4$ $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$; (distributividade)

$B4'$ $a + (b \cdot c) = (a + b) \cdot (a + c)$;

$B5$ $a + (-a) = 1$; (complementação)

$B5'$ $a \cdot (-a) = 0$.

Ou seja, uma álgebra de Boole é um modelo que satisfaz as fórmulas acima, considerando a linguagem formada pelas constantes 0 e 1, o símbolo funcional unário $-$ e os símbolos funcionais binários $+$ e $\cdot$.

Mantendo a coerência com a nomenclatura usada para modelos de linguagens de primeira ordem, dada uma álgebra de Boole $\mathcal{A} = (A, +, \cdot, -, 0, 1)$, chamamos o conjunto A de *domínio* de $\mathcal{A}$. Por abuso de notação, eventualmente denotaremos a álgebra $\mathcal{A}$ pelo seu domínio A.

Notemos que os axiomas de álgebras de Boole aparecem aos pares, sendo que em cada par um deles é o "espelho" do outro, trocando as operações $+$ e $\cdot$ e as constantes 0 e 1. Portanto, se demonstrarmos um teorema a partir desses axiomas, também vale o dual desse teorema (isto é, se trocarmos as operações e as constantes do enunciado do teorema), visto que podemos, na demonstração, substituir também os axiomas pelos seus duais. Veremos um exemplo disso no teorema seguinte, quando provarmos alguns resultados básicos sobre álgebras de Boole. Esses resultados também serão apresentados – quando for o caso – aos pares.

Teorema B.2. *Seja $\mathcal{A} = (A, +, \cdot, -, 0, 1)$ uma álgebra de Boole. Então, para todos $a, b \in A$ valem as seguintes propriedades:*

1. *$a + 0 = a$ e $a \cdot 1 = a$;*

2. *$a + a = a$ e $a \cdot a = a$ (idempotência);*

3. $a \cdot 0 = 0$ *e* $a + 1 = 1$*;*

4. Se $a \cdot b = 0$ *e* $a + b = 1$ *então* $b = -a$*;*

5. $-(-a) = a$*;*

6. $-(a \cdot b) = (-a) + (-b)$ *e* $-(a + b) = (-a) \cdot (-b)$ *(leis de De Morgan).*

Demonstração: Por B5' temos que $a + 0 = a + ((a) \cdot (-a))$, que é igual a a, por B3. A segunda parte do item 1 é análoga, trocando os símbolos + e $\cdot$ e os símbolos 0 e 1. Isto é, por B5 temos $a \cdot 1 = a \cdot ((a) + (-a))$, que é igual a a, por B3'.

A partir de agora, mostraremos apenas a primeira parte de cada item, quando for o caso, sendo que a segunda demonstra-se analogamente, por "espelhamento".

Pelo item 1 e por absorção, $a + a = a + (a \cdot 1) = a$, o que prova o item 2.

Por complementação e associatividade, $a \cdot 0 = a \cdot (a \cdot (-a)) = (a \cdot a) \cdot (-a)$. Pelo item 2 e por complementação concluímos que $a \cdot 0 = a \cdot (-a) = 0$, provando o item 3.

Suponhamos que $a \cdot b = 0$ e $a + b = 1$. Mostraremos que $b = -a$. De fato, pelo item 1 temos $-a = (-a) + 0$. Pela hipótese temos $(-a) + 0 = (-a) + (a \cdot b)$ e, pela distributividade, $(-a) + (a \cdot b) = ((-a) + a) \cdot ((-a) + b)$, que, pela complementação, é igual a $1 \cdot ((-a) + b)$. Pelo item 1, concluímos que $-a$ é igual a $(-a) + b$. Logo, usando o item 1, a hipótese, a distributividade e a absorção, temos

$$-a = (-a) + b = ((-a) \cdot 1) + b = ((-a) \cdot (a + b)) + b = ((-a) \cdot a) + ((-a) \cdot b)) + b =$$

$$(0 + (-a) \cdot b) + b = ((-a) \cdot b) + b = b$$

Pela complementação e comutatividade temos $(-a) \cdot a = 0$ e $(-a) + a = 1$. Logo, do item 4 segue que $a = -(-a)$, provando o item 5.

Mostraremos agora o item 6 (como sempre, a primeira parte). Pelo item 4, é suficiente provar que $((-a) + (-b)) \cdot (a \cdot b) = 0$ e $((-a) + (-b)) + (a \cdot b) = 1$.

Usando distributividade, associatividade, comutatividade e complementação, temos que

$$((-a) + (-b)) \cdot (a \cdot b) = ((-a) \cdot (a \cdot b)) + ((-b) \cdot (a \cdot b)) =$$

$$((-a) \cdot (a \cdot b)) + ((-b) \cdot (b \cdot a)) = 0 + 0 = 0$$

e

$$((-a)+(-b))+(a\cdot b)=(-a)+((-b)+(a\cdot b))=$$

$$(-a)+(((-b)+a)\cdot((-b)+b)=(-a)+((-b)+a)=1$$

■

A partir das operações, podemos definir uma ordem numa álgebra de Boole.

Definição B.3. Numa álgebra de Boole A, definimos a relação $\leq$ por $a \leq b$ se e somente se $a = a \cdot b$, para todos $a, b \in A$.

Teorema B.4. *A relação $\leq$ é uma ordem em uma álgebra de Boole.*

Demonstração: A reflexividade segue da idempotência: $a \cdot a = a$. A anti-simetria é consequência da comutatividade. De fato, se $a \cdot b = a$ e $b \cdot a = b$ então, como $a \cdot b = b \cdot a$, temos $a = b$. Mostremos a transitividade. Suponha que $a \leq b$ e $b \leq c$. Temos que $a \cdot c = (a \cdot b) \cdot c = a \cdot (b \cdot c) = a \cdot b = a$, provando que $a \leq c$. ■

Exercício: Verifique que 0 é o mínimo de A e 1 é o máximo. Verifique que a ordem numa álgebra de Boole é um *reticulado*, isto é, dois elementos quaisquer possuem sempre um supremo (o menor elemento maior ou igual a ambos) e um ínfimo (o maior elemento menor ou igual a ambos). O supremo e o ínfimo de a e b são, respectivamente, $a + b$ e $a \cdot b$, e, para mostrar que eles o são de fato precisamos mostrar o seguinte:

- $a \leq a + b$ e $b \leq a + b$;
- se $a \leq c$ e $b \leq c$ então $a + b \leq c$;
- $a \cdot b \leq a$ e $a \cdot b \leq b$;
- se $c \leq a$ e $c \leq b$ então $c \leq a \cdot b$.

B.2 Álgebras de conjuntos

Para entender melhor o que significam as operações de álgebras de Boole, o melhor exemplo são as álgebras de conjuntos, onde interpretamos a operação $+$ como união, a operação $\cdot$ como intersecção e $-$ como complemento.

Utilizaremos a notação $\mathcal{P}(X)$ para representar o *conjunto de todos os subconjuntos de* X.

Definição B.5. Seja X um conjunto não-vazio. Uma *álgebra de conjuntos sobre* X é uma família $\mathcal{A} \subset \mathcal{P}(X)$ que contém X e é fechado por intersecções finitas e complementos, isto é:

(a) $X \in \mathcal{A}$;

(b) Se $Y, Z \in \mathcal{A}$ então $Y \cap Z \in \mathcal{A}$;

(c) Se $Y \in \mathcal{A}$ então $X \setminus Y \in \mathcal{A}$.

Dessas três propriedades, deduzimos as seguintes:

(d) $\emptyset \in \mathcal{A}$;

(e) Se $Y, Z \in \mathcal{A}$ então $Y \cup Z \in \mathcal{A}$.

O próximo lema pode ser demonstrado através de uma simples verificação dos axiomas de álgebras de Boole.

Lema B.6. *Uma álgebra de conjuntos sobre X é uma álgebra de Boole, onde $0 = \emptyset$, $1 = X$ e as operações $\cdot$, $+$ e $-$ são, respectivamente, intersecção, união e complemento em relação a X.*

Dois exemplos bem conhecidos de álgebras de conjuntos são a álgebra $\mathcal{P}(\mathbb{N})$ (o conjunto de todos os subconjuntos de $\mathbb{N}$), e a álgebra $FinCofin(\mathbb{N})$ (o conjunto dos subconjuntos de $\mathbb{N}$ que são finitos ou cofinitos, isto é, cujo complementar em relação a $\mathbb{N}$ é finito).

Definição B.7. Dadas duas álgebras de Boole $\mathcal{A}$ e $\mathcal{B}$, de domínios A e B, respectivamente, um *homomorfismo* de $\mathcal{A}$ em $\mathcal{B}$ é uma função $h : A \longrightarrow B$ satisfazendo

$$h(0) = 0,\ h(1) = 1$$

e, para todos $x, y \in A$,

$$h(x \cdot y) = h(x) \cdot h(y),\ h(x + y) = h(x) + h(y),\ h(-x) = -h(x).$$

Um *isomorfismo* é um homomorfismo bijetor. Dizemos que $\mathcal{A}$ é *isomorfa* a $\mathcal{B}$ se existe um isomorfismo de $\mathcal{A}$ em $\mathcal{B}$.

A função inversa de um isomorfismo é um isomorfismo (exercício). Portanto, se $\mathcal{A}$ é isomorfo a $\mathcal{B}$ também teremos $\mathcal{B}$ isomorfo a $\mathcal{A}$, o que nos permite dizer, sem risco de ambiguidade, que $\mathcal{A}$ e $\mathcal{B}$ *são isomorfas*.

Na Seção B.4 mostraremos que toda álgebra de Boole é isomorfa a uma álgebra de conjuntos.

B.3 Álgebras de Lindenbaum

Outro exemplo de álgebra de Boole particularmente interessante para o estudo de lógica são as álgebras de Lindenbaum. Focaremos na álgebra de Lindenbaum da lógica proposicional, mas veremos como podemos construir uma álgebra de Lindenbaum a partir de uma ampla gama de sistemas lógicos, incluindo a lógica de primeira ordem.

A ideia geral da álgebra de Lindenbaum é simples: identificamos fórmulas equivalentes como se fossem a mesma, e os operadores $+$, $\cdot$ e $-$ passam a significar $\vee$, $\wedge$ e $\neg$, respectivamente.

Antes de definirmos a álgebra, começamos enunciando um lema cuja demonstração é simples e será deixada ao leitor:

Lema B.8. *Seja L o conjunto das fórmulas da lógica proposicional. Seja $\sim$ uma relação binária em L dada por $A \sim B$ se, e somente se, $A \leftrightarrow B$ é uma tautologia. Então $\sim$ é uma relação de equivalência em L.*

Definição B.9. Definimos a *álgebra de Lindenbaum sobre a lógica proposicional* como a seguinte álgebra de Boole:

- O domínio é $L/\sim$, isto é, o conjunto das classes de equivalência de $\sim$;
- A constante 0 é a classe das contradições, isto é, $0 = [p \wedge \neg p]$;
- A constante 1 é a classe das tautologias, isto é, $1 = [p \vee \neg p]$;
- A operação $+$ é definida como $[A] + [B] = [A \vee B]$;

- A operação $\cdot$ é definida como $[A] \cdot [B] = [A \wedge B]$;
- A operação $-$ é definida como $-[A] = [\neg A]$.

Há algumas coisas, nessa definição, que precisam ser mostradas. Primeiro, como usualmente acontece quando definimos operações em classes de equivalência, precisamos mostrar que as operações estão bem definidas, já que definimos a operação + escolhendo representantes das classes. Notemos, porém, que se $[A'] = [A]$ e $[B'] = [B]$ isso significa que A' é equivalente a A e B' é equivalente a B. Logo (fica como exercício ao leitor mostrar) $A' \vee B'$ é equivalente a $A \vee B$ e, em particular, $[A' \vee B'] = [A \vee B]$. Portanto, a definição de $[A] + [B]$ como $[A \vee B]$ independe da escolha dos representantes, e por isso está bem definida. O mesmo vale para as operações $\cdot$ e $-$.

Precisamos provar que essa definição satisfaz os axiomas de álgebras de Boole, conforme a Definição B.1. Mas isso é um simples exercício de verificação de tautologias, que o leitor poderá resolver sem dificuldades.

Analisemos a ordem na álgebra de Lindenbaum. Pela definição de ordem em álgebras de Boole, temos que $[A] \leq [B]$ se, e somente se, $[A] \cdot [B] = [A]$. Isto é, se $(A \wedge B) \leftrightarrow A$ é uma tautologia. Mas reparem que essa fórmula só será falsa se A for verdadeira e B for falsa. Logo, essa fórmula é equivalente a $A \to B$, o que nos leva ao seguinte resultado:

Lema B.10. *Na álgebra de Lindenbaum da lógica proposicional,* $[A] \leq [B]$ *se, e somente se,* $A \to B$ *é uma tautologia.*

Notem que $(p \wedge \neg p) \to A$ e $A \to (p \vee \neg p)$ são tautologias, para qualquer fórmula A. Ou seja, uma contradição implica qualquer fórmula, e qualquer fórmula implica uma tautologia. Isso justifica o fato já provado (para qualquer álgebra de Boole) de que $0 \leq x$ e $x \leq 1$, para qualquer x.

Falamos, na seção anterior, que toda álgebra de Boole pode ser representada por uma álgebra de conjuntos. Em particular, a álgebra de Lindenbaum pode ser representada por uma álgebra de conjuntos. Veremos uma maneira de fazer essa representação, o que irá esclarecer melhor ainda a relação entre os operadores lógicos e as operações conjuntísticas.

Seja X o conjunto de todas as valorações da lógica proposicional. Considere $\mathcal{P}(X)$ o conjunto das partes de X, isto é, o conjunto de todos os subconjuntos de X. Vamos definir uma função injetora f de $L/\sim$ em $\mathcal{P}(X)$ da seguinte forma:

$$f([A]) = \{V \in X : V(A) = 1\}$$

Ou seja, $f([A])$ é o conjunto das valorações para as quais A é verdadeira.

Notemos que f está bem definida pois, por definição, se A é equivalente a A' então as valorações que satisfazem A são as mesmas que satisfazem A'. Logo, $f([A])$ não depende da escolha de representantes. Também notemos que f é injetora. De fato, se $f([A]) = f([B])$ isso significa que, para toda valoração V, $V(A) = 1$ se, e somente se, $V(B) = 1$. Mas isso implica que $A \leftrightarrow B$ é uma tautologia e, portanto, $[A] = [B]$.

Como nenhuma valoração satisfaz uma contradição, temos que $f(0) = \emptyset$. Por outro lado, as tautologias são verdadeiras para qualquer valoração. Logo, $f(1) = X$. As valorações que satisfazem $A \wedge B$ são justamente aquelas que satisfazem A e satisfazem B. Logo, $f([A \wedge B]) = f([A]) \cap f([B])$. Analogamente, $f([A \vee B]) = f([A]) \cup f([B])$ e $f([\neg A]) = X \setminus f([A])$.

Portanto, f é um homomorfismo da álgebra de Lindenbaum na álgebra $\mathcal{P}(X)$. Se tomarmos $\mathcal{A}$ a imagem de f, as contas acima mostram que $\mathcal{A}$ é uma álgebra de conjuntos, e f é um isomorfismo sobre $\mathcal{A}$.

Resumindo: podemos identificar uma classe de equivalência de uma fórmula da lógica proposicional com o conjunto das valorações que a tornam verdadeira. Essa é uma maneira de interpretarmos os diagramas de Venn-Euler: cada ponto do diagrama representa uma valoração, e as regiões que pintamos são classes de equivalência de fórmulas, isto é, conjuntos de valorações. Notemos que, nos diagramas de Venn-Euler, duas fórmulas equivalentes são representadas pela mesma região. Ou seja, assim como acontece na álgebra de Lindenbaum, os diagramas de Venn-Euler não distinguem fórmulas equivalentes.

As álgebras de Lindenbaum também podem ser aplicadas, da mesma maneira, à lógica de primeira ordem. Veja que a construção de Henkin (Teorema 7.17) – usada para mostrar o teorema da completude da lógica de primeira ordem – se assemelha à das álgebras de Lindenbaum.

Descreveremos, agora, uma definição mais geral para as álgebras de Lindenbaum. Para isso, introduzimos a seguinte definição:

Definição B.11. Uma *lógica* é uma tripla $\mathcal{L} = (A_\mathcal{L}, L_\mathcal{L}, \vdash_\mathcal{L})$, onde $A_\mathcal{L}$ é um conjunto de símbolos, $L_\mathcal{L}$ é um conjunto não-vazio de fórmulas (que são sequências finitas de elementos de $A_\mathcal{L}$) e $\vdash_\mathcal{L}$ é uma relação contida em $\mathcal{P}(L_\mathcal{L}) \times L_\mathcal{L}$.

Dizemos que $\mathcal{L}$ é uma *extensão da lógica proposicional* se os símbolos $\vee$ e $\neg$ pertencem a $A_\mathcal{L}$ e valem as seguintes propriedades:

- Se A e B pertencem a $L_\mathcal{L}$, então $(\neg A)$ e $(A \vee B)$ pertencem a $L_\mathcal{L}$;

- Se A é uma instância de tautologia, então $\Gamma \vdash_{\mathcal{L}} A$, para todo $\Gamma \subset L_{\mathcal{L}}$;
- Se $\Gamma \vdash_{\mathcal{L}} A$ e $\Gamma \vdash_{\mathcal{L}} (\neg A) \vee B$ então $\Gamma \vdash_{\mathcal{L}} B$.

Além disso, dizemos que $\mathcal{L}$ é *consistente* se existe pelo menos uma fórmula $A \in L_{\mathcal{L}}$ tal que não ocorre $\emptyset \vdash_{\mathcal{L}} A$. Se $\mathcal{L}$ estende a lógica proposicional, isso equivale a dizer que não existe uma fórmula A tal que $\emptyset \vdash_{\mathcal{L}} A$ e $\emptyset \vdash_{\mathcal{L}} \neg A$.

A definição de instância de tautologia é análoga à Definição 6.1.

Se $\mathcal{L}$ é uma lógica que estende a lógica proposicional, podemos definir os conectivos $\wedge$, $\rightarrow$ e $\leftrightarrow$ do mesmo modo como fizemos para lógica proposicional e de primeira ordem (vejam Capítulos 2 e 4).

Escrevemos $\vdash_{\mathcal{L}} A$ quando $\emptyset \vdash_{\mathcal{L}} A$.

Enunciamos, agora, a definição geral de álgebra de Lindenbaum.

Definição B.12. Seja $\mathcal{L}$ uma lógica consistente que estende a lógica proposicional. Definimos a *álgebra de Lindenbaum da lógica* $\mathcal{L}$ como a estrutura $(\mathcal{A}, +, \cdot, -, 0, 1)$ definida como

- $\mathcal{A}$ é o quociente $\mathcal{L}/\sim$, onde $\sim$ é a relação de equivalência dada por $A \sim B$ se, e somente se, $\vdash_{\mathcal{L}} A \leftrightarrow B$;
- $[A] + [B]$ é definido como $[A \vee B]$;
- $[A] \cdot [B]$ é definido como $[A \wedge B]$;
- $-[A]$ é definido como $[\neg A]$;
- 0 é a classe $[A \wedge \neg A]$, para algum A em $L_{\mathcal{L}}$;
- 1 é a classe $[A \vee \neg A]$, para algum A em $L_{\mathcal{L}}$.

Precisamos provar, novamente, para essa definição geral de lógica, que a definição acima é boa. Isto é, precisamos mostrar que $\sim$ é, de fato, uma relação de equivalência, as operações $+$, $\cdot$ e $-$ independem da escolha do representante, e as definições de 0 e 1 independem da escolha da fórmula A.

Resta, é claro, provar que a definição acima é, de fato, uma álgebra de Boole. Para isso, é essencial a hipótese de que $\mathcal{L}$ é consistente.

O Lema B.10 vale para as álgebras de Lindenbaum em geral. Isto é, $[A] \leq [B]$ se, e somente se, $\vdash_{\mathcal{L}} A \rightarrow B$.

B.4 Teorema de representação de Stone

Antes de mostrarmos o teorema de representação de Stone, precisamos discutir sobre ultrafiltros em uma álgebra de Boole e, para isso, enunciaremos o lema de Zorn.

Introduzimos alguma definições sobre ordem. Chamamos de *conjunto ordenado* um par $(X, \leq)$, onde X é um conjunto não-vazio e $\leq$ é uma ordem sobre X. Uma *cadeia* em $(X, \leq)$ é um subconjunto de X que é totalmente ordenado com a ordem $\leq$. Isto é, $C \subset X$ é uma cadeia em $(X, \leq)$ se, para todos $x, y \in C$, temos $x \leq y$ ou $y \leq x$.

Um elemento m de X é *maximal* se não existe $x \in X$ tal que $m \leq x$ e $m \neq x$. Ou seja, m não necessariamente é maior que todos os elementos de X, mas *não é menor* que qualquer outro elemento de X.

Se S é um subconjunto não-vazio de X, dizemos que $s \in X$ é um *limitante superior* de S se $x \leq s$, para todo $x \in X$.

Teorema B.13 (Lema de Zorn)**.** *Seja $(X, \leq)$ um conjunto ordenado na qual toda cadeia admite um limitante superior. Então $(X, \leq)$ possui um elemento maximal.*

O lema de Zorn é uma consequência do axioma da escolha. De fato, ele é equivalente ao axioma da escolha, em ZF. Ou seja, se substituirmos o axioma da escolha pelo Lema de Zorn, em ZFC, obtemos um sistema equivalente a ZFC, provando exatamente os mesmos teoremas. Indicamos [9] para essa demonstração.

Definição B.14. Sejam $\mathcal{A} = (A, +, \cdot, -, 0, 1)$ uma álgebra de Boole e $\leq$ a ordem dada pela Definição B.3. Dizemos que um subconjunto F de A é um *filtro* sobre $\mathcal{A}$ se satisfaz as seguintes condições:

- $0 \notin F$;
- $1 \in F$;
- se $a \in F$ e $a \leq b$ então $b \in F$;
- se $a, b \in F$ então $a \cdot b \in F$;

Um filtro $u \subset A$ é um *ultrafiltro* sobre $\mathcal{A}$ se u não está contido propriamente em nenhum filtro. Isto é, se F é um filtro e $u \subset F$ então $u = F$.

Usando o lema de Zorn mostraremos que todo filtro pode ser estendido a um ultrafiltro, conforme o seguinte lema:

Lema B.15. *Sejam $\mathcal{A} = (A, +, \cdot, -, 0, 1)$ uma álgebra de Boole e F um filtro sobre $\mathcal{A}$.*

(a) *F é um ultrafiltro se, e somente se, para todo $a \in A$, temos $a \in F$ ou $-a \in F$, mas não ambos.*

(b) *Se F é um ultrafiltro e $a + b \in F$, então $a \in F$ ou $b \in F$.*

(c) *Existe um ultrafiltro u tal que $F \subset u$.*

Demonstração: Para mostrar a parte (a), suponha que F é um filtro e que, para todo $a \in A$, temos $a \in F$ ou $-a \in F$. Mostraremos que F é um ultrafiltro. De fato, suponha que existe um filtro G tal que $G \neq F$ e $F \subset G$. Isso significa que existe $a \in G$ tal que $a \notin F$. Mas, pela hipótese sobre F, temos que $-a \in F$ e, portanto, $a \in G$. Como G é um filtro, isso implica que $a \cdot (-a) \in G$. Mas, como $a \cdot (-a) = 0$, isso contradiz que G é um filtro.

Reciprocamente, se F é um filtro já vimos que não podemos ter ambos a e $-a$ pertencentes a F. Suponha, portanto, que F é um filtro e existe $a \in A$ tal que $a \notin F$ e $-a \notin F$. Mostraremos que F não é um ultrafiltro, provando que existe um filtro maior que F contendo a ou $-a$.

Suponha que existem $b \in F$ e $c \in F$ tais que $b \cdot a = 0$ e $c \cdot (-a) = 0$. Em particular, temos que $b \cdot c \in F$, $(b \cdot c) \cdot a = 0$ e $(b \cdot c) \cdot (-a) = 0$. Logo, usando distributividade e complementação, temos

$$0 = ((b \cdot c) \cdot a) + ((b \cdot c)(-a)) = (b \cdot c) \cdot (a + (-a)) = b \cdot c$$

Portanto, concluímos que $b \cdot c = 0$ e pertence a F, contradizendo que F é um filtro.

Com isso provamos, por absurdo, que $b \cdot a \neq 0$, para todo $b \in F$, ou $b \cdot (-a) \neq 0$, para todo $b \in F$. Seja a' igual a a ou $-a$, satisfazendo $b \cdot a' \neq 0$, para todo $b \in F$. Defina G como o seguinte conjunto:

$$G = \{x \in A : \exists y (y \in F \wedge y \cdot a' \leq x)\}$$

Mostraremos que G é um filtro. Da hipótese sobre a' segue que $0 \notin G$. Como $1 \in F$ e $1 \cdot a' \leq 1$, temos que $1 \in G$. Se $x \leq y$, para $x \in G$ e $y \in A$, então existe $b \in F$ tal que $b \cdot a' \leq x$. Pela transitividade de $\leq$, concluímos

que $b \cdot a' \leq y$ e, portanto, $y \in G$. Falta mostrar que, se b e c pertencem a G, então $b \cdot c \in G$.

Sejam b e c elementos de G. Temos que existem $b', c' \in F$ tais que $(b' \cdot a') \leq b$ e $(c' \cdot a') \leq c$. Isto é,

$$(b' \cdot a') \cdot b = b' \cdot a' \tag{1}$$

e

$$(c' \cdot a') \cdot c = c' \cdot a' \tag{2}$$

Como $b' \cdot c' \in F$, uma vez que F é um filtro, para mostrar que $b \cdot c$ pertence a G é suficiente mostrar que $(b' \cdot c') \cdot a' \leq b \cdot c$. Isto é, mostraremos que

$$(b' \cdot c' \cdot a') \cdot (b \cdot c) = b' \cdot c' \cdot a' \tag{3}$$

Usando (1), (2) a idempotência ($a' \cdot a' = a'$) e as propriedades de associatividade e comutatividade, temos que

$$(b'c') \cdot a' \cdot (bc) = (b' \cdot a' \cdot b) \cdot (c' \cdot a' \cdot c) = (b'c') \cdot a',$$

provando o que queríamos.

Provamos, portanto, que existe um filtro que contém propriamente o filtro F, mostrando que F não é um ultrafiltro e concluindo a parte (a) do lema.

A parte (b) segue da parte (a) e das leis de De Morgan. De fato, suponha que F é um ultrafiltro, $a + b \in F$ e tanto a quanto b não pertencem a F. Pela parte (a) isso significa que $-a \in F$ e $-b \in F$. Como F é um filtro, temos que $(-a) \cdot (-b) \in F$. Pelas leis de De Morgan, $-(a+b) = (-a) \cdot (-b)$. Portanto, tanto $a + b$ quanto $-(a + b)$ pertencem a F, de onde segue que $0 \in F$, contradizendo que F é um filtro.

Para a parte (c) usaremos o lema de Zorn. Seja X o conjunto de todos os filtros em $\mathcal{A}$ que contêm F, e seja C uma cadeia em $(X, \subset)$. Isto é, para todos F_1 e F_2 pertencentes a C, vale $F_1 \subset F_2$ ou $F_2 \subset F_1$. Deixamos como exercício ao leitor provar que $\bigcup C$ é um filtro que contém F. Em particular, $\bigcup C \in X$ e $G \subset \bigcup C$, para todo $G \in C$. Portanto, C possui limitante superior. Pelo lema de Zorn, $(X, \subset)$ possui um elemento maximal u. Isto é, u é um filtro, contém F, e não está contido em qualquer outro filtro sobre $\mathcal{A}$. Ou seja, u é um ultrafiltro que contém F, como queríamos provar. ■

Teorema B.16. *Toda álgebra de Boole é isomorfa a uma álgebra de conjuntos, com as operações usuais descritas no Lema B.6.*

Demonstração: Definimos $S(\mathcal{A})$ o conjunto dos ultrafiltros sobre $\mathcal{A}$ (chamado de *espaço de Stone* da álgebra $\mathcal{A}$). Defina uma função $f : A \longrightarrow \mathcal{P}(S(\mathcal{A}))$ do seguinte modo:

$$f(a) = \{u \in S(\mathcal{A}) : a \in u\},$$

para todo $a \in A$.

Seja X a imagem de f. Mostremos que a imagem de f é uma álgebra de conjuntos. De fato, $\emptyset \in X$, pois $f(0) = \emptyset$, uma vez que 0 não pertence a nenhum filtro. Por outro lado, como $1 \in u$, para todo ultrafiltro u, temos que $f(1) = S(\mathcal{A})$.

Pelo Lema B.15, parte (a), para todo ultrafiltro u temos que $a \in u$ se, e somente se $-a \notin u$. Portanto,

$$f(-a) = S(\mathcal{A}) \setminus f(a),$$

provando que X é fechado pela operação de complemento.

Verifiquemos que X é fechado por uniões e intersecções, provando que $f(a \cdot b) = f(a) \cap f(b)$ e $f(a + b) = f(a) \cup f(b)$.

Suponha que $u \in f(a \cdot b)$. Isto significa que u é um ultrafiltro e $a \cdot b \in u$. Portanto, como $a \cdot b \leq a$ e $a \cdot b \leq b$, temos que $a \in u$ e $b \in u$. Logo, $u \in f(a) \cap f(b)$. Reciprocamente, se $u \in f(a) \cap f(b)$, temos que $a \in u$ e $b \in u$ e, como u é um filtro, $a \cdot b \in u$, provando que $u \in f(a \cdot b)$.

Suponhamos, agora, que $u \in f(a + b)$. Temos que $a + b \in u$ e, pelo Lema B.15, parte (b), vale $a \in u$ ou $b \in u$, de onde segue que $u \in f(a) \cup f(b)$. Reciprocamente, se $u \in f(a)$, temos $a \in u$ e, como $a \leq a + b$, valem $a + b \in u$ e, portanto, $u \in f(a + b)$. Analogamente, se $u \in f(b)$ então $u \in f(a + b)$.

Mostramos não apenas que X é uma álgebra de conjuntos, mas que f é um homomorfismo de $\mathcal{A}$ em X. Para mostrarmos que f é um isomorfismo, basta provarmos que f é injetora. Sejam a e b dois elementos distintos de A e provemos que $f(a) \neq f(b)$.

Vejamos que $a \cdot (-b)$ ou $(-a) \cdot b$ é diferente de 0. Suponhamos, por absurdo, que ambos são iguais a 0. Pelo Teorema B.2, itens 5 e 6, $-(a \cdot (-b)) = (-a) + b$. Como $-0 = 1$ (exercício), disso segue que $(-a) + b = 1$. Logo, de $(-a) \cdot b = 0$ e do item 4 do Teorema B.2 segue que $b = -(-a)$ e, pelo item 5 do mesmo teorema, $b = a$.

Assumiremos, sem perda de generalidade, que $a \cdot (-b) \neq 0$. O caso $(-a) \cdot b \neq 0$ é análogo. Defina

$$F = \{x \in A : a \cdot (-b) \leq x\}$$

É fácil verificar que F é um filtro, e deixamos a prova por conta do leitor. Pelo Lema B.15, parte (c), existe um ultrafiltro u que contém F. Como $a \cdot (-b) \leq a$ e $a \cdot (-b) \leq b$ temos que a e $-b$ pertencem a u. Logo, pelo item (a) do Lema B.15, $b \notin u$. Isso prova que $u \in f(a)$ mas $u \notin f(b)$, provando que $f(a) \neq f(b)$. ■

Notas sobre o espaço de Stone: para quem já estudou topologia, convém ressaltar a importância da construção feita acima – mais que o próprio resultado do teorema – para esse ramo da matemática. O conjunto $S(\mathcal{A})$ é um espaço topológico compacto e 0-dimensional (isto é, possui uma base de abertos-fechados), considerando a topologia gerada pela imagem de f. Isto é, os abertos de $S(\mathcal{A})$ são as uniões arbitrárias de conjuntos da forma $f(a)$ (que, normalmente, indicamos por a^*).

Reciprocamente, todo espaço topológico compacto e 0-dimensional é homeomorfo ao espaço de Stone da álgebra de conjuntos dos abertos-fechados desse espaço. Dessa forma, o teorema de representação de Stone fornece um dualismo bastante útil entre as álgebras de Boole e os espaços topológicos compactos e 0-dimensionais.

Exercícios

1. Prove formalmente o Teorema B.2, usando a axiomatização da lógica de primeira ordem.

2. Seja $\mathcal{A} = (A, +, \cdot, -, 0, 1)$ uma álgebra de Boole. Um subconjunto não-vazio S de A é uma *família independente de* $\mathcal{A}$ se satisfaz a seguinte condição: se $n \in \mathbb{N}$, $a_1, \ldots, a_n$ são elementos distintos de S e $a'_1, \ldots a'_n$ são elementos de A tais que, para cada i, $a'_i = a_i$ ou $a'_i = -a_i$, então $a'_1 \cdot \ldots \cdot a'_n \neq 0$.

Prove que, na álgebra de Lindenbaum da lógica proposicional, as classes de equivalência das fórmulas atômicas formam uma família independente.

3. Seja $\mathcal{A} = (A, +, \cdot, -, 0, 1)$ uma álgebra de Boole. Dizemos que um subconjunto S de A *gera* a álgebra $\mathcal{A}$ se, para todo $a \in A \setminus \{1\}$, existem $b_1, \ldots, b_n \in A$ tais que $a = b_1 + \ldots + b_n$ e cada b_i é da forma $c^i_1 \cdot \ldots \cdot c^i_{m_i}$, onde, para cada $i \leq n$ e $j \leq m_i$, temos $c^i_j \in S$ ou $-c^i_j \in S$.

Uma álgebra de Boole é *livre* se é gerada por uma família independente.

Prove que a álgebra de Lindenbaum da lógica proposicional é livre.

4. Sejam n um número natural e $p_1, \ldots, p_n$ fórmulas atômicas da lógica proposicional. Seja L' o conjunto das fórmulas da linguagem da lógica proposicional que não possuem nenhhuma subfórmula atômica além das fórmulas de p_1 a p_n. Defina $\mathcal{A}$ como em B.9, tomando L' no lugar de L (isto é, $\mathcal{A}$ é a *álgebra de Lindenbaum da linguagem* L').

(a) Prove que o domínio de $\mathcal{A}$ possui 2^{2^n} elementos.

(b) No caso $n = 2$, descreva todos os elementos do domínio de $\mathcal{A}$, escolhendo um representante para cada classe de equivalência.

5. Prove que uma álgebra livre gerada por uma família independente de tamanho n tem 2^{2^n} elementos.

6. Prove que duas álgebras livres finitas, com a mesma quantidade de elementos (no domínio), são sempre isomorfas.

7. Mostre que o enunciado do exercício 6 não é verdadeiro se tirarmos a hipótese das álgebras serem livres. Isto é, mostre que existem duas álgebras finitas não isomorfas e que possuem a mesma quantidade de elementos.

Sugestão: Construa uma álgebra de conjuntos formada por 16 elementos e que é gerada por uma família não independente de conjuntos. Inspire-se nos diagramas de Venn-Euler.

Bibliografia

[1] Aragona, J. *Números Reais*. Editora Livraria da Física, São Paulo, 2010.

[2] Barker, S, F. *Filosofia da Matemática*, 2ª ed. Zahar Editores, Rio de Janeiro, 1976.

[3] Carnielli, W.; Epstein, R. L. *Computabilidade, Funções Computáveis, Lógica e os Fundamentos da Matemática*, 2ª ed. Editora Unesp, São Paulo, 2005.

[4] Chellas, B. *Modal Logic: an Introduction*. Cambridge University Press, Cambridge, 1980.

[5] Doxiadis, A.; Papadimitriou, C. H.; *Logicomix – An Epic Search for Truth*. Bloomsburry USA, Nova York, 2009.

[6] *Enciclopédia Barsa Universal*, 3ª ed. Editorial Planeta, S.A., 2010

[7] Ferreirós, J. *Labyrinth of Thought: a History of Set Theory and its Role in Modern Mathematics*. Birkhäuser, Berlin , 1999.

[8] Gödel, K. *On Formally Undecidable Propositions of Principia Mathematica and Related Systems*. Dover Publications, Nova York, 1992.

[9] Halmos, P. R. *Teoria Ingênua dos Conjuntos*. Editora Polígono, São Paulo, 1973.

[10] Hawking, S. *Uma Breve História do Tempo*. Editora Rocco, Rio de Janeiro, 1988.

[11] Hawking, S. *God Created the Integers*. Running Press Book Publishers, Filadélfia, 2007.

[12] Hofstadter, D. R. *Gödel, Escher, Bach: an Eternal Golden Braid*. Basic Bookes, Nova York, 1979.

[13] Jech, T. J. *The Axiom of Choice*. Dover Publications, Nova York, 2008.

[14] Kline, M. *Mathematical Thought – from Ancient to Modern Times*. Oxford University Press, Nova York, 1972.

[15] Koppelberg, S. *General Theory of Boolean Algebras*. Em Monk, J.D., editor, *Handbook of Boolean Algebras*. Elsevier Science Publishers B.V., Amsterdam, 1989.

[16] Kunen, K. *Set Theory. An Introduction to Independence Proofs*. North Holland, 1980.

[17] Miraglia, F. *Teoria dos Conjuntos: um Mínimo*. EDUSP, São Paulo, 1992.

[18] Navega, S. *Pensamento Crítico e Argumentação Sólida*. Publicações Intelliwise, São Paulo, 2005.

[19] Nagel, E.; Newman, J. R. *A Prova de Gödel*, 2ª ed. Perspectivas, São Paulo, 2009.

[20] Rosser, J. B. *Extensions of some theorems of Gödel and Church.* Journal of Symbolic Logic, 1: 87–91. 1936.

[21] Russell, B. *Ensaios Céticos*. LP&M editores, 1996.

[22] Russell, B.; Whitehead, A. N. *Principia Mathematica*. 2ª Ed. Cambridge University Press, Cambridge, 1927.

[23] Santos, L. H. L. *O Olho e o Microscópio*. Nau Editora, 2008.

[24] Silva, J. J. *Filosofias da Matemática*. Editora Unesp, São Paulo, 2007.

[25] Smullyam, R. M. *First-order Logic*. Dover Publications, Nova York, 1995.

[26] Smullyam, R. M. *O Enigma de Sherazade*. Jorge Zahar Editor, 1998.

[27] Smullyam, R. M. *Alice no País dos Enigmas*. Jorge Zahar Editor, 2000.

[28] Smullyam, R. M. *A Dama ou o Tigre?*. Jorge Zahar Editor, 2004.

[29] Stewart, I. *Almanaque das Curiosidades Matemáticas*. Jorge Zahar Editor, Rio de Janeiro, 2008.

[30] Stoll, R. R. *Set Theory and Logic*. Dover Publications, Nova York, 1979.

[31] Tiles, M. *The Philosophy of Set Theory: an Historical Introduction to Cantor's Paradise*. Dover Publications, Nova York, 1989.

Índice