UMA INTRODUÇÃO À LÓGICA, MATEMÁTICA E COMPUTACIONAL

AUGUSTO J. FRANCO DE OLIVEIRA
Universidade de Évora

LÓGICA & ARITMÉTICA

Introdução à Lógica, Matemática e Computacional

Terceira edição revista e ampliada

Capa:
Fotocomposição: Gradiva
Impressão e acabamento: *Manuel Barbosa e Filhos, Lda.*

Gradiva — Publicações, Lda.
Rua Almeida e Sousa, 21, r/c Esqº. , 1399-041 LISBOA
3.ª edição revista e ampliada da obra com
o título *Lógica e Artmética,* 2.ª edição, 1998.
Depósito legal Nº. */06*

AMS Subject Classification (2000): 03-01

À memória de António A. R. Monteiro
(1907-1980)

ÍNDICE

III. CÁLCULO DE PREDICADOS

IV. ARITMÉTICA DE PEANO

V. O QUE É A LÓGICA MATEMÁTICA?

Prefácio

Este livro pretende ser uma iniciação informal à lógica e aritmética (formais), tendo em conta opções e condicionamentos diversos, que se traduzem na escolha e nível de aprofundamento dos tópicos abordados, como a seguir se explica, sem, contudo, deixar de reflectir a preferência e a experiência pessoais. Por esses motivos, não aprofundo discussões filosóficas ou técnicas de questões de fundamentos. Mas alguma coisa vou dizendo, em curtas incisões, com maior desenvolvimento no final do Cap. IV e no Cap. V, onde são discutidas algumas questões de filosofia e fundamentos da matemática. As primeiras secções do último capítulo podem, aliás, ser lidas em primeiro lugar, ou logo após o primeiro, com algumas reservas.

No que respeita à lógica, trato essencialmente daquela parte da lógica «clássica» que analisa as proposições e sistematiza o raciocínio, nomeadamente as proposições matemáticas e o raciocínio dedutivo comum em matemática. Esta lógica é apresentada sob dois pontos de vista, o semântico, como motivação, e o sintáctico-dedutivo, e interessa, obviamente, a todo e qualquer ramo do saber ou pensamento. O primeiro capítulo é, a este respeito, bastante ameno e destina-se apenas a introduzir informalmente algumas ideias (formalização, interpretação, validade, consequência lógica), e notações (simbolismo lógico e não lógico) que são precisadas e desenvolvidas em capítulos posteriores. Por esta razão, o seu conteúdo matemático é praticamente nulo (exceptuando a última secção, sobre árvores).

O ponto de vista dedutivo é desenvolvido a partir do segundo capítulo através de um *sistema de dedução natural*, primeiro para o cálculo proposicional e depois para o cálculo de predicados com igualdade, sistema esse que é caracterizado por um grande número de regras de inferência de fácil aceitação e manipulação. O ponto de vista semântico, exigindo, em geral, maior destreza e maturidade matemática[1] e os resultados metamatemáticos mais importantes, são, no entanto, abordados mais levemente do que seria natural num livro ou curso avançado de lógica matemática. Assim, por exemplo, não demonstro as propriedade de validade (ou

[1] Por exemplo, algumas noções conjuntistas, como as noções de função ou aplicação e de estrutura matemática.

adequação) e de completude semântica do sistema dedutivo para o cálculo de predicados, mas chamo a atenção para a importância dessas propriedades.

Sem dificuldade se complementa o texto com as demonstrações omissas, se ele for utilizado como base de um curso universitário, mas entendo que tais demonstrações se justificam somente num livro ou curso um tanto mais avançado (talvez, quem sabe, numa futura reedição) quando há oportunidade para desenvolver e aplicar as suas inúmeras e importantes consequências. Por outro lado, é talvez mais vantajoso, num tal primeiro curso de lógica e fundamentos, complementar o texto dos primeiros capítulos com um pouco de teoria axiomática dos conjuntos ou de teoria da computabilidade.

No Cap. IV desenvolve-se um pouco a aritmética elementar (como teoria formal), outra disciplina lamentavelmente ausente dos programas liceais e universitários. Este capítulo termina com uma discussão, novamente informal, de alguns resultados limitativos acerca das teorias formais contendo a aritmética elementar, como os metateoremas de Gödel e Tarski, de grande importância para os fundamentos.

Em resumo, penso que a selecção e nível de aprofundamento dos assuntos abordados tipifica os interesses e necessidades de um vasto leque de potenciais leitores que poderão, assim, identificar mais facilmente as ideias centrais de uma disciplina de lógica concebida em moldes actuais e orientar-se para os tópicos ou variantes mais especializados, desde as lógicas não-clássicas (modais, deôntica, intuicionista, paraconsistente, etc.) às extensões infinitárias da lógica clássica. O último capítulo, o quinto, dá conta de algumas linhas directrizes de desenvolvimento dos tópicos apresentados e de possibilidades de extensão ou aplicação, e de alguns pontos de vista alternativos.

O estilo da prosa é intencionalmente informal, como já se disse, próprio de uma iniciação, mas suficientemente preciso para permitir voos mais altos a quem se queira aventurar seriamente na lógica matemática. Com esta finalidade se dão bastantes referências bibliográficas, quer em notas de rodapé, quer no final, criteriosamente escolhidas. Na sua grande maioria, tais referências existem nas nossas bibliotecas universitárias.

Os exercícios constituem parte integrante do livro, e muitos acompanham o texto, sobretudo nos capítulos intermédios. Alguns exercícios, no fim de cada capítulo, são acompanhados de sugestões, mas nenhum é excessivamente difícil. Os mais difíceis são, contudo, assinalados com *, podendo ser omitidos numa primeira leitura. No fim do livro encontram-se algumas soluções.

Uma versão reduzida dos três primeiros capítulos foi leccionada, com relativo sucesso, num encontro da Associação de Professores de Matemática (APM) em Viana do Castelo, em Outubro de 1989. O mesmo sistema dedutivo foi leccionado, durante alguns anos, no curso de Lógica Matemática, no primeiro e segundo anos da licenciatura em Matemática da Faculdade de Ciências de Lisboa.

Julgo parte do conteúdo (as secções não assinaladas com *) adequado para um primeiro contacto com coisas lógicas, ao nível dos anos terminais do ensino secundário ou do primeiro ano de uma licenciatura em Matemática, Informática,

Engenharia ou Letras (Filosofia), ou até para o leitor autodidacta. A escolha de assuntos e o nível de tratamento dos mesmos, com o mínimo de pressupostos, tem fortemente em conta este público vasto e heterogéneo. Mas trata-se, em todo o caso, do mínimo que o leitor intencional quererá saber (e *saber fazer*), tão bem como saberá, talvez, aplicar uma regra de três, resolver uma equação do segundo grau ou calcular uma área.

Dedico este trabalho à memória do matemático e lógico António Aniceto Ribeiro Monteiro que, em terras distantes de outro continente, fundou e expandiu uma escola de lógica matemática. Antes de partir, porém, publicou entre nós (em colaboração com José da Silva Paulo) um livrinho de Aritmética Racional, em 1945, que é do melhor que conheço em termos de iniciação matemática (e metamatemática!) em qualquer língua e época. Utilizei-o em algumas passagens e para os exercícios do Cap. IV. Além disso, recorro muitas vezes a ele pelo prazer da leitura e para inspiração no seu extraordinário sentido didáctico. Não apenas por estas razões, é um livrinho actualíssimo que urge reeditar. Aqui fica a recomendação.

Agradeço aos meus amigos Dr. Carlos Lourenço (CERN) e Prof. Paulo Almeida (IST) a paciente revisão e os inúmeros comentários que muito contribuíram para a clareza e acuidade da exposição; ao Prof. Paulo Almeida, em particular, por me ter convencido a reescrever o prefácio e acrescentar o capítulo final, cuja primeira parte (V.1-V.3) constitui uma versão revista e ampliada de um pequeno texto escrito noutra ocasião. Ao Departamento de Matemática da Faculdade de Ciências de Lisboa e ao Centro de Matemática e Aplicações Fundamentais agradeço as facilidades de preparação do manuscrito original. Devo também agradecer à APM (na 1.ª edição) e à Gradiva terem proporcionado esta nova experiência editorial. Espero que resulte num incentivo a todos os meus colegas e mestres para tornarem acessíveis a um vasto público (que por certo existe ou existirá) os frutos da sua experiência e labor.

A 2.ª edição (1996) teve algumas alterações e acrescentos à primeira, para além das correcções que se impunham (não muitas, aliás, mas mais do que gostaríamos fossem necessárias). Mais algumas correcções para a primeira edição brasileira foram incorporadas em 1968. O texto foi todo revisto e composto em $\mathbb{EXP}$ 5.0.2. Aumentou-se o leque de exercícios propostos e resolvidos de cada secção (alguns saídos em exames) e acrescentaram-se algumas secções novas para satisfazer os interesses dos vários públicos que, aparentemente, acolheram bem as duas primeiras edições. O Cap. IV foi o que teve menos alterações. As secções novas de índole mais técnica são assinaladas com * e podem ser omitidas sem quebra de continuidade ou deixadas para leitura posterior. Algumas dessas secções contêm aplicações não triviais para as quais se exigem alguns conhecimentos matemáticos.

Muitas matérias que eu gostaria de ver incluídas num manual de (introdução à) lógica matemática ficam ainda de fora, para não alterar substancialmente o carácter informal e popular que intencionalmente se quis imprimir à obra desde o primeiro momento. Mencionemos, entre outras, o cálculo de sequentes de Gentzen, um pouco de teoria dos modelos e de lógica e matemática intuicionistas e uma introdução folgada à teoria da computabilidade. Em todo o caso, o livro como está já

contém matéria que excede as possibilidades de leccionação num semestre universitário. O Prefácio da primeira edição foi ligeiramente retocado e a bibliografia foi também actualizada com algumas das melhores obras que têm sido publicadas nos últimos anos.

Agradeço particularmente a três pessoas e colectivamente a todas as outras, incluindo os meus alunos na Faculdade de Ciências da Universidade de Lisboa das cadeiras de *Lógica e Fundamentos da Geometria* e de *Lógica de Primeira Ordem* em anos recentes, e aos alunos de *Lógica Computacional* na Universidade de Évora. Aos Professores F. R. Dias Agudo e aos meus colegas Fernando Ferreira e Ana Isabel Matos, as críticas a alguns aspectos (terminológicos e não só) da primeira edição e ao acompanhamento da redacção das alterações e acrescentos na segunda, respectivamente, e ao Francisco Coelho pelo apoio logístico relativamente a esta edição. A todos os meus sinceros agradecimentos e votos para que continuem criticando e sugerindo melhorias.

Colégio Luís Verney
1 de Fevereiro de 2006.

AJFO

Capítulo I

ARGUMENTAÇÃO VÁLIDA. ELEMENTOS DE ANÁLISE LÓGICA

I.1 Argumentos

Um **argumento** é uma sequência finita de proposições (asserções, sentenças) de determinada linguagem, digamos

$$(*) \qquad \phi_1, ..., \phi_n, \psi \quad (n \geq 1)$$

As n primeiras proposições, $\phi_1, ..., \phi_n$, dizem-se as **premissas** do argumento $(*)$, e a última proposição, ψ, é a **conclusão** do dito argumento. Ao fazer a leitura de $(*)$ é costume inserir uma das locuções «portanto», «por conseguinte», «logo» (ou similares), entre as premissas e a conclusão, lendo, por exemplo,

$$\text{«}\phi_1, ..., \phi_n, \text{ portanto } \psi\text{»}.^{2}$$

E para sugerir esta leitura usam-se frequentemente as seguintes notações alternativas para $(*)$:

$$\frac{\phi_1, ..., \phi_n}{\psi}\,, \qquad \phi_1, ..., \phi_n / \psi\,, \quad \text{ou} \qquad \begin{array}{c} \phi_1 \\ \vdots \\ \phi_n \\ \hline \psi \end{array}\,.$$

Interessa distinguir entre os argumentos correctos ou válidos e os argumentos incorrectos, inválidos ou falaciosos (do latim *fallacia* — engano). Ao fazermos um raciocínio, ao argumentarmos com alguém, interessa-nos que as conclusões a que chegamos sejam pelo menos tão aceitáveis quanto as premissas de que partimos, e isto acontece se utilizarmos somente argumentos válidos, pois só estes *preservam a verdade*, isto é, forçam (racionalmente) a aceitação da conclusão como verdadeira sempre que as premissas forem aceites como verdadeiras.

Veremos adiante alguns exemplos de argumentos correctos e de argumentos incorrectos, mas tentemos primeiramente precisar um pouco o que foi dito.

---

[2] A ordem de colocação das premissas é irrelevante: é o conjunto $\{\phi_1, \ldots, \phi_n\}$ das premissas que se deve considerar como relevante. «Portanto» abrevia-se « $\therefore$ ».

1.1 Definição Um argumento $\phi_1, ..., \phi_n/\psi$ diz-se **correcto** ou **válido** sse a conclusão ψ for verdadeira sempre que as premissas $\phi_1, ..., \phi_n$ forem simultaneamente verdadeiras, e diz-se **incorrecto** ou **inválido** no caso contrário, isto é, sse alguma situação ou circunstância permitir que as premissas sejam simultaneamente verdadeiras e a conclusão falsa.

A definição anterior envolve-nos com os conceitos semânticos de *verdade* e *falsidade*, e com o conceito sintáctico de *proposição*, não sendo uma definição precisa enquanto estes conceitos não forem previamente definidos com rigor. Nenhuma destas tarefas é tão fácil quanto se poderia julgar. Sem problematizar, diremos apenas, de momento, que tomamos o termo «proposição» na acepção linguística corrente, como sinónimo de «frase (asserção, expressão) declarativa (ou enunciativa) de um juízo ou pensamento, que tem o verbo no indicativo, e pode ser afirmativa ou negativa»[3]. Isto quer dizer que, num determinado contexto ou referencial interpretativo, a cada proposição ϕ pode ser atribuído sem ambiguidade, pelo menos em princípio, um dos valores lógicos **verdade** (símbolo "V", ou "1") ou **falsidade** ("F", ou "0"); além disso, considera-se ϕ verdadeira se e somente se a situação ou estado de coisas que ϕ exprime acontece de facto [concepção tarskiana da verdade ou veracidade enquanto correspondência com os factos ou a (uma) realidade][4]. Exemplificando:

A proposição «A relva é verde» é verdadeira sse a relva é verde.[5]

Note-se que o valor lógico de uma proposição como «A relva é verde» não é um absoluto categórico e intemporal, pois depende do contexto interpretativo. Por exemplo, no contexto de um campo de golfe bem tratado, a dita proposição é certamente verdadeira, mas noutro contexto, como o alentejano no pino do estio ela é, provavelmente, falsa. Esta dependência do valor lógico relativamente ao contexto interpretativo é ainda mais evidente nas proposições matemáticas expressas em notação totalmente simbólica como, por exemplo, a proposição seguinte, que exprime a comutatividade de uma operação binária indeterminada $\odot$:

Para todo o x *e todo o* y, $x \odot y = y \odot x$.

Esta proposição é verdadeira em certas estruturas matemáticas (por exemplo, nos

---

[3] *Gr. Dic. da Líng. Port.*, Soc. Líng. Port., Lisboa, 1981, tomo IX, p. 462.

[4] Alfred Tarski (1902-1983), um dos maiores lógicos de todos os tempos, criador da moderna semântica, enquanto disciplina científica (também chamada *teoria dos modelos*, como ramo da lógica matemática). Autor de um dos primeiros livros de introdução à lógica moderna e à metodologia das teorias dedutivas destinados ao grande público, um clássico escrito durante a ascenção do nazismo na Alemanha, recentemente reeditado (ver bibliografia).

[5] Uma frase clássica com que se costuma exemplificar este ponto é devida a A. Tarski: a proposição «A neve é branca» é verdadeira sse a neve é branca. A expressão «sse» é uma abreviatura de «se e só se», ou de «se e somente se», muito do agrado dos matemáticos.

grupos comutativos, em que o símbolo " $\odot$ " denota a operação de grupo) e é falsa noutras estruturas matemáticas (por exemplo, nos grupos não comutativos).

Por outro lado, não é necessário que saibamos determinar, no momento actual, o valor lógico de cada proposição com que lidamos, mas apenas exigimos que ela possua um determinado valor lógico, independentemente do nosso conhecimento dele.[6] Por exemplo, não sabemos, de momento, qual o valor lógico da proposição aritmética

«existem infinitos pares de primos gémeos»[7],

mas admitimos que possua um valor lógico determinado no momento presente.

Analogamente para a proposição

«existe um bloco de cem zeros consecutivos na dízima infinita de π.»

Mas já não se poderá dizer que possua um valor lógico determinado no momento presente a frase (dita *contingente futura*)

«Qualquer dia vou ser eleito Presidente da República.»

Vejamos alguns exemplos de argumentos válidos e inválidos.

1.2 Exemplos (1) Consideremos o clássico

Todo o homem é mortal
Sócrates é homem

Sócrates é mortal.

Este argumento é válido: se as premissas forem ambas verdadeiras (e são, de facto, na acepção corrente), a conclusão é também verdadeira.

(2) Substituindo no argumento anterior «mortal» por «mudo», uma das premissas e a conclusão são falsas (interpretadas no sentido corrente); no entanto, o argumento continua válido: se ambas as premissas forem verdadeiras, a conclusão é verdadeira também.

---

[6] Esta questão não é pacífica. A suposição de que toda a proposição matemática possui um valor lógico, independentemente do nosso conhecimento, releva já de certa atitude filosófica, de índole idealista ou platonista, que não é partilhada por todos os lógicos e matemáticos, nomeadamente, pelos intuicionistas/construtivistas, para quem uma proposição matemática só possui valor lógico a partir do momento em que é demonstrada ou é refutada. Veja-se a secção V.5.

[7] Um par de primos gémeos é um par de números primos da forma $(p, p+2)$. O maior número primo p conhecido (Setembro de 2005) nestas condições, é

$$16\,869\,987\,339\,975 \cdot 2^{171\,960} - 1,$$

que se escreve com 51 779 algarismos.

(3) O argumento

$$\frac{\text{A relva é verde e o céu é azul}}{\text{A relva é verde}}$$

é obviamente válido, quaisquer que sejam a localização do relvado e o estado do tempo.

(4) Substituindo no argumento anterior «e» por «ou», obtém-se um argumento inválido, pois é concebível uma situação em que a relva não é verde, mas o céu é mesmo azul, tornando verdadeira a premissa, mas falsa a conclusão.

(5) O argumento

$$\frac{\text{Os mesões têm spin } \frac{1}{2} \text{ e a Lua é um queijo}}{\text{Os mesões têm spin } \frac{1}{2}}$$

é válido, e este facto é reconhecido por qualquer pessoa, mesmo que ignorante de Física ou que não tenha ido à Lua saborear o queijo!

I.2 Forma *vs.* conteúdo

Das ilações que podem ser tiradas dos exemplos acima, a mais importante é a de que a validade (ou invalidade) de um dado argumento é independente do seu conteúdo concreto ou significado das proposições intervenientes, e portanto é independente da sua verdade ou falsidade *factual*, só dependendo da presença ou não de uma certa relação entre a verdade (factual ou hipotética) das premissas e a verdade (factual ou hipotética) da conclusão, relação essa que tem o nome de **relação de consequência** (**lógica** ou **semântica**).[8] O argumento é válido se a relação de consequência se manifesta (dizendo-se neste caso que a conclusão é **consequência** das premissas) e é inválido no caso contrário. E tal relação está ou não presente num dado argumento somente por virtude da *forma lógica do argumento* a qual, por sua vez, depende da *forma lógica das proposições* intervenientes. Em última análise, pois, a validade ou invalidade de um argumento *só depende da sua forma*.

Antes de prosseguir, fixemos o conceito de consequência numa definição geral.

2.1 Definição Seja Σ um conjunto de proposições, ψ uma proposição. Dizemos que ψ é **consequência** (**lógica**, ou **semântica**) de Σ sse ψ é verdadeira sempre que as proposições de Σ são simultaneamente verdadeiras.

---

[8] A razão porque se utiliza o adjectivo «lógica», no presente contexto, é a seguinte: se $\phi_1, \ldots, \phi_n \vDash \psi$, isto acontece *somente por virtude do significado dos símbolos lógicos (conectivos) que ocorrem nas fórmulas* $\phi_1, \ldots, \phi_n, \psi$.

Escreve-se

$$\Sigma \vDash \psi$$

para exprimir que ψ é consequência (lógica, ou semântica) de Σ. A expressão «$\Sigma \vDash \psi$» também se pode ler «de Σ conclui-se (logica ou semanticamente) ψ», ou «Σ implica (logica ou semanticamente) ψ». Se Σ for finito, digamos $\Sigma = \{\phi_1, ..., \phi_n\}$, escrevemos simplesmente $\phi_1, ..., \phi_n \vDash \psi$ em vez de $\{\phi_1, ..., \phi_n\} \vDash \psi$. Se Σ for vazio ($\Sigma = \emptyset$) escrevemos $\vDash \psi$ em vez de $\emptyset \vDash \psi$. Comparando as definições 1.1 e 2.1 concluimos imediatamente que

$$\text{um argumento } \frac{\phi_1, ..., \phi_n}{\psi} \text{ é válido sse } \phi_1, ..., \phi_n \vDash \psi.$$

I.3 Análise lógica

Explicitar a forma lógica de uma proposição ϕ é explicitar o modo como essa proposição é formada ou construída a partir de proposições (ou condições) mais simples, por meio de certas operações (ou operadores) lógicas. Identificar e classificar as componentes lógicas e não lógicas das proposições (e demais expressões) de uma língua ou linguagem é uma tarefa, entre muitas, dos lógicos e linguistas, chamada **análise lógica**. É tarefa bem complexa e delicada. Graças à criação de um simbolismo adequado, entre outros factores, houve progressos notáveis desde meados do séc. XIX, particularmente no que respeita à linguagem (linguagens) da matemática (das teorias matemáticas), devidos a matemáticos e lógicos como Boole, De Morgan, Schröder, Peirce, Frege, Peano e Russell. As linguagens formais que abordaremos são o (um) resultado de tais progressos.

Há um consenso relativamente grande entre os lógicos sobre quais os conceitos lógicos fundamentais presentes nas expressões e proposições matemáticas. São os que dizem respeito aos chamados **conectivos proposicionais**, aos **quantificadores** (incluindo o uso de variáveis), e ao conceito de **igualdade**.[9]

Na tabela seguinte indicam-se os símbolos dos conectivos e dos quantificadores e sua interpretação a utilizar neste livro. A coluna da direita contém alguns dos símbolos mais antigos, já um tanto em desuso. O conectivo de condicionalização também é chamado de *implicação material*, e o de bicondicionalização de *equivalência material*.

Quanto à *igualdade* (símbolo " $=$ "), deve-se referir que em certos sistemas lógicos mais fortes do que os considerados neste livro (por exemplo, na chamada *lógica de segunda ordem*, ver III.10) e em certas teorias matemáticas (como a teoria axiomática dos conjuntos), a *igualdade* pode ser definida a partir de outros conceitos.

---

[9] V. o artigo de A. TARSKI "What are logical notions?", *Hist. and Phil. of Logic* **7**, n. 6, 1986, pp. 143-154.

Por outro lado, em certos sistemas lógicos desenvolvidos no final do séc. XIX e princípios deste, nomeadamente por Gottlob Frege e por Bertrand Russell, tentou-se considerar o conceito de *pertença* (símbolo " $\in$ "), conceito fundamental da teoria dos conjuntos, como conceito lógico, no âmbito de um ambicioso programa de redução da matemática à lógica (o chamado *programa logicista*). Tais sistemas revelaram-se, contudo, eivados de dificuldades (quando não contradições) e artificialismos inultrapassáveis, aceitando-se hoje em dia que aquele conceito é especificamente matemático, não lógico.[10]

CONECTIVOS E QUANTIFICADORES

Símbolo	Leitura	Operação lógica	Alternativos
$\wedge$	e	conjunção	$\&$, $\cdot$
$\vee$	ou	disjunção	$+$
$\neg$	não	negação	$\sim$, $-$, $^-$
$\rightarrow$	se..., então	condicionalização	$\Rightarrow$, $\supset$
$\leftrightarrow$	se e só se	bicondicionalização	$\Leftrightarrow$, $\equiv$
$\forall$	para todo	quantificação universal	Π, ( )
$\exists$	existe	quantificação existencial	Σ, E

A utilização de *variáveis*, que mais não são do que letras de certos alfabetos, é uma prática já centenária em matemática e nas ciências que utilizam a matemática, por exemplo, para exprimir leis físicas, identidades algébricas, etc. Em análise lógica as variáveis são imprescindíveis para exibir a *forma* das proposições e argumentos e até para podermos dizer algo acerca de proposições arbitrárias (como, por exemplo, na definição 1.1, em que utilizamos letras "ϕ_i", "ψ" para representar proposições arbitrárias).

É costume distinguir dois níveis de análise lógica das proposições — o *nível proposicional*, em que só nos interessa o modo como uma proposição é composta de proposições mais simples por meio dos conectivos proposicionais, e o *nível quantificacional*, em que todas as proposições, mesmo as encaradas como simples no nível proposicional, são analisadas na sua estrutura gramatical interna, por exemplo, na relação sujeito-predicado, na ligação das variáveis aos quantificadores, etc.

O simbolismo adoptado para efectuar a análise ao nível quantificacional é, obviamente, mais rico e variado do que o adoptado para a análise ao nível proposicional.

---

[10] Do ponto de vista da lógica tradicional os conceitos lógicos são aqueles que são os mais gerais e comuns a todos os ramos do saber (incluindo a matemática), mas há conceitos específicos de cada ramo que não fazem sentido noutros ramos. Por exemplo, o conceito botânico de semente não é um conceito específico em Química, do mesmo modo que o conceito de número primo não é um conceito específico da Biologia e o conceito matemático de pertença não é um conceito da lógica.

I.4 Nível proposicional

A este nível é costume usar as letras latinas p, q, r, ...,[11] possivelmente com índices, para representar proposições simples, e as letras gregas ϕ, ψ, θ,..., possivelmente com índices, para representar proposições arbitrárias, simples ou compostas. Os conectivos[12] $\wedge$, $\vee$, $\neg$, $\rightarrow$, $\leftrightarrow$ devem ser encarados como *operadores* que actuam sobre proposições e produzem proposições. Assim, se ϕ, ψ são proposições, também o são:

• $(\phi \wedge \psi)$ — a proposição conjunta (ou conjunção) com 1ª componente ϕ e 2.ª componente ψ, lê-se «ϕ e ψ»;

• $(\phi \vee \psi)$ — a proposição disjunta [ou disjunção (inclusiva)] com 1ª componente ϕ e 2.ª componente ψ, que se lê «ϕ ou ψ»;

• $\neg\phi$ — a negação de ϕ, que se lê «não ϕ», ou «não se tem ϕ»;

• $(\phi \rightarrow \psi)$ — a proposição condicional (ou implicação material) com *antecedente* ϕ e *consequente* ψ, que se pode ler de muitas maneiras diferentes: «se ϕ, então ψ», «ψ, se ϕ», «ϕ implica (materialmente) ψ», «ϕ, só (ou somente) se ψ», «ϕ é condição suficiente de (ou para) ψ», «ψ é condição necessária de (ou para) ϕ»;

• $(\phi \leftrightarrow \psi)$ — a proposição bicondicional (ou equivalência material) com 1ª componente ϕ e 2.ª componente ψ, que se lê «ϕ sse ψ», «ϕ é equivalente (materialmente) a ψ», «ϕ é condição necessária e suficiente de ψ».

Das leituras possíveis indicadas para $\rightarrow$ e $\leftrightarrow$ devem preferir-se as primeiras alternativas, por razões que mais adiante se explicam e têm a ver com os diferentes significados ou usos possíveis do termo «implica». Nomeadamente, é frequente lêr-se «ϕ implica ψ» para exprimir que a proposição $\phi \rightarrow \psi$ é verdadeira, daí a possível ambiguidade. Quando não houver possibilidade de confusão, podemos suprimir os parênteses (mais sobre esta supressão no Cap. II).

4.1 Exemplos Ao nível proposicional, os argumentos dos exemplos (1)-(5) acima podem ser simbolizados (ou formalizados) do seguinte modo:

---

[11] Recorde-se que para formar um nome de um símbolo ou de uma expressão se coloca esse símbolo ou expressão entre aspas " " ou entre comas ' '. Os lógicos recorrem muitas vezes, porém, à chamada *convenção autonómica*, segundo a qual cada símbolo ou expressão se considera como um nome de si própria, deixando-se para o leitor, conforme o contexto, a distinção uso/menção. Usando essa convenção, diremos, por exemplo: «a letra p denota uma proposição simples», em vez de «a letra 'p' denota…». A convenção autonómica não é utilizável em matemática: por exemplo, a letra 'π' denota em matemática um certo número irracional ($\pi = 3{,}14159\ldots$), mas não podemos usar a convenção autonómica relativamente a esta letra, pois um número não é uma letra.

[12] Alguns colegas de ofício sugerem que deveriámos dizer «as conectivas».

(1′) e (2′):
$$\frac{\begin{array}{c} p \\ q \end{array}}{r}$$

(3′) e (5′): $\dfrac{p \wedge q}{p}$ (4′): $\dfrac{p \vee q}{p}$

A validade de (3) [e de (5)] pode ser reconhecida através da forma (3′): sempre que atribuirmos valores lógicos às letras p, q de modo a tornar a premissa $p \wedge q$ verdadeira, resulta a conclusão p verdadeira também. E é assim devido ao modo como utilizamos 'e' na língua comum, que nos leva a considerar uma proposição conjuntiva como verdadeira quando e só quando ambas as componentes são verdadeiras. Este facto exprime-se esquematicamente, de modo condensado, na conhecida *tabela de verdade* para o conectivo $\wedge$ (ver adiante).

Do mesmo modo, a invalidade de (4) pode ser reconhecida pela forma (4′), e a tabela de verdade para $\vee$, que resulta do facto de uma disjunção (inclusiva) se considerar verdadeira quando e só quando uma, pelo menos, das componentes for verdadeira. Ora, é possível a premissa $p \vee q$ ser verdadeira e a conclusão p ser falsa: basta q ser verdadeira.

As tabelas de verdade para $\wedge, \vee, \neg, \rightarrow, \leftrightarrow$ são indicadas a seguir. Uma justificação da tabela de $\rightarrow$, nas linhas em que o antecedente tem o valor 0, será feita mais adiante mas, de qualquer modo, indicamos já o valor respectivo.

TABELAS DE VERDADE DOS CONECTIVOS

ϕ	$\neg\phi$
0	1
1	0

ϕ	ψ	$\phi \wedge \psi$	$\phi \vee \psi$	$\phi \rightarrow \psi$	$\phi \leftrightarrow \psi$
0	0	0	0	1	1
0	1	0	1	1	0
1	0	0	1	0	0
1	1	1	1	1	1

Nos casos em que o antecedente tem o valor 1, tenha-se em conta o modo como proposições da forma $\phi \rightarrow \psi$ são utilizadas em matemática. Muitos teoremas em matemática têm aquela forma condicional, e a sua demonstração procede normalmente (pelo chamado *método directo*) de ϕ para ψ, no sentido seguinte: admite-se ϕ como verdadeira e tenta-se demonstrar a veracidade de ψ. E, se porventura ϕ é verdadeira, mas ψ é falsa, então certamente que ϕ não implica ψ, isto é, a condicional $\phi \rightarrow \psi$ é falsa.

A validade do argumento (1) [ou (2)], porém, já não pode ser reconhecida pela forma proposicional (1′) (pois somos livres de atribuir a p, q, r os valores 1, 1, 0, respectivamente, por exemplo), o que mostra a insuficiência da análise lógica ao nível proposicional.

Necessitamos, pois, de passar a um nível mais profundo da análise, em que seja tida em conta a «estrutura interna» das proposições p, q, r do exemplo (1), consideradas simples ao nível proposicional, mas já não ao nível quantificacional, como veremos.

I.5 Nível quantificacional

No segundo nível da análise lógica das proposições encontramos como componente fundamental a ligação *sujeito-predicado*: certos objectos ou indivíduos têm certa propriedade, ou estão em certa relação com certos outros. Por exemplo, nas proposições

(6) Sócrates é homem,

(7) Manuel ama Maria,

(8) 3 está entre 3 e 4,

identificamos os indivíduos particulares

Sócrates, *Manuel*, *Maria*, 2, 3, 4

e os predicados e relações

$$\cdots \textit{ é homem},\ \cdots \textit{ ama } \cdots,\ \cdots \textit{ está entre } \cdots \textit{ e } \cdots,$$

sendo o primeiro predicado unário (uma posição livre ou «grau de liberdade», ou *aridade* 1), o segundo binário (duas posições livres ou dois «graus de liberdade», ou aridade 2) e o terceiro ternário (aridade 3). Em cada proposição analisada identificamos certos indivíduos ou objectos (de natureza qualquer, concreta ou abstracta) — os *sujeitos* — e certos predicados ou relações entre eles. Implícita ou explicitamente, pois, está um certo **domínio** ou **universo** (**do discurso**): uma colecção a que pertencem os indivíduos ou sujeitos referidos (cujos nomes podem ocupar as posições livres nos predicados).

5.1 Notações Neste capítulo usaremos as letras c, c_1, c_2, ..., d, ..., possivelmente com índices, como *nomes (próprios)* de indivíduos ou objectos particulares de um dado domínio. Tais letras são também chamadas *constantes.*[13] No lugar dos espaços em branco «$\cdots$» colocaremos *variáveis*, isto é, letras (do fim do alfabeto latino) x, y, z, ..., possivelmente com índices, para representar indivíduos arbitrários do domínio dado. Assim, os predicados e relações acima podem ser representados pelas expressões

(**) $\qquad x$ *é homem,* x *ama* y, x *está entre* y *e* z,

[13] Por razões que só serão explicadas no Cap. II, preferimos não utilizar as letras a, b, a', … para este fim.

respectivamente.[14] Mais geralmente, usaremos letras como

$$P, Q, R, ...,$$

possivelmente com índices, como nomes de predicados e relações (unários, binários, etc., conforme o caso), e colocaremos as variáveis e nomes de indivíduos à direita, ocupando tantas posições quanto o grau ou aridade respectivo. Assim, por exemplo, num dado contexto, um predicado unário pode ser expresso por Px, um predicado ou relação binária por Qxy e um ternário por $Rxyz$. Notações alternativas, por vezes mais convenientes, são

$$P(x),\ Q(x,y)\ \text{(ou}\ xQy),\ R(x,y,z),$$

respectivamente. Nada impede, porém, que num contexto diferente se denote por Pxy ou $P(x,y)$ um predicado ou relação binária, por $Rx_1...x_n$ uma relação n-ária ($n \geq 2$), etc.

Relativamente às proposições (6)-(8) acima, podemos abreviar as expressões $(**)$ em

$$Px,\ Qxy,\ R(x,y,z)$$

respectivamente, e se usarmos as letras c_1, c_2, c_3 como nomes dos indivíduos particulares

Sócrates, Manuel, Maria,

respectivamente, obtemos para expressão simbólica de (6)-(8)

$$Pc_1,\ Qc_2c_3,\ R(3,2,4),$$

respectivamente. Em exemplos matemáticos recorremos às notações comuns, como $x > 2$, $2 < 3 < 4$, etc.

I.6 Condições, substituição e quantificação[15]

Os símbolos P, Q, R, ... são chamados **símbolos predicativos** (ou **relacionais**), e expressões como Px, Qxy, $Rxyz$, $x = y$ ou similares são chamadas **condições simples** ou **atómicas**. A partir de condições atómicas outras condições (ou proposições) se podem obter, quer por meio das operações lógicas já indicadas, associadas aos conectivos proposicionais, quer por meio de duas outras operações

[14] Pese embora o facto de que, para números, dizer que *x* está entre y e z equivale (por definição) a dizer que y é menor do que *x* e *x* é menor do que z, ou z é menor do que *x* e *x* é menor do que y, simbolicamente $(y < x \wedge x < z) \vee (z < x \wedge x < y)$; mas nem por isso deixamos de ter aqui uma relação ternária num universo numérico (números inteiros, por exemplo). Em geometria (euclidiana), é conhecida a relação ternária *(estar situado) entre*, no domínio (plano, ou espaço) dos pontos.

[15] Definições mais precisas são dadas no Cap. III.

lógicas, a saber, a *substituição* de variáveis por outras variáveis ou por nomes e a *quantificação* de variáveis.

O resultado de substituir numa condição atómica uma variável por um nome pode ser uma proposição ou ainda uma condição, mas com menos variáveis. Por exemplo, substituindo x por a em Px, obtemos a proposição Pa mas, fazendo a mesma substituição na condição Qxy, obtém-se a condição na variável y, Qay.

Admitiremos então que, se ϕ, ψ forem condições (ou proposições, atómicas ou não), então também o são as expressões

$$\phi \wedge \psi,\ \phi \vee \psi,\ \neg\phi,\ \phi \rightarrow \psi,\ \phi \leftrightarrow \psi$$

(mesma leitura que a indicada na pág. 19), mas isto não esgota as possibilidades gramaticais para obter condições (ver adiante).

A substituição de uma variável por um nome (constante) pode efectuar-se, numa dada condição ϕ, desde que essa variável ocorra em ϕ, como é óbvio. É usual a notação

$$\phi(x_1, ..., x_n)$$

para indicar que ϕ é uma condição nas variáveis x_1, ..., x_n, pelo menos (quer dizer, outras variáveis além destas podem ocorrer em ϕ, excepto se algo se disser em contrário); e, se cada x_i for substituída por um nome c_i ($1 \leq i \leq n$), denota-se por

$$\phi(c_1, ..., c_n), \text{ ou } \phi(c_1/x_1, ..., c_n/x_n)$$

o resultado da substituição. Se todas as variáveis em ϕ forem substituídas por nomes (constantes), obtemos uma proposição, mas se permanecerem variáveis por substituir obteremos ainda uma condição.

Até este momento, a única maneira de obter proposições consistiu em substituir variáveis por nomes, em condições. Introduzimos agora outra maneira — a *quantificação* de variáveis. Todavia, a quantificação de condições nem sempre produz proposições, pois pode também produzir condições, mas com menos variáveis livres, isto é, não quantificadas.

Seja $\phi(x)$ uma condição numa variável x (e possivelmente noutras variáveis). Então podemos formar as seguintes expressões, por quantificação da variável x:

• $\forall x \phi(x)$ — a quantificada universalmente em x de $\phi(x)$, que se lê «para todo x, $\phi(x)$», ou «para qualquer x, $\phi(x)$», ou ainda «todo x tem a propriedade ϕ», ou similarmente;[16]

• $\exists x \phi(x)$ — a quantificada existencialmente em x de $\phi(x)$, com a leitura «existe (pelo menos um) x tal que $\phi(x)$», ou «para algum x, $\phi(x)$», ou «algum x tem a propriedade ϕ», ou similarmente.[17]

---

[16] Menos correcta, mas frequente, é a leitura «$\phi(x)$, para todo x», correspondente à escrita (formalmente incorrecta mas muito comum) «$\phi(x)$, $\forall x$».

[17] Também é frequente a leitura «$\phi(x)$, para algum x», que corresponde literalmente à escrita (incorrecta e absurda, que ninguém utiliza!) «$\phi(x)$, $\exists x$».

As expressões $\forall x$. $\exists x$ são os **quantificadores em** x. Em expressões da forma $\forall x \phi(x)$ ou $\exists x \phi(x)$, $\phi(x)$ é o **alcance** do quantificador em x, $\forall x$ ou $\exists x$, respectivamente, e naquelas expressões as ocorrências de x são **mudas** ou **aparentes**. Ocorrências de variáveis em condições que não são mudas dizem-se **livres**. Por abuso, dizemos que x é livre em ϕ se x tem, pelo menos, uma ocorrência livre em x. É claro que nas proposições não pode haver variáveis livres, pois todas as variáveis ou foram substituídas por nomes ou foram quantificadas. Observe-se, por outro lado, que, se somente x é livre em $\phi(x)$, então $\forall x\, \phi(x)$, $\exists x$ $\phi(x)$ são proposições (ou sentenças); se outras variáveis y, z, ... ocorrem livres em $\phi(x)$ [isto é, $\phi(x, y, z, ...)$ é uma condição nas variáveis x, y, z, ..., então as expressões $\forall x\, \phi(x, y, z, ...)$, $\exists x\, \phi(x, y, z, ...)$ são condições nas variáveis y, z, ... somente.

Enquanto uma condição em x, $\phi(x)$, exprime algo acerca de x, uma proposição da forma $\forall x\, \phi(x)$ ou da forma $\exists x\, \phi(x)$, pelo contrário, já *nada diz acerca de* x.

Por exemplo, na álgebra dos números inteiros (isto é, supondo que x, y, z, u, ... são variáveis para números inteiros), a condição em x

$$\exists y\, (x = y + y)$$

exprime algo acerca de x, nomeadamente «x é par»; do mesmo modo, a condição em u, $\exists y\, (u = y + y)$, exprime «u é par». Mas, em contrapartida, a proposição que se obtém da condição em x acima quantificando universalmente esta variável

$$\forall x\, \exists y\, (x = y + y)$$

já nada diz acerca de x, pois exprime «todo o número inteiro é par» (o que, por sinal, é falso), exactamente o mesmo que exprime

$$\forall z\, \exists y\, (z = y + y).$$

Analogamente, nada diz acerca de x a proposição

$$\exists x\, \exists y\, (x = y + y),$$

exprimindo «existe um número par» (o que é verdade), e exactamente o mesmo exprime a proposição seguinte onde nem sequer ocorre x

$$\exists u\, \exists y\, (u = y + y)$$

Como é também manifesto através destes exemplos, se quisermos, numa dada condição $\phi(x, ...)$, substituir a variável x por uma outra, digamos u, *devemos ter o cuidado de verificar que* u *não ocorre já em* $\phi(x, ...)$ pois, caso ocorra, resultaria, possivelmente, uma condição com significado totalmente diferente do pretendido, isto é, que não exprime acerca de u o mesmo que a inicial exprimia acerca de x. Assim é no caso acima, por exemplo, se se substituísse x por y em $\exists y(x = y + y)$, resultando a proposição $\exists y\, (y = y + y)$, que exprime que existe um número inteiro igual ao seu dobro (o que é verdade: é o inteiro zero, 0, elemento neutro para a adição).

A distinção livre/muda é também pertinente em expressões matemáticas, como por exemplo na seguintes condições

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2},$$
$$F(u) = \int_0^u f(x)\,dx,$$
$$\{x \in \mathbb{R} : -1 \leq x < n\} = [-1, n[,$$

nas quais as variáveis n, u são livres mas as variáveis i, x são mudas.

Sempre que efectuarmos substituições de variáveis (livres) por outras variáveis, neste capítulo, suporemos tacitamente que tais substituições são feitas com os devidos cuidados para evitar a alteração do significado.

I.7 Interpretações

As proposições da língua portuguesa

(9) Sócrates ama alguém,

(10) Toda a pessoa ama alguém,

podem ser simbolizadas por

(9′) $\exists y\, Qcy$,

(10′) $\forall x \exists y\, Qxy$,

respectivamente, desde que façamos as convenções seguintes:

— As variáveis x, y, ... denotam pessoas arbitrárias; por outras palavras, supomos fixado um **domínio** [ou **universo** (do discurso)] para as variáveis, isto é, uma colecção ou conjunto de objectos ou indivíduos onde as variáveis tomam valores;

— A constante c denota o indivíduo *Sócrates*;

— O símbolo Q denota a relação de amar, isto é, Qxy significa x *ama* y.

Em geral, a fixação de um domínio para as variáveis e a atribuição de significado aos nomes e aos símbolos predicativos de um dado simbolismo é o que se chama uma **interpretação** desse simbolismo, e é sempre através de uma interpretação (dissemos anteriormente: um contexto interpretativo; podemos também dizer: um referencial, etc.) que as proposições simbólicas podem tomar um ou outro dos valores lógicos **verdade** (1) ou **falsidade** (0).

7.1 Exemplos Simbolizemos agora os argumentos (1)-(5) ao nível quantificacional, indicando ao mesmo tempo a interpretação respectiva.

(1″) *Domínio:* (colecção das) pessoas; Px*:* x é homem; Qx*:* x é mortal; c*:* Sócrates:

$$\frac{\begin{array}{l}\forall x(Px \to Qx)\\ Pc\end{array}}{Qc.}$$

(2″) Idem, excepto que Qx*:* x é mudo: Idem.

(3″) *Domínio:* todas as coisas; Px*:* x é verde; Qx*:* x é azul; c*:* a relva; d*:* o céu:

$$\frac{Pc \wedge Qd}{Pc};$$

(4″) Idem. Idem, com $\vee$ no lugar de $\wedge$.

(5″) *Domínio:* todas as coisas; Px*:* x é um mesão; Qx*:* x tem spin $\frac{1}{2}$; Rx*:* x é um queijo; c*:* a Lua:

$$\frac{\forall x\,(Px \to Qx) \wedge Rc}{\forall x\,(Px \to Qx)}.$$

Devemos chamar a atenção para o facto de, na maioria dos casos, haver mais de uma simbolização e de uma interpretação possíveis. Só para dar um exemplo, na frase (7) acima podíamos ter preferido considerar, no domínio das pessoas, o predicado unário

Mx*:* x *é amante de Maria* (ou: x *ama Maria*),

de modo que (7) se simbolizaria simplesmente por Mc.

Outro exemplo mais complicado: a 2.ª componente da premissa do argumento (5), «A Lua é um queijo», pode ser simbolizada por

$$\exists x\,(x = c \wedge Rx).$$

A complicação é aqui dispensável, mas há casos em que é mesmo necessário utilizar o predicado de igualdade (interpretado como a relação de identidade, em cada domínio) na simbolização de um dado argumento, se queremos obter uma forma válida. O seguinte exemplo, famoso, é devido ao lógico americano Willard van Orman Quine.[18]

[18] W. van O. Quine (1908-2000), reputado lógico e filósofo da lógica e da linguagem da actualidade, professor na Universidade de Harvard, autor de alguns dos livros mais bem escritos de introdução à lógica, de estilo inconfundível (ver bibliografia).

7.2 Exemplo (11) Argumento:

Somente o General e a Sentinela sabem a senha de passagem
Alguém que sabe a senha de passagem rouba munições

O General ou a Sentinela rouba munições.

Interpretação: *Domínio:* pessoas; Px*:* x sabe a senha de passagem; Qx*:* x rouba munições; c*:* o General; d*:* a Sentinela. Formalização:

$$\begin{array}{l} \forall x\,(Px \rightarrow x = c \vee x = d) \\ \exists x\,(Px \wedge Qx) \\ \hline Qc \vee Qd \qquad\qquad . \end{array}$$

I.8 Sobre a igualdade. Descrições definidas

Quando escrevemos, por exemplo:

(12) $2 + 3 = 4 + 1$,

(13) Sócrates é o mestre de Platão,

(14) Lisboa é a capital de Portugal,

(15) A honestidade é a virtude que mais admiro,

estamos a utilizar o conceito de identidade, expresso pelo símbolo de igualdade, $=$. Isto é claro em (12): o resultado de somar 2 com 3 é o mesmo número que o resultado de somar 4 com 1. Mas também em (13)-(15) o «é» não é predicativo (como em «Sócrates é mortal») mas sim um «é idêntico a», podendo-se escrever, equivalentemente,

(13′) Sócrates $=$ mestre de Platão,

(14′) Lisboa $=$ capital de Portugal,

(15′) A honestidade $=$ a virtude que mais admiro,

respectivamente. Em geral, o símbolo de igualdade ‘ $=$ ’ emprega-se entre duas designações ou expressões designatórias para exprimir a identidade dos entes designados (e não, obviamente, das próprias designações: «Lisboa» $\neq$ «capital de Portugal»!).

Todavia, expressões como «o mestre de Platão», ou «o autor de *Os Maias*», são chamadas **descrições definidas** por Bertrand Russell.[19] Estamos encarando tais

[19] O termo é utilizado no trabalho monumental *Principia Mathematica* (1910-1913), de colaboração com A. N. Whitehead, em três volumes (dos quatro previstos), onde se procura pôr em prática o *programa logicista* de «redução» da matemática à lógica. Ver, a propósito, o artigo de L. HENKIN “A Matemática e a Lógica são idênticas?”, *Bol. Soc. Paranaense de Matemática*, vol. 7, n.º 3 (1964) [traduzido de *Science*, vol. 138 (1962) pp. 788-794, por AYDA ARRUDA].

expressões como descrições ou designações ordinárias (tal como os nomes próprios), para efeitos de simbolização de frases, mas a verdade é que nem sempre este modo de proceder é conveniente para efeitos de estabelecimento da validade de certas formas de argumentos. Damos a seguir outro exemplo, devido essencialmente a Quine, adaptado à nossa literatura.

(16) Argumento:

$$\frac{\text{O autor de } \textit{Os Maias} \text{ escreveu } \textit{O Crime do Padre Amaro}}{\text{Alguém escreveu } \textit{Os Maias} \text{ e } \textit{O Crime do Padre Amaro}}$$

Este argumento é válido. Consideremos a seguinte interpretação: *Domínio:* pessoas; Px*:* x escreveu *O Crime do Padre Amaro;* Mx*:* x escreveu *Os Maias;* c: o autor de *Os Maias*.

Com esta interpretação, o argumento acima tem a forma

$$(16') \qquad \frac{Pc}{\exists x\,(Mx \wedge Px)}$$

mas esta forma não é válida, como facilmente se verifica por um contra-exemplo obtido com uma interpretação diferente (exercício). A razão da discrepância reside no facto insuspeitado de a validade de (16) depender do predicado Mx, implícito na descrição «o autor de *Os Maias*», que se omitiu na premissa de (16′).

Reflectindo, vemos que a premissa de (16) afirma, implicitamente, que uma única pessoa escreveu *Os Maias* e que essa mesma pessoa escreveu *O Crime do Padre Amaro*, o que se pode simbolizar por

$$(17) \qquad \exists x\,(Mx \wedge \forall y\,(My \rightarrow x = y) \wedge Px).$$

Substituindo na forma (16′) a premissa por (17), já se obtém uma forma válida.

A *existência e unicidade* de um indivíduo ou objecto sujeito a certa condição também tem de ser expressa através do predicado de igualdade. Supondo $\phi(x)$ uma condição em x, exprime-se «existe um único x tal que $\phi(x)$» pela conjunção

$$\exists x \phi(x) \wedge \forall y \forall z\,((\phi(y) \wedge \phi(z)) \rightarrow y = z),$$

onde $\phi(y) = \phi(y/x)$ e $\phi(z) = \phi(z/x)$, ou, equivalentemente (equivalência a demonstrar no Cap. III), por

$$\exists x\,(\phi(x) \wedge \forall y\,(\phi(y) \rightarrow x = y)),$$

podendo qualquer destas expressões ser abreviada em

$$\exists^1 x\ \phi(x).$$

Bertrand Russell introduziu o chamado **operador de descrição** (definida), actualmente em desuso, ι (letra grega *iota*), com a finalidade de poder simbolizar expressões como «o único x tal que $\phi(x)$», abreviadamente

$$\iota_x\, \phi(x),$$

onde $\phi(x)$ é uma condição tal que a proposição $\exists^1 x\, \phi(x)$ é verdadeira. Em boa verdade, Russell não define $\iota_x\, \phi(x)$ explicitamente [isto é, não dá uma definição da forma $\iota_x\, \phi(x) =$ ---], antes fornece uma *definição em contexto*, isto é, diz como se deve encarar uma expressão em que ocorra a designação $\iota_x\, \phi(x)$, digamos $\psi(\iota_x \phi(x))$, a qual se considera como abreviatura de

$$\exists x(\phi(x) \wedge \forall y\, (\phi(y) \rightarrow x = y) \wedge \psi(x)).$$

Semanticamente, considera-se $\psi(\iota_x\, \phi(x))$ falsa se não existir nenhum objecto satisfazendo ϕ, ou se houver mais de um, e verdadeira no caso de haver um único tal objecto. Note-se que (17) acima é precisamente da forma $\psi(\iota_x\, \phi(x))$, pois não é mais que do que $P(\iota_x\, Mx)$, onde P e M são como acima se indicou.

Bertrand Russell (1872-1970)

David Hilbert (1862-1943)

Uns anos mais tarde, David Hilbert dá um tratamento inovador ao operador de descrição, substituindo ι por um operador mais simples e eficiente, o operador de **descrição indefinida**, ou de **selecção**, ε, que N. Bourbaki denota τ.[20] *Grosso modo*, este operador resulta de ι suprimindo a exigência de unicidade relativamente a uma condição $\phi(x)$ a que se aplique: $\tau_x\, \phi(x)$ denota um qualquer objecto x tal que $\phi(x)$, se existir pelo menos um, e não denota coisa alguma no caso contrário.

O que é mais interessante é que, considerando τ como primitivo, torna-se possível definir os quantificadores: define-se $\exists x\, \phi(x)$ como abreviatura de $\phi(\tau_x\, \phi(x))$ e depois $\forall x\, \phi(x)$ como abreviatura de $\neg\exists x\, \neg\phi(x)$.

---

[20] Ver os artigos de HILBERT insertos na colectânea de Van HEIJENOORT indicada na bibliografia, que também foram recentemente traduzidos em português, como Apêndices ao seu livro *Fundamentos da Geometria* (Gradiva, 2003). O livrinho de COSTA & CARRION apresenta a lógica com o operador de Hilbert, popularizado entre o mundo matemático a partir da década de 40 pelo tratado de N. BOURBAKI *Éléments de Mathématique.* É discutível, porém, se o operador de selecção (também dito de *escolha*) τ é de natureza puramente lógica. De qualquer modo, a lógica clássica prescinde dos operadores ι, τ (o que se faz com eles pode-se fazer sem eles), embora a «alta» matemática (e a teoria dos conjuntos), tendo como subjacente uma lógica sem o operador de Hilbert, não prescinda de um axioma (o chamado *Axioma da Escolha*) que desempenha, *grosso modo*, o papel atribuído a τ na lógica com este operador.

I.9 Resolução de ambiguidades

Casos há, também, em que uma dada proposição da língua natural possui um significado ambíguo, cabendo-nos resolver primeiro a ambiguidade, antes de passarmos à formalização.[21] Por exemplo,

Todo o pescador tem uma Santa Padroeira

tanto pode significar, do ponto de vista lógico, que cada pescador tem a sua padroeira, simbolicamente (com a interpretação óbvia, no domínio das pessoas)

$$\forall x(Px \rightarrow \exists y Syx)$$

como significar que há uma mesma Santa Padroeira para todos os pescadores (que é tendencialmente, digamos, o significado consensual), simbolicamente

$$\exists y \forall x(Px \rightarrow Syx)$$

Escusado será dizer que as duas formalizações não são equivalentes.[22]

Note-se ainda que o artigo indefinido «um» («uma») é utilizado como significando o mesmo que «um(a) qualquer», isto é, como um quantificador universal, como, por exemplo, na frase

Uma coisa bela é uma alegria eterna.

Também é frequente, em certas frases matemáticas e não só, a presença de *quantificadores implícitos*, que é necessário saber explicitar para uma boa compreensão do significado. Por exemplo, na frase

Os diâmetros de uma circunferência cortam-se num ponto,

estão implícitos nada menos que *três* quantificadores. Explicitando: «Para *toda* a circunferência *existe* um ponto no qual *todos* os diâmetros se cortam». Um outro exemplo de quantificador implícito muito frequente em matemática ocorre com a definição de limite, digamos de uma função real de variável real $f : \mathbb{R} \rightarrow \mathbb{R}$, com a convenção usual de que δ, ε são variáveis para números reais *positivos* (quer dizer, $\delta, \varepsilon \in \mathbb{R}$ e $\delta > 0, \varepsilon > 0$), e c, d são números reais (fixos): $\lim_{x \rightarrow c} f(x) = d$ sse

$$\forall \delta \, \exists \varepsilon \, (0 < |x - c| < \varepsilon \Rightarrow |f(x) - d| < \delta).$$

É claro que nesta expressão falta um quantificador em x, $\forall x$, imediatamente à direita do quantificador existencial em ε (supondo tacitamente que x é uma variável para números reais): devia ser

---

[21] A questão não é tão pertinente em se tratando de proposições matemáticas, até porque estas já se apresentam, frequentemente, semiformalizadas.

[22] Mas a frase que figurava em edições anteriores «Todos os pescadores têm uma Santa Padroeira» já tem o significado consensual. Agradecemos ao Prof. Francisco Calheiros a chamada de atenção para este ponto.

$$\forall\delta\,\exists\varepsilon\,\forall x\,(0<|x-c|<\varepsilon\Rightarrow|f(x)-d|<\delta).$$

Em certos manuais encontramos as notações mais antigas (de há cem anos trás) e a expressão

$$\underset{\delta}{\forall}\,\underset{\varepsilon}{\exists}\,(0<|x-c|<\varepsilon\,\dot{\Rightarrow}\,|f(x)-d|<\delta),$$

mas quantas vezes se esquecem as pessoas do ponto por cima do símbolo de implicação, " $\dot{\Rightarrow}$ ", que significa precisamente uma *implicação formal,* isto é, quantificada universalmente (no caso, em x)?![23]

Atendendo a que a interpretação de proposições com quantificadores é algo mais complexa do que no caso proposicional, reformulamos a definição de validade de um argumento (ou seja, a relação de consequência) de uma maneira um pouco mais explícita, fazendo intervir o conceito de interpretação.

9.1 Definição Sejam ϕ_1, ..., ϕ_n, ψ proposições. Um argumento $\phi_1, ..., \phi_n/\psi$ diz-se **válido** sse toda a interpretação que torne as premissas simultaneamente verdadeiras torna a conclusão verdadeira também.

Resulta que um argumento $\phi_1, ..., \phi_n/\psi$ é **inválido** sse existir uma interpretação, pelo menos, que torne verdadeiras as premissas e falsa a conclusão. Uma tal interpretação dir-se-á um **contra-exemplo** para a validade do argumento dado.

Todos os conceitos sintácticos e semânticos introduzidos informalmente neste capítulo serão precisados nos capítulos seguintes.

I.10 O silogismo aristotélico

Aristóteles (384-322 a. C.) foi discípulo de Platão durante cerca de vinte anos e é justamente considerado um dos maiores sábios da antiguidade, pois contemplou nos seus escritos todos os ramos do saber com grande profundidade. Fundou a *Escola Peripatética* (assim designada pelo facto de o mestre ensinar, passeando) em princípios que, em oposição à filosofia de Platão (*Amicus Plato, sed magis amica veritas*[24], provérbio traduzido de uma frase na *Ética*), substituíam à Dialética («Ciência das Ideias») a Metafísica («Ciência das Causas»). A maior obra de Aristóteles no campo das matemáticas e coisas afins é a sua formulação dos

---

[23] A colocação do quantificador em x é imediatamente antes do parêntese esquerdo. Notação alternativa é ' $\underset{x}{\Rightarrow}$ '. Estas notações foram utilizadas por Sebastião e Silva nos anos quarenta, e uma vintena de anos mais tarde nos seus manuais e guias para o ensino secundário (reforma das «matemáticas modernas»), razão porque ainda têm a preferência de algumas pessoas e ainda se encontram em alguns livros. Em Russell (Mathematical logic as based on the theory of types, *Amer. Journ. of Mathematics,* **30** (1908), 222-262; reprod. em Van HEIJENOORT, 150-182) encontramos a notação $\supset_x$.

[24] «Amigo de Platão, mas mais amigo da Verdade.»

princípios e regras da lógica (clássica e modal), a qual exerceu grande influência no desenvolvimento posterior dos métodos de exposição e tratamento das ciências matemáticas. É dele, também, o emprego de *letras* para a representação de grandezas e de proposições, exemplo seguido por Euclides nos seus tratados geométricos e aritméticos.

O *Organon* (ou *Lógica*) compreende as *Categorias*, as *Hermeneias* ou tratado da Proposição, as *Analíticas Primeiras,* ou tratado do Silogismo, as *Analíticas Segundas,* ou tratado da Demonstração, os *Tópicos* e os *Argumentos Sofísticos.* Nos *Analíticas Segundas*, Aristóteles formula o método hipotético-dedutivo (ou método axiomático) adoptado por Euclides nos *Elementos* (300 a. C.) e, desde então, característico das matemáticas (e não só) nas sua forma expositória mais perfeita.

Nas *Analíticas Primeiras* Aristóteles distingue quatro tipos básicos de proposições:

- Universal afirmativa (A): *Todo P é Q*;
- Universal negativa (E): *Nenhum P é Q*;
- Particular (ou existencial) afirmativa (I): *Algum P é Q*;
- Particular (ou existencial) negativa (O): *Algum P não é Q*.[25]

10.1 Exemplos

(A): Todo o homem é mortal;

(E): Nenhum lusitano é temeroso (ou, com o mesmo sentido: Todo o lusitano é não-temeroso);

(I): Algum aluno é aplicado;

(O): Algum professor não é competente.

Modernamente, estes quatro tipos de proposições podem ser representados simbolicamente (domínio das pessoas) por:

(A): $\forall x(Px \rightarrow Qx)$;

(E): $\neg\exists x(Px \wedge Qx)$ [ou $\forall x(Px \rightarrow \neg Qx)$];

(I): $\exists x(Px \wedge Qx)$;

(O): $\exists x(Px \wedge \neg Qx)$,

respectivamente.

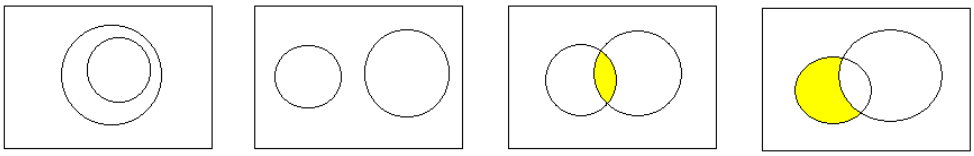
Também podemos dar uma representação conjuntista a estas quatro proposições simbólicas, interpretando P, Q como subconjuntos P, Q de um conjunto dado D

[25] As letras 'A' e 'I' são as duas primeiras vogais da palavra latina *«AFFIRMO»,* enquanto 'E' e 'O' são as da palavra *«NEGO»*.

(o domínio da interpretação) e as operações lógicas $\wedge$, $\vee$, $\neg$, $\rightarrow$ como as operações conjuntistas de intersecção ($\cap$), união ($\cup$), complementação relativamente ao domínio ($D \setminus$) e inclusão ($\subseteq$), respectivamente. Assim, representando por $\emptyset$ o conjunto vazio: as formas (A), (E), (I) e (O) significam

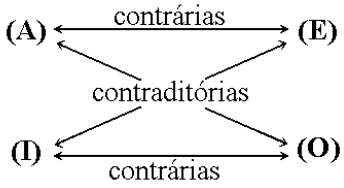
$$P \subseteq Q,\ P \cap Q = \emptyset \text{ [ou } P \subseteq Q^c\text{]},\ P \cap Q \neq \emptyset \text{ e } P \cap Q^c \neq \emptyset,$$

respectivamente, onde $Q^c = D \setminus Q$. Um passo mais adiante, e representamos tudo isto pelos chamados *diagramas de Venn*.[26] Nas figura seguintes, o círculo mais pequeno é P e o maior é Q; as zonas sombreadas são intersecções.



(A) **(E)** **(I)** **(O)**

As proposições dos tipos (A) e (E), ou (I) e (O) são ditas *contrárias*, enquanto (A) e (O), ou (E) e (I) são *contraditórias:*



Aristóteles entendia que uma universal afirmativa (A) implicava uma particular afirmativa (I) correspondente e, portanto, consideraria a proposição

Todo o unicórnio tem guelras

como falsa, por não existirem unicórnios. Neste aspecto estão os lógicos e matemáticos modernos em desacordo com Aristóteles, por considerarem a dita proposição verdadeira (*trivialmente*, como sói dizer-se), *precisamente por não existirem unicórnios:* a falsidade da proposição significaria a existência de, pelo menos, um unicórnio sem guelras, o que é impossível. Pela mesma razão, é

---

[26] Jonh Venn (1834-1923), lógico inglês que publicou o livro *Symbolic Logic* em 1881, onde tentou clarificar, mediante diagramas conjuntistas, a tentativa de «algebrização» da lógica do seu conterrâneo George Boole (1815-1864), que em 1854 publicara o importante tratado *An Investigation of the Laws of Thought on which are founded The Mathematical Theories of Logic and Probabilities*. A ideia de incluir os diagramas num rectângulo que representa o domínio ou universo do discurso é de outro lógico inglês, Charles Dodgson (1832-1898), mais conhecido por Lewis Carroll (autor de *Alice no País das Maravilhas).*

verdade que todo o camelo com asas é daltónico e que o conjunto vazio está contido em qualquer conjunto.

Um *silogismo* aristotélico é um argumento com duas premissas e uma conclusão, umas e outra de uma das formas acima, em que as premissas devem ter em comum uma única partícula predicativa (a que Aristóteles chama o *termo médio*) e a conclusão deve conter as outras duas partículas predicativas das premissas (os *extremos*).

Aristóteles identifica 14 silogismos, divididos em três *Figuras*, conforme as relações entre o termo médio e os extremos. As três Figuras podem ser representadas esquematicamente por[27]

$$\frac{R\text{–}Q}{P\text{–}R}\,, \qquad \frac{R\text{–}Q}{P\text{–}Q}\,, \qquad \frac{R\text{–}Q}{R\text{–}P}\,,$$

respectivamente; os silogismos destas Figuras foram designados, pelos escolásticos medievais, por nomes próprios com três vogais apenas (de entre *a, e, i, o:* as duas primeiras vogais respeitam à forma das premissas, e a terceira vogal à forma da conclusão), para fácil memorização.

O primeiro silogismo da Primeira Figura é o silogismo *Barbara* [premissas e conclusão da forma (A)], da forma

$$\text{Todo } R \text{ é } Q, \text{ Todo } P \text{ é } R \;/\; \text{Todo } P \text{ é } Q\,.$$

As designações dos silogismos da Primeira Figura são

Barbara, *Celarent*, *Darii* e *Ferio*;

os da Segunda Figura são

Cesare, *Camestres*, *Festino* e *Baroco*;

e os da Terceira Figura são

Darapti, *Felapton*, *Dimasis*, *Datisi*, *Bocardo* e *Ferison*

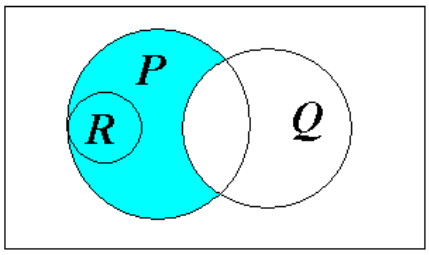
São todos válidos excepto, no moderno entendimento, os dois primeiros da Terceira Figura,

---

[27] Estes esquemas não são os aristotélicos. Aristóteles escreveria *B–A* para significar que o 'sujeito' *A* tem o atributo ou 'predicado' *B* (como, por exemplo, na universal afirmativa *Todo A é um B*), enquanto nós escrevemos *A–B* simplesmente para indicar a ordem (da esquerda para a direita) pela qual ocorrem as partículas predicativas. Para mais informações sobre a lógica aristotélica, ou a história da lógica em geral, consulte-se LUKASIEWICZ ou KNEALE & KNEALE. O livro de MATES tem um tratamento moderno da lógica aristotélica muito interessante.

Darapti: Todo R é Q, Todo R é P / Algum P é Q;
Felapton: Nenhum R é Q, Todo R é P / Algum P não é Q,

respectivamente. Como é de esperar, também os silogismos válidos podem ser representados por diagramas de Venn. Por exemplo, as premissas de *Felapton* correspondem às relações conjuntistas (E) $R \cap Q = \emptyset$ e (A) $R \subseteq P$, que representamos num mesmo rectângulo, no qual também se assinalou a sombreado a conclusão (O) $P \cap Q^c \neq \emptyset$:



I.11 Sobre a implicação material

A terminar, vamos dar uma justificação da tabela de verdade do conectivo $\rightarrow$, nos dois casos em que o antecedente é falso:

	ϕ	ψ	$\phi \rightarrow \psi$
(i)	0	1	**?**
(ii)	0	0	**?**

Vamos supor que *não sabemos* qual deva ser o valor lógico da condicional nestes dois casos. Consideremos a proposição aritmética

Todo o número natural primo é maior ou igual a 2,

que é verdadeira (por definição de número primo[28]). Convencionemos utilizar a letra 'n' como variável para os números naturais (0, 1, 2, ...), de modo que a referida proposição admite a seguinte simbolização (parcial)

$$\forall n \, (n \textit{ é primo} \rightarrow n \geq 2).$$

Sendo esta proposição universal verdadeira no domínio dos números naturais, há-de aceitar-se que *todas as suas particularizações são verdadeiras também*, atendendo ao significado intuitivo do quantificador «para todo». Em particular, pois, hão-de ser verdadeiras as particularizações a $n = 4$,

[28] Um número natural é primo sse é maior do que 1 e só é divisível por si próprio e por 1 (ver Cap. IV).

$$4 \textit{ é primo} \rightarrow 4 \geq 2,$$

e a $n = 1$

$$1 \textit{ é primo} \rightarrow 1 \geq 2,$$

respectivamente. Ambas estas particularizações (verdadeiras!) são da forma $\phi \rightarrow \psi$, a primeira com antecedente falso e consequente verdadeiro [caso (i)], a segunda com antecedente e consequente ambos falsos [caso (ii)].

Portanto, nas linhas (i) e (ii) da tabela acima, o valor lógico da condicional $\phi \rightarrow \psi$ que deve figurar é o valor 1, para que não se quebre a harmonia do universo da lógica!

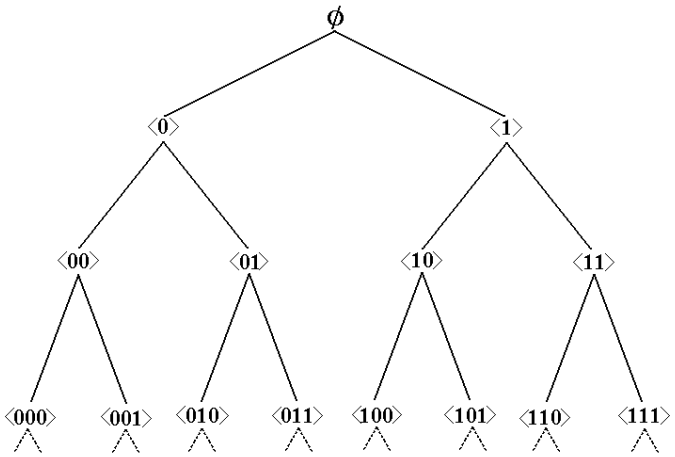
*I.12 Árvores

As árvores (matemáticas!) são estruturas ordenadas muito comuns na lógica e nas ciências da computação, cuja utilidade advém principalmente da sua adequação para a representação de quantidades finitas (ou até infinitas) de informação organizada: fórmulas, deduções formais, sucessões binárias e outras *bases de dados* diversas. Esta secção, de leitura opcional, contém algumas definições e resultados a utilizar noutras secções, também opcionais, que foram introduzidas na 3.ª edição e se destinam primordialmente a contemplar alguns assuntos mais próximos da chamada *lógica computacional,* que é uma parte da lógica mais vocacionada para as aplicações nas ciências da computação (programação em lógica, demonstração automática, análise de programas, etc.). A leitura profícua desta secção exige do leitor certos conhecimentos e maturidade matemática em maior grau do que as secções precedentes deste capítulo, uma vez que se destina a aplicações mais especializadas.

Antes de dar as definições pertinentes apresentamos um exemplo de uma árvore, a *árvore binária completa* (ver página seguinte)*,* cujos «nós» são ocupados pelas sucessões binárias finitas, isto é, sucessões finitas de 0's e 1's. Representamos abreviadamente tais sucessões por $\langle s_1 s_2 ... s_k \rangle$ $(k \geq 1)$, em vez de $\langle s_1, s_2, ..., s_k \rangle$, onde cada s_i é 0 ou 1. Esta árvore é habitualmente designada por $\{0,1\}^*$ (= conjunto das sucessões finitas de elementos de $\{0,1\}$), ou simplesmente por ${}^{\omega}2$. Observe-se que esta árvore «cresce de cima para baixo», sem nunca parar (algumas outras, a considerar no próximo capítulo, crescem «de baixo para cima» — trata-se apenas de conveniências de representação, e não de qualquer diferença conceptual). No topo ou *raiz* da árvore colocou-se a sucessão vazia, $\emptyset$, no *nível* imediatamente abaixo desta as duas sucessões de comprimento 1, no nível seguinte as quatro sucessões de comprimento 2, e assim sucessivamente. O leitor atento há-de reparar que esta árvore tem uma «lógica formativa» deveras simples e ordenada. Outras árvores podem diferir desta em diferentes aspectos, por exemplo, no número de nós por debaixo de cada nó, no número total de nós, no número de níveis, etc., mas todas elas têm algo em comum que será estipulado numa definição.

Precisamos de algumas noções sobre as ordens parciais (elas são dadas novamente em alguns exercícios do Cap. III, num contexto mais formal, ver pág. 229).

Uma *ordem parcial* num conjunto T é uma relação binária $\leq$ («menor ou igual») em T que é *reflexiva* ($x \leq x$, para qualquer elemento x de T), *anti-simétrica* (se $x \leq y$ e $y \leq x$, então $x = y$, para quaisquer elementos x, y de T) e *transitiva* (se $x \leq y$ e $y \leq z$, então $x \leq z$, para quaisquer elementos x, y, z de T).



São habituais as convenções seguintes: $y \geq x$ é sinónimo de $x \leq y$, e $x < y$ de $x \leq y \wedge x \neq y$, respectivamente ($<$ é a relação estrita associada a $\leq$). Na árvore ${}^{\omega}2$ acima (estamos supondo, claro está, a conformidade com a definição de árvore que será dada mais adiante) está de facto definida uma ordem parcial $\leq$: $\emptyset \leq \sigma$, para qualquer σ em ${}^{\omega}2$, e para quaisquer sucessões binárias não vazias σ e τ, tem-se $\sigma \leq \tau$ sse $\sigma = \tau$ ou $\sigma = \langle s_1 ... s_k \rangle$ e $\tau = \langle s_1 ... s_k s_{k+1} ... s_{k+m} \rangle$ para algum $k \geq 1$ e algum $m \geq 1$, onde cada s_i é 0 ou 1.[29] Por exemplo, $\langle 001 \rangle < \langle 00110 \rangle$, mas $\langle 001 \rangle \not< \langle 010 \rangle$ nem $\langle 010 \rangle \not< \langle 001 \rangle$ (dizemos que $\langle 001 \rangle$ e $\langle 010 \rangle$ são *incomparáveis*).

Uma ordem parcial $\leq$ é *ordem total,* ou uma *cadeia* sse a relação associada $<$ tiver a propriedade de tricotomia fraca (ver Nota 135, pág. 229): para quaisquer elementos x, y de T, tem-se $x < y$ ou $x = y$ ou $y < x$. Finalmente, uma ordem total $\leq$ é uma *boa ordem* sse não existir nenhuma cadeia infinita

---

[29] Por outras palavras, atendendo a que as sucessões finitas (e infinitas) são, afinal de contas, funções, tem-se $\sigma \leq \tau$ sse $\sigma \subseteq \tau$ (isto é, τ é uma *extensão* ou *prolongamento* de σ). Se $\sigma = \langle s_1 ... s_k \rangle$, σ é a função definida em $\{1, ..., k\}$ com valores em $\{0, 1\}$ tal que, para $i = 1, ..., k$, $\sigma(i) = \sigma i = s_i$. Uma maneira de obter uma extensão de uma sucessão finita $\sigma = \langle s_1 ... s_k \rangle$ é mediante a sua *concatenação* com uma qualquer sucessão finita $\tau = \langle t_1 ... t_m \rangle$: $\sigma^\frown\tau = \langle s_1 ... s_k s_{k+1} ... s_{k+m} \rangle$, onde $s_{j+k} = t_j$ para $j = 1, ..., m$, de modo que $\sigma \subseteq \sigma^\frown\tau$ para qualquer τ.

$\langle x_0, x_1, x_2, ...\rangle$ de elementos de T tais que

$$\cdots < x_2 < x_1 < x_0.$$

Pode acontecer que uma ordem parcial $\leq$ num conjunto T tenha um *primeiro elemento,* ou *elemento mínimo:* será um elemento a de T tal que $a \leq x$, para todo x em T, e não é difícil concluir que não pode haver mais de um primeiro elemento (exercício). Dado um elemento x de T, diz-se dos elementos y tais que $y < x$ que *precedem* x, ou que são os *predecessores* de x, e dos elementos z tais que $x < z$ que *sucedem* x, ou que são os *sucessores* de x; um *sucessor imediato* de x, se existir, é um sucessor z de x tal que não existe nenhum outro elemento t entre x e z, isto é, tal que $x < t < z$, e um *predecessor imediato* de x é um predecessor z de x tal que não existe nenhum elemento t entre z e x. Na árvore ${}^{\omega}2$, $\emptyset$ é o primeiro elemento, e qualquer elemento de ${}^{\omega}2$ tem exactamente dois sucessores imediatos (quais?). A ordem parcial $\leq$ em ${}^{\omega}2$ acima definida não é uma ordem total (porquê?) nem, por conseguinte, uma boa ordem, mas se pensarmos no conjunto dos predecessores de um elemento dado $\sigma = \langle s_1...s_k\rangle \neq \emptyset$, que são

$$\emptyset < \langle s_1\rangle < \langle s_1 s_2\rangle < \cdots < \langle s_1...s_{k-1}\rangle,$$

eles formam uma cadeia bem ordenada, mas é claro que esta cadeia pode ser estendida *ad infinitum,* de mais de uma maneira (aliás, de infinitas maneiras), por exemplo:

$$\emptyset < \langle s_1\rangle < \langle s_1 s_2\rangle < \cdots < \langle s_1...s_{k-1}\rangle < \langle s_1...s_{k-1}0\rangle < \langle s_1...s_{k-1}01\rangle < ...$$

Em geral, uma cadeia que não pode ser estendida de nenhuma maneira, nem com elementos intermédios nem com elementos no fim diz-se *maximal.* Observe-se que uma cadeia maximal em ${}^{\omega}2$ começa sempre com $\emptyset$ (porquê?). Outra propriedade que esta árvore possui em comum com todas as outras que serão consideradas neste livro é a de que todo o elemento, excepto a raiz, possui um único predecessor imediato.

Com o exemplo da árvore binária completa em mente, estamos prontos para a definição principal desta secção.

12.1 Definição Uma **árvore** é um conjunto não vazio T, a cujos elementos chamamos *nós,* no qual está definida uma ordem parcial $\leq$ com primeiro elemento, chamado *raiz,* e tal que os predecessores de todo o elemento diferente da raiz formam uma cadeia bem ordenada. Um *ramo* em T é uma cadeia maximal de elementos de T.[30]

---

[30] Estamos cometendo um pequeno abuso. Devíamos dizer que uma árvore é um par $(T, \leq_T)$, onde $\leq_T$ é uma ordem parcial em T, etc. Na prática, se não houver confusão possível, escreve-se simplesmente $\leq$ em vez de $\leq_T$ e designa-se a árvore por T. Observe-se, por outro lado, que da definição de árvore resulta que todo o elemento diferente da raiz possui um único predecessor imediato (porquê?).

Os *níveis* de uma árvore T definem-se indutivamente:[31] o nível 0 é constituído pela raiz; para cada natural $n \geq 0$, o nível $n+1$ é constituído por todos os sucessores imediatos dos nós do nível n. A *altura* (*cota* ou *profundidade*) de uma árvore T é o maior natural n tal que existe um nó de nível n, se existir um tal n, caso contrário a árvore tem altura infinita. De entre as árvores com altura infinita, têm altura ω aquelas cujos nós se dividem por todos os níveis n, para todo o natural n.[32]

Uma árvore diz-se *finita* ou *infinita* conforme tenha um número finito ou infinito de nós; diz-se de *ramificação finita* se cada nó possui, quando muito, um número finito de sucessores imediatos; diz-se n*-ária* (*binária,* se $n = 2$) se cada nó possui, quando muito, n sucessores imediatos. Um elemento que não possui sucessores diz-se *terminal*.

O principal resultado sobre as árvores de ramificação finita é o seguinte:

12.2 Lema de König

Toda a árvore infinita de ramificação finita tem, pelo menos, um ramo infinito.

Dem. Seja T uma árvore infinita de ramificação finita. Definimos indutivamente[33] um sucessão $\langle t_0, t_1, ..., t_n, ... \rangle$ de elementos de T que constitui um ramo infinito κ. Ponhamos $t_0 =$ raiz de T; é claro que t_0 possui uma infinidade de sucessores, visto que T é infinita, por hipótese. Supondo já definidos os primeiros n termos da sucessão, t_0, t_1, ..., t_{n-1}, nos níveis 0, 1, ..., $n-1$, respectivamente, de tal modo que cada t_i possui uma infinidade de sucessores, por hipótese t_{n-1} possui um número finito de sucessores imediatos, mas então um destes, pelo menos, digamos u, possui uma infinidade de sucessores (caso contrário t_{n-1} possuiría, ao todo, um número finito de sucessores). Ponhamos $t_n = u$, que está no nível n, e possui uma infinidade de sucessores, de modo que podemos prosseguir com a definição de t_{n+1} e, portanto, de κ.■[34]

Frequentemente, é apenas a forma ou «esqueleto» de uma árvore que é importante e não o conteúdo de cada nó. A mesma forma pode servir para vários conteúdos diferentes, mediante uma função que associa a cada nó um objecto de certa espécie. Uma tal função é chamada uma *etiquetagem,* e o objecto associado a

---

[31] Para uma discussão geral sobre definições indutivas ver secção II.3.

[32] ω é o primeiro ordinal infinito. Neste livro nunca consideraremos árvores de altura superior a ω. A árvore $^{\omega}2$ é um exemplo de árvore de altura ω. Nas árvores de altura finita ou ω, a propriedade de que todo o elemento diferente da raiz possui um único predecessor imediato implica a boa ordenação do conjunto (cadeia) dos predecessores de um tal elemento.

[33] Ou, mais propriamente, por recorrência. Uma ideia das definições por recorrência, num contexto muito particular, é dado no exercício 2.4 do Cap. II.

[34] O sinal '■', no final de um parágrafo de uma demonstração, quer dizer: fim da demonstração.

cada nó será a *etiqueta* que o nó recebe. Também é possível ordenar os nós de cada nível (ordem lexicográfica), mas não vamos prosseguir nestes desenvolvimentos. As árvores que utilizaremos aparecem já etiquetadas de origem, como é o caso das árvores de formação das fórmulas, que exemplificamos a seguir à definição de conectivo principal (pág. 51).

1.13 Programação em lógica

A lógica quantificacional (cálculo de predicados), até há poucas décadas, interessava apenas aos matemáticos, lógicos e filósofos, mas encontrou novas aplicações e motivos de interesse nas ciências informáticas ou da computação. Nesta secção descrevemos, mui abreviadamente, algumas destas novas perspectivas.

As linguagens de programação, como PASCAL, são essencialmente linguagens *procedimentais:* os seus programas consistem em grande parte de *instruções* para executar determinados algoritmos para resolver os problemas pretendidos. Outras linguagens mais recentes e próximas da lógica do discurso, como PROLOG (de PROgramação em LÓGica) são linguagens *declarativas* ou *descritivas,* e foram concebidas para organizar, manipular e extrair informação de *bases de dados,* bases estas que são constituídas por itens de dois tipos: (i) expressões predicativas como $P(a, b)$, $Q(c)$, etc. (mas são frequentes notações mais explícitas ou descritivas, como no exemplo seguinte), que representam *factos*, e (ii) *regras,* que são descrições de predicados na forma condicional.

13.1 Exemplo Uma base de dados para certa cadeia alimentar (em certo meio ambiente) é constituída por certos *factos,* em forma de *declarações* ou *descrições* predicativas, como

$$\begin{aligned}&\mathit{comer}(\mathtt{urso}, \mathtt{peixe})\\ &\mathit{comer}(\mathtt{urso}, \mathtt{mel})\\ &\mathit{comer}(\mathtt{gazela}, \mathtt{erva})\\ &\mathit{comer}(\mathtt{leão}, \mathtt{gazela})\,.\end{aligned}$$

Convencionamos que $\mathit{comer}(x, y)$ significa «x come y». Outros factos podem fazer parte da base de dados, como as descrições

$$\begin{aligned}&\mathit{animal}(\mathtt{urso})\\ &\mathit{animal}(\mathtt{peixe})\\ &\mathit{animal}(\mathtt{gazela})\\ &\mathit{animal}(\mathtt{leão})\\ &\mathit{planta}(\mathtt{erva})\\ &\mathit{líquido}(\mathtt{mel})\quad .\end{aligned}$$

Esta base de dados tem subjacente uma determinada interpretação, num domínio constituído por todos os entes (constantes) que são argumentos dos

predicados que lá estão, que no caso acima são: urso, peixe, mel, gazela, erva. Em qualquer momento a base de dados pode ser ampliada com novos factos e o respectivo domínio expandido com novos entes. Entre o utilizador e o programa é possível estabelecer certos *diálogos:* ao utilizador é permitido formular certas perguntas sobre os factos ou inquirir se certa conclusão é consequência dos factos que compõem a base de dados, ao que o programa responde SIM ou NÃO, ou fornece uma resposta de outro tipo (por exemplo, uma listagem de indivíduos), conforme a pergunta que for feita. Perguntas simples típicas são da forma:

- `base`(d): o facto d está na base de dados?
- `argumento`$(x : d)$: o ente x é um argumento do facto d?

Por exemplo, à pergunta `base`(***animal***(`peixe`)), o programa responde SIM, mas à pergunta `base`(***planta***(`mel`)) o programa responde NÃO. À pergunta `argumento`$(x :$ ***come***(`urso`$, x)$) responde com a lista

`peixe`
`mel` .

Perguntas mais elaboradas podem conter os conectivos `e`, `ou`, `não`, por exemplo, `argumento`$(x :$ ***come***(x, y) `e` ***planta***(y)), cuja resposta é a lista dos entes que comem plantas, no caso, somente a

`gazela`.

Os itens do segundo tipo de uma base de dados PROLOG chamam-se *regras* mas são, na realidade, descrições predicativas especiais, por tomarem a forma condicional, como, por exemplo, a regra para definir o predicado *carnívoro:*

carnívoro(x) `se` ***comer***(x, y) `e` ***animal***(y).

Isto exprime que x é carnívoro se x come animais. À pergunta `argumento`$(x :$ ***carnívoro***(x)) o programa responde com a lista

`urso`
`leão`.

1.15 Exercícios e Complementos

§1.1-1.9

1.1 Simbolize ao nível proposicional os seguintes argumentos:

(a) Se não existe petróleo no Algarve então os peritos estão certos ou o Governo mente. Existe petróleo no Algarve ou os peritos estão errados. Portanto, o Governo não mente;

(b) Os vencimentos aumentam somente se há inflação. Se há inflação, então o custo de vida aumenta. Os vencimentos não aumentam. Portanto, o custo de vida aumenta;

(c) Se 2 é primo, então é o menor primo. Se 2 é o menor primo, então 1 não é primo. 1 não é primo. Portanto, 2 é primo;

(d) Maria João é boa pianista ou é boa bailarina. Maria João é boa pianista. Portanto, Maria João não é boa bailarina;

(e) Só se eu ganhar o totoloto é que pago aos credores. Os credores não ficam satisfeitos excepto se eu lhes pagar. Portanto, ganho o totoloto ou os credores não ficam satisfeitos. [NB. «excepto se» considera-se sinónimo de «ou», ou de «se não»].

1.2 (a) Quais dos argumentos anteriores são válidos e quais são inválidos? [Sugestão: construa tabelas de verdade para as premissas e conclusão, e verifique, nelas, se a conclusão é verdadeira sempre que as premissas são simultaneamente verdadeiras.]

(b) O argumento

$$\frac{\begin{array}{l}\text{Todo o homem é mortal}\\ \text{Sócrates é homem}\\ 2+2=5\end{array}}{\text{Sócrates é mortal}}$$

é válido ou inválido?

1.3 Tendo em conta a interpretação com *Domínio:* conjunto dos números naturais (≥ 0); Px*:* x é par; Rx*:* x é primo; Ix*:* x é ímpar; $Q(x,y)$*:* x divide y, ou y é múltiplo de x, traduza para português coloquial as expressões simbólicas seguintes e diga quais as verdadeiras e quais as falsas para a interpretação dada:

(a) $\forall x\,(Q(2,x) \rightarrow Px)$;

(b) $\exists x\,(Px \wedge Q(x,3))$;

(c) $\exists x\,(Ix \wedge Q(0,x))$;

(d) $\forall x\,(\neg Px \rightarrow \neg Q(2,x))$;

(e) $\forall x\,(Px \rightarrow \forall y\,(Q(x,y) \rightarrow Py))$;

(f) $\forall x\,(Rx \rightarrow \exists y\,(Py \wedge Q(x,y)))$;

(g) $\forall x\,(Ix \rightarrow \forall y\,(Ry \rightarrow \neg Q(x,y)))$.

1.4 (a) Para cada um dos três grupos seguintes, fixe uma interpretação adequada e simbolize as proposições respectivas:

A. (1) Toda a modelo é vaidosa; (2) Algumas modelos são vaidosas; (3) Nenhuma modelo é vaidosa; (4) Algumas modelos não são vaidosas; (5) Somente

as modelos são vaidosas; (6) Todas são vaidosas, excepto as modelos; (7) Algumas modelos são bonitas, mas vaidosas.

B. (1) Todo o (número natural) primo maior que 2 é ímpar; (2) Existe um primo par; (3) Existe um e não mais de um primo par [não utilize $\exists^1$]; (4) Para todo o número existe um primo maior do que ele; (5) n é primo [utilizando $\leq$ e $\times$].

C. (1) Com toda a linha incidem, pelo menos, dois pontos;[35] (2) Por dois pontos passa, pelo menos, uma linha; (3) Por dois pontos não passa mais de uma linha; (4) Quaisquer duas linhas têm um ponto comum; (5) Duas linhas têm, quando muito, um ponto comum.

(b) Relativamente à parte C, dê um exemplo de uma interpretação (isto é, um domínio com pontos e linhas e uma relação de incidência, que pode ser a pertença de pontos em linhas, $\in$) com as propriedades 1-5).

1.5 Utilizando um símbolo predicativo binário R e simbolizando «x está na relação R com y» por xRy, exprima simbolicamente (utilizando $=$, quando necessário) que R é:

(a) Reflexiva; (b) Simétrica; (c) Transitiva;

(d) Anti-simétrica; (e) Conexa (ou dicotómica);

(f) Irreflexiva; (g) Não reflexiva; (h) Não vazia;

(i) Tricotómica fraca (com «...ou...ou...»);[36]

(j) Não transitiva; (k) Não simétrica;

(l) Definida em todo o domínio interpretativo[37] (isto é, todo o objecto está na relação R com algum objecto);

(m) Serial (isto é, todo o objecto está na relação R com algum outro);

(n) Funcional (isto é, todo o objecto está na relação R com, quando muito, um objecto);

(o) Uma função no domínio interpretativo; (p) Injectiva; (q) Sobrejectiva;

(r) Uma permutação do domínio interpretativo.

---

[35] Quando aqui se diz «dois» ou «duas» subentende-se «distintos(as)». Como domínio pode-se considerar a colecção dos objectos geométricos primitivos, não definidos (pontos e linhas), introduzindo-se neste domínio os predicados unários *a é ponto*, *a é linha* e o predicado binário de incidência *a incide com b* (ou *b passa por a*), simbolicamente aIb. Aliás, pode-se definir no domínio dos pontos e linhas: *a é ponto* $\leftrightarrow \exists y\, aIy$, *$b$ é linha* $\leftrightarrow \exists x\, xIb$. *"$a$ é ponto" pode-se abreviar Pa, e "b é linha" abrevia-se Lb.*

[36] A tricotomia *forte* é a propriedade de que, para quaisquer x, y, z, uma e uma só das condições $x = y$, xRy, yRx tem lugar.

[37] Não confundir o domínio interpretativo (universo do discurso) com o *domínio da relação R*, que é o conjunto dos elementos x do domínio interpretativo tais que xRy para algum y.

1.6 Simbolize ao nível quantificacional, fornecendo ao mesmo tempo uma interpretação conveniente, e diga se são válidos os argumentos seguintes:

(a) Todo o leão é feroz. Alguns leões não bebem água. Portanto, alguns animais ferozes não bebem água [domínio: animais];

(b) Todos os britânicos, excepto os escoceses, são fleumáticos. Ricardo Coração de Leão é britânico, mas não é fleumático. Portanto, Ricardo Coração de Leão é escocês [domínio: pessoas];

(c) Há, quando muito, um lógico incoerente. Frege é um lógico incoerente. Russell não é Frege. Portanto, Russell é um lógico coerente [use $=$] .

1.7 (a) Simbolize ao nível quantificacional, tendo em conta a seguinte interpretação: *Domínio:* todas as coisas; Mx*:* x é um problema matemático; Lx*:* x é um problema lógico; Sx*:* x é solúvel; Fxy*:* x é mais fácil de resolver do que y.

(1) Existem problemas matemáticos insolúveis;

(2) Nenhum problema lógico é insolúvel;

(3) Os problemas matemáticos são mais fáceis de resolver do que os problemas lógicos;

(4) Alguns problemas lógicos são mais fáceis de resolver do que *outros* (problemas lógicos).

(b) Idem, para a interpretação: *Domínio:* tudo; Px*:* x é uma pessoa; Cxy*:* x compreende y; a*: Alice no País das Maravilhas*; b*: Principia Mathematica*; c*: Lógica e Aritmética.*

(1) Quem compreende *Alice no País das Maravilhas* ou *Principia Mathematica* compreende *Lógica e Aritmética*;

(2) Ninguém compreende tudo;

(3) Ninguém compreende nada;

(4) Somente quem compreende *Principia Mathematica* compreende *Lógica e Aritmética*.

(c) Idem, para a interpretação com *domínio:* tudo; Px*:* x é uma pessoa; Dx*:* x é dinheiro; Rxy*:* x possui (ou tem) y; b*:* Bill Gates, e traduza em português coloquial a última proposição ou sentença:

(1) Existem pessoas sem dinheiro nenhum;

(2) Bill Gates tem algum dinheiro, mas não tem o dinheiro todo que há;

(3) Toda a gente tem algum dinheiro, mas não tem o dinheiro todo que há;

(4) $\forall x(Px \wedge \forall y(Dy \rightarrow Rxy) \rightarrow \forall z Rxz)$.

1.8 Numa mansão victoriana, várias pessoas são suspeitas de um crime. São elas o motorista (A), o cozinheiro (B), o mordomo (C) e o jardineiro (D). O famoso detective Sherlock Holmes investiga e descobre certos factos (ϕ_1, ϕ_2, ..., ϕ_7), a partir dos quais conclui, intuitiva ou semanticamente, qual dos suspeitos é o

culpado (ψ). Simbolize ao nível proposicional o argumento seguinte (cujas premissas são os sete factos descobertos por Sherlock Holmes), e proceda como Sherlock Holmes descobrindo o culpado:

«B é culpado somente se A é culpado. A é culpado sse o crime foi cometido com um revólver. B é culpado ou A é culpado, ou C é culpado ou D é culpado. Se C é culpado então o crime não foi cometido com um revólver. D não é culpado se o crime não foi cometido com um machado. Se o crime foi cometido com um revólver ou com um machado então o crime foi premeditado e foi cometido suavemente. O crime não foi cometido suavemente. Portanto, _____ é culpado.» [NB. Querendo, pode utilizar a, b, c, d, r, m, p, s como letras proposicionais].

1.9 Numa folha em branco, numere as páginas 1, 2 e escreva em cada página as frases seguintes: na página 1 escreva «A frase escrita na página 2 é verdadeira» e na página 2 escreva «A frase escrita na página 1 é falsa». Designando por ϕ a frase escrita na página 1, verifique que ϕ é verdadeira se e só se ϕ é falsa.[38]

§1.10

1.10 Simbolize e dê exemplos de silogismos aristotélicos válidos e contra-exemplos para os inválidos (*Darapti* e *Felapton*). Represente os silogismos válidos por relações entre subconjuntos (P, Q, R) de um domínio interpretativo. [Por exemplo, «todo P é Q» exprime que o conjunto P é subconjunto do conjunto Q, $P \subseteq Q$; «algum P é Q» exprime que a intersecção $P \cap Q$ é não vazia, etc.]

§1.13

***1.11** Dê exemplos de:

(a) uma árvore de ramificação finita que não seja n-ária para nenhum n;

(b) uma árvore infinita de altura 2;

(c) uma árvora de altura ω com apenas 2 ramos.

***1.12** Prove que uma ordem total $\leq$ num conjunto T é uma boa ordem sse todo o subconjunto não vazio S de T possui elemento mínimo.

***1.13** A *ordem lexicográfica* $\leq_L$ no conjunto de todos os pares ordenados de números naturais, $\mathbb{N}^2 = \mathbb{N} \times \mathbb{N} = \{(m, n) : m \in \mathbb{N} \wedge n \in \mathbb{N}\}$, define-se da seguinte maneira:

---

[38] A situação descrita é conhecida como o **paradoxo de Tarski** e constitui um dos mais conhecidos paradoxos de natureza semântica de que está eivada qualquer língua natural, como o português. Tais paradoxos mostram que as línguas naturais não são, possivelmente, as mais adequadas à expressão de teorias científicas, na medida em que permitem que nelas se exprima a sua própria semântica (quer dizer, tais línguas incluem a sua própria metalíngua), dando, assim, lugar a situações paradoxais, como a do paradoxo de Tarski.

$$(m, n) <_L (p, q) \text{ sse } m < p \text{ ou } (m = p \text{ e } n < q),$$

onde $\leq$ é a ordem usual em $\mathbb{N}$. Prove que $\leq_L$ é uma boa ordem.

***1.14** Mostre que o lema de König para árvores binárias é equivalente à compacidade do espaço $C = {}^{\omega}2 = {}^{\mathbb{N}}\{0, 1\} =$ conjunto de todas as sucessões (infinitas) de 0's e 1's, com a topologia produto da topologia discreta sobre $\{0, 1\}$. Este espaço é vulgarmente chamado *espaço de Cantor*. (Ver também II.14, final de II.16 e exercícios respectivos, especialmente 2.39, pág. 154).[39]

[39] Uma base para a topologia do espaço de Cantor C, descrita acima como a topologia produto da topologia discreta sobre $\{0, 1\}$, é o conjunto dos conjuntos da forma $[\sigma] = \{\tau \in \mathsf{C} : \tau \supseteq \sigma\}$, onde $\sigma \in {}^{\omega}2$, chamados *abertos básicos*. Isto significa que um conjunto $A \subseteq C$ é *aberto* sse para todo $\sigma \in A$ existe n tal que todas as sucessões em C que coincidem com σ nos primeiros n termos também pertencem a A. Os conjuntos *fechados* são os complementares dos abertos. A *compacidade topológica* de C pode ser formulada da seguinte maneira: toda a cobertura de C (formada por abertos) possui uma subcobertura finita. Equivalentemente: toda a família (não vazia) de fechados tal que toda a subfamília finita tem intersecção não vazia, tem ela mesma intersecção não vazia.

Capítulo II

CÁLCULO PROPOSICIONAL

II.1 Introdução

Tendo apresentado no capítulo anterior alguns elementos de análise lógica, diversos exemplos de argumentos e uma definição informal da noção de *validade* de um argumento, é altura de matematizar um pouco a discussão, passo indispensável para a tarefa de sistematização e classificação das formas de argumentação válida, entre outras coisas.

A fim de facilitar um pouco a nossa tarefa, concebemos uma linguagem artificial, com sintaxe e semântica perfeitamente definidas (matematicamente falando), coisa assaz difícil (quiçá impossível) de conseguir para uma língua natural. Tal linguagem é uma entidade abstracta e formal, mas sem grande esforço se compreende que ela formaliza um fragmento significativo da língua natural particularmente adequado à expressão de proposições e teorias matemáticas.

Por conveniência táctica, dividimos a nossa tarefa em duas etapas. A primeira, neste capítulo, lida apenas com a chamada **lógica proposicional** (ou **cálculo proposicional**), e a segunda, no capítulo seguinte, com a **lógica de primeira ordem** (ou **lógica elementar**, ou **cálculo de predicados**). Em ambos os casos especificaremos uma linguagem formal e um sistema dedutivo (dito de *dedução natural*), isto é, um sistema de *regras* (daí a tónica no aspecto *cálculo*), ditas *de inferência*, para efectuar deduções, regras essas correspondentes a formas particularmente simples de argumentos ou raciocínios válidos (incluindo os tradicionalmente chamados silogismos) ou a métodos demonstrativos muito comuns em matemática, como o *método directo,* o *método indirecto* ou de *redução ao absurdo* e o *método da demonstração por casos*. Após o desenvolvimento do sistema dedutivo diremos também alguma coisa sobre a semântica da linguagem e as relações entre o cálculo dedutivo e a noção semântica de consequência — a chamada *metateoria*, porventura a parte mais interessante dos estudos lógicos. Na parte final de cada capítulo estudaremos *outros* sistemas dedutivos (e respectiva metateoria) equivalentes ao sistema de dedução natural anteriormente proposto, com características e funcionalidas específicas, em função das aplicações pretendidas, nomeadamente, das aplicações à chamada *lógica computacional.*

II.2 A linguagem proposicional

Uma linguagem formal compreende sempre um alfabeto (ou vocabulário) primitivo e uma gramática ou sintaxe. Nesta secção introduzimos a linguagem do cálculo proposicional, $\mathcal{L}^0$. O **alfabeto** de $\mathcal{L}^0$ compreende os seguintes símbolos:

• Letras proposicionais p, q, r, ... (também chamadas *átomos,* possivelmente com índices[40]);

• Conectivos proposicionais primitivos $\wedge$, $\vee$, $\neg$, $\rightarrow$;

• Parênteses $($, $)$.

Com estes símbolos formaremos certas expressões[41], chamadas as *fórmulas* (subentenda-se, salvo aviso em contrário, *de* $\mathcal{L}^0$), de acordo com certas regras sintácticas ou gramaticais, regras essas que constituem a gramática ou sintaxe de $\mathcal{L}^0$. As **fórmulas** de $\mathcal{L}^0$ são definidas pelas seguintes **regras de formação**:

F_1. Toda a letra proposicional é uma fórmula;

F_2. Se ϕ é uma fórmula então $\neg\phi$ é uma fórmula;

F_3. Se ϕ, ψ são fórmulas então $(\phi \wedge \psi)$, $(\phi \vee \psi)$, $(\phi \rightarrow \psi)$ são fórmulas;

F_4. Nada mais é fórmula, isto é, uma expressão é uma fórmula sse puder ser obtida ou construída a partir de letras proposicionais de acordo com as regras F_2, F_3 aplicadas um número finito qualquer de vezes.

Exemplos de fórmulas de $\mathcal{L}^0$: p, q, r, $\neg p$, $\neg\neg\neg q$, $(p \wedge q)$, $((p \wedge q) \rightarrow \neg r)$; exemplos de expressões que não são fórmulas: $(\,)$, $p\,\neg$, $p \wedge q$, $(\neg\neg q)$, $\rightarrow(\neg pp$.

2.1 Convenções de escrita Note-se que não incluímos $\leftrightarrow$ como símbolo primitivo. Preferimos introduzir $\leftrightarrow$ como símbolo definido. Para quaisquer fórmulas ϕ e ψ, definimos

$$(\phi \leftrightarrow \psi) \;=\; ((\phi \rightarrow \psi) \wedge (\psi \rightarrow \phi)).^{42}$$

---

[40] Muitas vezes é conveniente supor que as letras proposicionais estão indexadas pelos numerais, p_0, p_1, p_2, ...

[41] Uma **expressão** sobre um alfabeto é simplesmente um arranjo, possivelmente com repetições, inteiramente arbitrário, dos símbolos do alfabeto, isto é, uma sequência finita obtida justapondo ou concatenando horizontalmente os símbolos do alfabeto. Admitimos tacitamente que os símbolos do alfabeto são distintos dois a dois, e que nenhum símbolo é uma sequência de outros símbolos. Isto garante que a escrita de expressões é única: se s_1, s_2, ..., s_n e s'_1, s'_2, ..., s'_m são símbolos e $s_1 s_2 \cdots s_n = s'_1 s'_2 \cdots s'_m$, então $n = m$ e $s_i = s'_i$ para $i = 1, \ldots, n$.

[42] Utilizamos o símbolo $=$ em definições, que se deve ler «idêntico a, por definição». Também é frequente encontrar-se, na literatura, $:=$, $=_{\mathrm{df}}$, com o mesmo significado. Em qualquer caso, numa definição, a expressão à esquerda de $=$ deve-se encarar como uma abreviatura da expressão que figura à direita de $=$. Analogamente, usa-se também o símbolo $\leftrightarrow$ (ou $\leftrightarrow_{\mathrm{df}}$) em definições, com o significado «equivalente a, por definição».

Note-se também que, em rigor, ϕ e ψ não são fórmulas, estritamente falando, antes são letras do alfabeto grego (privilégio do relator) que utilizamos como variáveis para fórmulas.[43]

Por outro lado, os parênteses $(,)$ são necessários para evitar ambiguidades de escrita e de leitura, mas convencionamos desde já suprimir alguns sempre que tal supressão se puder fazer sem comprometer a leitura correcta.[44] Nomeadamente, parênteses exteriores podem-se suprimir e, além disso, as expressões

$$(\phi \diamond \psi) \rightarrow \theta,\ \phi \rightarrow (\psi \diamond \theta),\ \phi \diamond (\psi \diamond \theta)$$

abreviam-se

$$\phi \diamond \psi \rightarrow \theta,\ \phi \rightarrow \psi \diamond \theta,\ \phi \diamond \psi \diamond \theta,$$

respectivamente, onde $\diamond$ é $\wedge$, ou é $\vee$. Finalmente, $\phi \rightarrow (\psi \rightarrow \theta)$ [ou seja, oficialmente, $(\phi \rightarrow (\psi \rightarrow \theta))$] abrevia-se $\phi \rightarrow \psi \rightarrow \theta$. Note que para $(\phi \rightarrow \psi) \rightarrow \theta$ não é proposta nenhuma abreviatura e não deve, pois, simplificar-se.

II.3 Definições indutivas. Valorações

A definição de fórmula que foi dada é um exemplo do que em lógica se chama uma **definição indutiva**. Tais definições são muito comuns em lógica, e há toda uma teoria relativamente sofisticada sobre a legitimidade, o alcance e as aplicações de definições desse tipo. Aqui diremos apenas umas breves palavras sobre tais definições, particularizadas à lógica proposicional.

A forma geral de uma definição indutiva é a seguinte. Supõem-se dados: um conjunto E, uma parte não vazia P de E, e um conjunto F de operações definidas em E com valores em E. Um conjunto $D \subseteq E$ diz-se **indutivo** sse

(i) $P \subseteq D$ (isto é, P é subconjunto de D), e
(ii) D é fechado para as operações de F (isto é, as operações de F aplicadas a elementos de D produzem elementos de D).

Note-se que há, pelo menos, um conjunto indutivo: o próprio conjunto E é indutivo mas, em geral, pode haver outros conjuntos indutivos contidos em E. O mais pequeno conjunto indutivo contido em E (isto é, a intersecção de todos os conjuntos indutivos contidos em E) denota-se F^*, e é este conjunto que se diz ter sido **definido indutivamente** (ou **gerado**) pelas operações de F com base P.

---

[43] São chamadas, na gíria dos lógicos, *metavariáveis,* ou *variáveis sintácticas*. A linguagem em que está escrito este texto, isto é, o português corrente é, relativamente à *linguagem objecto* $\mathcal{L}^0$ que acaba de ser criada, uma **metalinguagem**, chamada a *linguagem do observador* (ou *do relator*).

[44] A chamada *notação polaca*, ainda em uso por alguns lógicos (polacos, e não só) dispensa os parênteses. Nesta notação escreve-se $\wedge \phi\psi$, $\vee \phi\psi$, $\rightarrow \phi\psi$ em vez de $(\phi \wedge \psi)$, $(\phi \vee \psi)$, $(\phi \rightarrow \psi)$, respectivamente.

No nosso caso, E é o conjunto de todas as expressões de $\mathcal{L}^0$ (incluindo a expressão vazia), P é o conjunto das letras proposicionais e F o conjunto das operações lógicas em E determinadas pelos conectivos $\wedge$, $\vee$, $\neg$, $\rightarrow$. O conjunto F^* vem a ser, finalmente, o **conjunto das fórmulas** de $\mathcal{L}^0$, que também pode ser designado por uma das notações seguintes:

$$\text{Form}(\mathcal{L}^0), \text{ ou } \text{Prop}(P).$$

Em geral, é mais fácil mostrar que uma expressão *é* uma fórmula (se ela o é) do que mostrar que *não é* (se ela não é). No primeiro caso basta constatar que ela foi construída a partir de letras proposicionais (as letras proposicionais que nela ocorrem) de acordo com as regras F_1 a F_3. No segundo caso, o argumento tem de ser de outra natureza.

3.1 Exemplo Mostramos que a expressão $\rightarrow(\neg pp$ não é fórmula. Suponhamos, com vista a um absurdo, que esta expressão é fórmula, e seja F' o conjunto que se obtém de F^* suprimindo aquela suposta fórmula. Facilmente se vê que F' é indutivo. Por exemplo, se ϕ está em F', então $\neg\phi$ também está em F', pois o primeiro símbolo desta expressão é '$\neg$', enquanto o primeiro símbolo de $\rightarrow(\neg pp$ é '$\rightarrow$'. Como F^* é o mais pequeno conjunto indutivo, tem-se $F^* \subseteq F'$, logo $\rightarrow(\neg pp$ pertence a F', o que é absurdo. Uma outra maneira de caracterizar o conjunto das fórmulas de $\mathcal{L}^0$ será dada no primeiro exercício deste capítulo, mas convém ler primeiro o que segue sobre indução nas fórmulas.

Uma fórmula é um objecto concreto espácio-temporal: é uma sequência finita de símbolos. Como tal, tem um **comprimento**, que é o número total de símbolos que ocorrem na fórmula. E como esse número é um inteiro positivo, é possível e conveniente, por vezes, demonstrar certos factos acerca das fórmulas por indução no seu comprimento. Porém, atendendo a que a definição de fórmula é uma definição indutiva, é também possível uma indução de outro tipo, chamada **indução na complexidade das fórmulas**.

Seja Φ uma propriedades que as fórmulas podem ter ou não, e escrevamos $\Phi[\phi]$ para exprimir que a fórmula ϕ tem a propriedade Φ. Para provar, por indução na complexidade das fórmulas, que todas as fórmulas possuem certa propriedade Φ, isto é, que para todo $\phi \in \text{Form}(\mathcal{L}^0)$ se tem $\Phi[\phi]$, basta provar que:

I_1. As letras proposicionais possuem a propriedade Φ; em símbolos: $\Phi[p]$, para toda a letra proposicional p;

I_2. Sempre que ϕ possui a propriedade Φ, então $\neg\phi$ também possui a propriedade Φ; em símbolos: sempre que se tem $\Phi[\phi]$, então tem-se $\Phi[\neg\phi]$;

I_3. Sempre que ϕ e ψ possuem a propriedade Φ, então $(\phi \wedge \psi)$, $(\phi \vee \psi)$ e $(\phi \rightarrow \psi)$ também possuem a propriedade Φ; em símbolos: sempre que se tem $\Phi[\phi]$ e $\Phi[\psi]$, então tem-se $\Phi[(\phi \wedge \psi)]$, etc.

Com efeito, supondo demonstradas estas três cláusulas, e considerando o conjunto D constituído por todas as fórmulas com a propriedade Φ, facilmente se verifica que D é indutivo (exercício); mas D está contido em $F^* = \mathrm{Form}(\mathcal{L}^0)$ e este é o mais pequeno conjunto indutivo, logo necessariamente $D = \mathrm{Form}(\mathcal{L}^0)$, e portanto *todas* as fórmulas de $\mathcal{L}^0$ têm a propriedade Φ, como se queria demonstrar. Podemos enunciar assim, em termos gerais, o

3.2 Princípio de indução nas fórmulas

Se D é um conjunto indutivo de fórmulas de $\mathcal{L}^0$, então $D = \mathrm{Form}(\mathcal{L}^0)$.

Vejamos uma aplicação deste princípio. Uma expressão ϕ diz-se **equilibrada** sse tiver o mesmo número de parênteses esquerdos '(' que de parênteses direitos ')' (em notação óbvia: $e[\phi] = d[\phi]$). No resultado seguinte as fórmulas supõem--se escritas na notação *oficial* (isto é, construídas de acordo com as regras de formação, antes de se aplicarem as convenções relativas à supressão de parênteses).

3.3 Lema do equilíbrio

Toda a fórmula de $\mathcal{L}^0$ é equilibrada.

Dem. Exercício [*Sugestão:* mostre que o conjunto das fórmulas equilibradas é indutivo.].■

Da definição indutiva de fórmula resultam algumas outras propriedades das fórmulas, que não demonstramos (ver, todavia, os primeiros exercícios no final deste capítulo) mas que, em todo o caso, são intuitivamente evidentes. Mencionemos duas dessas propriedades.

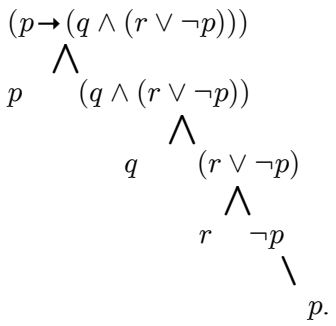
3.4 Propriedade da unicidade de representação

Toda a fórmula escreve-se de uma e uma só maneira como sucessão finita (justaposição, arranjo, ou concatenação) de símbolos do alfabeto.

Isto quer dizer, por exemplo, que se uma fórmula ϕ é uma conjunção, então existem e são bem determinadas fórmulas ψ, θ tais que ϕ é a fórmula $(\psi \wedge \theta)$. Analogamente para disjunções, etc. Se uma fórmula é uma negação, uma conjunção, uma disjunção ou uma condicional (ou bicondicional), então o seu **conectivo principal** é $\neg$, $\wedge$, $\vee$, $\rightarrow$ ($\leftrightarrow$), respectivamente.

***3.5 Árvores de formação** A formação de fórmulas de $\mathcal{L}^0$ pode ser representada por árvores finitas. Dada uma fórmula ϕ, que ocupa a raiz, ela terá um (ψ) ou dois (ψ, θ) sucessores imediatos, conforme se trate de uma negação ($\neg\psi$) ou uma conjunção, disjunção ou condicional ($\psi \wedge \theta$, $\psi \vee \theta$, $\psi \rightarrow \theta$), e analogamente para estas componentes, e assim sucessivamente até que, nos nós terminais, só figuram as letras proposicionais que ocorrem em ϕ. Exemplifiquemos com a

fórmula $(p \rightarrow (q \wedge (r \vee \neg p)))$:



Antes de enunciar outra propriedade, mencionemos o facto, intuitivamente evidente, de que, dada uma fórmula qualquer ϕ, construída a partir de certas letras proposicionais, digamos p_1, ..., p_k, por meio de alguns conectivos, e atribuídos certos valores lógicos às letras p_i, é possível determinar o valor lógico resultante para ϕ, bastando para isso consultar as tabelas dos conectivos (p. 20). Mais geralmente, é possível construir uma tabela de verdade para ϕ, com linhas de entrada para todos os arranjos possíveis (com repetições) dos valores lógicos 1, 0 atribuídos às letras proposicionais p_i que ocorrem em ϕ.

Note-se que, se em ϕ ocorrem k letras proposicionais, então há ao todo 2^k tais arranjos. Porém, a lista de letras proposicionais que podem ocorrer em fórmulas é infinita, daí a necessidade de uma noção mais geral do que a de arranjo, que atribua de uma vez só valores lógicos a *todas* as letras proposicionais de $\mathcal{L}^0$.

3.6 Definição Chamamos **valoração** (ou **valuação**) a toda a aplicação v do conjunto das letras proposicionais no conjunto dos valores lógicos, isto é,

$$v : P \rightarrow \{0, 1\}.$$

Se $v(p) = 1$ $(= 0)$, dizemos que p é **verdadeira** (**falsa**) para v, ou que v **satisfaz** ou **realiza** ou é um **modelo** de (**não satisfaz** ou **não realiza**, respectivamente) p.[45]

Dadas uma valoração v e uma fórmula qualquer ϕ, dizer que é possível determinar o valor lógico resultante para ϕ, calculado de acordo com as tabelas dos conectivos é, pois, dizer que a valuação v se pode *estender* (ou *prolongar*) *ao conjunto de todas as fórmulas, conformemente às tabelas dos conectivos* (p. 20), isto é, que existe uma aplicação

---

[45] Em algumas situações parece conveniente considerar valorações *parcias,* que são funções definidas em partes (usualmente finitas) de P com valores em $\{0, 1\}$. Por outro lado, alguns autores preferem os subconjuntos de P às valorações: a ideia é que cada valoração v não é mais do que a chamada *função característica* de um (único) conjunto $S \subseteq P$, nomeadamente, o subconjunto S formado por todos os $p \in P$ tais que $v(p) = 1$.

$$\widehat{v} : \text{Prop}(P) \to \{0, 1\}$$

que estende v [isto é, $\widehat{v}(p) = v(p)$ para todo p em P] e que satisfaz as condições seguintes, para quaisquer fórmulas ψ, θ:

$$\begin{array}{rll} \widehat{v}(\neg\psi) = 1 & \text{sse} & \widehat{v}(\psi) = 0, \\ \widehat{v}(\psi \wedge \theta) = 1 & \text{sse} & \widehat{v}(\psi) = 1 = \widehat{v}(\theta), \\ \widehat{v}(\psi \vee \theta) = 1 & \text{sse} & \widehat{v}(\psi) = 1 \text{ ou } \widehat{v}(\theta) = 1, \\ \widehat{v}(\psi \to \theta) = 1 & \text{sse} & \widehat{v}(\psi) = 0 \text{ ou } \widehat{v}(\theta) = 1. \end{array}$$

Uma aplicação $\widehat{v} : \text{Prop}(P) \to \{0, 1\}$ com estas propriedades diz-se uma **valuação** (ou **valoração**) **booleana**. Dizemos que $\widehat{v}$ **satisfaz** ou **realiza** ou é um **model**o de ϕ, ou ainda que ϕ é **verdadeira** para $\widehat{v}$ sse $\widehat{v}(\phi) = 1$, etc.

Podemos então enunciar a última das propriedades das fórmulas que nos interessa assinalar (ver sugestão para demonstração no exercício 2.4).

3.7 Propriedade de extensão das valorações

Toda a valoração v estende-se de uma e uma só maneira a uma valoração booleana $\widehat{v}$.■

II.4 Um sistema dedutivo: dedução natural

Iremos agora estabelecer um sistema (ou cálculo) dedutivo para a nossa linguagem $\mathcal{L}^0$, que será designado por

DNP (Dedução Natural Proposicional),

ou simplesmente **DN**, neste capítulo.

Tal sistema compreende duas coisas:

(i) uma lista finita de **regras de inferência**, que, como já foi dito, correspondem a certas formas muito simples e frequentes de argumentação válida;

(ii) um conceito de **derivabilidade** ou **dedutibilidade**, correspondente à noção intuitiva de demonstrabilidade em matemática, que se designa por $\vdash_{\mathbf{DN}}$, ou simplesmente $\vdash$,[46] se não houver possibilidade de confusão, e que é uma relação entre conjuntos de fórmulas e fórmulas (tal como a relação $\models$, com a qual, porém, não se deve confundir).

---

[46] O sinal ' $\vdash$ ' não pertence à linguagem $\mathcal{L}^0$, obviamente. Foi introduzido por Gottlob Frege (1848-1925), justamente considerado o maior lógico do seu tempo, num trabalho de 1879 intitulado *Begriffsschrift, eine der arithmetischen nachgebildete Formelsprache des reinen Denkens* (Uma Linguagem Simbólica, Modelada na Linguagem da Aritmética, para o Pensamento Puro), precisamente o trabalho onde se apresenta pela primeira vez a noção de linguagem formal e se desenvolvem, de maneira sistemática, o cálculo proposicional e o cálculo de predicados de feição moderna. V. HEIJENOORT, HATCHER.

Escrevemos

$$\phi_1, ..., \phi_n \vdash \psi$$

(ler: «de ϕ_1, ..., ϕ_n deduz-se (ou deriva-se) ψ» ou «ψ deduz-se de ϕ_1, ..., ϕ_n») para exprimir que ψ é **dedutível** ou **derivável** de ϕ_1, ..., ϕ_n (no sistema **DN**), e isto significa que existe uma sequência ou sucessão finita de fórmulas

$$\phi_1, ..., \phi_n, \phi_{n+1}, ..., \psi$$

tal que cada fórmula da sequência, incluindo ψ, é uma das n primeiras ϕ_1, ..., ϕ_n, ou é uma hipótese descarregada (ver adiante) ou é inferida (isto é, é a conclusão) de uma ou mais fórmulas precedentes (premissas) por uma das regras de inferência admitidas. Admitimos, pois, a possibilidade de ψ ser ela própria uma das fórmulas ϕ_i com $i \leq n$ já que isso em nada afecta o poder dedutivo do sistema.[47]

Se $\phi_1, ..., \phi_n \vdash \psi$, as primeiras n fórmulas (ϕ_1, ..., ϕ_n) de uma dedução ϕ_1, ..., ϕ_n, ϕ_{n+1}, ..., ψ são as **hipóteses** (**iniciais**), e a última fórmula ψ é a **tese** (**final**); as fórmulas ϕ_{n+1}, ... que precedem ψ são as fórmulas (hipóteses descarregadas ou teses) **intermédias**; uma tal sequência é chamada uma **derivação** (**formal**) ou uma **dedução** (**formal**) da tese ψ com hipóteses ϕ_1, ..., ϕ_n (sempre subentendido: no sistema **DN**).[48] Após a indicação de algumas regras e derivações daremos uma definição indutiva de derivação.

Vamos então indicar as regras do sistema **DN**. Para cada conectivo daremos duas ou três regras, umas de *introdução* e outras de *eliminação*. Em geral, as primeiras dizem-nos de que premissas podemos tirar uma conclusão em que ocorre o conectivo; as segundas dizem-nos que conclusões podemos tirar de premissas em que ocorre o conectivo em questão. Dizemos «em geral» porque, como veremos, há algumas excepções a este simplismo, nomeadamente, pelo facto de algumas regras fundamentais do sistema não terem a forma simples «premissas/conclusão».

II.5 Regras para a conjunção

As regras de inferência para a conjunção são as seguintes:

---

[47] Em rigor isto só é verdade desde que o sistema de regras seja suficientemente rico, isto é, tenha regras suficientes para de ψ poder deduzir ψ, o que, em todo o caso, acontecerá com todos os sistemas a utilizar neste livro. Em todo o caso, a regra H a introduzir adiante dá conta desta possibilidade.

[48] Admitiremos adiante a possibilidade de se ter $n = 0$, isto é, de deduções sem hipóteses, sendo nesse caso as teses apelidadas de **leis lógicas** (**proposicionais**). Por outro lado, a definição agora dada serve para os primeiros exemplos de regras e deduções, mas há-de ser reformulada de modo a admitir um conceito mais geral de regra de inferência a introduzir proximamente.

Eliminação da conjunção		Introdução da conjunção
$(\wedge\bar{}_1)$ $\dfrac{\phi \wedge \psi}{\phi}$,	$(\wedge\bar{}_2)$ $\dfrac{\phi \wedge \psi}{\psi}$;	$(\wedge^+)$ $\dfrac{\phi, \psi}{\phi \wedge \psi}$ [49]

Em cada aplicação de uma destas regras, no seio de uma derivação, dizemos que a conclusão **depende** das hipóteses de que dependem as premissas. Uma hipótese só depende de si mesma.

A regra $(\wedge\bar{}_1)$ diz-nos que de uma conjunção se pode inferir a primeira componente. Analogamente para a regra $(\wedge\bar{}_2)$. A regra $(\wedge^+)$ diz-nos que de duas premissas (não necessariamente distintas) se pode inferir a sua conjunção. Na maioria das vezes designaremos a regra de eliminação da conjunção simplesmente por $(\wedge^-)$, deixando para o contexto a identificação do caso, se o primeiro $(\wedge\bar{}_1)$, se o segundo $(\wedge\bar{}_2)$.

Mostramos de imediato que

(1) $\phi \vdash \phi$

(2) $\phi \wedge \psi \vdash \phi$ (2′) $\phi \wedge \psi \vdash \psi$

(3) $\phi, \psi \vdash \phi \wedge \psi$ (3′) $\phi, \psi \vdash \psi \wedge \phi$

Quanto a (1), a sequência

$$\phi$$

é uma dedução de ϕ com hipótese ϕ. Para (2), a sequência

$$\phi \wedge \psi, \phi$$

é uma derivação da tese ϕ com hipótese $\phi \wedge \psi$. Para (2′) é análogo. Quanto a (3), a sequência

$$\phi, \psi, \phi \wedge \psi$$

é uma derivação da tese $\phi \wedge \psi$ com hipóteses ϕ, ψ. Por outro lado, a sequência $\phi \wedge \phi$, ϕ é uma dedução de ϕ aplicando $(\wedge^-)$, e a sequência ϕ, $\phi \wedge \phi$ é uma dedução de $\phi \wedge \phi$ com hipótese ϕ, o que mostra que

(4) $\phi \wedge \phi \vdash \phi$; (4′) $\phi \vdash \phi \wedge \phi$

Para facilitar a verificação de que uma dada sucessão de fórmulas é, de facto, uma derivação de certa tese com certas hipóteses adoptaremos daqui em diante uma *disposição na vertical* das deduções, numerando consecutivamente as fórmulas, numa coluna à esquerda, e indicando, para cada linha, numa coluna à

[49] Como já acontecia no Cap. I com a noção de argumento, a ordem de colocação das premissas é irrelevante.

direita, a justificação respectiva, isto é, qual a regra que foi aplicada e qual ou quais os números de ordem das premissas de que a fórmula nessa linha foi inferida.

Para as hipóteses, indicaremos apenas na coluna à direita 'Hip', ou simplesmente 'H'. Na realidade, podemos também encarar (Hip) como uma regra sem premissas, a **regra de introdução de hipótese**. Assim, por exemplo, a dedução de (2) acima poderá ser apresentada esquematicamente por:

1	ϕ	H
2	ψ	H
3	$\phi \wedge \psi$	1, 2 ($\wedge^+$).

A fórmula da linha 3 foi inferida das fórmulas das linhas 1 e 2 por meio da regra ($\wedge^+$). Como estas são hipóteses, aquela depende destas na dedução.

II.6 Regras para a negação e o condicional

A nossa primeira regra para lidar com a negação é a seguinte:

Eliminação da dupla negação	
$(\neg\neg^-)$	$\dfrac{\neg\neg\phi}{\phi}$

É, como o nome indica, uma regra de *eliminação da dupla negação*, e não da negação simples, embora certos autores a designem como regra de eliminação da negação. A conclusão depende das hipóteses de que depende a premissa.

A introdução da negação podia ser formulada desde já como sendo a regra

$$(\neg^*) \qquad \frac{\phi \rightarrow (\psi \wedge \neg\psi)}{\neg\phi}$$

e, como tal, corresponde a uma versão do método de demonstração em matemática conhecido como **método de redução ao absurdo**: se ϕ «implica»[50] uma **contradição** (isto é, uma fórmula da forma $\psi \wedge \neg\psi$), então ϕ é falsa, logo $\neg\phi$ é verdadeira. Mas a formulação $(\neg^*)$ tem a desvantagem de envolver o condicional $\rightarrow$, para o qual ainda não demos qualquer regra, sendo, por isso, conveniente dar primeiro as regras para este conectivo, uma das quais permitirá simplificar um pouco a formulação da regra de introdução da negação. $(\neg^*)$ não será, por isso,

[50] Estamos aqui a afirmar, como é habitual fazer-se em matemática, que uma proposição ϕ implica uma outra ψ quando se quer apenas afirmar que a proposição condicional $\phi \rightarrow \psi$ é verdadeira. De facto, muitos autores afirmam «ϕ implica ψ» precisamente quando e só quando a proposição «$\phi \rightarrow \psi$» é verdadeira. Assim, não se deve ler «$\phi \rightarrow \psi$» como «ϕ implica ψ» excepto nos casos em que esta proposição é verdadeira.

adoptada como regra fundamental do sistema.

Eliminação do condicional	
$(\rightarrow^{-})$, ou (MP)	$\dfrac{\phi,\ \phi \rightarrow \psi}{\psi}$

Esta regra é de aplicação muito frequente em demonstrações matemáticas, embora passe despercebida, e é conhecida classicamente como *modus (ponendo) ponens:* se ϕ implica ψ e ϕ é verdadeira, então ψ é verdadeira. Numa aplicação desta regra, a conclusão depende das hipóteses de que dependem as premissas.

Vejamos uns exemplos de aplicação. Somente efectuamos algumas das deduções; as deduções que não exibirmos ficam como outros tantos exercícios.

(5) $\neg\neg\phi \vdash \phi$.

(6) $\phi, \phi \rightarrow \psi \vdash \psi$.

(7) $\phi, \phi \rightarrow \psi, \psi \rightarrow \theta$.

Dedução:

1	ϕ	H
2	$\phi \rightarrow \psi$	H
3	$\psi \rightarrow \theta$	H
4	ψ	1, 2 (MP)
5	θ	3, 4 (MP).

Como se vê, a fórmula da linha 4 depende das hipóteses das linhas 1 e 2, enquanto a fórmula da linha 5 depende das hipóteses de que dependem as linhas 3 e 4, ou seja, das hipóteses 1, 2 e 3.

(8) $\phi,\ \phi \rightarrow (\psi \rightarrow \theta),\ \phi \rightarrow \psi \vdash \theta$.

Dedução:

1	ϕ	H
2	$\phi \rightarrow (\psi \rightarrow \theta)$	H
3	$\phi \rightarrow \psi$	H
4	$\psi \rightarrow \theta$	1, 2 (MP)
5	ψ	1, 3 (MP)
6	θ	4, 5 (MP).

A regra de introdução do condicional $(\rightarrow^{+})$ que se formula a seguir é uma das mais importantes do nosso sistema, mas é de natureza um pouco diferente das anteriores, pois a sua premissa é, ela própria, uma derivação. Dissemos anteriormente que as nossas regras iriam corresponder a certas formas de argumentação válida frequentes. Acrescentaremos agora que algumas regras correspondem mais propriamente a certos *métodos de demonstração* em matemática. A regra $(\rightarrow^{+})$ é uma dessas, e as regras $(\neg^{+})$, $(\vee^{-})$ a indicar mais adiante serão outras.

No caso de $(\rightarrow^{+})$, o método em causa é o conhecido *método directo* para demonstrar uma proposição condicional, isto é, da forma $\phi \rightarrow \psi$. O que se faz, de acordo com este método, é admitir (temporariamente) o antecedente ϕ como nova hipótese e demonstrar o consequente ψ. Formalmente, no nosso cálculo dedutivo isto quer dizer construir uma dedução de ψ com hipótese adicional ϕ, digamos

$$\begin{array}{|ll} \phi & \mathrm{H} \\ \vdots & \\ \psi & \end{array}$$

A regra $(\rightarrow^{+})$ diz-nos que de uma tal dedução, como premissa, se pode inferir a conclusão $\phi \rightarrow \psi$, a qual, porém, *já não depende de* ϕ como hipótese, mas apenas das outras hipóteses iniciais (se algumas houver) de que ψ depende naquela dedução.

Introdução do condicional

$$\begin{array}{|ll} \phi & [\mathrm{H}] \\ \vdots & \\ \psi & \\ \hline \phi \rightarrow \psi & \end{array} \quad (\rightarrow^{+})$$

Colocámos 'H' entre parênteses rectos '[ ]' para chamar a atenção para o facto de ϕ ser somente hipótese relativamente a ψ, mas já não relativamente à conclusão final $\phi \rightarrow \psi$, pois esta não depende de ϕ como hipótese, mas apenas das hipóteses de que ψ depende, excluindo ϕ. Dizemos, por isso, que, quando se aplica a regra $(\rightarrow^{+})$, a hipótese temporária ϕ foi *descarregada, descartada* ou *eliminada.* Em vez de escrever '[H]' à direita de ϕ também se pode escrever 'Ø' para assinalar a eliminação da dependência[51] no momento de aplicação da regra. Cada linha de uma dedução fica a depender apenas das hipóteses não descarregadas utilizadas anteriormente para aceder a essa linha. As deduções continuam a ser sequências finitas de fórmulas, como anteriormente, mas o conceito de premissa deve ser alargado de modo a contemplar regras como $(\rightarrow^{+})$. Em vez do termo 'premissa' seria mais conveniente, por exemplo, o termo 'item' na definição de dedução, englobando os itens *singulares* ou premissas, no sentido prévio, e itens *compostos* ou derivações-premissa, no sentido alargado.[52]

---

[51] De notar que se uma hipótese (ϕ) descarregada por uma aplicação da regra $(\rightarrow^{+})$ [ou de uma das regras $(\neg^{+})$, $(\vee^{-})$ a introduzir mais adiante] voltar a ser utilizada numa linha posterior àquela em que foi descarregada ($\phi \rightarrow \psi$), tal linha posterior continua a depender daquela hipótese (ϕ).

[52] Podíamos admitir desde já o *caso degenerado* da regra $(\rightarrow^{+})$, $(\rightarrow^{+}_{\mathrm{o}})$ $\dfrac{\psi}{\phi \rightarrow \psi}$, tanto mais que esta regra se poderá justificar facilmente mediante (39), mas não o faremos.

A regra ($\rightarrow^+$) também é conhecida como *regra da dedução condicional*, *regra do método directo*, ou *regra da hipótese auxiliar*. Veremos adiante uma outra maneira de encarar esta regra, como *regra de eliminação de hipótese*. Alguns exemplos ajudarão a compreender melhor esta regra.

(9) $\phi \rightarrow \psi,\ \psi \rightarrow \theta \vdash \phi \rightarrow \theta$ (*silogismo hipotético*).

Dedução:

$\{1\}$	1	$\phi \rightarrow \psi$	H
$\{2\}$	2	$\psi \rightarrow \theta$	H
$\{3\}$	3	ϕ	[H]
$\{1, 3\}$	4	ψ	1, 3 (MP)
$\{1, 2, 3\}$	5	θ	2, 4 (MP)
$\{1, 2\}$	6	$\phi \rightarrow \theta$	3-5 ($\rightarrow^+$).

A justificação da linha 6 (coluna à direita) consiste na indicação da subderivação entre as linhas 3 e 5, com hipótese auxiliar ϕ e conclusão θ, e da regra ($\rightarrow^+$) que permite concluir a fórmula condicional. Para tornar visível a dependência, indicámos na coluna mais à esquerda (o número de ordem de) as hipóteses de que cada fórmula depende nesta dedução. Assim, por exemplo, a fórmula da linha 5 depende das hipóteses iniciais e da hipótese auxiliar, mas a tese na linha 6 já só depende das hipóteses iniciais uma vez que, por aplicação da regra ($\rightarrow^+$), a dependência da linha 3 foi eliminada.

Esta exibição das dependências pode ser feita relativamente a qualquer dedução, e permite um certo controlo sobre a aplicação das regras, mas, em geral, não sobrecarregamos a notação das deduções com a indicação das dependências. Aconselhamos o leitor a preencher as dependências de hipóteses para auto-controlo do processo dedutivo.

(9′) $\phi \rightarrow \psi \vdash (\psi \rightarrow \theta) \rightarrow (\phi \rightarrow \theta)$.

Dedução:

1	$\phi \rightarrow \psi$	H
2	$\psi \rightarrow \theta$	[H]
3	ϕ	[H]
4	ψ	1, 3 (MP)
5	θ	2, 4 (MP)
6	$\phi \rightarrow \theta$	3-5 ($\rightarrow^+$)
7	$(\psi \rightarrow \theta) \rightarrow (\phi \rightarrow \theta)$	2-6 ($\rightarrow^+$).

Se compararmos as deduções de (9) e de (9′), veremos que esta última só tem a mais a linha 7 e o facto de a hipótese 2 ser encarada como hipótese auxiliar, vindo a ser eliminada na linha 7, por aplicação de ($\rightarrow^+$). Tudo se passa, pois, como se ($\rightarrow^+$) funcionasse como regra de eliminação de hipótese, como acima se disse: qualquer hipótese pode ser eliminada, enquanto tal, por uma aplicação de ($\rightarrow^+$), passando a antecedente de uma implicação. E o que se pode fazer uma vez pode fazer-se duas ou três... Repetindo o feito à dedução de (9′), obtemos uma dedução de

$(9'')$ $(\phi \to \psi) \to (\psi \to \theta) \to (\phi \to \theta)$,

com a particularidade de nela estarem eliminadas todas as hipóteses. É o que se chama uma **dedução sem hipóteses**. Uma fórmula ϕ que possua uma dedução sem hipóteses é o que se chama uma **lei**, **teorema lógico** ou **princípio lógico** (proposicional), e escreve-se $\vdash \phi$ para exprimir esse facto.

Dos exemplos anteriores obtêm-se, sem dificuldade, aplicando $(\to^+)$ tantas vezes quantas as necessárias, as seguintes leis:

(10) $\phi \wedge \psi \to \phi$, $(10')$ $\phi \wedge \psi \to \psi$,

(11) $\phi \to \psi \to \phi \wedge \psi$, $(11')$ $\phi \to \psi \to \psi \wedge \phi$,

(12) $\neg\neg\phi \to \phi$, (13) $\phi \to (\phi \to \psi) \to \psi$.

Regressando à regra de introdução da negação $(\neg^+)$, podemos reformulá-la como uma regra estruturalmente semelhante a $(\to^+)$, em que a premissa é, ela própria, uma derivação de uma contradição (digamos $\psi \wedge \neg\psi$) a partir de uma hipótese auxiliar (ϕ) e a conclusão é uma negação ($\neg\phi$). Pode ser encarada, como já se disse, como uma versão ou variante (fraca) da regra de redução ao absurdo. Em todo o caso, a conclusão final ($\neg\phi$) só depende das hipóteses de que depende a conclusão da derivação-premissa ($\psi \wedge \neg\psi$), excluindo a hipótese temporária (ϕ). Trata-se da regra seguinte:

Introdução da negação

$$\begin{array}{lll} & \begin{array}{|l} \phi \\ \vdots \\ \psi \wedge \neg\psi \end{array} & [\mathrm{H}] \\ \hline (\neg^+) \text{ ou } (\mathrm{RA}^*) & \neg\phi & . \end{array}$$

Note-se que nada impede que ϕ seja, por sua vez, uma negação (digamos $\neg\theta$); a conclusão da regra continua a ser a negação de ϕ [no caso, $\neg\neg\theta$; para obter θ há que aplicar $(\neg\neg^-)$ — ver (RA) adiante]. Exactamente qual a contradição $(\psi \wedge \neg\psi)$ que a hipótese provisória (ϕ) permite obter não é possível saber-se de antemão: é coisa a descobrir caso a caso, conforme a fórmula ϕ cuja negação se pretende derivar.

Como primeira aplicação desta regra derivamos a clássica *modus (tolendo) tollens:*

$$(\mathrm{MT}) \qquad \frac{\phi \to \psi,\ \neg\psi}{\neg\phi}$$

Derivar esta regra é mostrar que das suas premissas é possível deduzir a sua conclusão usando as regras do sistema **DN**. Estas são ditas *primitivas*, e regras como (MT) que se possam derivar a partir das primitivas dizem-se *derivadas*. No exercício 2.8 estão duas outras versões desta regra, (MT'_i), $i = 1, 2$.

(14) $\phi \rightarrow \psi, \neg\psi \vdash \neg\phi,$ (15) $\phi \vdash \neg(\neg\phi \wedge \neg\psi),$

(16) $\phi \rightarrow \psi \vdash \neg\psi \rightarrow \neg\phi,$ (17) $\phi \vdash \neg\neg\phi,$

Dedução de (14):

1	$\phi \rightarrow \psi$	H
2	$\neg\psi$	H
3	ϕ	[H]
4	ψ	1, 3 (MP)
5	$\psi \wedge \neg\psi$	2, 4 ($\wedge^+$)
6	$\neg\phi$	3-5 (RA*).

Por razões a desenvolver no último capítulo, pode ser discutida a adequação da designação da regra ($\neg^+$) como «regra de redução ao absurdo». Não há dúvida de que na matemática clássica, que é o contexto privilegiado da lógica clássica, um grande número, senão a maioria das demonstrações pelo método de redução ao absurdo procedem de acordo com aquela regra pois, tipicamente, a proposição a demonstrar por tal método é negativa. Todavia, é sabido que na matemática intuicionista/construtivista, em que se utiliza a lógica intuicionista (ver último capítulo), *não se faz uso do método de redução ao absurdo* no estabelecimento de proposições não negativas (isto é, que não são negações). Ora, nesta lógica, a regra ($\neg^+$) é redundante, pois é um caso particular da regra ($\rightarrow^+$), atendendo à maneira *sui generis* como os intuicionistas definem habitualmente a negação [$\neg\phi = \phi \rightarrow \perp$, onde $\perp$ denota o *absurdo* (uma contradição indeterminada ou proposição sempre falsa)]. Não fica bem, portanto, ter uma regra (mesmo que derivada) com uma designação que choca claramente com a filosofia e *praxis* intuicionistas. Acontece que todas as regras do sistema **DN**, com excepção de ($\neg\neg^-$), são intuicionisticamente válidas, de modo que o ónus do classicismo está, portanto, nesta regra.[53]

Outra aplicação importante de ($\neg^+$), com o auxílio de ($\neg\neg^-$) como acima se explicou (pág. 60), é a regra derivada seguinte, a que chamaremos com propriedade regra de **redução ao absurdo** e designaremos (RA), a qual *não é,* em geral, adimita pelos intuicionistas:

---

[53] Como este livro é primordialmente de lógica clássica, a designação referida não é gravosa, mas reconheço a pertinência da objecção que me foi levantada pelo meu colega Prof. Fernando Ferreira a este respeito, a quem devo e agradeço a sugestão da inclusão da presente nota. Em consequência, reserva-se a designação (RA) para a regra derivada a introduzir adiante, clássica mas não intuicionisticamente válida, já que utiliza ($\neg\neg^-$) na sua derivação.

Redução ao absurdo		
	$\neg\phi$	[H]
	$\vdots$	
	$\psi \wedge \neg\psi$	
(RA)	ϕ	.

Veremos adiante algumas aplicações desta regra.

II.7 Introdução de teses

A regra (MT) pode ser utilizada em deduções, tal como se fosse uma regra primitiva sem que, por isso, fique alterada a força dedutiva do sistema. Quer dizer, não se obtêm teses nem leis que não possam já ser obtidas sem utilizar (MT), pela simples razão de (MT) ser derivável. Por outras palavras, em qualquer aplicação de (MT) no seio de uma dedução podemos substituir essa aplicação (aumentando o número de linhas) pela derivação (utilizando as regras primitivas) da conclusão da regra ($\neg\phi$) a partir das suas premissas ($\phi \rightarrow \psi$, $\neg\psi$).

Analogamente para a regra derivada correspondente a (17), *introdução da dupla negação*

$$(\neg\neg^{+}) \qquad \frac{\phi}{\neg\neg\phi}.$$

Utilizando as regras derivadas (MT) e ($\neg\neg^{+}$) derive-se, a título de exercício,

(18) $\neg\psi \rightarrow \neg\phi \vdash \phi \rightarrow \psi$.

Como continuação do exercício, derive-se novamente (18), utilizando somente regras primitivas.

O mesmo que se disse para (MT) e ($\neg\neg^{+}$) pode ser dito de outras regras derivadas. Na verdade, sempre que estabelecemos uma relação de derivabilidade da forma $\phi_1, ..., \phi_n \vdash \psi$ podemos formular uma regra derivada correspondente

$$\frac{\phi_1, ..., \phi_n}{\psi}$$

mas a maioria das regras assim obtidas não é suficientemente interessante para merecer uma designação especial e faria aumentar excessivamente o número de regras do sistema. Ao invés, formulamos um princípio geral, aplicável em qualquer dedução, cuja justificação pode ser dada exactamente nos mesmos termos em que acima se justificaram as regras derivadas como (MT).

7.1 Princípio de introdução de teses (T^+)

Em qualquer linha de uma dedução pode-se introduzir uma lei ou tese anteriormente deduzida, desde que as hipóteses de que essa tese depende (numa sua dedução) ocorram em linhas precedentes (não necessariamente como hipóteses) naquela mesma dedução.

Vejamos um exemplo de aplicação, no caso (18) acima:

1	$\neg\psi \rightarrow \neg\phi$	H
2	ϕ	[H]
3	$\neg\neg\phi$	2 (T^+, 17)
4	$\neg\neg\psi$	1, 3 (T^+, 14)
5	ψ	4 ($\neg\neg^-$)
6	$\phi \rightarrow \psi$	2-5 ($\rightarrow^+$).

II.8 Regras para a disjunção

Deixámos para o fim as regras da disjunção, por causa da maior complicação estrutural de uma delas, nomeadamente, da regra de eliminação da disjunção. Comecemos pelas mais simples regras de introdução da disjunção.

Introdução da disjunção	
$(\vee^+_1)$ $\dfrac{\phi}{\phi \vee \psi}$	$(\vee^+_2)$ $\dfrac{\psi}{\phi \vee \psi}$.

Numa dedução em que se aplique uma destas regras a conclusão depende das hipóteses de que dependem as premissas.

Antes de formular a regra de eliminação da disjunção, recordemos o conhecido *método de demonstração por casos* em matemática, em que, partindo de certa hipótese disjuntiva

$\phi \vee \psi$ [por exemplo, n é par ou n não é par (é ímpar)]

se pretende concluir certa tese θ.[54] Procede-se então *por casos*, procurando demonstrar θ no caso ϕ (no caso n par, ... θ) e também no caso ψ (no caso n ímpar, ... também θ).

---

[54] Na maior parte das vezes, a proposição a demonstrar θ é conhecida antes de se aventar uma hipótese disjuntiva que permita uma demonstração por (dois ou mais) casos, usualmente exclusivos e exaustivos. Muito frequentemente, também, uma tal hipótese disjuntiva é da forma $\phi \vee \neg\phi$ (*lei do terceiro excluído,* a deduzir adiante).

No nosso cálculo, isto significa admitir temporariamente ϕ e ψ como hipóteses e em cada um dos casos derivar θ, isto é, construir duas derivações:

(*)

ϕ H	ψ H
$\vdots$	$\vdots$
θ	θ

A regra ($\vee^-$) diz, precisamente, que de uma premissa disjuntiva $\phi \vee \psi$ e de duas derivações com hipóteses auxiliares ϕ e ψ, como em (*), respectivamente, se pode concluir θ. Estas derivações comportam-se, para todos os efeitos, como se fossem premissas ordinárias. Chama-se a atenção para que *a hipótese de uma subderivação* (*) *não deve ser utilizada como hipótese na outra*. Numa dedução em que se aplique esta regra a conclusão final θ não vai depender das hipóteses auxiliares ϕ e ψ, mas somente das hipóteses de que $\phi \vee \psi$ depende e das hipóteses de que θ depende nas subderivações (*) acima, excluindo ϕ e ψ, já que estas são descarregadas no momento de aplicação da regra.

Esquematicamente:

Eliminação da disjunção

		ϕ [H_1]	ψ [H_2]
		$\vdots$	$\vdots$
	$\phi \vee \psi$	θ	θ
($\vee^-$)		θ	

Vejamos dois exemplos onde se aplica esta regra. No segundo exemplo (exercício) a regra ($\vee^-$) utiliza-se duas vezes.

(19) $\phi \vee (\psi \wedge \theta) \vdash (\phi \vee \psi) \wedge (\phi \vee \theta)$

(20) $(\phi \vee \psi) \wedge (\phi \vee \theta) \vdash \phi \vee (\psi \wedge \theta)$

Dedução:

1	$\phi \vee (\psi \wedge \theta)$	H
2	ϕ	[H_1]
3	$\phi \vee \psi$	2 ($\vee^+$)
4	$\phi \vee \theta$	2 ($\vee^+$)
5	$(\phi \vee \psi) \wedge (\phi \vee \theta)$	3, 4 ($\wedge^+$)
6	$\psi \wedge \theta$	[H_2]
7	ψ	6 ($\wedge^-$)
8	$\phi \vee \psi$	7 ($\vee^+$)
9	θ	6 ($\wedge^-$)
10	$\phi \vee \theta$	9 ($\vee^+$)
11	$(\phi \vee \psi) \wedge (\phi \vee \theta)$	8, 10 ($\wedge^+$)
12	$(\phi \vee \psi) \wedge (\phi \vee \theta)$	1, 2-5, 6-11 ($\vee^-$).

II.9 Regras para o bicondicional

Atendendo à definição de $\leftrightarrow$ e às regras da conjunção, facilmente se justificam as seguintes regras derivadas para o bicondicional seguintes:[55]

$$(\leftrightarrow^{+}) \quad \frac{\phi \rightarrow \psi,\ \psi \rightarrow \phi}{\phi \leftrightarrow \psi}; \qquad (\leftrightarrow^{-}) \quad \frac{\phi \leftrightarrow \psi}{\phi \rightarrow \psi}, \quad \frac{\phi \leftrightarrow \psi}{\psi \rightarrow \phi}.$$

(21) $\vdash \phi \vee (\psi \wedge \theta) \leftrightarrow (\phi \vee \psi) \wedge (\phi \vee \theta)$ (*lei distributiva de* $\vee$ *com respeito a* $\wedge$)

(22) $\phi \leftrightarrow \psi,\ \psi \leftrightarrow \theta \vdash \phi \leftrightarrow \theta$

(23) $\vdash (\phi \rightarrow \theta) \rightarrow (\psi \rightarrow \theta) \rightarrow (\phi \vee \psi \rightarrow \theta)$

No que segue, escrevemos $\phi \dashv\vdash \psi$ para significar que $\phi \vdash \psi$ e $\psi \vdash \phi$; neste caso dizemos que ϕ e ψ são **interderiváveis**.

Em virtude das regras para $\rightarrow$ e $\leftrightarrow$ facilmente se justifica que:

(*) $\phi \vdash \psi$ sse $\vdash \phi \rightarrow \psi$ sse $\phi \rightarrow \psi$ é uma lei lógica, e

(**) $\phi \dashv\vdash \psi$ sse $\vdash \phi \leftrightarrow \psi$ sse $\phi \leftrightarrow \psi$ é uma lei lógica.

Iterando (*) um número suficiente de vezes conclui-se que

(***) $\phi_1, ..., \phi_n \vdash \psi$ sse $\vdash \phi_1 \rightarrow \phi_2 \rightarrow \cdots \rightarrow \phi_n \rightarrow \psi$.

II.10 Mais exemplos. Terceiro excluído

O exemplo seguinte está na base de uma importante *lei de conversão* [usando (**) acima]: a lei $(\phi \rightarrow \psi) \leftrightarrow \neg(\phi \wedge \neg\psi)$. Para a dedução utilize-se $(\neg^{+})$.

(24) $\phi \rightarrow \psi \dashv\vdash \neg(\phi \wedge \neg\psi)$

Muito útil no estabelecimento de outras leis de conversão, e não só, é a seguinte regra derivada, a chamada *regra de trivialização* (ou *regra do absurdo*) que, informalmente, nos diz que de um par de fórmulas contrárias (ϕ e $\neg\phi$) toda e qualquer coisa se pode inferir:

$$(\perp) \qquad \frac{\phi,\ \neg\phi}{\psi}.$$

que se justifica mostrando que

(25) $\phi, \neg\phi \vdash \psi$

---

[55] No caso de o bicondicional ser considerado como primitivo, seriam adoptadas estas duas regras como regras primitivas do sistema **DN**.

Dedução:

1	ϕ	H
2	$\neg\phi$	H
3	$\neg\psi$	[H]
4	$\phi \wedge \neg\phi$	1, 2 ($\wedge^+$)
5	$\neg\neg\psi$	3-4 ($\neg^+$)
6	ψ	5 ($\neg\neg^-$).

Uma primeira aplicação desta regra pode ser feita na dedução de

(26) $\phi \wedge \psi \vdash \neg(\neg\phi \vee \neg\psi)$.

Dedução:

1	$\phi \wedge \psi$	H
2	$\neg\phi \vee \neg\psi$	[H]
3	$\neg\phi$	[H_1]
4	ϕ	1 ($\wedge^-$)
5	$\theta \wedge \neg\theta$	3, 4 ($\perp$)
6	$\neg\psi$	[H_2]
7	ψ	1 ($\wedge^-$)
8	$\theta \wedge \neg\theta$	6, 7 ($\perp$)
9	$\theta \wedge \neg\theta$	2, 3-5, 6-8 ($\vee^-$)
10	$\neg(\neg\phi \vee \neg\psi)$	2-9 ($\neg^+$),

onde θ é uma fórmula qualquer (por exemplo, a fórmula p). Note-se a necessidade de obter *a mesma contradição* nas linhas 5 e 8, com vista a uma aplicação da regra ($\vee^-$) na linha 9; daí o artifício a que recorremos com $\theta \wedge \neg\theta$.

Alguns dos exemplos seguintes estão na base de outras tantas leis conhecidas, como as *leis associativas*, *comutativas*, *distributivas*, etc.

(27) $\phi \wedge \psi \dashv\vdash \psi \wedge \phi$

(28) $\phi \vee \psi \dashv\vdash \psi \vee \phi$

(29) $\phi \wedge (\psi \wedge \theta) \dashv\vdash (\phi \wedge \psi) \wedge \theta$

(30) $\phi \vee (\psi \vee \theta) \dashv\vdash (\phi \vee \psi) \vee \theta$

(31) $\phi \wedge (\psi \vee \theta) \dashv\vdash (\phi \wedge \psi) \vee (\phi \wedge \theta)$

(32) $(\phi \wedge \psi) \vee (\phi \wedge \neg\psi) \vdash \phi$

(33) $\phi \dashv\vdash \phi \vee (\psi \wedge \neg\psi)$

(34) $\phi \rightarrow (\psi \rightarrow \theta) \vdash (\phi \rightarrow \psi) \rightarrow (\phi \rightarrow \theta)$

(35) $\phi \rightarrow \psi \vdash (\psi \rightarrow \theta) \rightarrow (\phi \rightarrow \theta)$

(36) $\phi \rightarrow (\psi \rightarrow \theta) \dashv\vdash \phi \wedge \psi \rightarrow \theta$

(37) $\phi \leftrightarrow \psi \dashv\vdash \neg\phi \leftrightarrow \neg\psi$

(38) $\neg\phi \vdash \phi \rightarrow \psi$

(39) $\psi \vdash \phi \rightarrow \psi$

(40) $(\phi \rightarrow \psi) \rightarrow \phi \vdash \phi$

As leis que resultam de (38) e (39) são conhecidas tradicionalmente como *paradoxos da implicação material,* mas não são realmente paradoxos em nenhum sentido técnico. Informalmente, (38) interpreta-se assim: uma proposição falsa implica qualquer proposição; (39) pode-se interpretar: uma proposição verdadeira é implicada por qualquer proposição.

Se há algo de «paradoxal» nos paradoxos da implicação material é apenas o facto de, num caso como no outro, poder não haver qualquer «relação» entre antecedente e consequente na fórmula condicional que é deduzida. Semanticamente já sabíamos ser assim (ver secção I.11).

Uma lei da lógica clássica muito importante que não é uma condicional nem uma bicondicional é a chamada **lei do terceiro excluído**:

(41) $\vdash \phi \vee \neg\phi$

Dedução:			
	1	$\neg(\phi \vee \neg\phi)$	[H]
	2	ϕ	[H]
	3	$\phi \vee \neg\phi$	2 ($\vee^+$)
	4	$(\phi \vee \neg\phi) \wedge \neg(\phi \vee \neg\phi)$	1, 3 ($\wedge^+$)
	5	$\neg\phi$	2-4 (RA*)
	6	$\phi \vee \neg\phi$	5 ($\vee^+$)
	7	$(\phi \vee \neg\phi) \wedge \neg(\phi \vee \neg\phi)$	1, 6 ($\wedge^+$)
	8	$\neg\neg(\phi \vee \neg\phi)$	1-7 (RA*)
	9	$\phi \vee \neg\phi$	8 ($\neg\neg^-$).

A utilização desta lei em deduções, introduzida por meio de (T^+), facilita a derivação de certas outras como, por exemplo, a importante *lei de conversão* $(\phi \rightarrow \psi) \leftrightarrow \neg\phi \vee \psi$, que se obtém a partir das derivações indicadas a seguir:

(42) $\phi \rightarrow \psi \dashv\vdash \neg\phi \vee \psi$

Dedução: $\vdash$:			
	1	$\phi \rightarrow \psi$	H
	2	$\phi \vee \neg\phi$	(T^+)
	3	ϕ	[H]
	4	ψ	1, 3 (MP)
	5	$\neg\phi \vee \psi$	4 ($\vee^+$)
	6	$\neg\phi$	[H]
	7	$\neg\phi \vee \psi$	6 ($\vee^+$)
	8	$\neg\phi \vee \psi$	2, 3-5, 6-7 ($\vee^-$).

$\dashv$: Utilize os paradoxos da implicação material.

(43) $\phi \vdash (\phi \wedge \psi) \vee (\phi \wedge \neg\psi)$

(44) $\neg(\neg\phi \vee \neg\psi) \vdash \phi \wedge \psi$

Daqui sai facilmente a lei $\neg(\neg\phi \vee \neg\psi) \rightarrow \phi \wedge \psi$ e, contrapondo e eliminando a dupla negação, obtemos outra lei:

(45) $\vdash \neg(\phi \wedge \psi) \rightarrow \neg\phi \vee \neg\psi$

Analogamente, de (26) sai facilmente a lei $\phi \wedge \psi \rightarrow \neg(\neg\phi \vee \neg\psi)$, e desta, $\neg\phi \vee \neg\psi \rightarrow \neg(\phi \wedge \psi)$. Combinando os resultados, obtemos uma das *leis de De Morgan,*

(46) $\vdash \neg(\phi \wedge \psi) \leftrightarrow \neg\phi \vee \neg\psi$

A outra lei de De Morgan é igualmente muito útil:

(47) $\vdash \neg(\phi \vee \psi) \leftrightarrow \neg\phi \wedge \neg\psi$

Como *princípio estratégico geral* na construção de deduções, deve-se começar tentando uma abordagem directa; falhando esta (por vezes, é simples falta de persistência!) tente-se a indirecta [($\neg^+$), (RA), etc.]; como último recurso, introduza-se uma lei do terceiro excluído conveniente e prossiga-se por casos. Os paradoxos da implicação material e a regra ($\perp$) são também recursos muito úteis.

Finalizamos esta secção com uma breve apresentação alternativa à «linear vertical» da configuração das deduções, e as definições que foram prometidas acima, nomeadamente as de derivação com hipóteses e hipóteses descarregadas.

De facto, as deduções também podem ser configuradas como árvores binárias, com raiz em baixo e as hipóteses nos topos, podendo uma mesma hipótese figurar em mais de um topo. Vejamos o exemplo (27), da esquerda para a direita, a esta luz:

$$\dfrac{\dfrac{\phi \wedge \psi}{\psi} \qquad \dfrac{\phi \wedge \psi}{\phi}}{\psi \wedge \phi} \ .$$

Acrescentando mais um nível obtemos uma derivação da lei $\phi \wedge \psi \rightarrow \psi \wedge \phi$:

$$\dfrac{\dfrac{\dfrac{[\phi \wedge \psi]}{\psi} \qquad \dfrac{[\phi \wedge \psi]}{\phi}}{\psi \wedge \phi}}{\phi \wedge \psi \rightarrow \psi \wedge \phi} \ .$$

Se quisermos ser mais informativos, colocamos à direita de cada traço inferencial '———' a regra que foi aplicada e, se for o caso, o número, em índice superior, da hipótese (auxiliar) numerada que foi cancelada por aplicação dessa regra:

$$\dfrac{\dfrac{\dfrac{[\phi \wedge \psi]^1}{\psi}\,(\wedge^-) \quad \dfrac{[\phi \wedge \psi]^1}{\phi}\,(\wedge^-)}{\psi \wedge \phi}\,(\wedge^+)}{\phi \wedge \psi \to \psi \wedge \phi}\,(\to^+)^1.$$

Agora, as definições prometidas, após algumas notações. Designamos as derivações (sucessões finitas de fórmulas) em geral por $\mathcal{D}$, $\mathcal{D}'$, $\mathcal{D}''$, $\mathcal{D}_1$, $\mathcal{D}_2$, ..., mas escrevemos

$$\text{(D)} \qquad \begin{matrix}\mathcal{D}\\ \psi\end{matrix}, \qquad \begin{matrix}\phi\\ \mathcal{D}\\ \psi\end{matrix}$$

para indicar que $\mathcal{D}$ é uma derivação com última fórmula ψ (portanto, ψ faz parte de $\mathcal{D}$), e que $\mathcal{D}$ é uma derivação com hipótese ϕ a descarregar de seguida [quando se aplica uma das regras $(\to^+)$, $(\vee^-)$, $(\neg^-)$] e última fórmula ψ (portanto, ϕ e ψ fazem parte de $\mathcal{D}$), respectivamente. As regras de inferência são regras para construir derivações a partir de uma, duas ou três derivações dadas (como premissas), e têm uma das formas

$$\text{(R)} \qquad \frac{\mathcal{D}}{\psi}, \quad \frac{\mathcal{D}_1 \quad \mathcal{D}_2}{\psi}, \quad \frac{\mathcal{D} \quad \mathcal{D}_1 \quad \mathcal{D}_2}{\psi},^{56}$$

onde as premissas $\mathcal{D}$, $\mathcal{D}_1$, $\mathcal{D}_2$ serão sempre apresentadas como em (D), quer dizer, exibindo a última fórmula que faz parte da derivação; ψ é a conclusão da regra respectiva. Do lado esquerdo da regra indicamos o seu nome ou designação (como acima). Algumas regras são sujeitas a restrições especificadas a seguir.

10.1 Definição indutiva das derivações

I Parte: 1. (Regra H) Uma sucessão finita constituída por uma única fórmula ϕ, é uma derivação com hipótese ϕ. Não há hipóteses descarregadas nesta derivação.

2. (Regras de introdução e eliminação dos conectivos $\wedge, \vee, \to$) Se $\mathcal{D}$, $\mathcal{D}_1$, $\mathcal{D}_2$ são derivações, então

$$(\wedge^+) \quad \frac{\begin{matrix}\mathcal{D}_1 & \mathcal{D}_2\\ \phi & \psi\end{matrix}}{\phi \wedge \psi}, \quad (\wedge_1^-) \quad \frac{\mathcal{D}_1}{\phi \wedge \psi \quad \phi}, \quad (\wedge_2^-) \quad \frac{\mathcal{D}_1}{\phi \wedge \psi \quad \psi},$$

---

[56] Estas disposições correspondem às sucessões $\mathcal{D}, B$; $\mathcal{D}_1, \mathcal{D}_2, B$; $\mathcal{D}_1, \mathcal{D}_2, \mathcal{D}_3, B$, respectivamente, com a convenção de que se podem permutar as premissas $\mathcal{D}_i$ de qualquer maneira.

$$(\to^+)\ \dfrac{\begin{array}{c}[\phi]\\ \mathcal{D}\\ \psi\end{array}}{\phi\to\psi}\ ,\quad (\to^-)\ \dfrac{\begin{array}{cc}\mathcal{D}_1 & \mathcal{D}_2\\ \phi & \phi\to\psi\end{array}}{\psi}$$

$$(\vee_1^+)\ \dfrac{\begin{array}{c}\mathcal{D}_1\\ \phi\end{array}}{\phi\vee\psi}\ ,\quad (\vee_2^+)\ \dfrac{\begin{array}{c}\mathcal{D}_1\\ \psi\end{array}}{\phi\vee\psi}\ ,\quad (\vee^-)\ \dfrac{\begin{array}{ccc} & [\phi] & [\psi]\\ \mathcal{D} & \mathcal{D}_1 & \mathcal{D}_2\\ \phi\vee\psi & \theta & \theta\end{array}}{\theta}\ ,$$

são derivações.

3. (Regra de eliminação da dupla negação) Se $\mathcal{D}$ é uma derivação, então

$$(\neg\neg^-)\ \dfrac{\begin{array}{c}\mathcal{D}\\ \bot\end{array}}{\phi}$$

é uma derivação, onde $\bot$ representa uma contradição qualquer.

4. Nada mais é derivação.

II Parte: Além disso, em aplicações da regra $(\to^+)$, a hipótese ϕ em $\mathcal{D}$ é descarregada, se estiver presente (ver caso degenerado, nota 52, pág. 58); em aplicações da regra $(\vee^-)$, são descarregadas as hipóteses ϕ, ψ de $\mathcal{D}_1$, $\mathcal{D}_2$, respectivamente; e em aplicações da regra $(\neg^-)$ é descarregada a hipótese $\neg\phi$. Todas as hipóteses de uma premissa que não são descarregadas por uma destas regras permanecem não descarregadas, *activas* ou *abertas* após a aplicação da regra (e diz-se que a conclusão *depende* dessas hipóteses).

Pode-se dizer, por outras palavras, que o conjunto das derivações com hipóteses em Γ é o mais pequeno conjunto (de sucessões finitas de fórmulas) que contém as fórmulas de Γ (regra H) e é fechado para as outras regras. Este tipo de definição (indutiva) permite que se façam demonstrações (metamatemáticas) por indução nas derivações (ou, se quisermos, no comprimento das derivações).

Também se pode dar uma definição indutiva das derivações em forma de árvore, mas não iremos prosseguir nesta via com este sistema (ver II.16).

II.11 Semântica e metateoria

Suponhamos dadas ao acaso certas fórmulas ϕ_1, ..., ϕ_n, ψ, e que inquirimos

$$(Q_1) \qquad \phi_1, ..., \phi_n \vdash \psi \ ?$$

Como obter a resposta a uma questão deste tipo? *Se existe*, de facto, uma dedução de ψ com hipóteses ϕ_1, ..., ϕ_n, é muito possível que ao fim de algum

tempo se encontre uma mas, se ao fim de algum tempo (razoável) não for encontrada nenhuma dedução, duas explicações são possíveis:

(i) Não tentámos o tempo suficiente; ou

(ii) Não existe, de facto, nenhuma dedução.

Como saber qual destes casos se dá? Seria interessante poder responder a estas questões em tempo útil, antes de embarcarmos em tentativas de dedução que podem estar, afinal, condenadas ao fracasso.[57]

No cálculo proposicional as questões anteriores têm respostas afirmativas, e no melhor sentido possível, pois existe mesmo um algoritmo[58] para decidir questões do tipo (Q_1). Não será exactamente assim, porém, no cálculo de predicados, como veremos.

Antes de formular as respostas de maneira precisa, convém recordar as noções semânticas de consequência, valoração e valoração booleana. Em virtude da propriedade de extensão das valorações, enunciada na pág. 53, *podemos designar também por v a extensão booleana $\widehat{v}$* de uma valoração simples v, e deixaremos de usar o adjectivo «booleana».

Conforme os valores lógicos que uma fórmula ϕ pode tomar para as diferentes valorações possíveis [quer dizer, para os diferentes arranjos de valores lógicos atribuídos às letras proposicionais que ocorrem em ϕ (ver exercício 2.3)], obtemos a seguinte classificação das fórmulas de $\mathcal{L}^0$:

- ϕ é **taulológica**, ou uma **tautologia**, ou é **válida**: para toda a valoração booleana v, $v(\phi) = 1$;
- ϕ é **compatível**: existe v tal que $v(\phi) = 1$;
- ϕ é **contingente**: existem v, v' tais que $v(\phi) = 1$, $v'(\phi) = 0$.

As negações dos conceitos de fórmula válida, compatível, são **inválida** [isto é, existe v tal que $v(\phi) = 0$], **contraditória** [isto é, para todo v, $v(\phi) = 0$], respectivamente. Exemplos:

- Válidas: $p \vee \neg p$, $p \wedge q \rightarrow q$, $p \rightarrow (q \rightarrow p)$;

---

[57] Não seria a primeira vez. Durante muitos e muitos séculos os geómetras tentaram fazer a quadratura do círculo, a trissecção do ângulo arbitrário e a duplicação do cubo com régua e compasso. Os algebristas italianos da Renascença, e muitos outros depois deles tentaram descobrir fórmulas resolventes para equações algébricas de grau maior ou igual a 5. Somente durante o século XIX se descobriu porque uns e outros falharam nas suas tentativas: era impossível!

[58] Entendemos por **algoritmo** (**procedimento efectivo** ou **mecânico**) um sistema finito de regras deterministas que permite obter respostas a questões de certo tipo dado num número finito de passos. O ramo da lógica matemática que estuda os algoritmos chama-se *teoria da computabilidade* e desenvolveu-se grandemente a partir de meados dos anos trinta do século XX. Um dos criadores deste ramo, o matemático e lógico inglês Alan Turing, chefiou a equipa que decifrou o código secreto nazi *Enigma*, contribuindo para a vitória dos aliados na II Grande Guerra (ver Cap. V).

- Compatíveis: $p \wedge q,\ p,\ p \rightarrow r, p \vee \neg p$;
- Contingentes: $p,\ p \wedge q,\ p \vee q$;
- Contraditórias: $p \wedge \neg p$, $\neg(p \vee \neg p)$, qualquer $\neg\phi$, onde ϕ é válida.

A notação habitual para exprimir que uma fórmula ϕ é válida é a seguinte:

$$\vDash \phi.$$

Em termos de valorações, a definição de validade de um argumento ou de consequência é: um argumento $\phi_1, ..., \phi_n/\psi$ é válido, ou, equivalentemente, ψ é consequência de ϕ_1, ..., ϕ_n, e escrevemos

$$\phi_1, ..., \phi_n \vDash \psi,$$

se e somente se para toda a valoração v, se $\widehat{v}(\phi_1) = \cdots = \widehat{v}(\phi_n) = 1$, então $\widehat{v}(\psi) = 1$.

11.1 Definição Seja Σ um conjunto de fórmulas, ψ uma fórmula. Dizemos que ψ é **consequência lógica** de Σ, e escreve-se $\Sigma \vDash \psi$, se e só se toda a valoração v que satisfaz todas as fórmulas de Σ satisfaz ψ. ϕ é **logicamente equivalente a** ψ, e escreve-se $\phi \sim \psi$, sse $\phi \vDash \psi$ e $\psi \vDash \phi$ (ou seja, sse $\phi \longleftrightarrow \psi$ é válida).

Vejamos alguns exemplos de equivalências lógicas notáveis, e respectivas designações. Para quaisquer fórmulas ϕ, ψ e θ, tem-se:

$\phi \wedge \phi \sim \phi$	$\phi \vee \phi \sim \phi$	*idempotência*
$\phi \wedge \psi \sim \psi \wedge \phi$	$\phi \vee \psi \sim \psi \vee \phi$	*comutatividade*
$(\phi \wedge \psi) \wedge \theta \sim \phi \wedge (\psi \wedge \theta)$	$(\phi \vee \psi) \vee \theta \sim \phi \vee (\psi \vee \theta)$	*associatividade*
$(\phi \wedge \psi) \vee \phi \sim \phi$	$(\phi \vee \psi) \wedge \phi \sim \phi$	*absorção*
$(\phi \wedge \psi) \vee \theta \sim (\phi \wedge \theta) \vee (\psi \wedge \theta)$	$(\phi \vee \psi) \wedge \theta \sim (\phi \vee \theta) \wedge (\psi \vee \theta)$	*distributividade*
$\neg(\phi \wedge \psi) \sim \neg\phi \vee \neg\psi$	$\neg(\phi \vee \psi) \sim \neg\phi \wedge \neg\psi$	*DeMorgan*
$\neg\neg\phi \sim \phi$		*dupla negação*

Além disso:

$\phi \wedge \psi \sim \psi$	$\phi \vee \psi \sim \phi$	se ϕ é válida
$\phi \wedge \psi \sim \phi$	$\phi \vee \psi \sim \psi$	se ϕ é incompatível.

11.2 Definição Seja Σ um conjunto (finito ou infinito) de fórmulas de $\mathcal{L}^0$. Dizemos que Σ é **compatível** sse existe, pelo menos, uma valoração v que satisfaz todas as fórmulas de Σ. Uma valoração v que satisfaz uma fórmula ϕ também se diz um **modelo** de ϕ, e uma valoração v que satisfaz todas as fórmulas de um conjunto Σ diz-se um **modelo** de Σ.

Portanto, Σ é compatível sse possui, pelo menos, um modelo. De de acordo com a definição acima, também podemos dizer que $\phi_1, ..., \phi_n \vDash \psi$ sse todo o modelo de $\{\phi_1, ..., \phi_n\}$ é modelo de ψ.

Vê-se facilmente que, de acordo com as definições acima, a noção de validade para fórmulas é um caso particular da noção de consequência: $\emptyset \vDash \psi$ sse $\vDash \psi$, onde $\emptyset$ é o conjunto vazio.

Regressando às questões acima formuladas, podemos agora enunciar os resultados fundamentais que lhes dão resposta, os quais também são conhecidos como *metateoremas da lógica proposicional*:

11.3 Propriedade da validade (MV)

Para quaisquer fórmulas ϕ_1, ..., ϕ_n, ψ de $\mathcal{L}^0$, se $\phi_1, ..., \phi_n \vdash \phi$, então $\phi_1, ..., \phi_n \vDash \phi$. Em particular, se ϕ é uma lei lógica, então ϕ é válida: se $\vdash \phi$, então $\vDash \phi$.

Esta propriedade fornece imediatamente[59] um *critério de não dedutibilidade:* se ψ não é consequência de ϕ_1, ..., ϕ_n, então ψ não é, por certo, derivável das hipóteses ϕ_1, ..., ϕ_n. Em particular, se ψ não é válida, então ψ não é lei lógica. Por exemplo, p não é derivável das hipóteses $p \rightarrow q$, q pois, como facilmente se constata, p não é consequência de $p \rightarrow q$, q.

11.4 Corolário (Propriedade da consistência)

O sistema **DN** *é* ***consistente*** *(ou* ***não contraditório****), no sentido seguinte: não existe nenhuma fórmula ϕ tal que $\phi \wedge \neg\phi$ é derivável.*

Dem. Se alguma $\phi \wedge \neg\phi$ fosse derivável, isto é, fosse lei, então seria válida, o que é impossível (pois $\phi \wedge \neg\phi$ é contraditória, isto é, sempre falsa).■

Podemos argumentar a favor da plausibilidade da propriedade de validade, observando que as regras do sistema **DN** são válidas, isto é, preservam a verdade.[60] Ora, numa dedução em que tais regras são aplicadas, é óbvio que sempre que as hipóteses forem verdadeiras, cada linha que figure abaixo das hipóteses é verdadeira também (mesmo que só dependa de algumas das hipóteses), e em particular, a última linha, que contém a fórmula deduzida (tese final), é verdadeira. Mais pormenorizadamente, a propriedade de validade resulta do seguinte resultado um pouco mais geral:

---

[59] Por contraposição ao nível metalinguístico.

[60] Uma demonstração rigorosa pode ser feita por indução no comprimento das derivações. A validade de regras como as de introdução de $\rightarrow$ e de $\neg$ e a regra de eliminação de $\vee$ tem de ser entendida de modo apropriado. Particularizemos ao caso da regra ($\rightarrow^+$): a conclusão $\phi \rightarrow \psi$ é verdadeira sempre que todas as hipóteses de que ψ depende na subderivação-premissa, com excepção da hipótese auxiliar ϕ, são verdadeiras. Analogamente para as outras regras com subderivações-premissas ($\neg^+$) e ($\vee^-$).

11.5 Metateorema

Para cada fórmula ϕ de uma dedução com hipóteses em **DN**, *se ψ_1, ψ_2, ..., ψ_m são todas as hipóteses de que ϕ depende nessa dedução, então $\psi_1 \wedge \psi_2 \wedge ... \wedge \psi_m \rightarrow \phi$ é válida (ou, equivalentemente, $\psi_1, \psi_2, ..., \psi_m \vDash \phi$).*

Considera-se incluído o caso em que $m = 0$, e neste caso a conclusão é que ϕ é válida. O enunciado (**MV**) acima está obviamente contemplado como caso particular, quando ϕ é a última fórmula de uma dedução.

A demonstração é por indução nas deduções, ou melhor, no número de ordem (número da linha) $n \geq 1$ em que ϕ se insere numa dedução, linha essa que pode depender de algumas hipóteses iniciais e, eventualmente também, de algumas hipóteses auxiliares entretanto assumidas. Para simplificar, supomos que a regra (T^+) não foi utilizada. Precisando, o tipo de indução mais apropriado é o de *indução completa,* 2.ª forma (ver Cap. IV, pág. 252) que aqui reformulamos para a condição em n, $\Phi(n)$, que exprime que se ϕ é a fórmula número n (≥ 1) numa dedução e ϕ depende exactamente das hipóteses ψ_1, ψ_2, ..., ψ_m, então $\psi_1, \psi_2, ..., \psi_m \vDash \phi$. Diz o referido *princípio de indução completa* que se

(i) $\Phi(1)$ é verdadeira, e

(ii) para cada $n \geq 1$, se $\Phi(n+1)$ é verdadeira sempre que $\Phi(k)$ é verdadeira para todo $k \leq n$,

então $\Phi(n)$ é verdadeira para todo $n \geq 1$.

Dem. (i) Se ϕ é a linha 1 de uma dedução, ϕ só pode ser uma hipótese, que só depende de si mesma, e é óbvio que, neste caso, $\phi \vDash \phi$.

(ii) Seja $n \geq 1$ ao arbítrio e suponhamos (hipótese de indução) que $\Phi(k)$ é verdadeira para qualquer $k \leq n$, e que ϕ é inserida na linha $n+1$. Há vários casos a considerar, conforme a justificação para esta linha.

Caso Hip. ϕ é uma hipótese inicial ou auxiliar, e este caso trata-se como em (i).

Caso ($\wedge^+$). ϕ é da forma $\psi \wedge \theta$ e é inferida de ψ, θ em linhas precedentes por ($\wedge^+$), e as hipóteses de que ψ, θ dependem estão entre $\psi_1, \psi_2, ..., \psi_m$. Esquematicamente, estamos na situação seguinte:

⋮	⋮	} $\psi_1, \psi_2, ..., \psi_m$
i	ψ	
⋮	⋮	
j	θ	
⋮	⋮	
n+1	$\psi \wedge \theta$	i, j ($\wedge^+$)

Por hipótese de indução, $\psi_1, \psi_2, ..., \psi_m \vDash \psi$ e $\psi_1, \psi_2, ..., \psi_m \vDash \theta$,[61] donde se conclui facilmente que $\psi_1, \psi_2, ..., \psi_m \vDash \psi \wedge \theta$.

Caso ($\rightarrow^+$). ϕ é da forma $\psi \rightarrow \theta$, em que ψ é uma hipótese auxiliar (diferente das ψ_l, $1 \leq l \leq m$) de que ϕ não depende, mas θ depende de ψ e de algumas das ψ_l. Esquematicamente estamos na situação seguinte:

⋮	⋮	$\}\psi_1, \psi_2, ..., \psi_m$
i	ψ	H
⋮	⋮	
j	θ	
⋮	⋮	
n + 1	$\psi \rightarrow \theta$	i-j ($\rightarrow^+$)

Por hipótese de indução, $\psi_1, \psi_2, ..., \psi_m, \psi \vDash \psi$ (ver Nota 61) e $\psi_1, \psi_2, ..., \psi_m, \psi \vDash \theta$, donde $\psi_1, \psi_2, ..., \psi_m \vDash \psi \rightarrow \theta$.

Deixamos os outros casos como exercícios para o leitor.■

11.6 Definição Para qualquer conjunto (finito ou infinito) Γ de fórmulas de $\mathcal{L}^0$ e qualquer fórmula ϕ, diz-se que ϕ é **dedutível** (ou **derivável**) de Γ, ou ainda que é um **teorema** de Γ, e escreve-se

$$\Gamma \vdash \phi,$$

sse existe uma dedução de ϕ com hipóteses em Γ, isto é, existem $n \geq 0$ e $\phi_1, ..., \phi_n$ em Γ tais que $\phi_1, ..., \phi_n \vdash \phi$.[62]

Um conjunto Γ de fórmulas de $\mathcal{L}^0$ diz-se **consistente** ou **não contraditório** sse não existe nenhuma fórmula ψ tal que $\Gamma \vdash \psi \wedge \neg\psi$, e diz-se **inconsistente** ou **contraditório** no caso contrário, isto é, sse existe, pelo menos, uma fórmula ψ tal que $\Gamma \vdash \psi \wedge \neg\psi$.

A propósito da última parte desta definição observe-se que uma fórmula ψ tal que $\Gamma \vdash \psi \wedge \neg\psi$, se existir, *não tem de ser* necessariamente membro de Γ (e, em geral, não é). A consistência do sistema **DN** definida no enunciado do corolário acima não é mais do que a consistência do conjunto vazio $\Gamma = \emptyset$.

A propriedade de validade responde somente de modo parcial à questão (Q_1) acima. Para responder cabalmente a esta questão temos o resultado seguinte, que é a propriedade recíproca da propriedade de validade, porém, bem mais difícil de demonstrar. É, talvez, o resultado mais importante da metateoria do cálculo

---

[61] Por maioria de razão: se ψ (ou θ) depende de algumas das ψ_l e é consequência delas, por hipótese de indução, então é certamente consequência delas todas.

[62] O caso $n = 0$ é para contemplar a possibilidade de ϕ ser uma lei lógica. Quer dizer, *todas as leis lógicas são automaticamente teoremas de* Γ.

proposicional, pois é a prova de que o sistema dedutivo **DN** realiza completamente o objectivo que se propunha de «captar» dedutivamente a noção semântica de consequência.

11.7 Propriedade da completude semântica (MCS)

Para quaisquer fórmulas ϕ_1, ..., ϕ_n, ψ *de* $\mathcal{L}^0$, *se* $\phi_1, ..., \phi_n \vDash \psi$, *então* $\phi_1, ..., \phi_n \vdash \psi$. *Em particular, toda a fórmula válida é derivável: se* $\vDash \psi$, *então* $\vdash \psi$.

Há diversas demonstrações desta propriedade,[63] algumas das quais fornecem mesmo um método para construir uma derivação de ψ com hipóteses ϕ_1, ..., ϕ_n, conhecida uma tabela de verdade que estabeleça que ψ é consequência daquelas hipóteses, e outras há baseadas noutros sistemas dedutivos (ver secções finais deste capítulo). Refira-se ainda que quer uma quer outra das propriedades acima (validade e completude semântica) se pode generalizar a um conjunto arbitrário Γ de hipóteses. Denotamos as versões generalizadas de uma e outra por ($\mathbf{MV}_G$) e ($\mathbf{MCS}_G$), respectivamente. Todavia, não são estas mas sim outras versões das propriedades generalizadas que demonstramos, ficando por estabelecer a equivalência entre as duas versões de uma e de outra, o que será feito nos exercícios:

11.8 Completude semântica generalizada (2.ª versão)

(MCS'_G) *Para todo o conjunto* Γ *de fórmulas de* $\mathcal{L}^0$, *se* Γ *é consistente, então* Γ *é compatível*.

***Dem.** Em várias etapas. Alguns passos serão deixados para os exercícios. Estamos supondo $P = \{p_0, p_1, ...\}$, e deste simples facto podemos obter uma enumeração de *todas* as fórmulas de $\mathcal{L}^0$, possivelmente com repetições, digamos

(1) $$\phi_0, \phi_1, \phi_2, ..., \phi_n, ...$$

Existem várias maneiras de obter uma tal enumeração. Uma delas será: enumerar todas as fórmulas de comprimento 1 onde só ocorre p_0 (há só uma, o próprio p_0); de seguida, enumerar todas as fórmulas de comprimento ≤ 2 onde só podem ocorrer p_0 ou p_1; de seguida, todas as fórmulas de comprimento ≤ 3 onde só podem ocorrer letras proposicionais de entre p_0, p_1 e p_2, e assim sucessivamente.[64]

---

[63] Historicamente, a primeira foi obtida por E. Post para um sistema dedutivo diferente, embora equivalente ao nosso, a saber, para o sistema dedutivo dos *Principia Mathematica* de RUSSELL & WHITEHEAD. V. o artigo de E. POST "Introduction to a general theory of elementary propositions", *Amer. Journ. Math.* **43** (1921), 163-185, reproduzido em HEIJENOORT.

[64] Esta enumeração peca por excesso de repetições, como é óbvio. Uma enumeração mais comedida pode-se obter codificando os símbolos do alfabeto e as fórmulas por números naturais, por um processo explicado no Cap. IV. Uma terceira via seria recorrer ao teorema

Seja então Γ um conjunto consistente qualquer. Definimos indutivamente uma sucessão crescente de conjuntos de fórmulas

$$\Gamma_0 \subseteq \Gamma_1 \subseteq \Gamma_2 \subseteq \cdots \subseteq \Gamma_n \subseteq \Gamma_{n+1} \subseteq \cdots$$

pondo $\Gamma_0 = \Gamma$ e, para cada $n \geq 0$,

$$\Gamma_{n+1} = \begin{cases} \Gamma_n \cup \{\phi_n\} & \text{se este conjunto é consistente} \\ \Gamma_n \cup \{\neg\phi_n\} & \text{no caso contrário.} \end{cases}$$

Finalmente, definimos

$$\Gamma_\infty = \bigcup_{n=0}^{\infty} \Gamma_n.$$

É claro que $\Gamma \subseteq \Gamma_\infty$. Se provarmos que Γ_∞ é compatível, resultará Γ compatível. Vejamos primeiramente algumas propriedades dos conjuntos Γ_n e da sua união Γ_∞.

(2) para todo n, Γ_n é consistente.

Isto prova-se facilmente por indução matemática, tendo em conta que, para cada n, um ou outro dos conjuntos $\Gamma_n \cup \{\phi_n\}$, $\Gamma_n \cup \{\neg\phi_n\}$ é consistente [ver exercício 2.12 (b)].

(3) Γ_∞ é **consistente maximal**, isto é,

(i) Γ_∞ é consistente, e

(ii) para qualquer ϕ, se $\phi \notin \Gamma_\infty$, então $\Gamma_\infty \cup \{\phi\}$ é contraditório.

Quanto a (i), observe-se que se Γ_∞ fosse contraditório, então existiriam ψ_1, ..., ψ_k em Γ_∞ e ψ tais que $\psi_1, ..., \psi_k \vdash \psi \wedge \neg\psi$. Ora, como Γ_∞ é a união dos conjuntos Γ_n ($n \geq 0$) e estes formam uma sucessão crescente, cada ψ_i está em algum Γ_{n_i} e, para n suficientemente grande, ψ_1, ..., ψ_k estão todos em Γ_n, logo $\Gamma_n \vdash \psi \wedge \neg\psi$, contra o estabelecido em (2).

Quanto a (ii), dada ϕ ao arbítrio, existe ϕ_n tal que $\phi = \phi_n$, atendendo a que (1) é uma enumeração de todas as fórmulas. Se $\phi \notin \Gamma_\infty$, não pode ser $\Gamma_n \cup \{\phi\} = \Gamma_n \cup \{\phi_n\}$ consistente, porque neste caso teríamos

$$\phi \in \Gamma_{n+1} = \Gamma_n \cup \{\phi_n\} = \Gamma_n \cup \{\phi\} \subseteq \Gamma_\infty;$$

portanto, como $\Gamma_\infty \cup \{\phi\} \supseteq \Gamma_n \cup \{\phi\}$, $\Gamma_\infty \cup \{\phi\}$ também não é consistente.

Das propriedades anteriores outras resultam, a saber:

---

da teoria dos conjuntos que diz que a união numerável de conjuntos numeráveis é numerável, observando que o conjunto das fórmulas é a união dos conjuntos de fórmulas de comprimentos 1, 2, 3, etc. A demonstração do metateorema estende-se a conjuntos P arbitrários (não numeráveis) mas, para obter uma enumeração das fórmulas, neste caso, há que recorrer a instrumentos mais poderosos da teoria dos conjuntos, como o axioma da escolha ou o equivalente princípio da boa ordenação.

(4) Γ_∞ é **dedutivamente fechado**, isto é, para qualquer ϕ, se $\Gamma_\infty \vdash \phi$, então $\phi \in \Gamma_\infty$.

Com efeito, se ϕ fosse dedutível de Γ_∞ mas não pertencesse a Γ_∞, então, por (3ii), $\Gamma_\infty \cup \{\phi\}$ seria contraditório, logo $\Gamma_\infty \vdash \neg\phi$ (exercício), donde $\Gamma_\infty \vdash \phi \wedge \neg\phi$ [utilizando a regra ($\wedge^+$)], contra o estabelecido em (3i).

(5) Γ_∞ é **completo**, isto é, para qualquer ϕ, $\Gamma_\infty \vdash \phi$ ou $\Gamma_\infty \vdash \neg\phi$.

Se tivermos $\Gamma_\infty \nvdash \neg\phi$, então $\Gamma_\infty \cup \{\phi\}$ é consistente [exercício 2.17(c)], logo $\phi \in \Gamma_\infty$ por (3ii) e, portanto, $\Gamma_\infty \vdash \phi$.

De (4) e (5) resulta imediatamente

(6) Para qualquer ϕ, $\phi \in \Gamma_\infty$ ou $\neg\phi \in \Gamma_\infty$.

O conjunto Γ_∞ tem, também, as propriedades seguintes, a utilizar no último passo da demonstração:

(7) Para quaisquer fórmulas ϕ e ψ,

(i) $\phi \wedge \psi \in \Gamma_\infty$ sse $\phi \in \Gamma_\infty$ e $\psi \in \Gamma_\infty$;

(ii) $\phi \vee \psi \in \Gamma_\infty$ sse $\phi \in \Gamma_\infty$ ou $\psi \in \Gamma_\infty$;

(iii) $\phi \rightarrow \psi \in \Gamma_\infty$ sse $\phi \notin \Gamma_\infty$ ou $\psi \in \Gamma_\infty$.

Exemplifiquemos com a demonstração de (i), no sentido ($\Rightarrow$)[65]: suponhamos que $\phi \wedge \psi \in \Gamma_\infty$, com vista a provar que $\phi \in \Gamma_\infty$ e $\psi \in \Gamma_\infty$. Se fosse $\phi \notin \Gamma_\infty$ ou $\psi \notin \Gamma_\infty$, então, por (6), seria $\neg\phi \in \Gamma_\infty$ ou $\neg\psi \in \Gamma_\infty$, logo $\{\phi \wedge \psi, \neg\phi\} \subseteq \Gamma_\infty$ ou $\{\phi \wedge \psi, \neg\psi\} \subseteq \Gamma_\infty$ e, em qualquer dos casos, Γ_∞ seria contraditório, por conter um dos conjuntos $\{\phi \wedge \psi, \neg\phi\}$, $\{\phi \wedge \psi, \neg\psi\}$, ambos contraditórios.

Estamos próximos da conclusão da demonstração. Tendo em conta, principalmente, as propriedades (6) e (7), já se adivinha que o conjunto Γ_∞ tem algumas parecenças formais com as valorações booleanas, mais exactamente, é aparente uma analogia formal entre as condições «$\phi \in \Gamma_\infty$» e «ϕ é verdadeira». Tiramos partido desta analogia definindo uma valoração v pondo

$$v(p_i) = 1 \text{ sse } p_i \in \Gamma_\infty.$$

Por indução na complexidade das fórmulas prova-se facilmente que, para toda a fórmula ϕ,

$$v(\phi) = 1 \text{ sse } \phi \in \Gamma_\infty.$$

Isto significa que v é modelo de Γ_∞. Portanto, Γ_∞ é compatível e, por maioria de razão, Γ é compatível.■

---

[65] Utilizamos aqui o símbolo ' $\Rightarrow$ ' como abreviatura da expressão metalinguística «implica», ou «se...então» (exactamente as mesmas que motivaram o ' $\rightarrow$ ' de $\mathcal{L}^0$).

Das propriedades generalizadas da validade e da completude semântica, conjugadas, pode-se concluir a «equivalência» entre as abordagens semântica (valores lógicos, tabelas de verdade ou valorações, consequência, validade, etc.) e axiomático-dedutiva (regras de inferência, deduções formais, etc., sempre relativas ao sistema **DN**): para qualquer conjunto Σ de fórmulas e qualquer fórmula ϕ tem-se

$$\boxed{\Sigma \vdash \phi \text{ sse } \Sigma \vDash \phi.}$$

Não é demais sublinhar a importância filosófica deste resultado. Ele significa, pelo lado da validade ($\Sigma \vdash \phi \Rightarrow \Sigma \vDash \phi$) que o sistema dedutivo **DN** é *correcto* ou *adequado*, pois não permite deduzir de um conjunto Σ senão consequências semânticas de Σ e, pelo lado da completude semântica ($\Sigma \vDash \phi \Rightarrow \Sigma \vdash \phi$) que ele é *suficiente*, pois todas as consequências semânticas de Σ são dedutíveis de Σ. Relativamente à lógica proposicional clássica podemos dizer, portanto que foi plenamente atingido o objectivo tradicional dos estudos lógicos.

Por outro lado, atendendo a que a construção de uma tabela de verdade é um procedimento mecânico que termina ao fim de um número finito de passos (isto é, um algoritmo), podemos também concluir que o **problema de decisão** para a noção de dedutibilidade (de um número *finito* de hipóteses) tem solução positiva: existe um algoritmo para decidir questões do tipo (Q_1). A questão complica-se um pouco no caso de o conjunto de hipóteses ser infinito. A secção seguinte é uma mui breve e informal introdução a questões de decidibilidade na lógica proposicional.

*II.12 Decidibilidade, enumerabilidade efectiva, complexidade

Por mais de uma vez neste capítulo deparámos com certas questões de decisão que podem ser resolvidas algoritmicamente (ver Nota 58), a par de outras que poderíamos ter formulado e que também podem ser resolvidas algoritmicamente:

(1) Decidir se uma dada expressão no alfabeto de $\mathcal{L}^0$ é ou não uma fórmula de $\mathcal{L}^0$;

(2) decidir se uma sucessão de fórmulas ϕ_1, ..., ϕ_n é ou não uma dedução no sistema **DN** (ou num outro sistema);

(3) dedidir se uma dada fórmula ψ é ou não válida e, mais geralmente, se ela é ou não consequência de certas fórmulas ϕ_1, ..., ϕ_n;

(4) decidir se uma dada fórmula ψ é ou não uma lei lógica e, mais geralmente, se ela é ou não derivável de certas fórmulas ϕ_1, ..., ϕ_n no sistema **DN** (ou num outro sistema — ver adiante).

Se Σ é um conjunto infinito de fórmulas e queremos decidir questões da forma «$\Sigma \vDash \phi$?» ou da forma «$\Sigma \vdash \phi$?» depara-se logo uma dificuldade de ordem prática, pela impossibilidade de construção de tabelas de verdade com uma infinidade de entradas (linhas). Mas todas as questões anteriores são, em última análise, do tipo

(5) $a \in X$?

No caso (1), X é o conjunto das expressões sobre o alfabeto; no caso (2), X é o conjunto de todas as deduções no sistema **DN**, etc.

12.1 Definição Um conjunto X diz-se **decidível** sse existe um *algoritmo* (procedimento mecânico ou efectivo, descrito por um número finito de regras ou instruções e completamente determinista) que permite decidir, para cada objecto a, a questão (5) num número finito de passos. Um conjunto não decidível diz-se **indecidível**.

É decidível todo o conjunto finito, e alguns conjuntos infinitos são também decidíveis, como o conjunto das fórmulas válidas de $\mathcal{L}^0$ (estamos admitindo tacitamente que o alfabeto de $\mathcal{L}^0$ é decidível), mas não é de esperar que todo o conjunto infinito seja decidível, por um simples argumento de cardinalidade: a totalidade dos algoritmos é numerável mas, por exemplo, o conjunto de todos os conjuntos de expressões $\mathcal{P}(E)$ [de que Form($\mathcal{L}^0$) e o conjunto das fórmulas válidas são membros] é não numerável.

Se Σ é um conjunto infinito de fórmulas de $\mathcal{L}^0$, o conjunto de todas as consequências de Σ,

$$\Sigma^* = \{\phi \in \text{Form}(\mathcal{L}^0) : \Sigma \vDash \phi\} = \{\phi : \Sigma \vdash \phi\}$$

não é, em geral, decidível, mas podemos obter um resultado que está a meio caminho entre a decidibilidade e a indecidibilidade.

12.2 Definição Dizemos que um conjunto X é **efectivamente enumerável** sse existe um algoritmo que permite gerar, um a um, os elementos de X.

Se X for infinito, o algoritmo que gera os elementos de X não pára nunca mas, para cada objecto a, se realmente a está em X, então mais tarde ou mais cedo a será gerado. Mais precisamente, tem-se o seguinte resultado, que particularizamos a conjuntos de expressões mas se aplica também a situações mais gerais:

12.3 Lema
Um conjunto Σ de expressões é efectivamente enumerável sse existe um algoritmo que, para cada expressão σ, dá a resposta SIM se e só se $\sigma \in \Sigma$.[66]

Dem. Suponhamos Σ efectivamente enumerável e seja σ uma expressão qualquer. Iniciando o algoritmo $\mathcal{A}$ que gera Σ, ele começa a produzir expressões σ_0, σ_1, σ_2, ... Definimos um novo algoritmo $\mathcal{B}$ do seguinte modo: se e quando σ aparecer nesta listagem, o novo algoritmo dá a resposta SIM. Deste modo, se

[66] Se $\sigma \notin \Sigma$, o algoritmo poderá produzir a resposta NÃO ou continuar indefinidamente sem produzir resposta alguma, mas nunca terminará num SIM.

realmente $\sigma \in \Sigma$, o novo algoritmo acabará por dar a resposta SIM e termina aí. Se $\sigma \notin \Sigma$ o novo algoritmo continua esperando sem dar resposta nenhuma...

Reciprocamente, suponhamos que existe um algoritmo $\mathcal{B}$ que, para cada expressão σ, dá a resposta SIM sse $\sigma \in \Sigma$. Mostramos que existe um algoritmo $\mathcal{A}$ que gera todas as expressões de Σ, procedendo do seguinte modo: enumeramos por qualquer processo (ver início da demonstração do metateorema da completude semântica) todas as expressões, σ_0, σ_1, σ_2, ... e aplicamos o algoritmo $\mathcal{B}$ a cada uma destas, sucessivamente, mas, para que não se esgote o tempo todo com uma só expressão (o que poderia acontecer se ela não pertencer a Σ), procedemos assim:

1) testamos «$\sigma_0 \in \Sigma$?» durante 1 minuto;

2) testamos «$\sigma_0 \in \Sigma$?» durante 2 minutos e «$\sigma_1 \in \Sigma$?» durante mais 2 minutos;

3) testamos «$\sigma_0 \in \Sigma$?» durante 3 minutos, «$\sigma_1 \in \Sigma$?» durante mais 3 minutos e «$\sigma_2 \in \Sigma$?» durante 3 minutos, e assim sucessivamente.

Sempre que obtemos um SIM como resposta colocamos a expressão correspondente numa outra lista, a qual virá a constituir a enumeração efectiva pretendida.■

Das definições e lema precedentes facilmente de conclui a importante caracterização seguinte, cuja demonstração deixamos como exercício:

12.4 Teorema de Post

Um conjunto Σ é decidível sse Σ e o seu complementar no conjunto de todas as expressões, E, são ambos efectivamente enumeráveis.■

Mesmo que Σ seja decidível, o conjunto Σ^* das consequências de Σ não é, em geral, decidível mas é, em todo o caso, efectivamente enumerável.

12.5 Teorema da enumerabilidade efectiva

Se Σ é um conjunto decidível ou efectivamente enumerável de fórmulas de $\mathcal{L}^0$, então o conjunto das consequências de Σ é efectivamente enumerável.

Dem. Seja ϕ_0, ϕ_1, ... uma enumeração efectiva de Σ. Dada uma fórmula qualquer ϕ, podemos decidir algoritmicamente cada uma das questões

$$\phi_0 \vDash \phi \ ?,\ \ \phi_0, \phi_1 \vDash \phi \ ?,\ \ \phi_0, \phi_1, \phi_2 \vDash \phi \ ?, ...$$

Se e quando alguma destas questões tem resposta positiva, a resposta à questão «$\Sigma \vDash \phi$?» (isto é, «$\phi \in \Sigma^*$?») é SIM. Acontece que, se $\Sigma \vDash \phi$, então $\phi_0, \phi_1, ..., \phi_n \vDash \phi$ para algum n suficientemente grande, por um resultado a estabelecer adiante na secção II.14 (metateorema da compacidade). Assim, podemos realmente produzir uma enumeração efectiva das consequências de Σ.■

12.6 Algoritmos não deterministas Demos acima (pág. 80) uma ideia de algoritmo que, embora não totalmente precisa, está de acordo com o conceito informal clássico de algoritmo e é, apesar de tudo, útil no reconhecimento e na aplicação de certo tipo de procedimentos. Um exemplo típico de um algoritmo ou procedimento efectivo ou determinista é o da construção de tabelas de verdade para decidir se uma fórmula ao arbítrio é ou não válida (compatível, contingente, etc.). Uma característica deste e doutros algoritmos deterministas é que, para qualquer *entrada* ou *dado* (*«input»*), a computação e o resultado (*«output»*) são únicos e completamente determinados pela entrada. Além disso, esperamos que o algoritmo seja *adequado* ou *correcto*, isto é, que a resposta ou resultado produzido seja correcto. No caso das tabelas de verdade para decidir da validade ou não de uma fórmula dada, a correcção significa que o resultado do algoritmo é a conclusão de que a fórmula é válida sse a fórmula é realmente válida.

Admitiremos agora uma extensão do conceito de algoritmo — a de *algoritmo não determinista:* um procedimento descrito por um número finito de regras ou instruções, mas em que para uma entrada, pelo menos, possa haver mais de uma computação possível e, consequentemente, mais de um resultado possível. O algoritmo considera-se *correcto* sse pelo menos um resultado é correcto, para cada entrada.

12.7 Exemplos (1) Um exemplo típico de um algoritmo não determinista para a compatibilidade das fórmulas é o seguinte:

$\mathcal{A}$*: escolhemos* ao arbítrio uma atribuição de valores lógicos às letras proposicionais que ocorrem em ϕ (isto é, uma valoração v); se ϕ for verdadeira para essa atribuição (isto é, $v\phi = 1$), então ϕ é compatível.

É claro que se ϕ for compatível, então, para *alguma* atribuição v, o resultado é correcto (isto é, $v\phi = 1$). Outras respostas (para outras atribuições) podem não dar a resposta correcta (se ϕ vier falsa para elas), mas isto não impede que o algoritmo $\mathcal{A}$ seja considerado como correcto.

(2) Outros exemplos de algoritmos não deterministas são fornecidos pelas construções de derivações em alguns sistemas dedutivos: a partir de uma dada lista (finita) de premissas, escolhemos um de vários caminhos possíveis com vista a deduzir ϕ dada. Estes não são algoritmos não deterministas típicos, todavia, pois alguns deles podem ser montados de maneira a que toda a construção produza uma resposta correcta (se alguma existe).

12.8 Definição Dizemos que um algoritmo (melhor: uma qualquer computação do algoritmo) corre em *tempo polinomial* se o tempo durante o qual ele corre até produzir um resultado é majorado por um polinómio no comprimento n da entrada; e dizemos que corre em *tempo exponencial* se o referido tempo é minorado por 2^{cn} para alguma constante positiva c.

Estes conceitos são medidas da *eficiência* ou *complexidade computacional* dos algoritmos. O algoritmo das tabelas de verdade não é eficiente, pois, como se sabe,

para uma fórmula com n átomos, há que construir 2^n linhas: para fórmulas cujo comprimento é função polinomial do número de átomos, o algoritmo das tabelas de verdade cresce exponencialmente em complexidade. O método dos *tableaux* semânticos (ver adiante, II.16, pág. 106 e seguintes), embora geralmente mais eficiente que o das tabelas de verdade, ainda é, todavia, de complexidade exponencial para certos tipos de fórmulas.

O objectivo central da *teoria da complexidade*, um ramo recente (pouco mais de 40 anos) na fronteira da lógica matemática e das ciências da computação, é compreender a razão pela qual alguns problemas são computacionalmente fáceis e outros difíceis de resolver. Uma das aplicações de maior sucesso desta nova teoria é a criptografia, na qual se procuram, em geral, códigos difíceis de decifrar. Ora, precisamente, os especialistas da teoria da complexidade têm fornecido aos criptógrafos elementos sobre problemas computacionalmente difíceis, que estão na base da descoberta de novas codificações difíceis de decifrar.

12.9 As classes P e NP

O algoritmo $\mathcal{A}$ acima para a compatibilidade 12.7 (1) é bastante eficiente: é de crescimento polinomial como função do comprimento da fórmula. Dizemos por isso que a compatibilidade é um de classe NP, quer dizer, é solúvel por um algoritmo NP (Não determinista em tempo Polinomial). Uma questão central da *teoria da complexidade* ainda em aberto é a de saber se a compatibilidade é ou não de classe P (quer dizer, solúvel por um algoritmo determinista de complexidade polinomial). Como é evidente, todo o problema da classe P é de classe NP, mas a possibilidade de existir um problema de classe NP que não é de classe P permanece em aberto. Trata-se de uma questão, aparentemente, muito díficil de resolver, conhecida como o problema

$$\mathrm{P} = \mathrm{NP}?$$

Este problema foi formulado por S. A. Cook[67] em 1971. Deve dizer-se que a maioria dos resultados e indícios aponta no sentido de resposta negativa a esta questão. Cook demonstrou que o problema da compatibilidade na lógica proposicional é NP-*completo,* quer dizer, se este problema for de classe P, então todo o problema NP é P e, portanto, $\mathrm{P} = \mathrm{NP}$. Ora, são já conhecidas muitas centenas de problemas NP-completos. Se algum destes possuir uma solução determinista em tempo polinomial, todos os outros terão uma tal, mas todas as tentativas fracassaram até ao presente para encontrar tal coisa, o que torna $\mathrm{P} = \mathrm{PN}$ bastante improvável aos olhos dos especialistas. Não devemos perder de vista, todavia, que a teoria da computabilidade (noção de algoritmo, computação, função computável) subjacente a esta discussão é a clássica, nascida nos anos 30 do séc.

---

[67] Ver o artigo "The complexity of theorem-proving procedures", em *Proceedings of the Third Anual ACM Symposium on the Theory of Computing,* Association for Computing Machinery, 1971, pp. 151-158.

XX[68]. Não é improvável que a discussão adquira outras tonalidades se o conceito de algoritmo (computação, etc.) for alterado (computação quântica?...).

Para terminar, pensemos no problema *complementar* ao da compatibilidade, isto é, no problema da incompatibilidade ou da validade (porque ϕ é incompatível sse $\neg\phi$ é válida). Este problema é aparentemente mais difícil que o da compatibilidade, por razões expostas acima (é necessário considerar todas as valorações...). Trata-se de um problema de classe *co*-NP: classe dos problemas cujo complementar está em NP. Prova-se que *co*-NP $=$ NP sse o problema da incompatibilidade (ou o da validade) está em NP. Como tão-pouco sabemos se existe um algoritmo não determinista de crescimento polinomial para a incompatibilidade, permanece em aberto a questão: *co*-NP $=$ NP?

II.13 Completude funcional e formas normais

Uma fórmula ϕ de $\mathcal{L}^0$ determina uma função $u = u_\phi$ cujos argumentos e valores são valores lógicos. Por exemplo, a fórmula $p \wedge q \rightarrow r$ determina a função ternária u tal que, para quaisquer a, b, $c \in \{0, 1\}$,

$$u(a, b, c) = \begin{cases} \text{valor lógico de } p \wedge q \rightarrow r, \text{ quando se atribuem a} \\ p, q, r \text{ os valores lógicos } a, b, c, \text{ respectivamente.} \end{cases}$$

Por exemplo, $u(0, 1, 0) = 1$, $u(1, 1, 0) = 0$. Por outras palavras, as tabelas dos valores lógicos de ϕ e a tabela de u_ϕ são em tudo idênticas.

Isto mesmo exibimos na tabela seguinte:

p	a	q	b	r	c	$p \wedge q \rightarrow r$	$u(a, b, c)$
0		0		0		1	
0		0		1		1	
⋮		⋮		⋮		⋮	
1		1		0		0	
1		1		1		1	

Note-se, porém, que fórmulas diferentes podem corresponder à mesma função u, como é o caso das fórmulas $p \wedge q \rightarrow r$ e $p \rightarrow q \rightarrow r$. No entanto, duas tais fórmulas são sempre logicamente equivalentes (porquê?).

13.1 Definição Uma **função booleana** n-ária ($n \geq 0$) é uma função $u : \{0, 1\}^n \rightarrow \{0, 1\}$.[69] Se ϕ é uma fórmula de $\mathcal{L}^0$ onde ocorrem exactamente n letras proposicionais, digamos p_1, ..., p_n, a função booleana **associada** a ϕ é a

[68] As monografias de BRIDGES, de EPSTEIN & CARNIELLI, ou de BOOLOS, BURGESS & JEFFREY constituem excelentes introduções à moderna teoria da computabilidade.

[69] Recorde-se que para qualquer conjunto X e qualquer natural $n \geq 0$, $X^n = X \times \cdots \times X$ (n factores) e que, por convenção, $X^0 = \{\emptyset\}$, $X^1 = X$.

função booleana n-ária u_ϕ definida por

$$u_\phi(a_1, ..., a_n) = v(\phi), \quad \text{para qualquer valoração } v \text{ tal que } v_i(p_i) = a_i \text{ para } i = 1, ..., n.$$

Note-se que u_ϕ está bem definida, pois $v(\phi)$ só depende dos valores $v(p_i)$ para os p_i que ocorrem em ϕ (exercício 2.3). São particularmente importantes as funções booleanas correspondentes aos conectivos proposicionais, quer dizer, mais exactamente, correspondentes às fórmulas $\neg p_1$, $p_1 \wedge p_2$, $p_1 \vee p_2$, $p_1 \rightarrow p_2$, que se denotam $u_\neg$, $u_\wedge$, $u_\vee$, $u_\rightarrow$ respectivamente.

Existem, também, duas funções booleanas unárias, u_0 (ou $u_\perp$, ver adiante) e u_1, definidas por $u_0(\emptyset) = 0$, $u_1(\emptyset) = 1$, respectivamente. Observe-se, por outro lado, que se ϕ é uma fórmula onde ocorrem exactamente n letras proposicionais, digamos p_1, ..., p_n, a função booleana associada u_ϕ é única, como se viu acima, mas diferentes fórmulas (logicamente equivalentes) podem ter a mesma função booleana associada.

Devemos ainda observar que se u é uma função booleana n-ária e $m > n$, então existem funções booleanas m-árias u' que tomam exactamente os mesmos valores que u nos primeiros n argumentos a_1, ..., a_n desta: basta que u' não dependa realmente de a_{n+1}, ..., a_m, isto é, que para quaisquer a_1, ..., $a_m \in \{0, 1\}$ se tenha

$$u'(a_1, ..., a_n, a_{n+1}, ..., a_m) = u(a_1, ..., a_n)$$

Mais interessante é a questão seguinte, de que nos ocuparemos a seguir:

(Q_2) Dada uma função booleana ao arbítrio u, existe uma fórmula ϕ tal que u é a função booleana associada a ϕ, u_ϕ, isto é, tal que $u = u_\phi$?

Antes de dar a resposta a esta questão vamos reformulá-la em termos de *conectivos generalizados*. A partir dos primitivos $\neg$, $\wedge$, $\vee$ e $\rightarrow$, outros conectivos se podem definir, como já fizémos com $\leftrightarrow$ (ver exercício 2.19). Na realidade, podemos ter, em princípio, conectivos n-ários para qualquer $n \geq 0$, quer primitivos quer definidos.

Um conectivo 0-ário muito do agrado dos lógicos intuicionistas (Cap. V) e mesmo de alguns tratadistas de lógica clássica é o conectivo $\perp$ (*absurdo*) que, a nível sintáctico, é encarado tal como se fosse uma letra proposicional (modificando, em conformidade, a cláusula F_1 na definição de fórmula de $\mathcal{L}^0$) e, semanticamente, é suposto ter o valor lógico $v(\perp) = 0$ para qualquer valoração v. Intuitivamente, $\perp$ denota uma falsidade absoluta, incondicional. Podemos, então, definir

$$\neg\phi = \phi \rightarrow \perp .$$

Mais geralmente, podemos supor que no alfabeto de $\mathcal{L}^0$ está um (ou mais) conectivo n-ário Π, com $n \geq 1$ ao arbítrio, redifinindo a noção de fórmula de $\mathcal{L}^0$ para acomodar expressões da forma $\Pi\phi_1...\phi_n$ como fórmulas, se ϕ_1, ..., ϕ_n são fórmulas [ou $(\phi\Pi\psi)$, no caso de Π ser binário] e estipulando que,

semanticamente, a tabela de verdade de Π é a tabela correspondente a uma função booleana n-ária dada u (ou u_Π):

ϕ_1	ϕ_2	$\cdots$	ϕ_n	$\Pi\phi_1\phi_2\cdots\phi_n$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
a_1	a_2	$\cdots$	a_n	$u(a_1, a_2, ..., a_n)$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$

Dizemos que Π é o **conectivo generalizado n-ário associado a** (ou **determinado por**) u e podemos, querendo, designá-lo por Π_u.

Por exemplo, o conectivo ternário de *maioria* é o conectivo # com a tabela da seguinte. Observe-se que $\#\phi\psi\theta$ tem o valor 1 quando e só quando a maioria das componentes ϕ, ψ, θ tem o valor 1.

	ϕ	ψ	θ	$\#\phi\psi\theta$
1.	0	0	0	0
2.	0	0	1	0
3.	0	1	0	0
4.	0	1	1	1
5.	1	0	0	0
6.	1	0	1	1
7.	1	1	0	1
8.	1	1	1	1

A questão anterior, de saber se toda a função booleana u é a função booleana associada a alguma fórmula (da linguagem $\mathcal{L}^0$ primitiva), pode ser agora reformulada como a questão de saber se todo o conectivo generalizado pode ser definido a partir dos primitivos $\neg$, $\wedge$, $\vee$, $\rightarrow$.

A resposta é afirmativa, o que nos diz, também, que do ponto de vista expressivo da lógica proposicional clássica nada se ganha de essencial em possuír mais conectivos primitivos do que aqueles. Na realidade, eles nem são todos necessários (na lógica clássica).

13.2 Metateorema da completude funcional (MCF)

Para toda a função booleana n-ária ($n \geq 1$) u existe, pelo menos, uma fórmula ϕ de $\mathcal{L}^0$, contendo apenas os conectivos $\neg$, $\wedge$, $\vee$, tal que $u = u_\phi$.

Dem. Seja u uma função booleana n-ária ($n \geq 1$) qualquer. Há dois casos a considerar.

Caso 1. Para quaisquer valores lógicos a_i $(1 \leq i \leq n)$, $u(a_1, ..., a_n) = 0$. Neste caso toma-se para ϕ a fórmula contraditória

$$(p_1 \wedge \neg p_1) \vee (p_2 \wedge \neg p_2) \vee ... \vee (p_n \wedge \neg p_n).$$

Caso 2. Existe, pelo menos, um n-uplo de valores lógicos $(a_1, ..., a_n)$ onde u toma o valor 1. Numerando estes n-uplos onde u toma o valor 1,

$$(a_1^1, ..., a_n^1), (a_1^2, ..., a_n^2), ..., (a_1^k, ..., a_n^k)$$

(onde $1 \leq k \leq 2^n$ para certo k), ponhamos, para todo $j = 1, ..., k$ e todo $i = 1, ..., n$,

$$P_i^j = \begin{cases} p_i & \text{se } a_i^j = 1 \\ \neg p_i & \text{se } a_i^j = 0 \end{cases}.^{70}$$

De seguida definamos

$$\phi_i = P_1^j \wedge ... \wedge P_n^j \text{ para } j = 1, ..., k,$$

e, finalmente, ponhamos

$$\phi = \phi_1 \vee \phi_2 \vee ... \vee \phi_k.$$

Resta verificar, o que deixamos como exercício, que $u_\phi = u$, isto é, que a função booleana dada u é a função booleana associada à fórmula ϕ construída na demonstração.■

13.3 Exemplo Particularizando à função booleana u asociada ao conectivo ternário # acima considerado, que toma o valor 1 nas linhas 4, 6, 7 e 8, formamos as fórmulas

$$\phi_1 = \neg p_1 \wedge p_2 \wedge p_3, \quad \phi_2 = p_1 \wedge \neg p_2 \wedge p_3,$$
$$\phi_3 = p_1 \wedge p_2 \wedge \neg p_3, \quad \phi_4 = p_1 \wedge p_2 \wedge p_3,$$

e, finalmente,

$$\phi = \phi_1 \vee \phi_2 \vee \phi_3 \vee \phi_4.$$

Tem-se, então, $u_\phi = u$, e podemos afirmar que ϕ e $\#p_1p_2p_3$ são logicamente equivalentes, já que têm sempre os mesmos valores lógicos para as mesmas atribuições de valores lógicos às letras proposicionais p_1, p_2, p_3.■

Mais geralmente, se Π é um conectivo generalizado determinado por uma função booleana u, Π pode ser definido a partir dos conectivos $\neg$, $\wedge$, $\vee$, no sentido seguinte:

---

70 Letras proposicionais ou suas negações são chamadas *literais*.

13.4 Corolário

Para todo o conectivo generalizado n-ário ($n \geq 1$) Π, existe, pelo menos, uma fórmula ϕ de $\mathcal{L}^0$ com n letras proposicionais e os conectivos $\neg$, $\wedge$, $\vee$ tal que $u_\phi = u_\Pi$.■

13.5 Corolário

Para toda a fórmula ψ de $\mathcal{L}^0$ existe, pelo menos, uma fórmula ϕ com as mesmas letras proposicionais que ψ e somente os conectivos $\neg$, $\wedge$, $\vee$ tal que ϕ e ψ são logicamente equivalentes.

Dem. ψ tem uma função booleana associada u_ψ cuja aridade é o número de letras proposicionais que ocorrem em ψ. Pelo metateorema de completude funcional, obtemos ϕ com as mesmas letras proposicionais que ψ tal que $u_\phi = u_\psi$, ou seja, tal que ψ e ϕ têm os mesmos valores lógicos para as mesmas atribuições.■

Por virtude do metateorema de completude funcional (ou qualquer um dos corolários anteriores) dizemos que o conjunto $\{\neg, \wedge, \vee\}$ é **funcionalmente completo** (para a lógica proposicional clássica[71]). No exercício 2.20 estuda-se a possibilidade de economizar ainda mais.

Uma consequência adicional importante da demonstração do metateorema da completude funcional é o facto de ela fornecer *formas normais* para as fórmulas de $\mathcal{L}^0$.

A fórmula ϕ construída na demonstração do (MCF) é uma disjunção de conjunções de literais (ver Nota 70), que se diz estar na **forma normal disjuntiva**:

(FND) $$\bigvee_{j=1}^{k} \bigwedge_{i=1}^{n} P_i^j,$$

onde cada P_i^j é uma *literal* p_i ou $\neg p_i$. Uma demonstração (como exercício) análoga à que foi feita, mas trabalhando com as linhas onde a função booleana dada u toma os valores 0 permitiria construir ϕ' na chamada **forma normal conjuntiva**:

(FNC) $$\bigwedge_{j=1}^{k} \bigvee_{i=1}^{n} P_i^j .$$[72]

Temos, assim, justificação suficiente para concluir o

---

[71] A qualificação é necessária pois, para a lógica proposicional intuicionista, o referido conjunto não é funcionalmente completo.

[72] No caso de a função booleana u ter sempre o valor 1, a forma normal conjuntiva é a conjunção das disjunções $p_i \vee \neg p_i$ para $i = 1, ..., n$. Observe-se, por outro lado, que estamos pondo em prática a convenção de escrita de associação da direita para a esquerda (pág. 48), segundo a qual $\bigwedge_{i=1}^{n} \phi_i = \phi_1 \wedge \phi_2 \wedge \ldots \wedge \phi_n$ é uma abreviatura de $\phi_1 \wedge (\phi_2 \wedge \ldots (\phi_{n-1} \wedge \phi_n)\ldots)$. Analogamente para as disjunções.

13.6 Corolário (Formas normais)
Toda a fórmula de $\mathcal{L}^0$ é logicamente equivalente a uma fórmula na forma normal disjuntiva e a uma fórmula na forma normal conjuntiva.■

Regressando ao exemplo do conectivo ternário # acima (valor 0 nas linhas 1, 2, 3 e 5), obtemos a fórmula equivalente na FNC seguinte:

$$(p_1 \vee p_2 \vee p_3) \wedge (p_1 \vee p_2 \vee \neg p_3) \wedge (p_1 \vee \neg p_2 \vee p_3) \wedge (\neg p_1 \vee p_2 \vee p_3).$$

Todavia, muitas vezes é mais prático utilizar equivalências lógicas conhecidas para obter formas normais para uma dada fórmula ϕ do que recorrer à demonstração do metateorema da completude funcional. Escrevamos

$$\phi \sim \psi$$

para significar que ϕ e ψ são logicamente equivalentes, quer dizer,

$$\phi \sim \psi \text{ sse } \vDash \phi \leftrightarrow \psi$$

Observe-se (exercício) que $\sim$ é uma relação de equivalência no conjunto das fórmulas (e não um conectivo). Tem-se, por exemplo,

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

e esta última já está na forma normal conjuntiva (uma só componente conjuntiva, $k = 1$).

Em geral, dada uma fórmula qualquer, ϕ, para obter uma equivalente numa forma normal pode-se proceder sistematicamente do seguinte modo:

• substituir, se necessário, subfórmulas da forma $\psi \leftrightarrow \theta$ por $(\psi \rightarrow \theta) \wedge (\theta \rightarrow \psi)$, e $\psi \rightarrow \theta$ por $\neg\psi \vee \theta$, respectivamente — isto produz uma equivalente ϕ' sem ocorrências de $\leftrightarrow$, $\rightarrow$;

• substituir, se necessário, subfórmulas da forma $\neg\neg\psi$, $\neg(\psi \wedge \theta)$, $\neg(\psi \vee \theta)$ por ψ, $\neg\psi \vee \neg\theta$, $\neg\psi \wedge \neg\theta$, respectivamente, e repetir a operação até obter uma equivalente ϕ'' em que $\neg, \wedge, \vee$ se apliquem somente a letras proposicionais;

• utilizar as leis associativas e distributivas para obter equivalentes na FND ou FNC, conforme pretendido, e simplificar o resultado, eliminando das disjunções componentes da forma $p \wedge \neg p$ e eliminando das conjunções componentes da forma $p \vee \neg p$.

13.7 Fórmulas de Horn São muito importantes nas ciências da computação as fórmulas na FNC de um tipo particular, chamadas *fórmulas de Horn* (em homenagem ao lógico americano Alfred Horn que primeiro as identificou e estudou). Dizemos de uma literal que é *positiva* ou *negativa* conforme é uma letra proposicional ou uma negação de letra proposicional. Uma **fórmula de Horn** é então uma fórmula na FNC tal que cada disjunção contém, quando muito, uma literal positiva.

Por exemplo, $p \wedge (\neg q \vee r) \wedge \neg p$ é uma fórmula de Horn, mas $p \wedge (\neg q \vee \neg r) \wedge \neg p$ não é.

Mostramos a seguir que a pesquisa da compatibilidade de fórmulas de Horn é extraordinariamente eficiente em comparação com a construção de tabelas de verdade. Na realidade, basta fazer a pesquisa numa única linha! Este método é conhecido por *algoritmo da compatibilidade das fórmulas de Horn,* e consiste basicamente no seguinte:

Seja $\phi = \phi(p_1, ..., p_n) = \bigwedge_{j=1}^{k} \psi_j = \bigwedge_{j=1}^{k} \bigvee_{i=1}^{n} P_i^j$ uma fórmula de Horn contendo apenas as letras proposicionais p_1, ..., p_n. Cada $\psi_j = \bigvee_{i=1}^{n} P_i^j$ $(1 \leq j \leq k)$ é uma disjunção de literais e é chamada uma *componente disjuntiva* de ϕ. Começamos por dispor estas letras e ϕ como no cabeçário de uma tabela de verdade para ϕ, mas deixando espaço para uma única linha:

p_1	p_2	...	p_n	ϕ
		...		

I Etapa. A primeira coisa a fazer é verificar se alguma (algumas) p_j é uma componente disjuntiva da conjunção, por si mesma (isto é, a componente disjuntiva $\psi_j = \bigvee_{i=1}^{n} P_i^j$ reduz-se a p_j); nos casos afirmativos, colocamos "1" na coluna j respectiva e, por baixo de ϕ, também colocamos 1's ou 0's debaixo das posições onde se encontre p_j ou $\neg p_j$, respectivamente.

Por exemplo, se $\phi = p \wedge (q \vee \neg r) \wedge (\neg p \vee \neg r)$, o resultado após esta primeira etapa do algoritmo é:

p	q	r	$p \wedge (q \vee \neg r) \wedge (\neg p \vee \neg r)$
1			1 0

II Etapa. Em seguida, tentamos completar o máximo possível a tabela, atribuindo 1's ou 0's, conforme o caso, a todas as outras letras nas diferentes componentes disjuntivas (ocorrências positivas) que permitam atribuir o valor 1 a essas componentes, não perdendo de vista que estamos tentando obter uma valoração que satisfaça a fórmula de Horn dada. O algoritmo termina quando não for possível continuar este procedimento.

No exemplo dado, tendo atribuído o valor 1 a q, de modo a obter o valor 1 para a segunda componente $(q \vee \neg r)$, obtemos:

(1)

p	q	r	$p \wedge (q \vee \neg r) \wedge (\neg p \vee \neg r)$
1	1		1 1 0

Se, ao invés, tivéssemos atribuído o valor 0 a r, com vista a tornar verdadeira a segunda e a terceira disjunção, obteríamos

(2)

p	q	r	$p \wedge (q \vee \neg r) \wedge (\neg p \vee \neg r)$
1		0	1 1 0 1

No caso (1) ainda podemos prosseguir e atribuir a r o valor 0, de modo a tornar verdadeira a última disjunção, ficando

(2′)

p	q	r	$p \wedge (q \vee \neg r) \wedge (\neg p \vee \neg r)$
1	1	0	1 1 1 0 1 .

Já se vê, em (2), que não é necessário continuar, pois as três componentes disjuntivas são verdadeiras (qualquer que seja o valor a atribuir a q). Mas ainda não se vê isso em (1). Atribuindo a q o valor 1, obtemos

(1′)

p	q	r	$p \wedge (q \vee \neg r) \wedge (\neg p \vee \neg r)$
1	1	0	1 1 1 0 1 ,

e agora sim, já terminou a pesquisa, com a certeza de que a fórmula dada é compatível.

Vejamos outro exemplo, com $\phi = p \wedge (\neg q \vee \neg p) \wedge q$. Após a primeira etapa do algoritmo obtemos

p	q	$p \wedge (\neg q \vee \neg p) \wedge q$
1	1	1 0 0 1,

e já não há nenhuma solução possível, isto é, nenhuma valoração satisfaz a fórmula, pois a segunda disjunção é forçosamente falsa. A fórmula dada é, portanto, incompatível.

Em geral, quando já não é possível prosseguir na execução da etapa II, atribuindo valores às letras proposicionais de modo a tornar verdadeiras certas componentes disjuntivas (o algoritmo terminou) uma de duas coisas tem de acontecer:

(a) tendo em conta todos os valores possíveis atribuídos às letras proposicionais em jogo, conforme os requisitos das duas etapas, resulta forçosamente o valor 0 para alguma componente disjuntiva: — neste caso, a fórmula dada é incompatível;

(b) alguma atribuição de valores lógicas a algumas ou a todas as letras proposicionais que ocorrem na fórmula faz com que todas as componentes disjuntivas sejam verdadeiras; neste caso a fórmula dada é compatível, e podemos completar a atribuição de valores lógicos às letras proposicionais que ainda não receberam nenhum valor (se algumas houver) de maneira arbitrária — por exemplo, só com 0's, para fixar ideias.

O leitor pode nesta altura resolver alguns exercícios [2.25(c)] e ficar intuitivamente convencido que o algoritmo é *correcto,* isto, produz sempre e exactamente o resultado que é suposto produzir, nomeadamente, testar e classificar correctamente, para qualquer fórmula de Horn dada, se ela é ou não compatível. Isto pode e deve ser demonstrado. Damos de seguida uma ideia dademonstração.

13.8 Correcção do algoritmo (compatibilidade das fórmulas de Horn)

Seja dada ao arbítrio uma fórmula de Horn, ϕ. Ou ϕ é compatível ou não é, mas o que interessa é saber como o algoritmo de comporta relativamente a ϕ.

Se ϕ é realmente compatível, o algoritmo classifica ϕ como tal, pois a única maneira de resultar para ϕ o valor 0 (e, portanto, ϕ ser incompatível) é sermos «forçados» a isso quando nenhuma atribuição às letras proposicionais que ocorrem em ϕ satisfaz esta fórmula (o que é impossível, pois ϕ é compatível, por hipótese).

Falta mostrar que, reciprocamente, se o algoritmo classifica ϕ como compatível, isto é, se não somos «forçados» a dar a ϕ o valor 0 (pelo facto de alguma componente disjuntiva ter de ser falsa), então ϕ é realmente compatível. Ora ϕ é da forma $\phi = \bigwedge_{j=1}^{k}\psi_j = \bigwedge_{j=1}^{k}\bigvee_{i=1}^{n}P_i^j$ onde, para cada índice j, quando muito uma das literais P_1^j, P_2^j, ..., P_n^j é positiva. Para ϕ ser satisfeita por certa valoração v basta, portanto, que cada componente $\psi_j = \bigvee_{i=1}^{n}P_i^j$ seja satisfeita por v; e, para isto acontecer, basta que uma, pelo menos, das literais P_1^j, P_2^j, ..., P_n seja satisfeita por v, para cada j.

Se a componente ψ_j se reduz a uma letra proposicional, foi-lhe atribuído o valor 1 na primeira etapa do algoritmo; se a componente tem uma literal positiva e também algumas literais negativas, então, ou

(i) cada uma das literais negativas acabou por receber o valor 0 e, neste caso, a única literal positiva tem de ter o valor 1 (conforme execução da etapa II), ou

(ii) durante a execução, o algoritmo atribuiu 0 a uma letra proposicional cuja negação é uma literal que ocorre em ψ_j; neste caso estamos na presença de uma disjunção de literais negativas, mas, como suposemos que ϕ não foi classificada como falsa, uma destas literais negativas nunca recebeu o valor 0 durante a execução do algoritmo, e pôde finalmente receber o valor 1, pois a letra que lhe deu origem recebeu o valor 0:

...	q	...	$\psi_j = \cdots \vee \neg q \vee \cdots$
...	0	...	1

.■

Terminamos esta secção com uma outra consequência do (MCF), que vem confirmar que, excepto em casos especiais, numa tautologia da forma $\phi \rightarrow \psi$, há sempre algo comum a ϕ e ψ que faz a «ponte» de uma a outra.

13.9 Lema de interpolação (LI)

Se $\vDash \phi \rightarrow \psi$*, então*

(i) ϕ *é uma contradição, ou*

(ii) ψ *é válida, ou*

(iii) *existe uma* interpoladora *entre* ϕ *e* ψ*, isto é, uma fórmula* θ *cujas letras proposicionais ocorrem em* ϕ *e em* ψ*, e tal que*

$$\vDash \phi \rightarrow \theta \quad \text{e} \quad \vDash \theta \rightarrow \psi.$$

Dem. Dadas ϕ e ψ, adoptemos, para esta demonstração, as notações seguintes: p_1, ..., p_n são as letras proposicionais que ocorrem simultaneamente em ϕ e em ψ,

q_1, ..., q_m são as letras proposicionais em ϕ mas não em ψ, e r_1, ..., r_k são as exclusivas de ψ. Admitimos que alguns dos inteiros m, n, k possam ser nulos, o que significa que não há que considerar as letras proposicionais respectivas.

Mostramos que, se nem (i) nem (ii), então $n \geq 1$ e tem-se (iii). De facto, se fosse $n = 0$, então existe um modelo v_1 de ϕ (pois ϕ é compatível) e existe uma valoração v_2 tal que $v_2(\psi) = 0$ (pois ψ é inválida). Se v coincide com v_1 em q_1, ..., q_m e com v_2 em r_1, ..., r_k, então $v(\phi) = v_1(\phi) = 1$ e $v(\psi) = v_1(\psi) = 0$, logo $v(\phi \rightarrow \psi) = 0$, contra a hipótese de $\phi \rightarrow \psi$ ser válida. Portanto, $n \geq 1$, quer dizer, há uma letra proposicional, pelo menos, comum a ϕ e ψ. Falta encontrar uma interpoladora.

Definamos uma função booleana n-ária u pondo

$$u(a_1, ..., a_n) = \begin{cases} 1 & \text{se existe } v \text{ tal que } v(p_i) = a_i \text{ para } i = 0, ..., n \text{ e } v(\phi) = 1 \\ 0 & \text{no caso contrário.} \end{cases}$$

Pelo (MCF) existe θ nas letras proposicionais p_1, ..., p_n tal que $u = u_\theta$ e, por construção, $\vDash \phi \rightarrow \theta$. Vejamos que também $\vDash \theta \rightarrow \psi$. Pois seja v ao arbítrio tal que $v(\theta) = 1$, com vista a mostrar que $v(\psi) = 1$. Pondo $a_i = v(p_i)$ para $i = 1, ..., n$, vem $u_\theta(a_1, ..., a_n) = 1$, logo existe v' tal que v' coincide com v nos p_i e $v(\phi) = 1$. E se v'' coincide com v' nos p_i e nos q_j e com v nos r_l, então

$$v''(\phi) = v'(\phi) = 1 \text{ e } v''(\psi) = v(\psi).$$

Mas $\phi \rightarrow \psi$ é válida, por hipótese, logo $v''(\psi) = v(\psi) = 1$.■

Observe-se que a demonstração anterior é *construtiva:* conhecendo apenas a tabela de verdade de ϕ e as letras proposicionais comuns a ϕ e ψ, podemos construir u e, portanto, uma interpoladora θ [no caso (iii)].

*II.14 Compacidade proposicional e aplicações

Mencionemos um outro resultado, com aplicações não triviais em matemática,[73] que se pode demonstrar directamente, de diferentes maneiras, ou como corolário da segunda versão da propriedade de completude semântica generalizada (ver exercício 2.17). As duas aplicações que dele fazemos requerem do leitor um pouco mais de sofisticação matemática do que tem sido o mote neste livro e são, por isso, de leitura opcional.

---

[73] V. o nosso artigo "Sobre os conceitos de verdade em matemática", in *Boletim da Soc. Port. de Mat.*, N. 3-4 (1980). Neste artigo refere-se um sistema dedutivo diferente de **DN**, embora este facto em nada influa na obtenção do metateorema de compacidade ou das suas aplicações. Aí se mostra, também, a ligação do referido metateorema com a topologia, que explica a razão de designação «compacidade».

14.1 Metateorema da compacidade (MC′)

Um conjunto Σ de fórmulas de $\mathcal{L}^0$ é compatível sse todo o subconjunto finito de Σ é compatível.

***Dem.** É claro que se Σ é compatível, então também é compatível qualquer parte de Σ, finita ou infinita. Suponhamos, reciprocamente, que toda a parte finita de Σ é compatível (mas, é claro, diferentes partes finitas podem ter modelos diferentes). Suporemos, para esta demonstração, que as letras proposicionais estão enumeradas: $P = \{p_0, p_1, ...\}$ (ver Nota 40, p. 48).

Uma sequência finita de 0's e 1's, $\langle a_0, a_1, ..., a_n\rangle$, diz-se *prestável* sse para toda a parte finita Σ' de Σ existe um modelo v de Σ' tal que $v(p_i) = a_i$ para $i = 0, ..., n$.

Mostramos que toda a sequência prestável $\langle a_0, a_1, ..., a_n\rangle$ pode estender-se a uma sequência prestável $\langle a_0, a_1, ..., a_n, a_{n+1}\rangle$.

Seja $\langle a_0, a_1, ..., a_n\rangle$ uma sequência prestável ao arbítrio. Ora, ou $\langle a_0, a_1, ..., a_n, 0\rangle$ é prestável, e então nada mais há a fazer, ou não é, o que significa que *existe uma parte finita* Σ_0 *de* Σ *tal que, para todo o modelo* v *de* Σ_0*, se* $v(p_i) = a_i$ *para* $i = 0, ..., n$, *então* $v(p_{i+1}) = 1$. Ponhamos, neste caso, $a_{n+1} = 1$, e mostremos que a sequência $\langle a_0, a_1, ..., a_n, a_{n+1}\rangle = \langle a_0, a_1, ..., a_n, 1\rangle$ é prestável.

Seja Σ' uma parte finita qualquer de Σ, de modo que $\Sigma_0 \cup \Sigma'$ (com Σ_0 como no parágrafo anterior) ainda é uma parte finita de Σ. Como a sequência $\langle a_0, a_1, ..., a_n\rangle$ é prestável, por hipótese, existe um modelo v' de $\Sigma_0 \cup \Sigma'$ tal que $v'(p_i) = a_i$ para $i = 0, ..., n$; mas, como v' é modelo de Σ_0, então é $v'(p_{n+1}) = 1$, o que mostre que Σ' possui um modelo v' tal que $v'(p_i) = a_i$ para $i = 0, ..., n, n + 1$ e, portanto, que $\langle a_0, a_1, ..., a_n, 1\rangle$ é prestável.

Note que a sequência vazia é prestável, atendendo à hipótese sobre Σ, e o argumento anterior adapta-se trivialmente para mostrar que existe a_0 tal que $\langle a_0\rangle$. Resulta do que precede que existe uma sequência infinita de 0's e 1's, $\langle a_0, a_1, ..., a_n, a_{n+1}, ...\rangle$,[74] tal que, para todo n, a sequência $\langle a_0, a_1, ..., a_n\rangle$ é prestável. Definindo v por

$$v(p_i) = a_i, \text{ para } i = 0, 1, ...,$$

é fácil verificar que v é modelo de Σ: se $\phi \in \Sigma$, para n suficientemente grande, todas as letras proposicionais que ocorrem em ϕ estão entre p_0, ..., p_n, e existe um modelo v' de ϕ tal que $v'(p_i) = a_i$ para $i = 0, ..., n$; então v e v' coincidem nas letras proposicionais que ocorrem em ϕ e, portanto, coincidem em ϕ, logo $v(\phi) = 1$.■

---

[74] O processo de definição de $\langle a_0, a_1, \ldots, a_n, a_{n+1}, \ldots\rangle$ é um exemplo de definição por *recorrência,* no qual cada novo valor a_{n+1} depende de todos os valores anteriormente obtidos a_0, a_1, …, a_n. Por outro lado, a demonstração do metateorema de completude semântica generalizado (p. 76) pode ser adaptada para se obter outra demonstração do (MC): substituir «consistente» por «finitamente compatível» (significando que toda a parte finita é compatível).

14.2 O problema do casamento Seja dado um conjunto M de rapazes e um conjunto N de raparigas suas namoradas. O *problema do casamento* é o problema de casar cada rapaz com uma das suas namoradas, sem que seja cometida bigamia.[75] Sob certas condições, o problema é solúvel. O caso finito é contemplado no seguinte resultado (exercício 2.24).

14.3 Lema do casamento
Se M é um conjunto finito de $m \geq 1$ rapazes tal que, para cada $k \leq m$, quaisquer k rapazes dispõem de, pelo menos, k namoradas, então o problema do casamento tem solução.

Trataremos agora do caso infinito, isto é, do caso em que o conjunto dos rapazes e o conjunto das raparigas são infinitos.

14.4 Teorema do casamento
Se M é um conjunto infinito (numerável) de rapazes, cada rapaz tem um número finito de namoradas e, para cada inteiro positivo k, quaisquer k rapazes dispõem de, pelo menos, k namoradas, então o problema do casamento tem solução.

Dem. Seja $M = \{\boldsymbol{r}_0, \boldsymbol{r}_1, ...\}$ o conjunto dos rapazes, $N = \{\boldsymbol{s}_0, \boldsymbol{s}_1, ...\}$ o conjunto das raparigas, e ponhamos

$$P = M \times N = \{(\boldsymbol{r}_i, \boldsymbol{s}_j) \,:\, i \geq 0, j \geq 0\}.$$

Para facilitar a notação, ponhamos $p_{ij} = (\boldsymbol{r}_i, \boldsymbol{s}_j)$ para $i \geq 0$, $j \geq 0$. Consideremos os p_{ij} como letras proposicionais da linguagem proposicional sobre P e, nesta linguagem, os conjuntos de fórmulas

$$\Gamma_1 = \{p_{ii_1} \vee ... \vee p_{ii_n} \,:\, i \geq 0 \text{ e } \boldsymbol{s}_{i_1}, ..., \boldsymbol{s}_{i_n} \text{ são as namoradas de } \boldsymbol{r}_i\},$$
$$\Gamma_2 = \{\neg(p_{ij} \wedge \neg p_{ik}) \,:\, i, j, k \geq 0, j \neq k\},$$
$$\Gamma_3 = \{\neg(p_{ik} \wedge p_{jk}) \,:\, i, j, k \geq 0, i \neq j\}.$$

O significado intuitivo das fórmulas que compõem estes conjuntos é claro, se encararmos p_{ij} como verdadeira sse o rapaz $\boldsymbol{r}_i$ casa com a rapariga $\boldsymbol{s}_j$. Por exemplo, a fórmula

$$p_{22_1} \vee ... \vee p_{22_n}$$

exprime que o rapaz $\boldsymbol{r}_2$ casa com uma das suas namoradas $\boldsymbol{s}_{2_1}$, ..., $\boldsymbol{s}_{2_n}$. As fórmulas de Γ_2 e Γ_3 exprimem que não há bigamia.

---

[75] Para a história deste problema ver P. HALMOS & H. VAUGHAN, "The marriage problem", *Amer. J. Math.* **72** (1950), 214-215.

Para que o problema do casamento tenha solução basta, pois, que o conjunto $\Gamma = \Gamma_1 \cup \Gamma_2 \cup \Gamma_3$ seja compatível e, para isto acontecer, basta, por (MC′), que toda a parte finita de Γ seja compatível. É o que mostramos de seguida.

Seja Γ_0 uma parte finita qualquer de Γ. Em Γ_0 há somente um número *finito* de fórmulas de Γ, nas quais ocorrem ao todo, pois, também um número finito de letras p_{ij}, as quais dizem respeito a um número finito de rapazes, digamos

$$\boldsymbol{r}_{i_1}, ..., \boldsymbol{r}_{i_m}$$

Pelo Lema do Casamento (cujas hipóteses são as mesmas que as do teorema, excepto no que respeita ao número de rapazes), o problema do casamento tem solução para estes rapazes. Feito o casamento destes m rapazes com m raparigas, sem bigamia, *definimos a valoração* v_0 pondo

$$\begin{aligned} v_0(p_{ij}) = 1 \text{ sse } & \text{ o rapaz } \boldsymbol{r}_i \text{ casou com a rapariga } \boldsymbol{s}_j, \\ & \text{para } i = i_1, ..., i_m, j = j_1, ..., j_m, \end{aligned}$$

e $v_0(p_{ij}) = 0$ (este valor é, porém, irrelevante) para os p_{ij} que não ocorrem em fórmulas de Γ_0. Assim dito e feito, facilmente verificamos que todas as fórmulas de Γ_0 são satisfeitas por v_0, isto é, que v_0 é modelo de Γ_0. Portanto, Γ_0 é compatível.

Como acima se disse, Γ é compatível, por compacidade. Falta agora a grande núpcia final. Seja v um modelo de Γ. *Definimos o casamento* da totalidade dos rapazes do seguinte modo:

$$\text{casamos } \boldsymbol{r}_i \text{ com } \boldsymbol{s}_j \text{ sse } v(p_{ij}) = 1.$$

Por v ser modelo de Γ, e atendendo ao que as fórmulas de Γ exprimem, vê-se que o problema do casamento tem solução e o teorema está demonstrado.■

14.5 O problema das quatro cores Chamemos **mapa** a um conjunto M de regiões fechadas (com interior não vazio) do plano euclidiano, duas a duas disjuntas ou adjacentes mas, neste último caso, a parte comum das fronteiras não se reduzindo a pontos isolados. O *problema das quatro cores* é um problema clássico de coloração de mapas: colorir as regiões do mapa utilizando somente 4 cores, mas de tal modo que duas regiões adjacentes recebam cores diferentes. Digamos de uma tal coloração que é *própria*. A *Conjectura de Guthrie*, ou *conjectura das quatro cores*, é a conjectura de que *todo* o mapa finito admite uma coloração própria. Foi formulada por um jovem licenciado da Universidade de Londres em 1852, Francis Guthrie, que a passou a seu irmão Frederick, estudante de Física, que por sua vez a passou ao seu mestre A. De Morgan. De Morgan mostrou facilmente que 3 cores não são suficientes, e também mostrou (mais difícil) que não é possível 5 regiões de um mapa estarem numa posição tal que cada uma delas seja adjacente às outras quatro, mas quanto à conjectura... passou-a aos seus discípulos e colegas. Arthur Cayley fez publicar a conjectura nos *Proceedings* da Sociedade Matemática de Londres em 1878 e, desde então, muitos matemáticos investiram na tentativa de

resolver a conjectura. Finalmente, em 1976, após quatro anos de labor intenso e mais de 1200 horas de cálculo num super-computador, dois jovens matemáticos da Universidade de Ilinnois, nos E.U.A., anunciaram[76] ter demonstrado o

14.6 Teorema das quatro cores (caso finito)
Todo o mapa planar finito admite uma coloração própria.

Pela primeira vez na história da matemática, partes substanciais e cruciais de uma demonstração (?) foram realizadas por um computador, utilizando ideias formuladas durante e como consequência do próprio decurso da computação. A validade e legitimidade da demonstração foram questionadas por alguns críticos, já que repousava ou parecia repousar na *crença* de que o programa utilizado fazia exactamente o que os seus autores haviam projectado. Assim, um novo tipo de argumentação matemática parece ter nascido: a análise da correcção de um programa computacional. Em todo o caso, e dando o teorema das quatro cores como provado, no caso finito, provaremos a versão infinita do mesmo:

14.7 Teorema das quatro cores (caso infinito)
Todo o mapa infinito (numerável) $M = \{R_0, R_1, ...\}$ *admite uma coloração própria*.

Dem. Designemos as quatro cores por 1, 2, 3 e 4 e consideremos a linguagem proposicional cujas letras proposicionais são

$$p_{ij}, \text{ para todo } i \geq 0, 1 \leq j \leq 4.$$

Pensemos nos conjuntos de fórmulas

$$\Gamma_1 = \{p_{i1} \vee p_{i2} \vee p_{i3} \vee p_{i4} \,:\, i \geq 0\},$$
$$\Gamma_2 = \{p_{ij} \rightarrow \neg p_{ik} \,:\, i \geq 0, 1 \leq j \leq 4, 1 \leq k \leq 4, j \neq k\},$$
$$\Gamma_3 = \{p_{ik} \rightarrow \neg p_{jk} \,:\, i, j \geq 0, 1 \leq k \leq 4, R_i \text{ e } R_j \text{ são adjacentes}\}.$$

Se interpretarmos intuitivamente p_{ij} como verdadeira sse a região R_i recebe a cor j, as fórmulas do conjunto $\Gamma = \Gamma_1 \cup \Gamma_2 \cup \Gamma_3$ exprimem que o mapa M admite uma coloração própria. Para demonstrar o teorema basta mostrar, pois, que o conjunto Γ é compatível e *definir a coloração* a partir de um modelo v de Γ do

[76] K. APPEL & W. HAKEN, "Every planar map is four colorable", *Bull. Amer. Math. Soc.* **82** (1976), 711-712; "The solution of the four-color-map problem", *Scientific American*, vol. **237** (1977), 108-121. Sobre o assunto ver também o livrinho de E. B. DYNKIN & V.A. USPENSKI, *Multicolor Problems*, Heath & Co., 1963 e o Cap. 7 de K. DEVLIN, *Mathematics: The New Golden Age*, Penguin Books, 1988. Para um tratamento matemático mais detalhado ver T. L. SAATY & P. C. KAINEN, *The Four Colour Problem*, McGraw-Hill, 1977.

seguinte modo:

$$R_i \text{ recebe a cor } j \text{ sse } v(p_{ij}) = 1.$$

Para mostrar que Γ é compatível basta mostrar que toda a parte finita de Γ é compatível e aplicar o metateorema da compacidade. É o que fazemos de seguida.

Seja Γ_0 uma parte finita qualquer de Γ. Nas fórmulas de Γ_0 há não mais do que um número finito de letras p_{ij}, as quais dizem respeito a um número *finito* de regiões e formam, portanto, um mapa finito, digamos

$$M_0 = \{R_{i_1}, ..., R_{i_m}\}.$$

Pelo teorema das quatro cores no caso finito, este mapa admite uma coloração própria. *Definimos a valoração* v_0 pondo

$$v_0(p_{ij}) = 1 \text{ sse } R_i \text{ recebeu a cor } j, \text{ para } i = i_1, ..., i_m,\ 1 \leq j \leq 4,$$

e $v_0(p_{ij}) = 0$ nos outros casos (na ralidade, estes outros valores de v_0 são irrelevantes). Facilmente se pode concluir que v_0 (ou melhor, a valoração booleana correspondente $\widehat{v}_0$) satisfaz todas as fórmulas de Γ_0, logo este conjunto é compatível. Por exemplo, se a fórmula $p_{ij} \rightarrow \neg p_{ik}$ está em Γ_0, então a região R_i está em M_0; se esta região recebeu a cor j, então não recebeu nenhuma outra cor, logo $v_0(p_{ij}) = 1$ e $v_0(p_{ik}) = 0$ para todo $k \neq j$, donde $\widehat{v}_0(p_{ij} \rightarrow \neg p_{ik}) = 1$.■

*II.15 Introdução às Álgebras de Boole

A utilização de leis lógicas ou tautologias notáveis (como as leis distributivas, as leis de De Morgan, etc.) permite manipular «algebricamente» as fórmulas para obter fórmulas logicamente equivalentes, utilizando a transitividade da relação de equivalência lógica: se $\phi \sim \psi$ e $\psi \sim \theta$, então $\phi \sim \theta$.

Já vimos um exemplo de tal manipulação na pág. 89. Outro exemplo:

$$\begin{aligned} p \rightarrow (q \rightarrow r) \sim & \quad \neg p \vee (q \rightarrow p) \sim \neg p \vee (\neg q \vee r) \\ \sim & \quad (\neg p \vee \neg q) \vee r \sim \neg(p \wedge q) \vee r \sim (p \wedge q) \rightarrow r. \end{aligned}$$

A sistematização e desenvolvimento deste procedimento é um dos aspectos característicos da chamada «lógica algébrica», que trata do estudo da lógica do ponto de vista algébrico, e foi iniciada em meados do séc. XIX por G. Boole (1815-1864) e continuada por A. De Morgan (1806-1871), C. S. Pierce (1839--1914) e outros. Já nos nossos dias o assunto foi retomado com grande fôlego por A. Lindenbaum (jovem matemático polaco falecido em 1941, durante o cerco de Varsóvia), A. Tarski. P. Halmos, D. Monk e também o nosso António Aniceto Monteiro. Nesta secção fazemos uma breve introdução a algumas questões pertinentes neste tipo de abordagem da lógica, no que respeita à lógica proposicional clássica.

A primeira coisa a fazer é considerar os conectivos (ou conectivas) proposicionais como operações algébricas no conjunto $F = \text{Form}(\mathcal{L}^0)$. Quer dizer,

vamos encarar F como uma «álgebra», na qual distinguimos as seguintes operações: as operações binárias usuais de disjunção ($\vee$), conjunção ($\wedge$), uma operação unária de negação ($\neg$), e duas constantes ou operações 0-árias menos familiares, $\bot$ e T (secção II.12). Intencionalmente, T representa uma fórmula válida (sempre verdadeira) e $\bot$ uma contradição (sempre falsa).

À estrutura

$$\mathfrak{F} = (F,\ \vee,\ \wedge, \neg,\ \bot\ , \mathsf{T}),$$

chamamos **álgebra das fórmulas** de $\mathcal{L}^0$. Outra estrutura do mesmo tipo que $\mathfrak{F}$ é a **álgebra dos valores lógicos**

$$\mathfrak{B}_0 = (B_0,\ +\ ,\ \cdot\ ,\ -\ , 0, 1),$$

onde $B_0 = \{0, 1\}$ é o conjunto dos valores lógicos e $+$, $\cdot$, $-$ são as operações usuais sobre valores lógicos correspondentes às tabelas de $\vee$, $\wedge$ e $\neg$, respectivamente:

$$\begin{gathered} 0 + 0 = 0, \quad 0 + 1 = 1 + 0 = 1 + 1 = 1; \\ 0 \cdot 0 = 0 \cdot 1 = 1 \cdot 0 = 0, \quad 1 \cdot 1 = 1; \\ -0 = 1, \quad -1 = 0. \end{gathered}$$

Note-se que alguns autores preferem as notações «$a \vee b$» e «$a \wedge b$» a «$a + b$» e «$a \cdot b$», respectivamente, e neste caso

$$\mathfrak{B}_0 = (B_0,\ \vee,\ \wedge, -, 0, 1).$$

Por outro lado, a operação unária $-\,: B_0 \to B_0$ é usualmente chamada *complementação*, e $-a$ é o *complemento* de a.

As valorações booleanas $\widehat{v} : F \to B_0$ são, como sempre, determinadas pelas valorações $v : P \to B_0$, mas como agora se consideram os símbolos $\bot$ e T como elementos de P estipulamos $v(\bot) = 0$ e $v(\mathsf{T}) = 1$. Como, para quaisquer fórmulas ϕ, ψ se tem

$$\begin{aligned} &\widehat{v}(\phi \vee \psi) = \widehat{v}(\phi) + \widehat{v}(\psi), \quad &&\widehat{v}(\phi \wedge \psi) = \widehat{v}(\phi) \cdot \widehat{v}(\psi), \\ &\widehat{v}(\neg\phi) = 1 - \widehat{v}(\phi), &&\widehat{v}(\bot) = 0, \quad \widehat{v}(\mathsf{T}) = 1, \end{aligned}$$

podemos dizer, utilizando a terminologia algébrica usual, que uma valoração booleana é um **homomorfismo sobrejectivo** (ou **epimorfismo**) $\widehat{v} : \mathfrak{F} \to \mathfrak{B}_0$.

A relação $\sim$ em F é uma relação de equivalência. As classes de equivalência modulo $\sim$ são os conjuntos de fórmulas da forma

$$[\phi] = \{\psi \in F\ : \psi \sim \phi\}$$

Em particular, $[\bot]$ é o conjunto das contradições, enquanto $[\mathsf{T}]$ é o conjunto das fórmulas válidas ou tautologias de $\mathcal{L}^0$. O conjunto quociente $F/_{\sim}$ é o conjunto das classes de equivalência modulo $\sim$, que resulta de F «identificando» fórmulas

logicamente equivalentes:

$$[\phi] = [\psi] \text{ sse } \phi \sim \psi.$$

Em homenagem a G. Frege, a quem se devem várias distinções pertinentes na teoria das linguagens formais, é costume chamar **proposições** às classes de equivalência modulo $\sim$. A distinção fregeana, neste caso, é entre o objecto sintáctico que é a fórmula ϕ e a proposição ou significado da fórmula. Diferentes fórmulas podem ser logicamente equivalentes, possuindo todas elas, pois, o mesmo significado, dando assim origem a uma só proposição — a classe de equivalência de ϕ modulo $\sim$ [77]. Assim, o conjunto quociente $F/_\sim$ é o **conjunto das proposições**.

Põe-se naturalmente a questão de «algebrizar» o conjunto das proposições de modo a obter uma «álgebra de proposições» do mesmo tipo que $\mathfrak{F}$ e $\mathfrak{B}_0$. Tal é possível, por um processo familiar aos algebristas, a *passagem ao quociente* das operações $\vee$, $\wedge$ e $\neg$, atendendo a que a relação $\sim$ é uma congruência com respeito àquelas operações: para quaisquer fórmulas ϕ, ψ, θ e χ, se $\phi \sim \theta$ e $\psi \sim \chi$, então

$$\phi \vee \psi \sim \psi \vee \chi, \quad \phi \wedge \psi \sim \psi \wedge \chi, \quad \neg\phi \sim \neg\theta.$$

Deixamos a verificação destes factos como outros tantos exercícios. Deste modo, ficam bem definidas as operações em $F/_\sim$ seguintes:

$$[\phi] \,\widetilde{\vee}\, [\psi] = [\phi \vee \psi], \quad [\phi] \,\widetilde{\wedge}\, [\psi] = [\phi \wedge \psi],$$
$$\widetilde{\neg}\, [\phi] = [\neg\phi], \quad \widetilde{\bot} = [\,\bot\,], \quad \widetilde{\mathsf{T}} = [\mathsf{T}\,].$$

Com estas definições obtém-se a **álgebra das proposições** ou **álgebra de Lindenbaum** de $\mathcal{L}^0$,

$$\mathfrak{L}_0 = (F/_\sim, \widetilde{\vee}, \widetilde{\wedge}, \widetilde{\neg}, \widetilde{\bot}, \widetilde{\mathsf{T}}).$$

Por abuso, esperando que o leitor saiba interpretar bem o contexto, continuaremos a utilizar os símbolos habituais $\vee$, $\wedge$, $\neg$, $\bot$, T em vez de $\widetilde{\vee}$, $\widetilde{\wedge}$, $\widetilde{\neg}$, $\widetilde{\bot}$, $\widetilde{\mathsf{T}}$. Examinemos as propriedades algébricas desta estrutura.

Os elementos de $\mathfrak{L}_0$ satisfazem certas identidades, como

$$a \vee b = b \vee a, \; a \wedge a = a, \; a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c),$$

e muitas outras vêm imediatamente à ideia. Para verificar qualquer delas, por exemplo, a primeira, podemos proceder do seguinte modo: supondo $a = [\phi]$,

---

[77] Estamos simplificando muito o que é, na realidade, uma teoria bastante elaborada. Para melhor esclarecimento ver a *Introdução* (68 páginas!) da monografia de A. CHURCH, *Introduction to Mathematical Logic I*, Princeton Univ. Press, 1956. (O volume II desta obra nunca chegou a ser publicado.)

$b = [\psi]$, tem-se

$$a \vee b = [\phi] \vee [\psi] = [\phi \vee \psi] = [\psi \vee \phi] = [\psi] \vee [\phi] = b \vee a.$$

Seria interessante poder conhecer $\mathfrak{L}_0$ através da especificação de *todas* as identidades válidas entre os seus elementos. Tarefa impossível, pois existem infinitas tais identidades! Mas talvez seja possível *caracterizá-las* de alguma maneira «finitária»...

A resolução deste problema pode ser feita de diferentes maneiras. Começamos por mostrar que este problema é equivalente a um problema do mesmo género relativo à álgebra dos valores lógicos, $\mathfrak{B}_0$.

15.1 Metateorema

As identidades válidas em $\mathfrak{L}_0$ são exactamente as mesmas que as válidas em $\mathfrak{B}_0$.

Antes de tentar demonstrar este resultado devemos tornar preciso o seu enunciado, nomeadamente, precisando os conceitos de «identidade» e de «identidade válida em $\mathfrak{L}_0$» (ou em $\mathfrak{B}_0$, ou em qualquer outra estrutura do mesmo tipo, isto é, com duas operações binárias, uma unária e dois elementos fixos). Estes conceitos, e o resultado em questão, pertencem à chamada *lógica equacional*, um ramo particularmente simples da lógica de primeira ordem com igualdade, a estudar no Cap. III. Todavia, as ideias básicas são suficientemente simples e naturais para anteciparmos (informalmente) alguns aspectos, os suficientes para se entender o enunciado e a sua demonstração.

Chamemos **identidade** a toda a igualdade da forma

$$s = t,$$

onde s e t são expressões designatórias ou *termos* construídos de acordo com as regras seguintes:

(i) as variáveis a, b, c, ... (possivelmente com índices) e as constantes $\bot$ e T são termos;

(ii) se s e t são termos, então $(s \vee t)$, $(s \wedge t)$ e $(-s)$ são termos;

(iii) nada mais é termo.

Trata-se, como é óbvio, de uma definição indutiva de *termo*, utilizando os símbolos operatórios " $\vee$ ", " $\wedge$ " preferivelmente a " $+$ " e " $\cdot$ ", respectivamente. Os parênteses podem ser omitidos, se não houver possibilidade de confusão na leitura dos termos. Por exemplo,

$$((a \vee b) \wedge c) = ((a \wedge c) \vee (b \wedge (-c)))$$

é uma identidade, que se abrevia

$$(a \vee b) \wedge c = (a \wedge c) \vee (b \wedge -c).$$

Será muito conveniente a notação

(*) $$s(a, b, ...) = t(a, b, ...)$$

para representar uma identidade entre os termos $s(a, b, ...)$ e $t(a, b, ...)$ construídos, de acordo com a definição, utilizando as variáveis a, b, ...

Seja $\mathfrak{B} = (B, \vee, \wedge, -, \bot, \top)$ uma estrutura do mesmo tipo que $\mathfrak{L}_0$. Dizemos que uma identidade (*) é **válida em** $\mathfrak{L}_0$ sse resultar de (*) uma igualdade verdadeira sempre que às variáveis a, b, ... forem dados valores no domínio ou suporte B de $\mathfrak{B}$ e os símbolos operatórios que ocorrem em $s(a, b, ...)$ ou em $t(a, b, ...)$ forem interpretados da maneira natural.

Por exemplo, a identidade

$$a \vee b = b \vee a,$$

que acima se mostrou ser válida em $\mathfrak{L}_0$, é também válida em $\mathfrak{B}_0 = (B_0, +, \cdot, -, 0, 1)$: quaisquer que sejam os valores em B_0 atribuídos a a e b, obtém-se uma igualdade verdadeira, como se pode verificar exaustivamente:

$$0 + 0 = 0 + 0, \quad 0 + 1 = 1 + 0,$$
$$1 + 0 = 0 + 1, \quad 1 + 1 = 1 + 1.$$

Ao invés, a identidade $(a \vee b) \wedge c = (a \wedge c) \vee (b \wedge -c)$ do exemplo de construção não é válida em $\mathfrak{B}_0$: tem-se o contra-exemplo

$$(0 + 1) \cdot 1 \neq (0 \cdot 1) + (1 \cdot -1)$$

Para a demonstração do metateorema necessitamos de alguns resultados preliminares.

15.2 Lema

Se h é um homomorfismo de $\mathfrak{L}_0$ em $\mathfrak{B}_0$ e $t(a, b, ...)$ é um termo, então, para quaisquer fórmulas ϕ, ψ, ...

$$ht([\phi], [\psi], ...) = t(h[\phi], h[\psi], ...).^{78}$$

Dem. Exercício, por indução na complexidade dos termos.■

15.3 Lema

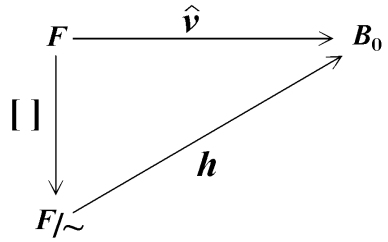
Para toda a valoração booleana $\widehat{v} : \mathfrak{F} \to \mathfrak{B}_0$ existe um único epimorfismo $h : \mathfrak{L}_0 \to \mathfrak{B}_0$ tal que, para toda a fórmula ϕ, $\widehat{v}(\phi) = h[\phi]$.

Dem. Muito simples: dada $\widehat{v}$, defina-se h pondo $h[\phi] = \widehat{v}(\phi)$ (ver diagrama seguinte). h está bem definido, quer dizer, $h[\phi]$ só depende de $[\phi]$ e não do

---

[78] Escrevemos ht em vez de $h(t)$, por vezes, para simplificar a notação.

representante ϕ, e é claramente um epimorfismo. A unicidade é também óbvia, já que h é determinado por $\widehat{v}$.■



Este lema já permite demonstrar uma parte do metateorema 15.1: as identidades válidas $\mathfrak{B}_0$ são válidas em $\mathfrak{L}_0$. Pois suponhamos a identidade

$$s(a, b, ...) = t(a, b, ...)$$

válida em $\mathfrak{B}_0$, e sejam ϕ, ψ, ... fórmulas quaisquer, com vista a provar que a igualdade

$$s([\phi], [\psi], ...) = t([\phi], [\psi], ...)$$

é verdadeira em $\mathfrak{L}_0$. Ora, tanto $s([\phi],[\psi],...)$ como $t([\phi],[\psi],...)$ são elementos de $F/_\sim$, isto é, são classes de equivalência, digamos

$$[\theta_1] = s([\phi], [\psi], ...),\ [\theta_2] = t([\phi], [\psi], ...),$$

para certas fórmulas θ_1, θ_2.[79] Queremos mostrar que $[\theta_1] = [\theta_2]$, isto é, que $\theta_1 \sim \theta_2$, ou seja, que para toda a valoração booleana v, $v(\theta_1) = v(\theta_2)$.

Tem-se, com efeito, para qualquer valoração booleana v, tomando h como no lema 15.3,

$$\begin{aligned}
v(\theta_1) = h[\theta_1] \quad &= hs([\phi], [\psi], ...) \\
&= s(h[\phi], h[\psi], ...) && \text{pelo lema 2} \\
&= s(v(\phi), v(\psi), ...) && \text{pelo lema 3} \\
&= t(v(\phi), v(\psi), ...) && \text{pois } s = t \text{ em } \mathfrak{B}_0 \\
&= t(h[\phi], h[\psi], ...) \\
&= ht([\phi], [\psi], ...) \\
&= h[\theta_2] = v(\theta_2),
\end{aligned}$$

o que demonstra uma parte do metateorema. Para demonstrar a outra parte utiliza-se o resultado seguinte.

---

[79] De facto, pode-se tomar para θ_1 a fórmula $s(\phi, \psi, \dots)$, e analogamente para θ_2.

15.4 Lema
Para todo o epimorfismo $h : \mathfrak{L}_0 \to \mathfrak{B}_0$, *se* $v : P \to B_0$ *é definida por* $v(p_i) = h[p_i]$, $v(\bot) = 0$ *e* $v(\mathsf{T}) = 1$, *então* v *estende-se a uma valoração booleana* $\widehat{v}$ *tal que* $\widehat{v}(\phi) = h[\phi]$, *para toda a fórmula* ϕ.

Dem. Exercício, por indução na complexidade das fórmulas.■

Outro exercício finaliza a demonstração do metateorema 1.■

Uma álgebra

$$\mathfrak{B} = (B, \vee, \wedge, -, \bot, \mathsf{T})$$

[ou $\mathfrak{B} = (B, \vee, \wedge, -, 0, 1)$, ou ainda $\mathfrak{B} = (B, +, \cdot, -, 0, 1)$ — para cada gosto a sua notação, desde que subentendido que B é um conjunto com, pelo menos, dois elementos 0 e 1, etc.] que valida exactamente as mesmas identidades que $\mathfrak{L}_0$ (ou $\mathfrak{B}_0$, como vimos) diz-se uma **álgebra de Boole**. Em particular, $\mathfrak{B}_0$ é a álgebra de Boole dita *matriz* ou *minimal*. Veremos de seguida uma outra maneira de obter álgebras de Boole.

Seja I um conjunto não vazio, $\mathcal{P}(I)$ o conjunto das partes ou subconjuntos de I, e consideremos em $\mathcal{P}(I)$ as operações de união $\cup$, intersecção $\cap$ e complementação com respeito a I, que denotamos simplesmente $-$; considerando ainda os conjuntos $\emptyset$ e I, como objectos distintos de B, obtemos a **álgebra dos subconjuntos** (ou **das partes**) **de** I,

$$\mathfrak{P}_I = (\mathcal{P}(I), \cup, \cap, -, \emptyset, I).$$

Mais geralmente, em vez de $\mathcal{P}(I)$ podemos considerar uma parte $B \subseteq \mathcal{P}(I)$ fechada para $\cup$, $\cap$ e complementação relativa, tal que $\emptyset \in B$ e $I \in B$. Uma estrutura assim definida,

$$\mathfrak{B} = (B, \cup, \cap, -, \emptyset, I),$$

diz-se uma **álgebra de conjuntos** (sobre I).

15.5 Teorema
Toda a álgebra de conjuntos é uma álgebra de Boole.

Dem. Mostramos, apenas, que toda a identidade válida em $\mathfrak{B}_0$ é válida em $\mathfrak{P}_I$. Definamos, para cada $i \in I$, $h_i : \mathcal{P}(I) \to B_0$ por

$$h_i(X) = 1 \text{ sse } i \in X.$$

Cada h_i é um homomorfismo de $\mathfrak{P}_I$ em $\mathfrak{B}_0$ (exercício) e, para quaisquer X, $Y \in \mathcal{P}(I)$, tem-se

$$X = Y \text{ sse para todo } i \in I,\ h_i(X) = h_i(Y).$$

Supondo $s(a, b, ...) = t(a, b, ...)$ válida em $\mathfrak{B}_0$, bastará ver que, para quaisquer $X, Y \in \mathcal{P}(I)$,

$$\text{para todo } i \in I,\ h_i s(X, Y, ...) = h_i t(X, Y, ...).$$

Tem-se, de facto, para cada $i \in I$,

$$\begin{aligned} h_i s(X, Y, ...) &= s(h_i(X), h_i(Y), ...), && \text{por } h_i \text{ ser homomorfismo,} \\ &= t(h_i(X), h_i(Y), ...), && \text{por } s = t \text{ ser válida em } \mathfrak{B}_0, \\ &= h_i t(X, Y, ...), && \text{por } h_i \text{ ser homomorfismo.}\blacksquare \end{aligned}$$

Um homomorfismo bijectivo $h : \mathfrak{B}_1 \to \mathfrak{B}_2$ entre duas álgebras do mesmo tipo diz-se um **isomorfismo**. Pode-se demonstrar (mas a demonstração sai fora do âmbito deste curso) o seguinte

*15.6 Teorema de representação de Stone

Toda a álgebra de Boole é isomorfa a uma álgebra de conjuntos.

Isto quer dizer, por outras palavras, que as álgebras de conjuntos são as álgebras de Boole típicas. A álgebra de conjuntos minimal sobre um conjunto não vazio I é a álgebra de Boole

$$\mathfrak{P}_0 = (\{\emptyset, I\},\ \cup\ ,\ \cap\ ,\ -\ , \emptyset, I),$$

que é isomorfa a $\mathfrak{B}_0$. $\mathfrak{P}_I$ é, por outro lado, a álgebra de conjuntos (portanto, de Boole) maximal sobre I. Não demonstramos o teorema de representação de Stone mas demonstramos o seguinte, como melhor aproximação:

15.7 Teorema

A álgebra de Lindenbaum $\mathfrak{L}_0$ é isomorfa a uma álgebra de conjuntos.

Dem. Seja $\widehat{V}$ o conjunto de todas as valorações booleanas $\widehat{v} : F \to B_0$. Façamos corresponder a cada classe $[\phi] \in F/_\sim$ o conjunto $\overline{\phi} = h[\phi]$ das valorações $\widehat{v} \in \widehat{V}$ que satisfazem ϕ. Fica como exercício mostrar que a função $h : F/_\sim \to \mathcal{P}(\widehat{V})$ assim definida é o isomorfismo procurado.■

A definição de álgebra de Boole que foi dada é de pouca utilidade ou conveniência prática (embora importante do ponto de vista da motivação histórica), visto que a quantidade e variedade de identidades válidas em $\mathfrak{B}_0$ é infinita! O procedimento típico de um matemático numa situação como esta é, como Euclides tentou fazer com a geometria há dois mil e trezentos anos atrás, o de tentar *axioma-*

tizar as identidades válidas em $\mathfrak{B}_0$, isto é, procurar de entre elas um pequeno número (os axiomas ou postulados), e montar um *cálculo* dedutivo, de tal modo que todas as outras se possam deduzir logicamente a partir daquelas primeiras. Deste modo, embora não possamos enumerar todas as identidades válidas de uma vez só, podemos montar um sistema que vai permitir gerá-las uma a uma; se o sistema estiver bem montado e tivermos escolhido bem os axiomas, todas elas e só elas serão mais cedo ou mais tarde geradas pelo sistema. O resultado das pesquisas que foram feitas no sentido indicado permitiu concluir que as identidades seguintes (na notação $+$, $\cdot$, $-$, 0, 1 — é simples rotina transcrever para outra notação) são suficientes para o fim em vista. Elas são chamadas, naturalmente, os *axiomas das álgebras de Boole*. Quanto às regras do cálculo dedutivo, elas são simplesmente as propriedades e regras lógicas da igualdade (reflexividade, simetria, transitividade e substituibilidade de iguais por iguais em termos), a estudar mais em pormenor no Cap. III.

O leitor pode ensaiar (mas não é imediato!) uma demonstração da equivalência entre as duas definições propostas de álgebra de Boole:

(i) uma álgebra $\mathfrak{B}$ que valida exactamente as mesmas identidades que $\mathfrak{B}_0$;

(ii) uma álgebra $\mathfrak{B}$ não qual são válidas as 11 identidades acima.

AXIOMAS DAS ÁLGEBRAS DE BOOLE

$$
\begin{array}{ll}
a+(b+c)=(a+b)+c, & a\cdot(b\cdot c)=(a\cdot b)\cdot c,\\
a+b=b+a, & a\cdot b=b\cdot a,\\
a+(b\cdot c)=(a+b)\cdot(a+c), & a\cdot(b+c)=(a\cdot b)+(a\cdot c),\\
a+0=a, & a\cdot 1=a,\\
a+(-a)=1, & a\cdot(-a)=0,
\end{array}
$$

$$0\neq 1.$$

Utilizando a álgebra de Lindenbaum $\mathfrak{L}_0$ e o teorema de representação de Stone é possível dar uma outra demonstração, inteiramente algébrica, do metateorema de completude semântica para o sistema **DN**.[80] Para tal, porém, é mais conveniente uma outra axiomatização da lógica proposicional (ver II.18).

*II.16 Outros sistemas dedutivos (I): *tableaux* semânticos

Dissemos acima (pág. 47) que iríamos apresentar outros sistemas dedutivos, alternativos ao sistema de dedução natural para $\mathcal{L}^0$. O primeiro a ser aqui apresentado é o sistema **BP**, ou simplesmente **B**, dos *tableaux semânticos de Beth* (1955), que constitui um método para examinar sistematicamente as possibilidades

[80] Pode-se consultar uma tal prova nos capítulos iniciais de BELL & SLOMSON. Sobre álgebras de Boole veja-se também o Cap. 5 de STOLL, ou o livrinho de P. HALMOS, *Lectures on Boolean Algebras*, Springer-Verlag, 1977.

de uma fórmula dada tomar os valores lógicos 0 ou 1 e, como tal, também pode ser considerado um método alternativo ao das tabelas de verdade, e um tanto mais eficiente que este. A construção de um *tableau* para uma fórmula proposicional composta ϕ é feita indutivamente, à custa de *tableaux* para as componentes de ϕ. Cada *tableau* é uma árvore binária (ver secção I.12), cujos *nós* ou *entradas* são *fórmulas valoradas*, isto é, expressões de uma das formas $V\phi$, $F\phi$, que exprimem intuitivamente «ϕ é verdadeira», «ϕ é falsa», respectivamente.

Os *tableaux atómicos* são os *tableaux* seguintes, dois para letras proposicionais ou átomos e dois para cada conectivo principal (incluindo $\leftrightarrow$).

TABLEAUX ATÓMICOS

1a.	Vp	1b.	Fp
2a.	$V\neg\phi$ | $F\phi$	2b.	$F\neg\phi$ | $V\phi$
3a.	$V(\phi\wedge\psi)$ | $V\phi$ | $V\psi$	3b.	$F(\phi\wedge\psi)$ $\wedge$ $F\phi \quad F\psi$
4a.	$V(\phi\vee\psi)$ $\wedge$ $V\phi \quad V\psi$	4b.	$F(\phi\vee\psi)$ | $F\phi$ | $F\psi$
5a.	$V(\phi\rightarrow\psi)$ $\wedge$ $F\phi \quad V\psi$	5b.	$F(\phi\rightarrow\psi)$ | $V\phi$ | $F\psi$
6a.	$V(\phi\leftrightarrow\psi)$ $\wedge$ $V\phi \quad F\phi$ | | $V\psi \quad F\psi$	6b.	$F(\phi\leftrightarrow\psi)$ $\wedge$ $V\phi \quad F\phi$ | | $F\psi \quad V\psi$.

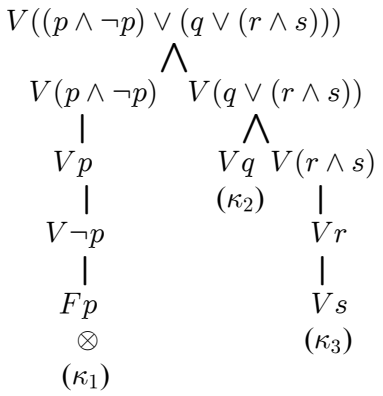
Por exemplo, em 4a, a fórmula valorada $V(\phi \vee \psi)$ *ramifica-se* nas valoradas $V\phi$ e $V\psi$ — a ramificação significa «ou»; em 5b, a fórmula valorada $F(\phi \rightarrow \psi)$ dá origem à *sequência* $V\phi$ e $F\psi$ — sequência significa «e». Nestes e nos outros casos observa-se uma conformidade com o significado intuitivo dos conectivos e respectivas tabelas de verdade.

Antes de dar a definição geral de *tableau* semântico para uma fórmula valorada arbitrária damos um exemplo, para a fórmula valorada

$$V((p \wedge \neg p) \vee (q \vee (r \wedge s))).$$

Esta fórmula valorada será colocada no topo ou raiz, desdobrando-se de cima para baixo de acordo com os *tableaux* atómicos, até que cada ramo termine com uma fórmula atómica valorada.

16.1 Exemplo



Neste exemplo há 3 ramos (κ_1, κ_2 e κ_3). O ramo mais à esquerda, κ_1, é *contraditório,* e por isso foi também assinalado com $\otimes$, o que significa que tem duas entradas que se contradizem (no caso, Vp e Fp). Os outros dois ramos não são contraditórios. Que conclusão podemos tirar do *tableau* acima?

Podemos concluir que a fórmula $(p \wedge \neg p) \vee (q \vee (r \wedge s))$ é verdadeira sob certas condições, nomeadamente, quando q é verdadeira (ramo κ_2), ou quando r e s são ambas verdadeiras (ramo κ_3). Podemos ainda encarar a construção do *tableau* como uma *tentativa sistemática para satisfazer a fórmula dada,* a qual, finalmente, teve sucesso. Analogamente, um *tableau* com raiz $F\phi$ pode-se encarar como uma *tentativa para falsificar a fórmula* ϕ. Uma e outra destas tentativas consideram-se falhadas se, no final, todos os ramos forem contraditórios; no caso da raiz $V\phi$, isto significa que é impossível satisfazer a fórmula e, portanto, ela é incompatível; e no caso da raiz $F\phi$, significa que é impossível falsificar a fórmula dada e, por isso, ela é válida. É essencialmente por esta última razão que o método dos *tableaux* semânticos de Beth constitui um sistema dedutivo equivalente ao sistema de dedução natural — tal como este, o método de Beth permite derivar todas as fórmulas válidas, e somente fórmulas válidas, como veremos —, e, além

disso, fornece um método de decisão alternativo e mais eficiente do que o método das tabelas de verdade. É altura de dar algumas definições rigorosas.

16.2 Definição (1) Um ***tableau*** semântico é uma árvore binária de fórmulas valoradas, também chamadas as **entradas** do *tableau*, satisfazendo as seguintes regras indutivas:

(i) os *tableaux* atómicos são *tableaux* finitos;

(ii) se T é um *tableau* finito, κ um ramo de T e X uma entrada em κ, e T' resulta de T apensando o único *tableau* atómico com raiz X no nó terminal de κ, então T' é um *tableau* finito.[81]

(iii) Se T_0, T_1, ..., T_n, ... é uma sucessão finita ou infinita de *tableaux* tal que, para cada $n \geq 0$, T_{n+1} é construído a partir de T_n por aplicação de (ii), então $T = \bigcup_{n\geq 0} T_n$ é um *tableau*.

(2) uma entrada X diz-se **reduzida** (**usada** ou **marcada)** num dado ramo κ de um *tableau* sse X for a raiz de um *tableau* atómico de tal modo que todas as entradas num ramo através daquele *tableau* atómico ocorrem em κ, e diz-se **não reduzida** no caso contrário;

(3) um ramo de um *tableau* diz-se **contraditório** sse contiver as entradas $V\phi$ e $F\phi$, para certa fórmula ϕ, e diz-se **não contraditório**, no caso contrário;

(4) um *tableau* diz-se **terminado** (ou **completo**[82]) sse nenhum dos seus ramos não contraditórios tiver nós não usados, caso contrário diz-se **não terminado**;

(5) um *tableau* diz-se **contraditório** sse todos os seus ramos forem contraditórios, e no caso contrário diz-se **não contraditório**.

16.3 Algoritmo de construção indutiva dos *tableaux* completos

Constrói-se um *tableau* semântico para uma fórmula ϕ procedendo por etapas, do seguinte modo:

Etapa inicial (ou etapa 0): coloca-se uma fórmula valorada, $V\phi$ ou $F\phi$, como raiz;

Supondo construído um *tableau* T_n na etapa n, estende-se T_n a um *tableaux* T_{n+1} na etapa seguinte, reduzindo certas entradas de T_n (que não voltarão a ser reduzidas):

Etapa $n+1$*:* de entre todos os níveis de T_n contendo entradas não reduzidas, escolhe-se o que estiver mais próximo da raiz de T_n e, neste nível, escolhe-se a entrada não reduzida mais à esquerda, digamos X; cada ramo não contraditório

---

[81] Chama-se a atenção para o facto de, em princípio, a entrada X ser reinserida por baixo do nó terminal de κ. Acontece que no cálculo proposicional esta *reinserção* pode ser dispensada na prática, mas no sistema de *tableaux* para o cálculo de predicados ela é mesmo indispensável.

[82] Nesta secção tomamos «terminado» e «completo» como sinónimos, mas não será assim na secção 12 do Cap. III.

que passa por X estende-se acrescentando à entrada terminal do ramo o sucessor ou sucessores de um tableau atómico com raiz X.

A construção termina quando todo o ramo não contraditório já não tiver entradas não reduzidas, e o *tableau* construído é

$$T = \bigcup_{n\geq 0} T_n,$$

onde T_n é o tableau construído na etapa n. Observe-se que todo o T_n é finito.

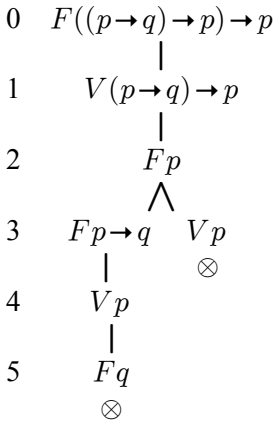
Embora a definição acima contemple tableaux infinitos, acontece que no caso da lógica proposicional todos os tableaux assim construídos são finitos — o algoritmo acima termina sempre com a produção de um tableau completo e finito $T = \bigcup_{n\geq 0} T_n = \bigcup_{n=0}^{m} T_n$, para certo m suficientemente grande. Este facto é intuitivamente plausível, uma vez que cada nível tem um número finito de entradas e cada entrada é reduzida mais tarde ou mais cedo, uma única vez, resultando sempre em fórmulas valoradas de menor complexidade lógica (menos conectivos), até chegarmos a fórmulas atómicas valoradas, a partir das quais é impossível reduzir mais. Voltaremos a esta questão a seguir à definição seguinte e alguns exemplos.

16.4 Definição Uma **derivação à Beth** de uma fórmula ϕ é um *tableau* completo e contraditório com raiz $F\phi$; ϕ diz-se **derivável à Beth**, ou **derivável-B** sse existir uma derivação à Beth de ϕ, e escreve-se neste caso

$$\vdash_{\mathbf{B}} \phi.$$

Uma **refutação à Beth** de ϕ é um *tableau* completo e contraditório com raiz $V\phi$; ϕ diz-se **refutável à Beth**, ou **refutável-B** sse existir uma refutação à Beth de ϕ.

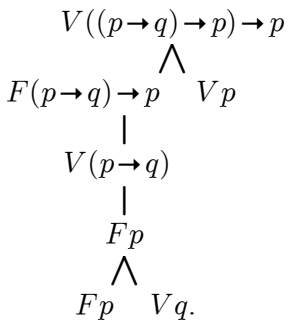
16.5 Exemplos Aplicamos o algoritmo acima na construção de dois *tableaux* para a chamada *lei de Peirce* $((p\to q)\to p)\to p$.



Este *tableau* é contraditório, o que quer dizer que a tentativa de falsificar a lei de Peirce falhou — ela é derivável à Beth (e válida, como sabíamos). Numerámos

os níveis de 1 a 5, numa coluna à esquerda, para melhor se observar a aplicação do algoritmo: na etapa inicial apenas se escreve o nível 0 (raiz); na etapa 1 resultam os níveis 1 e 2, usando a entrada na raiz; o nível 3 resulta da etapa 2, usando a única entrada não reduzida no nível 1.

Façamos agora a tentativa para satisfazer a mesma fórmula:



Aqui não há ramos contraditórios: a fórmula não é refutável à Beth (ela é compatível, como já sabíamos).

Retomemos a questão da possibilidade de *tableaux* infinitos que, pelo menos no caso das derivações, parece chocar com a ideia de que uma dedução, derivação ou demonstração deve ser essencialmente um objecto finito, «visualizável», ao menos em princípio.

É o lema de König que nos vem reconfortar a este respeito.

16.6 Metateorema dos *tableaux* contraditórios (MTC)

Se $T=\bigcup_n T_n$ *é um* tableau *contraditório, então* T_m *é um* tableau *contraditório, para algum* m. *Em particular, toda a derivação à Beth é um* tableau *finito*.

Dem. Recordemos, para começar, que T é uma árvore de ramificação finita. Pensemos no conjunto de todas as entradas de T sem predecessores contraditórios (quer dizer, dada ao arbítrio uma entrada de T, no ramo em que ela está, e nela e acima dela não há duas entradas contraditórias, isto é, da forma $V\theta$ e $F\theta$). Se este conjunto é infinito, então ele constitui uma árvore T' «contida» em T que também é de ramificação finita, logo, pelo lema de König (p. 39), tem um ramo infinito, digamos κ'. É claro que κ' é não contraditório e também é um ramo de T, o que contradiz o facto de todo o ramo em T ser contraditório. Portanto, o tal conjunto de entradas T' é finito e, consequentemente, tais entradas estão todas em níveis $\leq$ que certo nível n de T. Isto quer dizer que toda a entrada de nível $n+1$ de T é contraditória com alguma predecessora de nível inferior, ou há dois predecessores dela que são contraditórios. Assim, existe m tal que T e T_m coincidem até ao nível $n+1$, inclusive. Ora, todo o ramo κ em T_m é um ramo em T (terminando numa entrada de nível $\leq n$) ou contém uma entrada de nível $n+1$. No 1.º caso, κ é contraditório, por hipótese sobre T. No 2.º caso, κ é contraditório, por escolha de n e m. Assim, T_m é o *tableau* finito e contraditório pretendido.

Em particular, se $T = \bigcup_n T_n$ é uma derivação construída de acordo com o algoritmo acima e m é o mínimo possível tal que T_m é contraditório, então T_m já não pode ser estendido em mais nenhuma etapa da construção de T, e portanto $T = T_m$ é finito.■

Devemos agora encetar as provas das propriedades de validade ($\vdash_{\mathbf{B}} \phi \Rightarrow \models \phi$) e de completude semântica ($\models \phi \Rightarrow \vdash_{\mathbf{B}} \phi$) do sistema de Beth, das quais resultará que

$$\vdash_{\mathbf{B}} \phi \Leftrightarrow \vdash_{\mathbf{DN}} \phi,$$

embora esta última equivalência também pudesse ser estabelecida directamente.

Recorde-se que a definição de *tableaux* é indutiva, o que sugere imediatamente a possibilidade de uma indução nos *tableaux,* ou melhor, no seu comprimento, entendendo por *comprimento* de um *tableaux* o número de *tableaux* atómicos utilizados na sua construção. Deixamos ao cuidado do leitor a formulação de um tal princípio de indução nos *tableaux,* pois estamos certos que não terá dificuldade de maior se atender ao seguinte exemplo de demonstração da propriedade dos *tableaux*

$\Phi(T)$: o número de nós de T é maior ou igual ao número de ramos.

Se T é atómico é imediato, por simples inspecção. Suponhamos (hipótese de indução) que o número de nós de T é maior ou igual ao número de ramos, e seja T' o resultado de estender T com um *tableaux* atómico (conforme o algoritmo indicado na pág. 109). Se o nó terminal deste é $V\neg\phi$ ou $F\neg\phi$, o número de nós aumenta uma unidade, mas o número de ramos permanece o mesmo. Nos outros casos, há sempre, pelo menos, mais dois nós e não mais de dois ramos novos, pelo que a relação $\geq$ entre nós e ramos se mantém.

16.7 Definição Seja κ um ramo de um *tableau* T, $K = \{N_1, N_2, ..., N_k\}$ o conjunto das entradas em κ, onde cada N_i é uma fórmula valorada: para cada i, $N_i = V\phi$, ou $N_i = F\phi$, para alguma fórmula ϕ. Dizemos que uma valoração booleana v **concorda** com o ramo κ sse para todo $i = 1, 2, ..., k$,

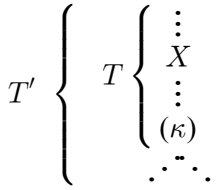
$$N_i = V\phi \Rightarrow v\phi = 1,\ N_i = F\phi \Rightarrow v\phi = 0.$$

16.8 Lema básico

Se uma valoração booleana v concorda com a raiz de um tableau *(isto é, $v\phi = 1$ se a raiz é $V\phi$, e $v\phi = 0$ se a raiz é $F\phi$), então v concorda com algum ramo do* tableau.

Dem. Por indução nos *tableaux.* A propriedade é obviamente verdadeira para *tableaux* atómicos. Suponhamos que ela é verdadeira para T, e seja T' uma extensão T com um *tableau* atómico com raiz X, no final de um ramo κ de T,

conforme o algoritmo na pág. 109.



Há dois casos a considerar.

Caso 1: v concorda com todos os nós em κ; então v concorda com X e, portanto (examine os *tableaux* atómicos a este respeito!), concorda com um dos ramos (possivelmente há um só ramo na continuação de κ) do *tableau* atómico com raiz X. Então existe um ramo κ_1 de T' que assim estende κ, com o qual v concorda.

Caso 2: v não concorda com κ, mas concorda com a raiz de T (caso contrário não haveria nada para provar). Por hipótese de indução, existe outro ramo κ' de T com o qual v concorda. Mas κ' também é ramo de T', logo neste caso também há um ramo de T' com o qual v concorda.■

16.9 Metateorema da validade (MV)

*Se ϕ é derivável-***B**, *então ϕ é válida:* $\vdash_{\mathbf{B}} \phi \Rightarrow \vDash \phi$.

Dem. Por contraposição. Suponhamos que $\nvDash \phi$. Então existe v tal que $v\phi = 0$, logo, pelo lema básico, v concorda com algum ramo κ de qualquer *tableau* com raiz $F\phi$ que seja construído, e portanto um tal ramo é não contraditório, o que prova que ϕ não é derivável-**B**.■

16.10 Lema de Hintikka

Seja κ um ramo não contraditório de um tableau completo T. Se v é uma valoração booleana tal que

$$v(p) = \begin{cases} 1 & \text{se } Vp \text{ é uma entrada em } \kappa \\ 0 & \text{no caso contrário,} \end{cases}$$

então v concorda com o ramo κ.

Este lema fornece um algoritmo para a obtenção de um contra-exemplo para a pretensa validade de certa fórmula ϕ: construindo um *tableau* completo com raiz $F\phi$, se ele é contraditório, então ϕ é realmente válida, mas se o *tableau* exibir um ramo não contraditório κ, o lema mostra como construir uma valoração booleana que falsifica ϕ. Antes da demonstração, vejamos num exemplo concreto de como isto funciona.

16.11 Exemplo Determinar v tal que $v((p \to q) \leftrightarrow (p \vee q)) = 0$.

$$
\begin{array}{c}
F((p \to q) \to (p \vee q)) \\
| \\
V(p \to q) \\
| \\
F(p \vee q) \\
\bigwedge \\
Fp \quad\quad Vq \\
| \quad\quad\ | \\
Fp \quad\quad Fp \\
| \quad\quad\ | \\
Fq \quad\quad Fq \\
(\kappa_1) \quad\quad \otimes \\
\quad\quad\ (\kappa_2)
\end{array}
$$

Aplicando o lema ao único ramo não contraditório, κ_1, definimos v tal que $vp = vq = 0$ **(**não interessam os valores lógicos dos restantes átomos), e então tem-se $v((p \to q) \leftrightarrow (p \vee q)) = 0$.

Dem. Por indução nas fórmulas que entram em κ como fórmulas valoradas.

(i) Se p é um átomo e Vp é uma entrada em κ, então $vp = 1$ e v concorda com κ; se Fp é uma entrada em κ, então Vp não o é, pois κ não é contraditório, logo $vp = 0$.

(ii) Admitamos a propriedade verdadeira para ϕ e para ψ. Se $V(\phi \wedge \psi)$ é uma entrada em κ, então, como T é completo, esta entrada foi reduzida alguma vez e a sequência

$$
\begin{array}{c}
V\phi \\
| \\
V\psi
\end{array}
$$

faz parte de κ, de modo que $V\phi$ e $V\psi$ são entradas em κ. Por hipótese de indução, $v\phi = 1$ e $v\psi = 1$, logo $v(\phi \wedge \psi) = 1$. Se $F(\phi \wedge \psi)$ é uma entrada em κ, então, como T é completo, esta entrada foi reduzida alguma vez e um dos ramos da ramificação

$$
\begin{array}{cc}
\multicolumn{2}{c}{\bigwedge} \\
F\phi & F\psi
\end{array}
$$

faz parte de κ, quer dizer, ou $F\phi$ ou $F\psi$ é uma entrada de κ. Em qualquer dos casos, por hipótese de indução tem-se $v\phi = 0$ ou $v\psi = 0$, conforme o caso, e portanto $v(\phi \wedge \psi) = 0$.

Os casos dos restantes conectivos são deixados como outros tantos exercícios.■

16.12 Metateorema da completude semântica (MCS)

*Se ϕ é válida, então ϕ é derivável-***B**: $\vDash \phi \Rightarrow \vdash_{\mathbf{B}} \phi$. *Além disso, todo o* tableau *completo com raiz $F\phi$ é uma derivação à Beth de ϕ.*

Dem. Se ϕ é válida, então $v\phi = 1$ para toda a valoração booleana v. Suponhamos, com vista a um absurdo, que ϕ não é derivável-**B**. Construamos um tableau completo com raiz $F\phi$ (por exemplo, usando o algoritmo). Um tal *tableau* tem, pelo menos, um ramo não contraditório. O lema de Hintikka mostra como construir uma valoração booleana v que concorda com este ramo e, em particular, com a sua raiz $F\phi$, isto é, $v\phi = 0$, o que é absurdo. Portanto, ϕ é derivável-**B**.■

Este resultado, e o lema em que se baseia, fornecem um *método de decisão* para a validade de fórmulas proposicionais: se tentamos construir (pelo algoritmo) um *tableau* completo com raiz $F\phi$, ou conseguimos uma derivação à Beth (e neste caso a fórmula é válida), ou não conseguimos, mas neste caso será por existir nesse *tableau* um ramo não contraditório, o qual, pelo lema, nos permite obter uma valoração que falsifica ϕ e, portanto, temos a certeza de que ϕ não é válida.

Os resultados anteriores para a derivabilidade à Beth e a validade possuem correspondentes para a refutabilidade à Beth e a compatibilidade, respectivamente, com justificações semelhantes, *mutatis mutandis:*[83]

ϕ é refutável-**B** sse ϕ é incompatível.

16.13 *Tableaux* com hipóteses

Finalizamos esta secção com uma breve discussão da *derivabilidade (à Beth) com hipóteses:* $\Sigma \vdash_{\mathbf{B}} \phi$, onde Σ é um conjunto arbitrário (finito ou infinito) de fórmulas, $\Sigma = \{\psi_0, \psi_1, ..., \psi_m\}$ ou $\Sigma = \{\psi_0, \psi_1, ..., \psi_m, ...\}$, a que chamamos *hipóteses*. A única diferença para a definição de derivabilidade que foi dada ($\vdash_{\mathbf{B}} \phi$, pág. 110) é que, na construção de *tableaux*, agora chamados *tableaux com hipóteses em* Σ, é permitido entrar fórmulas valoradas da forma $V\psi$, onde ψ é uma hipótese. Na definição de *tableau* (pág. 109), a claúsula (ii) desdobra-se em duas, (ii_1) como (ii), e a seguinte:

(ii_2) Se T é um tableau finito com hipóteses em Σ e $\psi \in \Sigma$, então o *tableau* que se forma entrando $V\psi$ no término de cada ramo não contraditório que não contenha $V\psi$ é um *tableau* finito com hipóteses em Σ.

É claro que o algoritmo de construção de *tableaux* (pág. 109) terá uma etapa correspondente a esta claúsula: desdobram-se as etapas a seguir à inicial em etapas pares e ímpares, reservando as pares para este efeito. Por outro lado, na definição de *tableau* completo com hipóteses em Σ, entende-se que existe uma entrada com $V\psi$ em cada ramo não contraditório, para cada hipótese ψ. Assim, o algoritmo resulta sempre num tableau completo.

---

[83] Expressão latina que significa «mudando o que deve ser mudado».

No exemplo da página seguinte escrevemos apenas as entradas da árvore, e não as linhas das sequências ou ramificações.

Os resultados anteriores conducentes às propriedades de validade e de completude semântica estendem-se imediatamente (com as modificações pertinentes) à derivabilidade com hipóteses.

• Assim, por exemplo, no enunciado do Lema Básico para *tableaux* com hipóteses, há que supor que a valoração satisfaz todas as hipóteses.

• Na demonstração do metateorema da validade generalizado ($\Sigma \vdash_{\mathbf{B}} \phi \Rightarrow \Sigma \vDash \phi$), supondo que ϕ não é consequência de Σ, existe v que satisfaz todas as hipóteses mas não satisfaz ϕ, e a demonstração prossegue como dantes.

16.14 Exemplo $p \vee q, p \rightarrow r, q \rightarrow s \vdash_{\mathbf{B}} r \vee s$:

$$
\begin{array}{cccc}
 & & F(r \vee s) & \\
 & & Fr & \\
 & & Fs & \\
 & & V(p \vee q) & \\
 & Vp & & Vq \\
 V(p \rightarrow r) & & & V(p \rightarrow r) \\
Fp & Vr & Fp & Vr \\
\otimes & \otimes & V(q \rightarrow s) & \otimes \\
 & & Fq \quad Vs & \\
 & & \otimes \quad \otimes . &
\end{array}
$$

• No Lema de Hintikka, a valoração v é definida exactamente da mesma maneira e, ao concordar com o ramo não contraditório κ do tableau completo T, vai necessariamente concordar com todas as hipóteses, uma vez que todas elas são entradas em κ.

• Na demonstração do metateorema de completude semântica generalizado ($\Sigma \vDash \phi \Rightarrow \Sigma \vdash_{\mathbf{B}} \phi$), aplica-se o algoritmo modificado para construir um *tableau* completo com hipóteses em Σ e raiz $F\phi$ e utiliza-se a nova versão do Lema de Hintikka.

Vale a pena expandir um pouco a discussão sobre a «finitude» das derivações com hipóteses, tendo em vista, especialmente, o facto de o conjunto Σ de hipóteses ser infinito. O Lema de König aplica-se tal e qual na demonstração do metateorema dos *tableaux* contraditórios (pág. 0), para *tableaux* com hipóteses, que aqui designamos por

16.13 Metateorema da finitude

Se $T = \bigcup_n T_n$ *é um* tableau *contraditório com hipóteses em* Σ*, então* T_m *é um* tableau *contraditório com hipóteses em* Σ*, para algum* m*. Em particular, toda a derivação à Beth com hipóteses em* Σ *é um* tableau *finito*.

Da segunda parte deste resultado resulta a propriedade seguinte, que lhe dá o nome:

$(*)$ $\quad \Sigma \vdash_{\mathbf{B}} \phi$ sse $\Sigma_0 \vdash_{\mathbf{B}} \phi$ para alguma parte finita Σ_0 de Σ.

Este resultado pode ser encarado como a versão sintáctica do *metateorema da compacidade* (MC) (ver exercícios 2.12 e 2.22):

$(**)$ $\quad \Sigma \vDash \phi$ sse $\Sigma_0 \vDash \phi$ para alguma parte finita Σ_0 de Σ.

É claro que $(**)$ resulta imediatamente de $(*)$ pelos metateoremas de validade e completude semântica para o sistema dos *tableaux* com hipóteses, mas pode ser demonstrado independentemente de várias maneiras. Damos a seguir uma demonstração baseada no Lema de König.

Dem. do (MC). Supomos $\Sigma = \{\psi_i : i \geq 0\}$, $P = \{p_i : i \geq 0\}$. Num sentido (esquerda para a direita) é imediato. No outro sentido ($\Leftarrow$), suponhamos que toda a parte finita de Σ é compatível. Definimos uma árvore T de sucessões binárias finitas, onde $\sigma \leq_{\mathrm{T}} \tau$ sse τ é uma extensão de σ ($\sigma \subseteq \tau$, ver pág. 37 e Nota 29). Designamos por $c(\sigma)$ o *comprimento* de σ [$c(\sigma) = k$ se $\sigma = \langle \sigma 1, ..., \sigma k \rangle$, onde cada $\sigma i = \sigma(i)$ é 0 ou 1] e definimos

$$T = \{\sigma : \text{existe } v \text{ tal que, para todo } i \leq c(\sigma),\ v(\psi_i) = 1, \\ \text{e } v(p_i) = 1 \text{ sse } \sigma i = 1\}.$$

Quer dizer, σ é uma entrada na árvore T excepto se, encarando σ como uma sucessão de valores lógicos (valoração v) atribuídos aos p_i com $i \leq c(\sigma)$, isso já força a falsidade de uma ψ_j [$j \leq c(\sigma)$], pelo menos.

Começamos por mostrar que

(1) existe um ramo infinito em T sse Σ é compatível.

Se v é um modelo de Σ, então, por definição, o conjunto de todas as sucessões finitas σ tais que $\sigma i = 1$ sse $v(p_i) = 1$, é um ramo em T. Reciprocamente, suponhamos que $\kappa = \langle \sigma_j : j \geq 0 \rangle$ é um ramo infinito em T, e seja v a única valoração que estende as valorações parciais determinadas pelos σ_j, isto é, tal que $v(p_i) = 1$ sse $\sigma_j(i) = 1$ para algum j, ou seja, sse $\sigma_j(i) = 1$ para todo $i \leq c(\sigma_j)$.[84] Se v não fosse modelo de Σ, existiria $\psi_j \in \Sigma$ tal que $v(\psi_j) = 0$. Mas este facto só depende dos valores lógicos atribuídos a um número *finito* de letras proposicionais

[84] Não perder de vista que as sucessões binárias finitas que constituem um ramo, no caso κ, formam uma cadeia, isto é, são totalmente ordenadas pela relação de extensão $\leq$, ou $\subseteq$.

[as que ocorrem em ψ_j — ver exercício 2.3(b)]. Sem perda de generalidade, podemos supor que elas são p_0, p_1, ..., p_n. Da definição de T resulta então que nenhuma σ com comprimento $\geq n$ pode estar em T. Isto contradiz a hipótese de κ ser um ramo infinito em T, visto que só há um número finito de sucessões binárias de comprimento $\leq n$. Portanto, $v \vDash \Sigma$.

Mostramos a seguir que

(2) para todo n, existe uma sucessão binária σ em T de comprimento n.

Por hipótese, toda a parte finita de Σ é compatível. Então, em particular, para cada n existe um modelo v_n de $\{\psi_i : i \leq n\}$. Definamos σ pondo $\sigma(i) = 1$ sse $v_n(p_i) = 1$ para $i \leq n$. Tal σ está em T, por definição de T.

Concluindo: por (2), T é infinita, logo, pelo Lema de König, possui um ramo infinito. Por (1), Σ é compatível.■

*II.17 Outros sistemas dedutivos (II): cálculo de sequentes

Na secção anterior vimos um método de decisão para a validade proposicional baseado nos *tableaux* semânticos, os quais, como se disse (pág. 106), é um método para examinar sistematicamente as possibilidades de uma fórmula dada tomar os valores lógicos 0 ou 1, alternativo ao método das tabelas de verdade. Nesta secção veremos um método de decisão para a derivabilidade em **DN** (e, portanto, também para a validade) baseado numa *mecanização,* no maior grau possível, do processo dedutivo, que permite responder sem ambiguidade a todas as questões do tipo: dada uma linha (fórmula) qualquer de uma dedução, que linha ou linhas a devem preceder para que a linha (fórmula) dada seja inferida dessa ou dessas precedentes por uma das regras dadas? Requeremos, além disso, que este processo regressivo termine sempre, mais tarde ou mais cedo. Os sistemas de dedução natural são «progressivos» ou «de cima para baixo», embora as estratégias dedutivas sejam, em larga medida «naturais», mas existem, em geral, diversas estratégias «ganhantes» possíveis, isto é, diversas maneiras de deduzir correctamente uma fórmula (a partir de hipóteses dadas). O novo método que vamos apresentar é essencialmente «regressivo» ou «de baixo para cima»: partindo de ϕ, buscamos sistematicamente a única ou únicas premissas que podem ter ϕ como conclusão; ao fim de um número finito de passos obtemos, ou uma derivação no sistema ou a confirmação de que tal não é possível.

O novo sistema dedutivo é um *cálculo de sequentes,*[85] de Gentzen, e designa-se por **GP**, ou simplesmente por **G**, neste capítulo. As deduções ou derivações no sistema **G** são sucessões (ou árvores — ver adiante) finitas de *itens sequenciais,* ou *sequentes,* sendo cada sequente uma sucessão finita de fórmulas, da forma

$$\phi_1, \phi_2, ..., \phi_n \ (n \geq 1).$$

[85] Existem diversas versões, esta é apenas uma das mais simples.

Os sequentes são designados por gregas maiúsculas Γ, Δ, Θ, ..., possivelmente com índices. As regras de inferência são de uma das formas

$$\frac{\Gamma}{\Theta}, \qquad \frac{\Gamma \mid \Delta}{\Theta} \quad \left(\text{ou } \frac{\begin{array}{c}\Gamma\\ \Delta\end{array}}{\Theta}\right).$$

A interpretação intencional de um sequente $\Gamma = \phi_1, \phi_2, ..., \phi_n$ é a de que Γ corresponde a uma *disjunção* dos ϕ_i, isto é, a vírgula ',' funciona como uma disjunção disfarçada, com a associatividade já imbuída na própria notação.

Este sistema tem as propriedades seguintes:

Gerhard Gentzen
(1909-1945)

(1) é dedutivamente equivalente a **DN**;

(2) para qualquer sequente Θ existe, quando muito, uma regra de **G** da qual esse sequente pode ser a conclusão por uma das regras, sendo a premissa ou premissas bem determinadas (a menos de uma permutação).

As regras de inferência de **G** são, todas elas, regras de introdução de conectivos e certas combinações de conectivos. Por comodidade abrevia-se $\phi_1, \phi_2, ..., \phi_n$ em ϕ_1, Δ ou ϕ_1, ϕ_2, Δ, sendo agora Δ a parte final, possivelmente vazia, de um sequente.

REGRAS DE G

$(\neg\neg+)$	$\dfrac{\phi, \Delta}{\neg\neg\phi, \Delta}$		
$(\wedge+)$	$\dfrac{\phi, \Delta \mid \psi, \Delta}{\phi \wedge \psi, \Delta}$	$(\neg\wedge+)$	$\dfrac{\neg\phi, \neg\psi, \Delta}{\neg(\phi \wedge \psi), \Delta}$
$(\vee+)$	$\dfrac{\phi, \psi, \Delta}{\phi \vee \psi, \Delta}$	$(\neg\vee+)$	$\dfrac{\neg\phi, \Delta \mid \neg\psi, \Delta}{\neg(\phi \vee \psi), \Delta}$
$(\rightarrow+)$	$\dfrac{\neg\phi, \psi, \Delta}{\phi \rightarrow \psi, \Delta}$	$(\neg\rightarrow+)$	$\dfrac{\phi, \Delta \mid \neg\psi, \Delta}{\neg(\phi \rightarrow \psi), \Delta}$.

Fazemos, além disso, as seguintes convenções e restrições:

(a) A ordem das fórmulas nas premissas é irrelevante;

(b) a ordem das fórmulas numa conclusão, somente literais (átomos p_i ou suas negações) podem preceder a fórmula introduzida pela regra;

(c) num sequente (numa premissa ou conclusão) podem omitir-se fórmulas repetidas;

(d) uma fórmula é um sequente.

Como ilustração de (b), a regra ($\neg\neg+$) pode-se aplicar à premissa $p, q, p\rightarrow q$, e pode ter como conclusão $\neg\neg p, q, p\rightarrow q$ e $q, \neg\neg p, p\rightarrow q$, entre outras, mas não $p\rightarrow q, q, \neg\neg p$ nem $p\rightarrow q, \neg\neg p, q$. Como ilustração de (c), no sequente $\neg p, q, \neg p, p\rightarrow r$ pode-se omitir uma única das ocorrências de "$\neg p$".

Com estas convenções e restrições fica garantida a propriedade (2) acima, e para saber qual a regra e premissa ou premissas para obter Θ como conclusão basta inspeccionar Θ da esquerda para a direita até se encontrar a primeira fórmula que não é uma literal, sendo a regra em causa

$$\neg\neg+,\ \ \wedge+,\ \ \neg\wedge+,\ \ \vee+,\ \ \neg\vee+,\ \ \rightarrow+,\ \ \neg\rightarrow+$$

conforme essa primeira fórmula é da forma

$$\neg\neg\phi,\ \phi\wedge\psi,\ \neg(\phi\wedge\psi),\ \phi\vee\psi,\ \neg(\phi\vee\psi),\ \phi\rightarrow\psi,\ \neg(\phi\rightarrow\psi),$$

respectivamente.

17.1 Definição (i) Um **axioma** de **G** é um sequente $\phi_1, \phi_2, ..., \phi_n$ ($n \geq 2$) em que algum ϕ_i é uma negação $\neg\phi_j$ ($1 \leq i, j \leq n$).

(ii) Uma **dedução** ou **derivação** em **G** é uma sucessão finita de sequentes $\Delta_1, \Delta_2, ..., \Delta_m$ ($m \geq 1$), na qual cada Δ_i é um axioma ou é inferido de um ou dois sequentes precedentes por uma regra.

Por exemplo, os sequentes $\neg\neg p, q, \neg p$ e $\phi\rightarrow\psi, \neg\theta, \neg(\phi\rightarrow\psi)$ são axiomas.

Na pág. seguinte apresentamos uma lista de 15 sequentes, que constitui uma derivação da fórmula

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

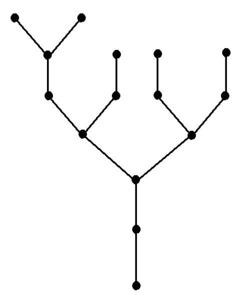
Para se compreender bem a derivação, convém percorrê-la *de baixo para cima,* tentanto perceber como cada linha (conclusão) determina uma regra e uma ou duas linhas imediatamente acima dela. Na linha 10 pode-se omitir a fórmula repetida $\neg r$.

Para esta análise regressiva e, até, para a construção de uma derivação (se alguma existe — ver adiante) de baixo para cima, a configuração «vertical» não é a mais conveniente, mas sim a configuração em árvore, com a raiz em baixo e os axiomas no topo (nós terminais), como exemplificamos logo a seguir à derivação na vertical, assinalando com 'Ax' os topos que são axiomas. A árvore não tem 15 nós, mas apenas 11, pois juntamos num mesmo nó duas premissas, correspondentes aos pares de linhas 1 e 2, 7 e 8, 9 e 10, 11 e 12 na derivação vertical.

1	$p, q, \neg p, r$	Axioma
2	$p, q, \neg q, r$	Axioma
3	$p, q, \neg(p \vee q), r$	1, 2 $\neg\vee+$
4	$p, \neg r, \neg(p \vee q), r$	Axioma
5	$q, \neg r, \neg(p \vee q), r$	Axioma
6	$\neg r, \neg(p \vee q), r$	Axioma
7	$p, q, p \vee q \to r$	3 $\to+$
8	$\neg r, p, p \vee q \to r$	4 $\to+$
9	$q, \neg r, p \vee q \to r$	5 $\to+$
10	$\neg r, \neg r, p \vee q \to r$	6 $\to+$
11	$p, \neg(p \to r), p \vee q \to r$	7, 8 $\neg\to+$
12	$\neg r, \neg(q \to r), p \vee q \to r$	9, 10 $\neg\to+$
13	$\neg(p \to r), \neg(q \to r), p \vee q \to r$	11, 12 $\neg\to+$
14	$\neg((p \to r) \wedge (q \to r)), p \vee q \to r$	13 $\neg\wedge+$
15	$(p \to r) \wedge (q \to r) \to (p \vee q \to r)$	14 $\to+$.

$$\text{Ax} \qquad \text{Ax}$$
$$\underline{p, q, \neg p, r \mid p, q, \neg q, r} \qquad \text{Ax} \qquad \text{Ax} \qquad \text{Ax}$$
$$\underline{p, q, \neg(p \vee q), r} \quad \underline{p, \neg r, \neg(p \vee q), r} \quad \underline{q, \neg r, \neg(p \vee q), r} \quad \underline{\neg r, \neg(p \vee q), r}$$
$$\underline{p, q, p \vee q \to r \mid p, \neg r, p \vee q \to r} \qquad \underline{\neg r, q, p \vee q \to r \mid \neg r, \neg r, p \vee q \to r}$$
$$\underline{p, \neg(p \to r), p \vee q \to r \qquad \mid \qquad \neg r, \neg(q \to r), p \vee q \to r}$$
$$\underline{\neg(p \to r), \neg(q \to r), p \vee q \to r}$$
$$\underline{\neg((p \to r) \wedge (q \to r)), p \vee q \to r}$$
$$(p \to r) \wedge (q \to r) \to (p \vee q \to r).$$

A forma ou esqueleto desta árvore é



As derivações obtidas neste e noutros exemplo (ver exercícios 2.36) não são ainda inteiramente deterministas, pois resta uma margem de arbitrariedade no que diz respeito à ordenação das fórmulas nas premissas, à medida que vamos «subindo» na árvore. Para eliminar completamente esta réstea de indeterminação

descrevemos um algoritmo para a construção de possíveis derivações em forma de árvore.

17.2 Algoritmo para a construção de possíveis derivações em G.
Dado um sequente qualquer $\phi_1, \phi_2, ..., \phi_n$ ($n \geq 1$) como raiz:

• se o sequente é um axioma o algoritmo pára, e tal sequente é uma derivação em **G**;

• se o sequente não é um axioma mas toda a fórmula do sequente é uma literal (p_i ou $\neg p_i$), o algoritmo pára — este caso será analisado mais adiante;

• se o sequente não é um axioma e alguma fórmula não é uma literal, há uma primeira tal fórmula (contando da esquerda para a direita), digamos ϕ_k.

Há sete casos a considerar, conforme a forma de ϕ_k, que resumimos no quadro seguinte, onde a 2ª coluna contém o sequente dado (da forma Δ, ϕ_k, Θ, sendo Δ, Θ possivelmente vazias) e a 3ª coluna contém a premissa ou premissas de que esse sequente é conclusão por uma das 7 regras do sistema, premissa ou premissas essas que são escritas por cima do sequente dado.

Observando o quadro da página seguinte, não há dúvida de que, agora, a premissa ou premissas são bem determinadas, e não apenas a menos de uma permutação. Além disso, *o peso de uma premissa* $\Gamma = \phi_1, \phi_2, ..., \phi_n$,

$$\text{peso}(\Gamma) = \text{peso}(\phi_1) + \text{peso}(\phi_2) + \cdots + \text{peso}(\phi_n),$$

(ver definição de peso no exercício 2.35, pág. 153) *é sempre menor que o peso da conclusão*. Obtida a premissa ou premissas, aplica-se a cada uma o procedimento acima, até que todos os topos são axiomas ou são sequentes formados por literais, o que tem de acontecer mais tarde ou mais cedo, atendendo à diminuição progressiva dos pesos.

Casos	Sequente dado	Premissas
I.	$\Delta, \neg\neg\phi, \Theta$	Δ, ϕ, Θ
II.	$\Delta, \phi \wedge \psi, \Theta$	$\Delta, \phi, \Theta \quad \Delta, \psi, \Theta$
III.	$\Delta, \neg(\phi \wedge \psi), \Theta$	$\Delta, \neg\phi, \neg\psi, \Theta$
IV.	$\Delta, \phi \vee \psi, \Theta$	$\Delta, \phi, \psi, \Theta$
V.	$\Delta, \neg(\phi \vee \psi), \Theta$	$\Delta, \neg\phi, \Theta \quad \Delta, \neg\psi, \Theta$
VI.	$\Delta, \phi \rightarrow \psi, \Theta$	$\Delta, \neg\phi, \psi, \Theta$
VII.	$\Delta, \neg(\phi \rightarrow \psi), \Theta$	$\Delta, \phi, \Theta \quad \Delta, \neg\psi, \Theta.$

Se todos os topos da árvore assim obtida forem axiomas, então a árvore é uma derivação no sistema **G**, que facilmente se converte numa derivação sequencial (linear vertical). Se algum topo não for axioma, teremos de provar, para completar o método de decisão, que o sequente não é derivável e, no caso de ser uma fórmula, que ela é inválida.

17.3 Relações entre diferentes conceitos de derivabilidade

Resumindo, estabelecemos as seguintes relações entre a derivabilidade nos sistemas **DN** e **G** e a noção de validade:

(1) $\text{Teor}_{\mathbf{DN}} \subseteq \text{Val}$: os teoremas lógicos de **DN** são válidos. Esta é a propriedade de validade do sistema **DN**, já demonstrada anteriormente (pp. 73-75);

(2) $\text{Val} \subseteq \text{Teor}_{\mathbf{DN}}$: as fórmulas válidas são teoremas lógicos de **DN**. Esta é a propriedade de completude semântica do sistema **DN**, também já demonstrada anteriormente (pp. 76-78);

(3) $\text{Val} \subseteq \text{Teor}_{\mathbf{G}}$: as fórmulas válidas são deriváveis em **G**. Esta é a propriedade de completude semântica do sistema **G**, que demonstramos a seguir;

(4) $\text{Teor}_{\mathbf{G}} \subseteq \text{Teor}_{\mathbf{DN}}$: as fórmulas deriváveis em **G** são deriváveis em **DN**. Será demonstrado directamente, donde se conclui, por (1) e (3),

(5) $\text{Teor}_{\mathbf{G}} = \text{Teor}_{\mathbf{DN}} = \text{Val}$.

A última igualdade já fora estabelecida anteriormente [por (1) e (2)], mas a maneira como agora é estabelecida [de maneira alternativa e independente de (2)], via **G** e (3), fornece ao mesmo tempo um método de decisão para a derivabilidade em **DN**, o que, afinal de contas, é o objectivo fundamental da concepção do sistema de Gentzen.

Dem. de (3). Mostramos, ao invés, que se ϕ não é derivável em **G**, então ϕ não é válida. Pois apliquemos a ϕ o algoritmo da pág. 122 até obter uma árvore que não possa prolongar-se mais em nenhum ramo, o que é possível atendendo à diminuição sucessiva dos pesos dos sequentes. Tal árvore não é uma derivação em **G**, o que só é possível porque algum topo não é axioma, digamos

$$\Gamma = P_1, P_2, ..., P_n,$$

onde cada P_i é literal (p_i ou $\neg p_i$) mas nenhum deles é a negação de um outro. É então possível definir uma valoração v nos átomos que falsifique *todos* os P_i (se P_i é p_i, dá-se a p_i o valor 0, e se é $\neg p_i$ dá-se a p_i o valor 1 — não interessam os valores lógicos dos átomos que não ocorrem no sequente Γ). Dizemos que Γ é inválido. Mais geralmente, um sequente $\phi_1, \phi_2, ..., \phi_n$ é **inválido** sse existe uma valoração que falsifica todas as fórmulas (o que está de acordo com o considerar-se a vírgula ‘,’ como uma disjunção disfarçada). Ora, pesquisando caso a caso, verificamos facilmente que *se uma premissa* (de uma regra de **G**) *é inválida, então a conclusão é inválida.* Deste modo, todos os sequentes do ramo da árvore que termina em Γ é formado por sequentes inválidos. Em particular, portanto ϕ é inválida, o que prova (3).■

17.4 Exemplo Aplicando o algoritmo a $(p \rightarrow q \vee r) \rightarrow (q \rightarrow r \vee p)$, obtemos:

$$\begin{array}{cc} (*) & \text{Ax} \\ \underline{\neg q, \neg q, r, p} & \underline{\neg r, \neg q, r, p} \\ \underline{\neg q, \neg q, r \vee p} & \underline{\neg r, \neg q, r \vee p} \\ \vdots \quad \underline{\neg q, q \to r \vee p} & \underline{\neg r, q \to r \vee p} \\ \underline{p, q \to r \vee p \quad | \quad \neg(q \vee r), q \to r \vee p} & \\ \underline{\neg(p \to q \vee r), q \to r \vee p} & \\ (p \to q \vee r) \to (q \to r \vee p). & \end{array}$$

Com $(*)$ assinala-se um topo que não é axioma mas não se pode prolongar mais, e não se completou o ramo à esquerda por ser desnecessário fazê-lo para o fim em vista, que é confirmar que o topo assinalado e, portanto, todos os sequentes por baixo dele, até à raiz, são inválidos: basta definir v pondo $v(q) = 1$, $v(r) = v(p) = 0$.

Quanto a (4), o procedimento indicado seria por indução no comprimento das deduções (configuração linear vertical) de ϕ em **G**. Mas precisamos, antes de mais, de saber traduzir sequentes $\Gamma = \phi_1, \phi_2, ..., \phi_n$ em fórmulas de $\mathcal{L}^0$. A tradução óbvia é numa disjunção dos ϕ_i, mas qual? Na realidade, não interessa qual, mas para justificar isso há que recorrer à *associatividade generalizada* da disjunção em **DN**. Podíamos simplesmente adoptar a convenção de escrita de associação da direita para a esquerda (pág. 48 e Nota 72), ou outra, mas não se ganharia grande coisa com isso.

17.5 Definição Chama-se **disjunção sobre** $\{\phi_1, \phi_2, ..., \phi_n\}$ a qualquer fórmula construída de acordo com as seguintes regras:

(i) cada ϕ_i é uma disjunção sobre $\{\phi_1, \phi_2, ..., \phi_n\}$;

(ii) se ψ, θ são disjunções sobre $\{\phi_1, \phi_2, ..., \phi_n\}$, então $(\psi \vee \theta)$ é uma disjunção sobre $\{\phi_1, \phi_2, ..., \phi_n\}$.

Chama-se **disjunção de** $\{\phi_1, \phi_2, ..., \phi_n\}$ a qualquer disjunção sobre $\{\phi_1, \phi_2, ..., \phi_n\}$ que não seja uma disjunção sobre nenhum subconjunto próprio de $\{\phi_1, \phi_2, ..., \phi_n\}$.

Analogamente para as conjunções.

Note-se que toda a disjunção *de* é uma disjunção *sobre,* mas não reciprocamente. Por exemplo, $(\phi_2 \vee \phi_1) \vee \phi_2$ é uma disjunção sobre $\{\phi_1, \phi_2, \phi_3\}$, mas não é disjunção de $\{\phi_1, \phi_2, \phi_3\}$, pois falta uma ocorrência de ϕ_3. Necessitamos do seguinte resultado, cuja demonstração deixamos para o exercício 2.38:

17.6 Metateorema da subdisjunção (MSD)

Se ψ *é uma disjunção sobre* $\{\phi_1, \phi_2, ..., \phi_n\}$ *e* θ *é uma disjunção de* $\{\phi_1, \phi_2, ..., \phi_n\}$*, então* $\psi \vdash_{\mathbf{DN}} \theta$.■

Nas condições deste enunciado, ψ diz-se uma *subdisjunção* de θ. Podemos então prosseguir com a demonstração de (4), mas esta propriedade resulta imediatamente do seguinte

17.7 Metateorema

Se o sequente $\phi_1, \phi_2, ..., \phi_n$ *é derivável em* **G** *e* θ *é uma disjunção de* $\{\phi_1, \phi_2, ..., \phi_n\}$*, então* $\vdash_{\mathbf{DN}} \theta$.

Dem. Por indução completa (2.ª forma, ver pág. 74) no comprimento k das deduções do sequente $\phi_1, \phi_2, ..., \phi_n$ em **G**.

(i) $k = 1$: $\phi_1, \phi_2, ..., \phi_n$ é um axioma, digamos que $\phi_i = \neg\phi_j$. Ora $\phi_j \vee \neg\phi_j$ é uma lei lógica (3º excluído) de **DN**, e é uma subdisjunção de θ, logo $\vdash_{\mathbf{DN}} \theta$.

(ii) Suponhamos (hip. de indução) que a propriedade a demonstrar é verdadeira para todas derivações com $\leq k$ linhas, e que $\phi_1, \phi_2, ..., \phi_n$ é derivável em $k + 1$ linhas. Há oito casos a considerar, um para cada regra de **G**, e mais um para os axiomas. Lidamos apenas com este último e dois dos primeiros sete, deixando os restantes como exercícios.

Caso 0. $\phi_1, \phi_2, ..., \phi_n$ é um axioma. Trata-se como em (i).

Caso II. $\phi_1, \phi_2, ..., \phi_n$ é obtido pela regra $\wedge+$. Quer dizer que ϕ_1 é da forma $\psi' \wedge \psi''$, e cada uma das premissas (a menos de permutação)

$$\text{(a) } \psi', \phi_2, ..., \phi_n, \quad \text{(b) } \psi'', \phi_2, ..., \phi_n$$

possui derivações de comprimento $\leq k$. Seja δ uma disjunção qualquer de $\{\phi_1, \phi_2, ..., \phi_n\}$; então $\psi' \vee \delta$ e $\psi'' \vee \delta$ são disjunções de (a) e (b), respectivamente, e, por hipótese de indução,

$$\text{(a}') \vdash_{\mathbf{DN}} \psi' \vee \delta \quad \text{e} \quad \text{(b}') \vdash_{\mathbf{DN}} \psi'' \vee \delta.$$

Ora, θ é $(\psi' \wedge \psi'') \vee \delta$ ou alguma outra disjunção de $\{\psi' \wedge \psi'', \phi_1, \phi_2, ..., \phi_n\}$, em todo o caso interderivável com $(\psi' \wedge \psi'') \vee \delta$ pelo (**MSD**). Podemos obter do

seguinte modo uma dedução de θ em **DN**:

1	$\psi' \vee \delta$	(T^+) (a′)
2	ψ'	[H_1]
3	$\psi'' \vee \delta$	(T^+) (b′)
4	ψ''	[H'_1]
5	$\psi' \wedge \psi''$	2, 4 ($\wedge^+$)
6	$(\psi' \wedge \psi'') \vee \delta$	5 ($\vee^+$)
7	δ	[H'_2]
8	$(\psi' \wedge \psi'') \vee \delta$	7 ($\vee^+$)
9	$(\psi' \wedge \psi'') \vee \delta$	3, 4-6, 7-8 ($\vee^+$)
10	δ	[H_2]
11	$(\psi' \wedge \psi'') \vee \delta$	10 ($\vee^+$)
12	$(\psi' \wedge \psi'') \vee \delta$	1, 2-9, 10-11 ($\vee^+$)
⋮	⋮	
12 + m	θ	(T^+) de 12, pelo (**MSD**).

Caso V. $\phi_1, \phi_2, ..., \phi_n$ é obtido pela regra $\neg\vee+$. Então ϕ_1 é da forma $\neg(\psi' \vee \psi'')$, e cada uma das premissas (ou uma sua permutação)

$$\text{(c)}\ \neg\psi', \phi_2, ..., \phi_n, \quad \text{(c)}\ \neg\psi'', \phi_2, ..., \phi_n$$

possui derivações de comprimento $\leq k$. Seja δ como anteriormente. Por hipótese de indução,

$$\text{(c}')\ \vdash_{\mathbf{DN}} \neg\psi' \vee \delta \quad \text{e} \quad \text{(d}')\ \vdash_{\mathbf{DN}} \neg\psi'' \vee \delta,$$

e θ é $\neg(\psi' \vee \psi'') \vee \delta$ ou uma outra disjunção de $\{\neg(\psi' \vee \psi''), \phi_1, \phi_2, \ ..., \phi_n\}$, em todo o caso interderivável com $\neg(\psi' \vee \psi'') \vee \delta$ pelo (**MSD**). Podemos obter do seguinte modo uma dedução de θ em **DN**: de (c′) e (d′) obtemos, por uma conhecida lei de conversão [(42), pág. 67],

$$\text{(c}'')\ \vdash_{\mathbf{DN}} \psi' \rightarrow \delta \quad \text{e} \quad \text{(d}'')\ \vdash_{\mathbf{DN}} \psi'' \rightarrow \delta,$$

respectivamente, e usando estas duas é fácil obter $\vdash_{\mathbf{DN}} (\psi' \vee \psi'') \rightarrow \delta$ (exercício), ou seja, pela mesma lei de conversão, $\vdash_{\mathbf{DN}} \neg(\psi' \vee \psi'') \vee \delta$.■

*II.18 Outros sistemas dedutivos (III): axiomatização à Hilbert

Os sistemas de dedução natural, mais do que quaisquer outros, pretendem «modelar» de maneira natural os raciocínios lógicos, enquanto os de Gentzen mecanizam em maior grau o processo dedutivo e se prestam melhor a uma análise estrutural das deduções em si mesmas (tópico predilecto da chamada *teoria da demonstração*). Por outro lado, sistemas como o dos *tableaux* semânticos de Beth e os sistemas de resolução (secção seguinte) são sistemas *refutacionais,* na medida em que se procura essencialmente *refutar* determinada fórmula ou consequência,

no sentido de estabelecer que ela é incompatível. O insucesso da tentativa de refutação corresponde à busta do sucesso da derivação nos anteriores sistemas. Todavia, todos estes sistemas, concebidos com características e objectivos específicos em mente, são de génese mais recente do que os primeiros sistemas dedutivos para a lógica concebidos no final do séc. XIX e princípios do séc. XX, nomeadamente por Frege, Russell e Whitehead, Lukasiewicz e outros. Estes sistemas constituem axiomatizações da lógica num sentido tradicional, e são conhecidos genericamente por *axiomatizações à Hilbert,* por terem sido preferidos por Hilbert e a sua escola nos estudos de fundamentos nos anos vinte do século passado, e caracterizam-se pela *economia de meios,* o que, por um lado, dificulta e artificializa o processo dedutivo em si mesmo, mas, em compensação, facilita grandemente os estudos metateóricos. Uma axiomatização à Hilbert consta tipicamente de um certo número de *axiomas* (numa linguagem com o mínimo possível de primitivos) e de um pequeno número de *regras de inferência*.

São conhecidas muitas axiomatizações à Hilbert para a lógica proposicional clássica, conforme a lista dos conectivos adoptados como primitivos e as listas de axiomas e regras, mas em todas elas os axiomas são fórmulas válidas e as regras são válidas, de modo a garantir a propriedade de validade e a consistência do sistema e, é claro também, são escolhidos de modo a garantir a propriedade recíproca, de completude semântica.

Fiéis à economia de meios que pervade as axiomatizações à Hilbert, consideramos como primitivos somente $\neg$ e $\rightarrow$, e como definidos $\wedge$ e $\vee$ e $\leftrightarrow$ [$\phi \wedge \psi$ abrevia $\neg(\phi \rightarrow \neg\psi)$, e $\phi \vee \psi$ abrevia $\neg\phi \rightarrow \psi$; $\leftrightarrow$ define-se à custa de $\rightarrow$ e $\wedge$ pelo modo habitual]. É claro que na definição de fórmula (p. 48) só se retém, em F_3, a parte respeitante a $\rightarrow$.

Designamos por **H** o sistema dedutivo com os axiomas e regras seguintes[86]:

18.1 Axiomas e regras proposicionais de H

As fórmulas e regras de uma das formas seguintes são os axiomas e regras do sistema **H**:

(H_1) $\phi \rightarrow (\psi \rightarrow \phi)$;

(H_2) $((\phi \rightarrow (\psi \rightarrow \theta)) \rightarrow ((\phi \rightarrow \psi) \rightarrow (\phi \rightarrow \theta))$;

(H_3) $(\neg\phi \rightarrow \neg\psi) \rightarrow ((\neg\phi \rightarrow \psi) \rightarrow \phi)$.[87]

Regra de inferência *modus ponens* (MP): $\dfrac{\phi,\ \phi \rightarrow \psi}{\psi}$.

A *deribabilidade* e a *derivabilidade com hipóteses* neste sistema definem-se como é de esperar:

---

[86] Este sistema é designado por **L** em MENDELSON, p. 35.

[87] Pode não parecer à vista descuidada, mas a lista compreende uma infinidade de axiomas, mas um número finito de *esquemas de axiomas:* por exemplo, sob o esquema (H_1) estão compreendidas *todas as fórmulas de* $\mathcal{L}^0$ *da forma* $\phi \rightarrow (\psi \rightarrow \phi)$, de que são casos (axiomas) particulares as fórmulas $p_0 \rightarrow (p_0 \rightarrow p_0)$, $p_0 \rightarrow (p_1 \rightarrow p_0)$, $p_1 \rightarrow (p_1 \rightarrow p_1)$, $p_1 \rightarrow (p_0 \rightarrow p_1)$, etc.

• $\vdash_{\mathbf{H}} \phi$ sse existe uma sucessão finita de fórmulas $\phi_1, \phi_2, ..., \phi_n$ $(n \geq 1)$, a última das quais é ϕ, tal que cada ϕ_i com $i \leq n$ é um axioma ou é inferida de duas fórmulas precedentes ϕ_j, ϕ_k $(j, k < i)$ pela regra (MP); uma tal sucessão é uma *derivação* ou *dedução* de ϕ;

• se Γ é um conjunto de fórmulas (finito ou infinito), $\Gamma \vdash_{\mathbf{H}} \phi$ sse existe uma sucessão finita de fórmulas $\phi_1, \phi_2, ..., \phi_n$ $(n \geq 1)$, a última das quais é ϕ, tal que cada ϕ_i com $i \leq n$ é um axioma, ou é uma hipótese (em Γ), ou é inferida de duas fórmulas precedentes ϕ_j, ϕ_k $(j, k < i)$ pela regra (MP); uma tal sucessão é uma *derivação* (ou *dedução*) *de* ϕ *com hipóteses em* Γ (ou: *a partir de* Γ).

Se $\vdash_{\mathbf{H}} \phi$, dizemos que ϕ é *derivável* (em **H**), um *teorema lógico* ou uma *lei lógica,* e se $\Gamma \vdash_{\mathbf{H}} \phi$ dizemos que ϕ é um *teorema com hipóteses em* Γ, ou que é *derivável de* Γ, ou simplesmente que é um *teorema de* Γ. Como se vê pelas definições, os axiomas são trivialmente deriváveis, e a derivabilidade é um caso particular da derivabilidade com hipóteses, quando o conjunto de hipóteses é $\Gamma = \emptyset$. Além disso, todo o teorema lógico é um teorema de Γ, qualquer que seja o conjunto Γ. Por outro lado, o facto de todas as derivações serem sucessões *finitas* de fórmulas implica logo a *propriedade de finitude:*

(PF) $\Gamma \vdash_{\mathbf{H}} \phi$ sse existe uma parte finita Γ_0 de Γ tal que $\Gamma_0 \vdash_{\mathbf{H}} \phi$.

18.2 Exemplos (1) $\vdash_{\mathbf{H}} \phi \to \phi$ (*lei da identidade)*.

Deduzimos $p \to p$; para obter uma dedução de $\phi \to \phi$, qualquer que seja ϕ, é só substituir em toda a parte "p" por "ϕ":

1	$p \to ((p \to p) \to p)$	Ax. (H_1)
2	$(p \to ((p \to p) \to p)) \to ((p \to (p \to p)) \to (p \to p))$	Ax. (H_2)
3	$((p \to (p \to p)) \to (p \to p))$	1, 2 (MP)
4	$p \to (p \to p)$	Ax. (H_1)
5	$p \to p$	3, 4 (MP).

(2) $\neg\psi \vdash_{\mathbf{H}} (\neg\phi \to \psi) \to \phi$

1	$\neg\psi$	Hip.
2	$\neg\psi \to (\neg\phi \to \neg\psi)$	(H_2)
3	$\neg\phi \to \neg\psi$	1, 2 (MP)
4	$(\neg\phi \to \neg\psi) \to ((\neg\phi \to \psi) \to \phi)$	(H_3)
5	$(\neg\phi \to \psi) \to \phi$	3, 4 (MP).

Por estes exemplos já se vê como são «artificiais» as deduções no sistema **H**, pelo menos em comparação com as deduções em **DN**. Mas alguma coisa se pode fazer no sentido de facilitar o trabalho dedutivo, nomeadamente, através de *regras derivadas* (tal como se fez para **DN**). O primeiro e mais importante passo nesse

sentido é o resultado seguinte, que corresponde à regra de introdução de $\rightarrow$, ($\rightarrow^{+}$), no sistema de dedução natural.

18.3 Metateorema da dedução (MD, Herbrand-Tarski, 1930)

Se $\Gamma \cup \{\phi\} \vdash_{\mathbf{H}} \psi$, *então* $\Gamma \vdash_{\mathbf{H}} \phi \rightarrow \psi$.

Dem. Mostraremos como transformar toda a derivação de ψ com hipóteses em $\Gamma \cup \{\phi\}$ numa derivação de $\phi \rightarrow \psi$ com hipóteses em Γ.

Pois seja

$$(*) \qquad \phi_1, ..., \phi_{m-1}, \phi_m$$

uma derivação qualquer de $\psi = \phi_m$ com hipóteses em $\Gamma \cup \{\phi\}$. ϕ pode estar ou não entre os ϕ_i ($1 \leq i \leq m$), e analogamente para as fórmulas de Γ, mas, quando muito, um número finito delas [pela propriedade de finitude (PF)]. Em seguida forme-se a sucessão

$$(**) \qquad \phi \rightarrow \phi_1, ..., \phi \rightarrow \phi_{m-1}, \phi \rightarrow \phi_m,$$

a qual não é, em geral, uma derivação de $\phi \rightarrow \psi$ com hipóteses em Γ, embora a última fórmula seja a pretendida. Acontece, porém, que inserindo mais algumas fórmulas nos locais apropriados se obtém uma tal derivação. Para cada $i = 1, ..., m$, as fórmulas a inserir antes de $\phi \rightarrow \phi_i$ dependem da justificação de ϕ_i na derivação $(*)$. Há, portanto, vários casos a considerar:

Caso 1. ϕ_i é uma hipótese em Γ. Neste caso inserimos as duas fórmulas seguintes

$$\phi_i, \phi_i \rightarrow (\phi \rightarrow \phi_i)$$

imediatamente antes de $\phi \rightarrow \phi_i$, e é claro que esta é inferida daquelas duas por (MP), sendo a segunda delas um axioma (H_1). Esquematicamente, as transformações efectuadas foram:

							1	$\phi \rightarrow \phi_1$	
1	ϕ_1			1	$\phi \rightarrow \phi_1$		⋮		
⋮				⋮			i	ϕ_i	Hip. (Γ)
i	ϕ_i	Hip. (Γ)	$\rightsquigarrow$	i	$\phi \rightarrow \phi_i$	$\rightsquigarrow$	i+1	$\phi_i \rightarrow (\phi \rightarrow \phi_i)$	(H_1)
⋮				⋮			i+2	$\phi \rightarrow \phi_i$	i, i+1 (MP)
m	ϕ_m			m	$\phi \rightarrow \phi_m$				
							m+2	$\phi \rightarrow \phi_m$	

Caso 2. ϕ_i é ϕ, e podemos supor, sem perda de generalidade, que esta fórmula não está em Γ (caso 1). Neste caso inserimos imediatamente antes de $\phi \rightarrow \phi_i = \phi \rightarrow \phi$ as quatro primeiras linhas da dedução de $\phi \rightarrow \phi$, como no exemplo 1 acima (com "ϕ" no lugar de "p").

Caso 3. ϕ_i é um axioma — trata-se de maneira análoga à do caso 1.

Caso 4. ϕ_i é inferida de duas fórmulas precedentes ϕ_j, ϕ_k por (MP). Deixamos os pormenores como exercício.

Obtemos, portanto, uma dedução de $\phi \to \psi$ com hipóteses em Γ, exactamente as mesmas que as hipóteses de Γ utilizadas em $(*)$.■

18.4 Exemplos (3) Como exemplo de aplicação, utilizando o exemplo 2 acima podemos concluir imediatamente que

$$\vdash_{\mathbf{H}} \neg\psi \to ((\neg\phi \to \psi) \to \phi),$$

sem necessidade de fazer qualquer derivação adicional.

(4) O (MD) facilita enormemente o processo dedutivo de fórmulas condicionais. Por exemplo, começando por estabelecer

(4a) $$\phi \to (\psi \to \theta), \psi, \phi \vdash_{\mathbf{H}} \theta,$$

[exercício deveras simples, que só utiliza a regra (MP)], obtemos sucessivamente, por (MD),

(4b) $$\phi \to (\psi \to \theta), \psi \vdash_{\mathbf{H}} \phi \to \theta,$$

(4c) $$\phi \to (\psi \to \theta) \vdash_{\mathbf{H}} \psi \to (\phi \to \theta),$$

e, finalmente, a *lei de permutação dos antecedentes*

(4d) $$\vdash_{\mathbf{H}} (\phi \to (\psi \to \theta)) \to (\psi \to (\phi \to \theta)).$$

(5) $\phi \to \psi, \psi \to \theta, \phi \vdash_{\mathbf{H}} \theta$ (exercício), donde

(5a) $$\phi \to \psi, \psi \to \theta \vdash_{\mathbf{H}} \phi \to \theta \quad \textit{(silogismo hipotético)}.$$

(6) $\vdash_{\mathbf{H}} \neg\neg\phi \to \phi$ *(lei de eliminação da dupla negação).* Fazemos uma derivação *abreviada,* recorrendo num certo passo à lei da identidade (1) anteriormente estabelecida e, noutros passos, a teses anteriormente derivada de duas fórmulas precedentes, correspondentes a (4b) e a (5a) acima. Sem estes recursos teríamos de «encaixar» no seio da derivação seguinte mais quatro linhas a seguir à primeira e, a seguir à actual segunda, inserir tantas quantas as necessárias correspondentes a (4b):

1	$(\neg\phi \to \neg\neg\phi) \to ((\neg\phi \to \neg\phi) \to \phi)$	(H_3)
2	$\neg\phi \to \neg\phi$	(1) [com "ϕ" em vez de "p"]
3	$(\neg\phi \to \neg\neg\phi) \to \phi$	1, 2 (4b)
4	$\neg\neg\phi \to (\neg\phi \to \neg\neg\phi)$	(H_1)
5	$\neg\neg\phi \to \phi$	3, 4 (5a).

O leitor reconhece nos expedientes utilizados nesta derivação abreviada uma situação descrita anteriormente no sistema **DN**: o *Princípio da Introdução de Teses* (T^+) (p. 63). A justificação deste princípio no presente sistema é exactamente a mesma que foi aí dada e acima exemplificada duas vezes. O seu enunciado até se pode simplificar um pouco, omitindo as referências às «dependências de hipóteses», mas escusamos fazê-lo. Todavia, aplicaremos o princípio todas as vezes que for conveniente, abreviando, assim, o comprimento das derivações.

(7) $\vdash_{\mathbf{H}} \phi \to \neg\neg\phi$ *(lei de introdução da dupla negação)*:

1	$(\neg\neg\neg\phi \to \neg\phi) \to ((\neg\neg\neg \to \phi) \to \neg\neg\phi)$	(H_3)
2	$\neg\neg\neg\phi \to \neg\phi$	T^+ (6)
3	$(\neg\neg\neg\phi \to \phi) \to \neg\neg\phi$	1, 2 (MP)
4	$\phi \to (\neg\neg\neg\phi \to \phi)$	(H_1)
5	$\phi \to \neg\neg\phi$	3, 4 T^+ (5a).

(8) $\neg\phi\,, \phi \vdash_{\mathbf{H}} \psi$ [exercício: use (H_1), (H_2) e (MD)], donde

(8a) $$\vdash_{\mathbf{H}} \neg\phi \to (\phi \to \psi).$$

(9) $\neg\psi \to \neg\phi,\ \phi \vdash_{\mathbf{H}} \psi$:

1	$\neg\psi \to \neg\phi$	Hip.
2	ϕ	Hip.
3	$\neg\neg\phi$	2 T^+ (7)
4	$\neg\neg\phi \to ((\neg\psi \to \neg\phi) \to \psi)$	T^+ (3)
5	$(\neg\psi \to \neg\phi) \to \psi$	3, 4 (MP)
6	ψ	1, 5 (MP).

Então, por (MD),

(9a) $$\neg\psi \to \neg\phi \vdash_{\mathbf{H}} \phi \to \psi.$$

(10) $\phi \to \psi \vdash_{\mathbf{H}} \neg\psi \to \neg\phi$:

1	$\phi \to \psi$	Hip.
2	$\neg\neg\phi \to \phi$	T^+ (6)
3	$\neg\neg\phi \to \psi$	1, 2 T^+ (5a)
4	$\psi \to \neg\neg\psi$	T^+ (7)
5	$\neg\neg\phi \to \neg\neg\psi$	1, 2 T^+ (5a)
6	$\neg\psi \to \neg\phi$	5 T^+ (9a).

(11) $\vdash_{\mathbf{H}} (\phi \to \psi) \to ((\phi \to \neg\psi) \to \neg\phi)$, para o que basta mostrar que

$$\phi \to \psi\,, \phi \to \neg\psi \vdash_{\mathbf{H}} \neg\phi.$$

Ora, pela lei (6) $\neg\neg\phi\rightarrow\phi$, a primeira hipótese $\phi\rightarrow\psi$ e o silogismo hipotético (5a) resulta (i) $\neg\neg\phi\rightarrow\psi$; analogamente, usando agora a segunda hipótese, resulta (ii) $\neg\neg\phi\rightarrow\psi$; usando o axioma ($H_3$), (i), (ii) e a regra (MP), duas vezes, obtemos $\neg\phi$, como se pretendia.

(12) $\vdash_{\mathbf{H}} \phi\rightarrow(\neg\psi\rightarrow\neg(\phi\rightarrow\psi))$: exercício.

(13) $\vdash_{\mathbf{H}} (\phi\rightarrow\psi)\rightarrow((\neg\phi\rightarrow\psi)\rightarrow\psi)$: exercício.

Uma observação importante a respeito da demonstração do metateorema da dedução (MD) é que, para as transformações a efectuar, apenas são necessários os axiomas (H_1) e (H_2), e a regra (MP). Isto significa que o (MD) é válido para diversos subsistemas de **H** (nomeadamente, para o da lógica proposicional sem negação) e para subsistemas de sistemas que sejam variantes de **H** ou que, pelo menos, contem (H_1) e (H_2) entre os seus axiomas e a regra (MP). Além disso, a demonstração é construtiva, pois mostra como construir efectivamente uma derivação a partir de uma derivação dada.

Um exemplo paradigmático do que acabamos de dizer é o sistema seguinte, que designamos por **K**, devido essencialmente a S.C. Kleene (1952), nos primitivos $\neg$, $\rightarrow$, $\wedge$ e $\vee$, o que, além de facilitar a comparação com outros sistemas com estes primitivos e, até, com sistemas com outros primitivos, como **H**.

18.5 Axiomas e regras proposicionais de K

As fórmulas e regras de uma das formas seguintes são os axiomas e regras do sistema **K**:

(K_1) $\phi\rightarrow(\psi\rightarrow\phi)$;

(K_2) $((\phi\rightarrow(\psi\rightarrow\theta))\rightarrow((\phi\rightarrow\psi)\rightarrow(\phi\rightarrow\theta))$;[88]

(K_3) $\phi\rightarrow(\psi\rightarrow\phi\wedge\psi)$;

(K_{4a}) $\phi\wedge\psi\rightarrow\phi$; ($K_{4b}$) $\phi\wedge\psi\rightarrow\psi$;

(K_{5a}) $\phi\rightarrow\phi\vee\psi$; ($K_{5b}$) $\psi\rightarrow\phi\vee\psi$;

(K_6) $(\phi\rightarrow\theta)\rightarrow((\psi\rightarrow\theta)\rightarrow(\phi\vee\psi\rightarrow\theta))$;

(K_7) $(\phi\rightarrow\psi)\rightarrow((\phi\rightarrow\neg\psi)\rightarrow\neg\phi)$;

(K_8) $\neg\neg\phi\rightarrow\phi$.

Regra de inferência *modus ponens* (MP) $\dfrac{\phi,\ \phi\rightarrow\psi}{\psi}$.

---

[88] No sistema original de Kleene a numeração dos axiomas é ligeiramente diferente, e em vez dos axiomas (K_2) = (H_2) encontramos $(\phi\rightarrow\psi)\rightarrow((\phi\rightarrow(\psi\rightarrow\theta))\rightarrow(\phi\rightarrow\theta))$. Como se disse, a diferença não é essencial, em virtude da lei de permutação dos antecedentes do exemplo (4), a qual também se deriva sem dificuldade no sistema **K**.

A diferença mais significativa relativamente ao sistema **H** (descurando as diferenças mais óbvias, pelo facto de as listas de primitivos serem diferentes também), reside nos axiomas (K_7) e (K_8), os quais, grosso modo, e na presença dos dois primeiros, possuem uma força dedutiva equivalente ao axioma (H_3). A razão fundamental para a escolha por Kleene destas axiomas [em vez de, por exemplo, juntar simplesmente (K_3)-(K_6) a (H_1)-(H_2)] é a seguinte: mediante a omissão de um único axioma, (K_8), obtém-se uma axiomatização da lógica proposicional intuicionista, $\mathbf{K}_I$, nos primitivos $\neg$, $\rightarrow$, $\wedge$ e $\vee$ (ver final do Cap. V). Os exemplos (1)-(13) acima, juntamente com os exercícios 2.40, serão suficientes para convencer o leitor de que o sistema **H** é, pelo menos, tão forte como o sistema **K**:

$$\phi_1, \phi_2, ..., \phi_n \vdash_{\mathbf{K}} \psi \implies \phi_1, \phi_2, ..., \phi_n \vdash_{\mathbf{H}} \psi.$$

A propriedade recíproca desta também vale. Para isso, limitamo-nos a mostrar que $\vdash_{\mathbf{K}}$ (H_3), isto é, $\vdash_{\mathbf{K}} (\neg\phi \rightarrow \neg\psi) \rightarrow ((\neg\phi \rightarrow \psi) \rightarrow \phi)$,[89] para o que basta mostrar que $\neg\phi \rightarrow \neg\psi, \neg\phi \rightarrow \psi \vdash_{\mathbf{K}} \phi$: a partir das duas hipóteses, utilizando (K_7) $(\neg\phi \rightarrow \psi) \rightarrow ((\neg\phi \rightarrow \neg\psi) \rightarrow \neg\neg\phi)$ e (MP), duas vezes, obtemos $\neg\neg\phi$, e daqui são ϕ, eliminando a dupla negação.

A propriedade recíproca do metateorema da dedução,

$(*)$ se $\Gamma \vdash_{\mathbf{K}} \phi \rightarrow \psi$, então $\Gamma \cup \{\phi\} \vdash_{\mathbf{K}} \psi$,

é muito simples de provar (em **H** e em **K**), pois basta acrescentar duas linhas a uma dedução de $\phi \rightarrow \psi$ com hipóteses em Γ para obter uma dedução de ψ com hipóteses em $\Gamma \cup \{\phi\}$:

1 ⋮		} Hip. em Γ
m	$\phi \rightarrow \psi$	
m+1	ϕ	Hip.
m+2	ψ	m, m+1 (MP).

Para facilitar a comparação de **K** com **DN** e não só, é conveniente dispor de algumas propriedades adicionais da relação de derivabilidade em **K**, que podemos encarar como *propriedades de introdução e de eliminação dos conectivos*. Abreviamos $\Gamma \cup \{\phi\}$ em Γ, ϕ e $\vdash_{\mathbf{K}}$ em $\vdash$. Tal como em **DN**, o tratamento do bicondicional ($\leftrightarrow$) reduz-se à sua definição (pág. 48) e às propriedades da conjunção.

---

[89] Esta lei justifica a versão forte do método de *redução ao absudo,* clássica mas não intuicionisticamente válido, enquanto (K_7) é a versão fraca do referido método, a qual já é intuicionisticamente válido. Para mais pormenores veja-se o capítulo V e, em particular, a nota 53, p. 61.

18.6 Metateorema (Introdução e eliminação dos conectivos)

(a) *Introdução dos conectivos:*

(I$\rightarrow$) = (MD): $\Gamma, \phi \vdash \psi \Rightarrow \Gamma \vdash \phi \rightarrow \psi$;

(I$\wedge$): $\phi, \psi \vdash \phi \wedge \psi$;

(I$\vee$): $\phi \vdash \phi \vee \psi$; $\psi \vdash \phi \vee \psi$;

(I$\neg$) = (RA*): $\Gamma, \phi \vdash \psi$ e $\Gamma, \phi \vdash \neg\psi \Rightarrow \Gamma \vdash \neg\phi$.

(I$\leftrightarrow$): $\phi \rightarrow \psi, \psi \rightarrow \phi \vdash \phi \leftrightarrow \psi$.

(b) *Eliminação dos conectivos:*

(E$\rightarrow$) = (MP): $\phi, \phi \rightarrow \psi \vdash \psi$;

(E$\wedge$): $\phi \wedge \psi \vdash \phi$; $\phi \wedge \psi \vdash \psi$;

(E$\vee$): $\Gamma, \phi \vdash \theta$ e $\Gamma, \psi \vdash \theta \Rightarrow \Gamma, \phi \vee \psi \vdash \theta$;

(E$\neg\neg$): $\neg\neg\phi \vdash \phi$;

(E$\neg$) = ($\perp$): $\phi, \neg\phi \vdash \psi$.

(E$\leftrightarrow$): $\phi \leftrightarrow \psi \vdash \phi \rightarrow \psi$; $\phi \leftrightarrow \psi \vdash \psi \rightarrow \phi$.

Dem. As justificações são, na maioria, imediatas. Como ilustração, justificamos (I$\neg$), (E$\vee$) e (E$\neg$).

(I$\neg$): supondo $\Gamma, \phi \vdash \psi$ e $\Gamma, \phi \vdash \neg\psi$, pelo metateorema da dedução vem $\Gamma \vdash \phi \rightarrow \psi$ e $\Gamma \vdash \phi \rightarrow \neg\psi$, donde, utilizando os axiomas (K_7) e a regra (MP), duas vezes, obtém-se $\Gamma \vdash \neg\phi$.

(E$\vee$): supondo $\Gamma, \phi \vdash \theta$ e $\Gamma, \psi \vdash \theta$, pelo metateorema da dedução vem $\Gamma \vdash \phi \rightarrow \theta$ e $\Gamma \vdash \psi \rightarrow \theta$, donde, utilizando os axiomas (K_6) e (MP), obtém-se $\Gamma \vdash \phi \vee \psi \rightarrow \theta$, e finalmente $\Gamma, \phi \vee \psi \vdash \theta$, por ($*$) acima.

(E$\neg$): tem-se, trivialmente, $\phi, \neg\phi, \neg\psi \vdash \phi$ e $\phi, \neg\phi, \neg\psi \vdash \neg\phi$, donde $\phi, \neg\phi \vdash \neg\neg\psi$, por (I$\neg$), e como $\neg\neg\psi \vdash \psi$, por (E$\neg\neg$), vem $\phi, \neg\phi \vdash \psi$.■

As propriedades acima desempenham o papel de *regras derivadas* e algumas podem, é claro, ser formuladas como tal, por exemplo

$$(I\wedge)\ \frac{\phi, \psi}{\phi \wedge \psi}\ , (E\neg) = (\perp)\ \frac{\phi, \neg\phi}{\psi}, \text{ etc.}$$

Tratamos de seguida da relação entre **K** e **DN**. Não é difícil prever que

$$\text{Teor}_{\mathbf{K}} = \text{Teor}_{\mathbf{DN}}.$$

Para chegar a este resultado há duas vias, a *directa* (mostrando que para qualquer fórmula ϕ se tem $\vdash_{\mathbf{K}} \phi \iff \vdash_{\mathbf{DN}} \phi$), e a *indirecta,* passando pelos metateoremas da validade e da completude semântica para um ou outro dos

sistemas, por exemplo,

$$\text{Teor}_{\mathbf{K}} \subseteq \text{Val} \subseteq \text{Teor}_{\mathbf{K}}.$$

A primeira inclusão é simples de estabelecer por indução no comprimento das deduções, atendendo a que os axiomas de **K** são válidos e a regra (MP) é válida. A segunda inclusão (na versão generalizada) demonstra-se exactamente como para **DN** (pp. 76-78 e exercícios respectivos). Deixamos os pormenores ao cuidado do leitor.

*II.19 Outros sistemas dedutivos (IV): resolução

Uma propriedade desejável de um sistema dedutivo é a facilidade de mecanizar eficientemente a busca de derivações. Diferentes sistemas satisfazem este requisito de diferentes maneiras. Num extremo, os sistemas à Hilbert são ineficazes na busca. Os sistemas de dedução natural, dos *tableaux* ou de Gentzen são bastante bons para a lógica proposicional, mas perdem eficiência na lógica de primeira ordem. O método dedutivo chamado *resolução* é o sistema mais eficiente para a lógica proposicional, nele se baseando a linguagem PROLOG, e é particularmente vantajoso na lógica de primeira ordem. É um método *refutacional,* tal como o dos *tableaux* de Beth, com o qual tem, aliás, algumas semelhanças, e está no cerne de muitas aplicações da lógica às ciências da computação. Foi concebido em 1963 pelo lógico americano J. A. Robinson.[90]

O método de resolução só se aplica, porém, a fórmulas na FNC, pelo que é conveniente conhecer técnicas para obter fórmulas logicamente equivalentes na FNC mais expeditas do que a exposta em II.13. Um tal procedimento algoritmico, que descrevemos mais adiante, depende de certos conhecimentos e propriedades, como:

(1) *Equivalências lógicas* diversas, incluindo as referentes às leis de De Morgan, às leis associativas, comutativas e distributivas, e outras equivalências lógicas como

$$\begin{gathered}\phi \vee \phi \sim \phi, \qquad \phi \wedge \phi \sim \phi,\\ \phi \wedge (\psi \vee \neg\psi) \sim \phi, \quad \phi \vee (\psi \wedge \neg\psi) \sim \phi,\\ \neg\neg\phi \sim \phi;\end{gathered}$$

(2) a *transitividade da relação de equivalência lógica:* se $\phi_1 \sim \phi_2$ e $\phi_2 \sim \phi_3$, então $\phi_1 \sim \phi_3$;

(3) a *propriedade de substituição de equivalentes:* se σ_1 é uma subfórmula de $\phi = \phi[\sigma_1]$, $\phi' = \phi[\sigma_2]$ resulta de ϕ substituindo uma ou mais ocorrências de σ_1 pela fórmula σ_2, e $\sigma_1 \sim \sigma_2$, então $\phi \sim \phi'$.

---

90 "A Machine oriented logic based on the resolution principal", *J. ACM,* **12** (1965), pp. 23-41; reproduzido em SIECKMANN & WRIGHTSON (onde também se reproduzem outros trabalhos seminais sobre a demonstração automática).

Por exemplo, de

$$\phi = \phi[q \to r] = p \vee (q \to \neg(q \to r)),$$

resulta $\phi' = \phi[\neg q \vee r] = p \vee (q \to \neg(\neg q \vee r)) \sim \phi,$

pois $q \to r \sim \neg q \vee r$.

A propriedade (3) pode-se demonstrar facilmente por indução na complexidade das fórmulas.

Ao mesmo tempo que descrevemos o **algoritmo de conversão na FNC**, aplicamo-lo à fórmula

$$\phi = \neg((p \vee q) \wedge (\neg p \vee \neg q)) \wedge r.$$

O algoritmo consiste em instruções para, dada ϕ ao arbítrio (na linguagem com primitivos $\neg$, $\wedge$, $\vee$, $\to$ e, possivelmente, com o bicondicional definido $\leftrightarrow$) obter ϕ' tal que ϕ' está na FNC e $\phi' \sim \phi$ (ver quadro seguinte).

Etapas do algoritmo:	***Exemplo de aplicação a ϕ:***
1. Substituir toda a subfórmula de ϕ da forma $\sigma \to \theta$ por $\neg\sigma \vee \theta$, e $\sigma \leftrightarrow \theta$ por $(\neg\sigma \vee \theta) \wedge (\neg\theta \vee \sigma)$;	Nada a fazer a ϕ nesta etapa.
2. Mover as negações para junto das fórmulas atómicas (letras proposicionais) utilizando as leis de De Morgan (1);	$\phi \sim (\neg(p \vee q) \vee \neg(\neg p \vee \neg q)) \wedge r$ $\sim ((\neg p \wedge \neg q) \vee (\neg\neg p \wedge \neg\neg q)) \wedge r$
3. Juntar as literais dos mesmos átomos utilizando as leis associativas e comutativas, simplificar as duplas negações $\neg\neg p_i$, as iteradas $p_i \wedge p_i$ e $p_i \vee p_i$ e eliminar $p_i \wedge \neg p_i$ e $p_i \vee \neg p_i$, conforme as equivalências lógicas (1), utilizando a propriedade de substituição (4);	$\sim ((\neg p \wedge \neg q) \vee (p \wedge q)) \wedge r$
4. Aplicar as leis distributivas (1);	$\sim (((\neg p \wedge \neg q) \vee p) \wedge ((\neg p \wedge \neg q) \vee q)) \wedge r$
5. Regressar às etapas 3 e 4 tantas vezes quantas necessárias, até obter uma equivalente a ϕ na FNC.	$\sim (\neg p \vee p) \wedge (\neg q \vee p) \wedge (\neg p \vee q) \wedge$ $\wedge (\neg q \vee q) \wedge r$ $\sim (\neg p \vee q) \wedge (\neg p \vee q) \wedge r.$

Para aplicar o método de resolução é conveniente apresentar as fómulas não na FNC usual (conjunção de disjunções de literais)

$$\phi = (P_{11} \vee \cdots \vee P_{1k_n}) \wedge (P_{21} \vee \cdots \vee P_{2k_n}) \wedge \cdots \wedge (P_{n1} \vee \cdots \vee P_{nk_n}),$$

mas na chamada *forma clausural,* quer dizer, como um *conjunto de conjuntos de literais*

$$\mathcal{C}_\phi = \{\{P_{11}, ..., P_{1k_n}\}, \{P_{21}, ..., P_{2k_n}\}, ..., \{P_{n1}, ..., P_{nk_n}\}\},$$

o qual, por abuso, por vezes também designamos por ϕ. Cada membro $\{P_{i1}, ..., P_{ik_n}\}$, $i = 1, ..., n$ desta forma clausural é chamado uma *cláusula.* Note-se o papel diferenciado da vírgula ‘, ’ separando as literais dentro das cláusulas — correspondente a ‘ $\vee$ ’ — e separando as cláusulas dentro da forma clausural — como se fosse ‘ $\wedge$ ’.

Por exemplo,

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

tem a forma clausural

$$\phi = \mathcal{C}_\phi = \{\{\neg q, p\}, \{\neg p, q\}, \{r\}\}.$$

19.1 Definição Dizemos que uma valoração booleana $\widehat{v}$ *satisfaz* (ou é *modelo de*) uma cláusula $C_i = \{P_{i1}, ..., P_{ik_n}\}$ sse $\widehat{v}$ satisfaz alguma literal P_{ij} (isto é, sse satisfaz a disjunção $P_{i1} \vee \cdots \vee P_{ik_n}$), e dizemos que $\widehat{v}$ satisfaz a forma clausural $\mathcal{C} = \{C_1, ..., C_n\}$ sse $\widehat{v}$ satisfaz todas as cláusulas C_1, ..., C_n. Uma forma clausural $\mathcal{C}$ é *compatível* sse $\mathcal{C}$ tem, pelo menos, um modelo.

No exemplo acima, $\widehat{v}$ tal que $\widehat{v}p = \widehat{v}q = \widehat{v}r = 1$ satisfaz $\mathcal{C}_\phi$, pois satisfaz as três cláusulas $C_1 = \{\neg q, p\}$, $C_2 = \{\neg p, q\}$, $C_3 = \{r\}$.

Por razões técnicas, admitiremos que existe uma *cláusula nula* (ou *vazia*), designada por

$$\square,$$

a qual *é incompatível, por convenção*.[91] Por virtude desta convenção, não devemos confundir $\square$ com o *conjunto vazio* de literais, $\emptyset$, já que este é trivialmente compatível.[92] É claro, portanto, que *qualquer forma clausural $\mathcal{C}$ contendo $\square$ é incompatível,* pois nenhuma valoração booleana satisfaz $\square$.

19.2 Notações da «programação em lógica»

Em várias versões do PROLOG e da «Programação em lógica» são comuns a terminologia e as notações seguintes:

Se ϕ é da forma $p_1 \vee \cdots \vee p_k \vee \neg q_1 \vee \cdots \vee \neg q_\mathrm{m}$, onde os p_i’s e os q_j’s são átomos, então, pelas leis de De Morgan, comutativas e de conversão,

$$\phi \sim p_1 \vee \cdots \vee p_k \vee \neg(q_1 \wedge \cdots \wedge q_\mathrm{m}) \sim q_1 \wedge \cdots \wedge q_\mathrm{m} \rightarrow p_1 \vee \cdots \vee p_k,$$

---

[91] Queremos assim, pois não deixamos de interpretar $\square$ (e qualquer outra cláusula) como «verdadeira» quando e só quando uma, pelo menos, das literais em $\square$ é verdadeira (como se $\square$ continuasse a ser uma disjunção aos nossos olhos).

[92] Na realidade, para qualquer $\widehat{v}$, $\widehat{v}$ satisfaz todas as fórmulas de $\emptyset$, caso contrário existiria, pelo menos, uma fórmula $\phi \in \emptyset$ que não era satisfeita por $\widehat{v}$, o que é impossível.

sendo todavia mais comum a escrita sinónima

(1) $$p_1 \vee \cdots \vee p_k \leftarrow q_1 \wedge \cdots \wedge q_m,$$

(que se lê e significa intencionalmente: «p_1 ou $\cdots$ ou p_k se q_1 e $\cdots$ e q_m), que os lógicos informáticos abreviam em

(2) $$p_1; ...; p_k :- q_1, ..., q_m.$$

Com $k = 1$, obtemos

(3) $$p_1 :- q_1, ..., q_m,$$

que é, portanto, uma abreviatura de $p_1 \leftarrow q_1 \wedge \cdots \wedge q_m$ («p_1, se q_1 e $\cdots$ e q_m), ou seja, de $q_1 \wedge \cdots \wedge q_m \rightarrow p_1$, proveniente de uma fórmula de Horn (p. 89), razão por que se chama também a (3), ou à cláusula $\{p_1, \neg q_1, \cdots, \neg q_m\}$, uma *cláusula de Horn.*

Observe-se ainda que um conjunto de cláusuras, $\mathcal{C}$, pode ser considerado como uma *base de dados,* onde as cláusulas que constituem $\mathcal{C}$ representam informação sobre as relações entre as cláusulas. Em termos de «derivabilidade» ou da escrita de programas, interpretamos intuitivamente a afirmação (como «verdadeira») de uma cláusula de Horn (4) como a especificação das condições em que o objectivo p_1 é «verdadeiro». Como estamos normalmente interessados em estabelecer certo resultado, o átomo p_1 é o *objectivo («goal»)* ou a *cabeça* de (3), e as componentes q_1, ..., q_m formam o *corpo* de (3) (será caso para dizer, em conformidade, que o símbolo ' $:-$ ' representa o *pescoço* que liga a cabeça ao tronco). Os átomos do corpo q_1, ..., q_m também são chamados os *subobjectivos:* intuitivamente, (3) diz-nos que, para estabelecer p_1, devemos primeiro estabelecer q_1, ..., q_m — primeiro o corpo, e depois, a cabeça. A esta terminologia junta-se uma outra, a do sucesso/fracasso: o objectivo p_1 é *bem sucedido* se for «verdadeiro» quando os subobjectivos são «verdadeiros» (em termos de programação, isto pode significar ter uma derivação de p_1 a partir do corpo), e, no caso contrário, o objectivo *falhou* ou *fracassou*.

Se $k = 0$ em (2), a cláusula de Horn fica reduzida a

(4) $$:- q_1, ..., q_m,$$

que é chamada uma *cláusula de objectivo definido* ou *objectivo de programa,* e, por ser equivalente a $\neg q_1 \vee \cdots \vee \neg q_m$, significa que um dos q_j, pelo menos, é «falso» ou fracassou. Se $m = 0$, a cláusula

(5) $$p_1 :-$$

é uma *cláusula unitária,* e significa simplesmente que p_1 é «verdadeira» ou bem sucedida e, por isso, também é chamada um *facto*.

19.3 Regra de resolução

O sistema de resolução, **R**, é baseado numa única regra, a *regra de resolução,* (R), que a cada par de cláusulas, C_1 e C_2 em certas condições, faz corresponder uma outra cláusula D, chamada uma *resolvente* daquelas duas, o que pode ser indicado por um esquema como

$$\frac{C_1,\ C_2}{D}, \quad \text{ou} \quad \begin{matrix} C_1 & C_2 \\ & \bigvee \\ & D \end{matrix}.$$

Para se poder aplicar a regra (R) às cláusulas C_1 e C_2 é necessário que para alguma literal L se tenha $L \in C_1$ e $\overline{L} \in C_2$, onde

$$\overline{L} = \begin{cases} \neg p & \text{se } L = p, \\ p & \text{se } L = \neg p. \end{cases}$$

Nestas condições, a resolvente de C_1 e C_2 é

$$D = (C_1 \setminus \{L\}) \cup (C_2 \setminus \{\overline{L}\}).$$

Resumindo, se $L \in C_1$ e $\overline{L} \in C_2$ para alguma literal L, então a regra tem a forma

(R) $$\frac{C_1, \quad C_2}{(C_1 \setminus \{L\}) \cup (C_2 \setminus \{\overline{L}\})}.$$

19.4 Exemplos (1)

$$\frac{\{\neg p, q\}, \{p, r\}}{\{q, r\}};$$

(2)

$$\frac{\{p_1, p_2, ..., p_k, \neg q_1, ..., \neg q_m\}, \{\neg p_1, p_2, ..., p_k, \neg r_1, ..., \neg r_l\}}{\{p_2, ..., p_k, \neg q_1, ..., \neg q_m, \neg r_1, ..., \neg r_l\}}.$$

(3) Se $\mathcal{C} = \{C_1, ..., C_n\}$ é um conjunto finito de cláusulas, a regra (R) poderá aplicar-se a vários pares de cláusulas. Por exemplo, se $\mathcal{C} = \{C_1, C_2, C_3\}$, onde

$$C_1 = \{p, \neg q, \neg r\},\ C_2 = \{q, s\},\ C_3 = \{\neg p, \neg s\},$$

então a regra de resolução pode-se aplicar aos três pares possíveis:

$$\frac{C_1, \quad C_2}{\{p, \neg r, s\}}, \quad \frac{C_1, \quad C_3}{\{\neg q, \neg r, \neg s\}}, \quad \frac{C_2,\ C_3}{\{q, \neg p\}}.$$

Às resolventes $D_1 = \{p, \neg r, s\}$ e $D_2 = \{\neg q, \neg r, \neg s\}$, podemos voltar a aplicar a regra (R):

$$\frac{D_1, D_2}{\{p, \neg r, \neg q\}}.$$

Em geral, se $\mathcal{C} = \{C_1, ..., C_n\}$, chama-se **conjunto resolvente** de $\mathcal{C}$ ao conjunto de cláusulas

$$R(\mathcal{C}) = \mathcal{C} \cup \{D : D \text{ é uma resolvente de duas cláusulas em } \mathcal{C}\}.$$

Para o exemplo $\mathcal{C} = \{C_1, C_2, C_3\}$ acima, tem-se

$$R(\mathcal{C}) = \{C_1, C_2, C_3, \{p, \neg r, s\}, \{\neg q, \neg r, \neg s\}, \{q, \neg p\}\}.$$

Definimos recursivamente os conjuntos de cláusulas $R^n(\mathcal{C})$ ($n \geq 0$) por

$$\begin{aligned} &R^0(\mathcal{C}) = \mathcal{C}, \\ &R^1(\mathcal{C}) = R(\mathcal{C}), \\ &R^2(\mathcal{C}) = R(R(\mathcal{C})), \\ &..., \\ &R^{n+1}(\mathcal{C}) = R(R^n(\mathcal{C})), \\ &..., \end{aligned}$$

e, finalmente, o **fecho** de $\mathcal{C}$ por R, pondo

$$R^*(\mathcal{C}) = \bigcup_{n=0}^{\infty} R^n(\mathcal{C}) = \mathcal{C} \cup R(\mathcal{C}) \cup R^2(\mathcal{C}) \cup \cdots.$$

Note-se que, se $\mathcal{C}$ é finito, então cada conjunto $R^n(\mathcal{C})$ também é finito mas, é claro, o fecho $R^*(\mathcal{C})$ pode não ser finito, pelo menos em princípio, mesmo que $\mathcal{C}$ seja finito.

Por outro lado, é conveniente ter em conta uma outra definição possível (equivalente à dada — veja-se a secção II.3, pág. 49, e o exercício 2.1) de fecho $R^*(\mathcal{C})$: é o mais pequeno conjunto de cláusulas contendo (as cláusulas de) $\mathcal{C}$ e fechado para R, isto é, o mais pequeno conjunto de cláusulas tal que:

(i) se $C \in \mathcal{C}$, então $C \in R^*(\mathcal{C})$;

(ii) se $C_1, C_2 \in \mathcal{C}$ e D é uma resolvente de C_1 e C_2, então $D \in R^*(\mathcal{C})$.

19.5 Observações 1) Um par de cláusulas pode ter mais do que uma resolvente, por exemplo,

$$\frac{\{p, q\}, \{\neg p, \neg q\}}{\{q, \neg q\}}, \qquad \frac{\{p, q\}, \{\neg p, \neg q\}}{\{p, \neg p\}};$$

2) Uma resolvente possível é a cláusula vazia, por exemplo,

$$\frac{\{p\}, \{\neg p\}}{\square}.$$

3) Recorde-se que uma cláusula $C = \{p_1, ..., p_k, \neg q_1, ..., \neg q_l\}$ representa uma disjunção $(p_1 \vee \cdots \vee p_k \vee \neg q_1 \vee \cdots \vee \neg q_l)$, e que uma forma clausural ou conjunto de cláusulas $\mathcal{C} = \{C_1, ..., C_n\}$ representa uma conjunção («$C_1 \wedge \cdots \wedge C_n$») e, por conseguinte, uma fórmula na FNC: $\mathcal{C} = \mathcal{C}_\phi = \phi = \bigwedge\bigvee P_{ij}$. Assim, facilmente se compreende e demonstra que *a regra de resolução é válida: sempre que uma valoração booleana v satisfaz as cláusulas C_1 e C_2, e D é uma resolvente de C_1 e C_2, então v satisfaz D.* Mais geralmente, tem-se o seguinte:

19.6 Lema [Validade da regra (R)]

Se uma valoração booleana $\widehat{v}$ satisfaz uma forma clausal $\mathcal{C}$, então v satisfaz $R(\mathcal{C})$. Por conseguinte, a regra (**R**) *preserva a compatibilidade: se $\mathcal{C}$ é compatível, então $R(\mathcal{C})$ é compatível.*

Dem. Atendendo à definição de $R(\mathcal{C})$, basta realmente mostrar que se uma valoração v é modelo das cláusulas C_1 e C_2, e D é uma resolvente de C_1 e C_2, então v é modelo de D. Sem perda de generalidade podemos supor $C_1 = C_1' \cup \{L\}$, $C_2 = C_2' \cup \{\overline{L}\}$ (com $L \notin C_1'$ e $\overline{L} \notin C_2'$). Ora, se v satisfaz ambas as cláusulas, então v satisfaz *uma* das literais L, $\overline{L}$, pelo menos, *e também* uma das literais em $C_1' \cup C_2'$, a qual ainda está na resolvente D, logo v é modelo de D.■

Montaremos agora o sistema dedutivo baseado na regra de resolução, mediante a definição do que constitui um derivação neste sistema.

19.7 Definição Uma **derivação**-R a partir de um conjunto de cláusulas (em particular, a partir de uma forma clausural $\mathcal{C} = \mathcal{C}_\phi$, ou, abusivamente, a partir de ϕ) é uma sequência finita de cláusulas D_1, ..., D_m de tal modo que, para cada $i = 1$, ..., m, $D_i \in \mathcal{C}$ ou existem j, $k < m$ tais que $D_i \in R(\{D_j, D_k\})$. Uma cláusula D diz-se **derivável**-R a partir de $\mathcal{C} = \mathcal{C}_\phi$ (ou de ϕ), e escreve-se

$$\mathcal{C} \vdash_{\mathbf{R}} D \text{ (ou } \phi \vdash_{\mathbf{R}} D),$$

sse existe, pelo menos, uma derivação a partir de $\mathcal{C}$ cuja última cláusula é precisamente D (e dizemos que se se trata de uma derivação de D a partir de $\mathcal{C}$). Se $D = \square$, a derivação de D a partir de $\mathcal{C}$ chama-se uma **refutação**-R de $\mathcal{C}$, e D é **refutável**-R a partir de $\mathcal{C}$ sse existe uma **refutação**-R de D a partir de $\mathcal{C}$.[93]

---

[93] Na prática, podem-se omitir o prefixo «-R» e a expressão «a partir de $\mathcal{C}$» quando não houver perigo de confusão. Por outro lado, nesta definição de derivabilidade a partir de $\mathcal{C}$, $\mathcal{C}$ é um conjunto arbitrário (finito ou infinito) de cláusulas e, por isso, estende-se natural e

Observe-se que esta definição assegura, desde logo, a *propriedade de finitude:* se $\mathcal{C} \vdash_{\mathbf{R}} C$, então existe um conjunto finito de cláusulas $\mathcal{C}_0 \subseteq \mathcal{C}$ tal que $\mathcal{C}_0 \vdash_{\mathbf{R}} C$.

Atendendo ao lema acima e ao facto de $\square$ ser incompatível, compreende-se que, se $\square$ é derivável-R de $\mathcal{C}$, então uma tal derivação é uma indicação de que $\mathcal{C}$ é incompatível (ver metateorema da validade mais adiante).

19.8 Exemplos (1) Vamos determinar $R^*(\mathcal{C})$, onde $\mathcal{C} = \{\{p, q\}, \{\neg p, \neg q\}\}$. Ora, as resolventes possíveis são $\{q, \neg q\}$ e $\{p, \neg p\}$, de modo que

$$R^1(\mathcal{C}) = \{\{p, q\}, \{\neg p, \neg q\}, \{q, \neg q\}, \{p, \neg p\}\}.$$

De quaiquer duas destas quatro cláusulas não se obtém nenhuma resolvente nova e, portanto, podemos concluir que $R^1(\mathcal{C}) = R^2(\mathcal{C}) = R^*(\mathcal{C})$.

(2) Dada $\phi = (p \leftrightarrow (q \rightarrow r)) \wedge (p \leftrightarrow q) \wedge (p \leftrightarrow \neg r)$, mostramos que ϕ é incompatível, construindo uma derivação-R de $\square$ a partir de ϕ. A primeira coisa a fazer, todavia, é obter ϕ na FNC e, depois, na forma clausal. Tem-se

$$\begin{aligned} \phi \quad \sim \quad & (\neg p \vee \neg q \vee r) \wedge (q \vee r) \wedge (\neg r \vee p) \wedge (\neg p \vee q) \wedge (\neg q \vee p) \wedge \\ & \wedge (\neg p \vee \neg r) \wedge (r \vee \neg p), \end{aligned}$$

e, portanto,

$$\mathcal{C} = \mathcal{C}_\phi = \{\{\neg p, \neg q, r\}, \{q, p\}, \{\neg r, p\}, \{\neg p, q\}, \{\neg q, p\}, \{\neg p, \neg r\}, \{r, \neg p\}\}.$$

Exibimos a seguir a prova de que

$$(p \leftrightarrow (q \rightarrow r)) \wedge (p \leftrightarrow q) \wedge (p \leftrightarrow \neg r) \vdash_{\mathbf{R}} \square.$$

Derivando:

1.	$\{q, p\}$	$\mathcal{C}$
2.	$\{\neg q, p\}$	$\mathcal{C}$
3.	$\{p\}$	1, 2 R
4.	$\{\neg p, \neg q, r\}$	$\mathcal{C}$
5.	$\{\neg p, \neg r\}$	$\mathcal{C}$
6.	$\{\neg p, \neg q\}$	4, 5 R
7.	$\{\neg p, q\}$	$\mathcal{C}$
8.	$\{\neg p\}$	6, 7 R
9.	$\square$	3, 8 R.

---

imediatamente à derivabilidade a partir de $\mathcal{C}_1, \ldots, \mathcal{C}_n$ considerando a união $\mathcal{C} = \bigcup_{i=1}^{n} \mathcal{C}_i$. Se $\mathcal{C} = \{C_1, \ldots, C_n\}$, abreviamos '$\mathcal{C} \vdash D$' em '$C_1, \ldots, C_n \vdash D$'

As derivações-R também podem ser apresentadas sob a forma de árvore. Exemplificando:

$$\begin{array}{c} \{\neg p, \neg q, r\} \quad \{\neg p, \neg r\} \\ \vee \\ \{q, p\} \quad \{\neg q, p\} \quad \{\neg p, \neg q\} \quad \{\neg p, q\} \\ \vee \qquad\qquad \vee \\ \{p\} \qquad\qquad \{\neg p\} \\ \vee \\ \square. \end{array}$$

(3) $\{\{p, \neg q\}, \{\neg p, \neg q, \neg r\}, \{\neg p, \neg q, r\}\} \vdash_{\mathbf{R}} \{\neg q\}$:

$$\begin{array}{c} \{\neg p, \neg q, \neg r\} \quad \{\neg p, \neg q, r\} \\ \vee \\ \{p, \neg q\} \quad \{\neg p, \neg q\} \\ \vee \\ \{\neg q\}. \end{array}$$

Daqui também podemos facilmente obter uma outra derivação que mostre que:

$$\{\{p, \neg q\}, \{\neg p, \neg q, \neg r\}, \{\neg p, \neg q, r\}, \{q\}\} \vdash_{\mathbf{R}} \square.$$

Até final desta secção ocupamo-nos da metateoria, nomeadamente, dos metateoremas da validade e da completude semântica.

A derivabilidade-R pode ser caracterizada em termos do fecho por R do seguinte modo:

19.9 Lema (Caracterização da derivabilidade-R)

*Para toda a cláusula C e forma $\mathcal{C}$, existe uma derivação-*R *de C a partir de $\mathcal{C}$ sse $C \in R^*(\mathcal{C})$; em particular, C é refutável-*R *a partir de $\mathcal{C}$ sse $\square \in R^*(\mathcal{C})$:*

$$\mathcal{C} \vdash_{\mathbf{R}} C \;\Leftrightarrow\; C \in R^*(\mathcal{C}); \textit{ em particular, } \mathcal{C} \vdash_{\mathbf{R}} \square \;\Leftrightarrow\; \square \in R^*(\mathcal{C}).$$

Dem. As definições da derivabilidade e do fecho por R são ambas indutivas, o que vai permitir demonstrar o lema por indução, em ambos os sentidos. Isto acarreta, em ambas as demonstrações, que se demonstre um pouco mais do que o que aparenta ser necessário.

($\Rightarrow$) Suponhamos que $\mathcal{C} \vdash_{\mathbf{R}} C$. Provamos, por indução no comprimento n das derivações C_1, C_2, ..., C_n de $C = C_n$ a partir de $\mathcal{C}$, que para todo $i \leq n$ se tem $C_i \in R^*(\mathcal{C})$ [com $i = n$ resulta, em particular, que que $C \in R^*(\mathcal{C})$]. Se esse comprimento é $n = 1$, só pode ser $C \in \mathcal{C}$, e é evidente que $C \in R^*(\mathcal{C}) = \mathcal{C} \cup \ldots$. Suponhamos que a propriedade em questão é verdadeira para n e seja C_1, C_2, ...,

C_n, C_{n+1} uma derivação de C de comprimento $n+1$. Então, por hipótese de indução, C_1, C_2, ..., $C_n \in R^*(\mathcal{C})$, e dois casos se podem dar:

(i) $C_{n+1} \in \mathcal{C}$ — neste caso é imediato que $C_{n+1} \in R^*(\mathcal{C})$; ou

(ii) C_{n+1} é uma resolvente de C_j e C_k para alguns j, $k \leq n$; como C_j, $C_k \in R^*(\mathcal{C})$ por hipótese de indução, digamos C_j, $C_k \in R^m(\mathcal{C})$ com m suficientemente grande, então $C_{n+1} \in R^{m+1}(\mathcal{C}) \subseteq R^*(\mathcal{C})$.

($\Leftarrow$) Reciprocamente, suponhamos que $C \in R^*(\mathcal{C})$, digamos $C \in R^k(\mathcal{C})$. Bastará provar, por indução em n, que toda a cláusula de $R^n(\mathcal{C})$ é derivável-R a partir de $\mathcal{C}$. Deixamos os pormenores ao cuidado do leitor.■

Até final desta secção ocupamo-nos da metateoria, nomeadamente, dos metateoremas da validade e da completude semântica. O lema 19.6 acima (p. 0) é a chave para o resultado mais «fácil».

19.10 Metateorema da validade do sistema de resolução

*Se $\mathcal{C}$ é refutável-*R*, então $\mathcal{C}$ é incompatível:*

$$\mathcal{C} \vdash_{\mathbf{R}} \square \Rightarrow \mathcal{C} \text{ incompatível.}$$

Dem. Iterando o lema 19.6 tantas vezes quantas as necessárias, vê-se que se $\mathcal{C}$ for compatível e C_1, ..., C_n for uma derivação a partir de $\mathcal{C}$, então cada C_i ($1 \leq i \leq n$) é compatível. Como $\square$ é incompatível, nenhuma tal derivação pode ser uma derivação de $\square$.■

19.11 Lema

*Se $\mathcal{C}$ é uma forma incompatível contendo apenas literais nos átomos p_1, ..., p_k ($k \geq 1$), e $\mathcal{C}^{k-1}$ é o conjunto da cláusulas deriváveis-*R *a partir de $\mathcal{C}$ contendo apenas literais nos átomos p_1, ..., p_{k-1}, então $\mathcal{C}^{k-1}$ é incompatível.*

Dem. Tomando $\mathcal{C}$ e $\mathcal{C}^{k-1}$ como no enunciado, e supondo $\mathcal{C}^{k-1}$ compatível, com vista a uma contradição, seja v um modelo de $\mathcal{C}^{k-1}$ e sejam v_1, v_2 valorações que coincidem com v em p_1, ..., p_{k-1} e tais que

$$v_1(p_k) = 1, \; v_2(p_k) = 0.$$

Como $\mathcal{C}$ é incompatível, por hipótese, existe alguma cláusula em $\mathcal{C}$, digamos $C_1 \in \mathcal{C}$ que não é satisfeita por v_1. Então $\neg p_k \in C_1$, pois, se assim não fosse, ou

(a) $p_k \notin C_1$, caso em que $C_1 \in \mathcal{C}^{k-1}$ e v_1 satisfaz C_1, o que é absurdo, pois $v_1(p_k) = 1$; ou

(b) $p_k \in C_1$, e neste caso v_1 satisfaz $\mathcal{C}^{k-1}$ e $v_1(p_k) = 1$, logo v_1 satisfaz C_1, o que é igualmente absurdo.

Analogamente se pode chegar à conclusão que existe $C_2 \in \mathcal{C}$ que não é satisfeita por v_2 e tal que $p_k \in C_2$.

Ponhamos

$$D = (C_1 \setminus \{\neg p_k\}) \cup (C_2 \setminus \{p_k\}).$$

Então D é uma resolvente de C_1 e C_2 e $D \in \mathcal{C}^{k-1}$, por conseguinte, v satisfaz D. Isto conduz a uma das condições seguintes:
(a′) v satisfaz $C_1 \setminus \{\neg p_k\}$, logo v_1 satisfaz C_1, o que é absurdo, ou
(b′) v satisfaz $C_2 \setminus \{p_k\}$, logo v_2 satisfaz C_2, o que é igualmente absurdo.
Portanto, $\mathcal{C}^{k-1}$ é incompatível.■

19.12 Metateorema da completude semântica do sistema R

*Se $\mathcal{C}$ é uma forma clausural finita e incompatível, então $\mathcal{C}$ é refutável-*R*:*

$$\mathcal{C} \text{ incompatível } \Rightarrow \mathcal{C} \vdash_{\mathbf{R}} \square.$$

Dem. Se $\mathcal{C}$ é uma forma clausural finita e incompatível, então $\mathcal{C}$ contém apenas um número finito de literais, digamos, nos átomos p_1, ..., p_k, e podemos aplicar o lema 19.11 uma vez, obtendo $\mathcal{C}^{k-1}$ incompatível, com literais nos átomos p_1, ..., p_{k-1}. Repetindo k vezes, concluimos que $\mathcal{C}^0$ é incompatível, mas, como em $\mathcal{C}^0$ não há literais alguns, só pode ser $\mathcal{C}^0 = \{\square\}$ e, portanto, $\square \in R^*(\mathcal{C})$.■

II.20 Exercícios e Complementos

§II.1

2.1 Uma **construção formativa** de uma expressão σ é uma sequência finita de expressões σ_1, σ_2, ..., σ_n ($n \geq 1$) tal que $\sigma_n = \sigma$ e para cada $i = 1, ..., n$, σ_i é uma letra proposicional, ou existe $j < i$ tal que $\sigma_i = \neg\sigma_j$, ou existem j, $k < i$ tais que $\sigma_i = (\sigma_j \diamond \sigma_k)$, onde $\diamond$ é $\wedge$, $\vee$ ou $\rightarrow$. O inteiro positivo n é o *comprimento* da construção formativa σ_1, σ_2, ..., σ_n. Por exemplo, p, $\neg p$, q, $(q \wedge \neg p)$ é uma construção formativa de $(q \wedge \neg p)$ de comprimento 4 e p, $\neg p$, r, q, $(q \wedge \neg p)$ é outra, de comprimento 5. As fórmulas que antecedem a fórmula ϕ numa construção formativa de ϕ [ver (a) e (b) adiante] de comprimento mínimo são as **subfórmulas próprias** de ϕ. Denota-se F_* o conjunto das expressões que possuem construções formativas.

(a) Prove, por indução na complexidade das fórmulas, que Prop$(P) \subseteq F_*$, isto é, toda a fórmula possui, pelo menos, uma construção formativa.

*(b) Mostre, por indução completa no comprimento das construções formativas das expressões, que $F_* \subseteq$ Prop(P)[94], e conclua que $F^* = F_* =$ Prop(P).

---

[94] Mostre que (i) toda a expressão que possui uma construção formativa de comprimento 1 pertence a Prop(P) e que (ii) para todo n, se toda a expressão que possui uma construção formativa de comprimento $\leq n$ pertence a Prop(P) (hipótese de indução), então toda a expressão que possui uma construção formativa de comprimento $n + 1$ pertence a Prop(P).

2.2 Seja $\sigma = s_1 \cdots s_n$ uma expressão de comprimento $n \geq 1$ (onde os s_i são, portanto, símbolos do alfabeto). Um **segmento inicial próprio** de σ é uma expressão da forma $s_1 \cdots s_k$ com $1 \leq k < n$.

(a) Prove que nenhum segmento inicial próprio de uma fórmula de $\mathcal{L}^0$ é fórmula. [Sugestão: mostre que, para toda a fórmula ϕ, os segmentos iniciais próprios de ϕ começam com $\neg$ ou têm mais parênteses esquerdos do que direitos.]

(b) Utilize o resultado anterior para demonstrar a Propriedade de Unicidade de Representação das fórmulas.

2.3 Demonstre, por indução na complexidade das fórmulas, as seguintes propriedades:

(a) Lema do Equilíbrio.

(b) Para toda a fórmula ϕ e toda a valoração booleana v, $v(\phi)$ *só depende dos valores* $v(p_i)$ *atribuídos às letras proposicionais* p_i *que ocorrem em* ϕ. [Sugestão: para quaisquer valorações v e v' tais que $v(p_i) = v'(p_i)$ para toda a letra proposicional p_i que ocorre em ϕ, tem-se $v(\phi) = v'(\phi)$.]

***2.4** A *Propriedade de Extensão das Valorações* é um caso particular de um princípio mais geral de *definição de funções por recorrência.* O contexto adequado para enunciar e demonstrar este princípio, na sua máxima generalidade, é a teoria dos conjuntos. Não pretendemos aqui embarcar nessa generalidade, mas fornecemos as indicações suficientes para demonstrar a referida propriedade.

Sejam $u_\neg$, $u_\wedge$, $u_\vee$, $u_\rightarrow$ as funções booleanas correspondentes aos conectivos proposicionais. Dada uma valoração $v : \mathrm{Prop}(P) \to \{0, 1\}$, pretende-se provar que existe uma única valoração booleana $\widehat{v}$ tal que

(i) $\widehat{v}(p) = v(p)$ para todo p em P,

(ii) para qualquer fórmula ϕ, $\widehat{v}(\neg\phi) = u_\neg(\widehat{v}(\phi))$ e

(iii) para quaisquer fórmulas ϕ, ψ, $\widehat{v}(\phi \diamond \psi) = u_\diamond(\widehat{v}(\phi), \widehat{v}(\psi))$, onde $\diamond$ é $\wedge$, $\vee$ ou $\rightarrow$, respectivamente.

(a) Dê uma definição indutiva de $\widehat{v}$, como conjunto de pares ordenados $(\phi, \boldsymbol{i})$, com ϕ em $\mathrm{Prop}(P)$ e $\boldsymbol{i}$ em $\{0, 1\}$;[95]

(b) Enuncie e demonstre para $\widehat{v}$ um princípio de indução;

(c) Prove que $\widehat{v}$ é uma função definida em $\mathrm{Prop}(P)$;

(d) Prove que $\widehat{v}$ é a única função definida em $\mathrm{Prop}(P)$ tal que (i), (ii) e (iii).

Este modo de proceder é legitimado por uma versão do *Princípio de Indução Completa* nos números naturais (ver Cap. IV).

[95] Não perder de vista que uma função de um conjunto A para um conjunto B é, tecnicamente, uma relação de A para B (isto é, um subconjunto do produto cartesiano $A \times B$) definida em A (todo o elemento de A está em relação com um elemento de B) e funcional (nenhum elemento de A está em relação com mais de um elemento de B [ver exercícios 1.5 (n), (o)].

2.5 Efectue todas as deduções que foram indicadas no texto, explicitando as dependências de hipóteses.

2.6 Três indivíduos, aqui designados por A, B e C, suspeitos de um crime, fazem os seguintes depoimentos, respectivamente: ϕ:— B é culpado, mas C é inocente; ψ:— Se A é culpado, então C é culpado; θ:— Eu estou inocente, mas um dos outros dois é culpado.

(a) Os três depoimentos são compatíveis?

(b) Algum dos depoimentos é consequência dos outros dois?

(c) Construa deduções correspondentes à alínea anterior.[96]

(d) Supondo os três réus inocentes, quem mentiu?

(e) Supondo que todos disseram a verdade, quem é inocente e quem é culpado?

(f) Supondo que os inocentes disseram a verdade e os culpados mentiram, quem é inocente e quem é culpado?[97]

2.7 (a) Mostre que um conjunto $\Sigma = \{\phi_1, ..., \phi_n, \neg\psi\}$ é incompatível sse $\phi_1, ..., \phi_n \vDash \psi$ (ou, equivalentemente, que o conjunto Σ é compatível sse $\phi_1, ..., \phi_n \nvDash \psi$). Mais geralmente, para qualquer conjunto Γ e qualquer fórmula ϕ,

$$\Gamma \cup \{\neg\phi\} \text{ é incompatível sse } \Gamma \vDash \phi$$

(b) Prove que, se Γ é incompatível, então para qualquer ϕ, $\Gamma \vDash \phi$.

§II.4-II.10

2.8 Mostre que as seguintes versões de *modus tollens* são regras derivadas no sistema **DN**:

$$(\mathrm{MT}'_1) \qquad \frac{\phi \vee \psi,\ \neg\psi}{\phi}, \qquad (\mathrm{MT}'_2) \qquad \frac{\phi \vee \psi,\ \neg\phi}{\psi}.$$

2.9 (Substituições) Seja ϕ uma fórmula, p uma letra proposicional que pode ou não ocorrer em ϕ, ψ uma fórmula qualquer, na qual também p pode ou não ocorrer. Denota-se por $\phi[\psi]$ o resultado de substituir todas as ocorrências de p em ϕ por ψ, se algumas houver. Se não houver ocorrências de p em ϕ tem-se $\phi[\psi] = \phi$. A fim de chamar a atenção para a(s) possível(eis) ocorrência(s) de p em ϕ e para a substituição efectuada podemos denotar ϕ por $\phi[p]$ e $\phi[\psi]$ por $\phi[p/\psi]$, respectivamente.

(a) Prove, por indução na complexidade das fórmulas (ϕ) que $\phi[p/\psi]$ é fórmula.

(b) Demonstre a seguinte:

---

[96] Note que alguma hipótese pode ser redundante, isto é, não necessita ser utilizada na dedução da tese.

[97] Este exercício [sem a parte (c)] correu o mundo e é devido ao lógico americano H. J. Keisler.

Propriedade de substituição numa tautologia
Para quaisquer fórmulas ϕ, ψ *e letra proposicional* p, *se* $\vDash \phi$, *então* $\vDash \phi[p/\psi]$.[98]

[Sugestão: estude primeiramente um caso particular, utilizando tabelas de verdade. Observe que, em geral, para cada valoração booleana v, o valor $v(\phi[\psi])$ é igual ao valor $v'(\phi[p])$, onde v' é como v, excepto que $v'(p) = v(\psi)$.]

2.10 Formule todas as leis que resultam de deduções efectuadas e descubra leis não formuladas anteriormente. [Por exemplo, formule e justifique diversas leis de conversão, as leis de De Morgan, etc.]

2.11 (a) Deduza $u \rightarrow s$ com hipóteses $p \wedge (q \vee r)$, $\neg s \vee r$, $(p \wedge r) \leftrightarrow t$, $(\neg s \rightarrow \neg t) \wedge \neg q$ no sistema **DN**.

(b) Seja ϕ uma fórmula qualquer de $\mathcal{L}^0$. Prove que $\phi \leftrightarrow \neg\phi$ é interderivável (no sistema **DN**) com a contradição $\phi \wedge \neg\phi$.

§II.11

2.12 (a) Demonstre, a partir da definição 3 (p. 75), a importante propriedade seguinte:

Propriedade de finitude (MF)
Para quaisquer conjunto Γ *e fórmula* ϕ, *se* $\Gamma \vdash \phi$, *então* $\Gamma_0 \vdash \phi$ *para alguma parte finita* Γ_0 *de* Γ.

(b) Demonstre a seguinte

Propriedade da validade generalizada ($\mathbf{MV_G}$)
Para quaisquer conjunto Γ *e fórmula* ϕ, *se* $\Gamma \vdash \phi$, *então* $\Gamma \vDash \phi$.

2.13 Mostre que: (a) um conjunto Γ é contraditório sse é **trivial**, no sentido: para toda a fórmula ϕ, $\Gamma \vdash \phi$;

(b) se Γ é consistente, então, para qualquer fórmula ϕ, um dos conjuntos $\Gamma \cup \{\phi\}$, $\Gamma \cup \{\neg\phi\}$ é consistente.

2.14 Mostre que o conjunto $\Gamma = \{p, (\neg p \vee q) \wedge r, \neg q \vee \neg r\}$ é inconsistente, derivando uma contradição com hipóteses em Γ, no sistema **DN**.

2.15 Se Σ é um conjunto de fórmulas de $\mathcal{L}^0$, denota-se $\mathrm{Cn}(\Sigma)$ o conjunto das consequências lógicas ou semânticas de Σ, e denota-se $\mathrm{Tma}(\Sigma)$ o conjunto dos teoremas de Σ.

(a) Diga se são verdadeiras ou falsas as asserções metateóricas seguintes, justificando com uma demonstração (utilizando apenas noções semânticas) ou um contra-exemplo, conforme o caso:

---

[98] Este resultado pode-se generalizar a mais de uma substituição simultânea $\phi[p_1/\psi_1, \ldots, p_k/\psi_k]$ e também a substituições iteradas $(\ldots(\phi[p_1/\psi_1])\ldots)[p_k/\psi_k]$, $k \geq 2$.

(1) Para quaisquer conjuntos Σ, Γ, se $\Sigma \subseteq \Gamma$ então $\mathrm{Cn}(\Sigma) \subseteq \mathrm{Cn}(\Gamma)$;

(2) Para quaisquer conjuntos Σ, Γ, se $\mathrm{Cn}(\Sigma) \subseteq \mathrm{Cn}(\Gamma)$ então $\Sigma \subseteq \Gamma$;

(3) Para qualquer conjunto Σ, $\mathrm{Cn}(\Sigma) \subseteq \mathrm{Cn}(\mathrm{Cn}(\Sigma))$;

(4) Para qualquer conjunto Σ, $\mathrm{Cn}(\mathrm{Cn}(\Sigma)) \subseteq \mathrm{Cn}(\Sigma)$.

(b) Análogo a (a), substituindo em toda a parte "Cn" por "Tma", e utilizando somente noções sintácticas nas demonstrações.

2.16 Enuncie e demonstre propriedades análogas às do exercício 2.7 substituindo em toda a parte " $\models$ " por " $\vdash_{\mathbf{DN}}$", «compatível» por «consistente» e «incompatível» por «contraditório», respectivamente.

2.17 (a) Demonstre, utilizando (MV_{G}), a propriedade seguinte, que é outra versão da referida propriedade:

($\mathrm{MV}'_{\mathrm{G}}$) Para todo o conjunto Γ de fórmulas, se Γ é compatível, então Γ é consistente.

(b) Demonstre, utilizando a propriedade de completude semântica generalizada, que se Γ é consistente, então Γ é compatível. [Sugestão: 2.7(b).]

(c) Prove que para qualquer conjunto Γ e qualquer fórmula ϕ, $\Gamma \cup \{\neg\phi\}$ é consistente sse $\Gamma \nvdash \phi$ (equivalentemente, $\Gamma \cup \{\neg\phi\}$ é inconsistente sse $\Gamma \vdash \phi$).

(d) Prove, utilizando apenas noções semânticas, que para qualquer conjunto Γ e qualquer fórmula ϕ, $\Gamma \cup \{\neg\phi\}$ é compatível sse $\Gamma \not\models \phi$ (equivalentemente, $\Gamma \cup \{\neg\phi\}$ é incompatível sse $\Gamma \models \phi$).

2.18 (a) Dê exemplos de conjuntos Γ e fórmula ϕ tais que $\Gamma \nvdash \phi$ e $\Gamma \nvdash \neg\phi$.

(b) Complete os passos que faltam na demonstração do metateorema da completude semântica generalizado.

§II.12

2.19 (a) Mostre que se Σ e Δ são conjuntos efectivamente enumeráveis de expressões, então $\Sigma \cap \Delta$ e $\Sigma \cup \Delta$ também são.

(b) Mostre que se Σ e Δ são conjuntos decidíveis de expressões, então $\Sigma \cap \Delta$, $\Sigma \cup \Delta$, $\Sigma \backslash \Delta$ ($= \{\sigma : \sigma \in \Sigma \text{ e } \sigma \notin \Delta\}$) e $E \backslash \Sigma$ também são.

(c) Mostre que se Σ é efectivamente enumerável e, para toda a fórmula ϕ, $\Sigma \models \phi$ ou $\Sigma \models \neg\phi$, então $\Sigma^* = \mathrm{Cn}(\Sigma)$ é decidível.

§II.13-II.14

2.20 Discuta a possibilidade de definir alguns dos conectivos à custa de outros, economizando, assim, na lista dos símbolos primitivos de $\mathcal{L}^0$, nomeadamente nos casos indicados a seguir:

(a) Definir $\wedge$, $\rightarrow$ à custa de $\neg$, $\vee$;

(b) definir $\vee$, $\rightarrow$ à custa de $\neg$, $\wedge$;

(c) definir $\vee$, $\wedge$ à custa de $\neg$, $\rightarrow$;

(d) definir o conectivo de *disjunção exclusiva* $\dot{\vee}$ à custa dos conectivos $\neg$, $\wedge$, $\vee$. [Por exemplo, pode-se definir

$$\phi \wedge \psi \ = \neg(\ \neg\phi \vee \ \neg\psi),$$

pois as fórmulas $\phi \wedge \psi$ e $\neg(\ \neg\phi \vee \neg\psi)$ são lógica e dedutivamente equivalentes.]

2.21 (a) Quantas funções booleanas n-árias ($n \geq 0$) existem? E quantos conectivos generalizados n-ários?

(b) Determine todos os conectivos generalizados binários (além dos já conhecidos).

(c) Mostre que os conjuntos $\{\neg, \wedge\}$, $\{\neg, \vee\}$, $\{\neg, \rightarrow\}$ são funcionalmente completos (exercício 2.17).

(d) Mostre que $\{\wedge, \vee\}$ não é funcionalmente completo. [Sugestão: fórmulas construídas só com $\wedge$, $\vee$ são sempre verdadeiras para todas as valorações que atribuem o valor 1 a todos os p_i's.]

(e) Os **conectivos de Sheffer** são os conectivos binários de *rejeição* $\barwedge$ [«nem-nem», $\phi \barwedge \psi = \neg(\phi \vee \psi)$] e de *incompatibilidade* $\uparrow$ [«negação conjunta», $\phi \uparrow \psi = \neg(\phi \wedge \psi)$]. Mostre que os conjuntos $\{\barwedge\}$, $\{\uparrow\}$ são funcionalmente completos, mas $\{\dot{\vee}\}$ não é funcionalmente completo.

(f) Mostre que os únicos conectivos binários Π tais que $\{\Pi\}$ é funcionalmente completo são os conectivos de Sheffer.

2.22 (a) Mostre que a versão (MC′) do metateorema da compacidade é equivalente à proposição seguinte:

(MC) *Para qualquer conjunto de fórmulas* Σ *e qualquer fórmula* ϕ, $\Sigma \vDash \phi$ *sse existe uma parte finita* Σ_0 *de* Σ *tal que* $\Sigma_0 \vDash \phi$.

(b) Demonstre a versão anterior directamente a partir dos metateoremas da validade e da completude semântica generalizados.

(c) Mostre que o conjunto

$$\Gamma = \{p_i \vee p_{i+1}, \neg p_i \vee \neg p_{i+1} \ : \ i = 0, 1, 2, ...\}$$

é compatível.

(d) Idem, para o conjunto

$$\Gamma = \{p_0, p_1, p_0 \wedge p_1, p_2, p_0 \wedge p_2, p_3, p_0 \wedge p_3, ...\}.$$

***2.23** Um grupo abeliano (numerável) $(G, +, 0)$ diz-se **ordenável** sse existe uma relação binária $<$ em G que é uma ordem total estrita e, para quaisquer elementos a, b, c de G, se $a < b$, então $a + c < b + c$.

Prove que um grupo abeliano é ordenável sse todo o subgrupo finitamente gerado é ordenável. [Sugestão: exprima por fórmulas proposicionais que o grupo é ordenável, usando letras $p_{a,b}$ para cada par ordenado (a, b) de elementos de G; intuitivamente, $p_{a,b}$ é verdadeira sse $a < b$; utilize o metateorema da compacidade.]

2.24 Demonstre o Lema do Casamento. [Sugestão: por indução completa em $m \geq 1$, na versão seguinte. A propriedade é verdadeira para $m = 1$; supondo (hipótese de indução) que é verdadeira para todo $n < m$, prove que é verdadeira para m, considerando os dois casos (i) para todo $k < m$, quaisquer k rapazes têm, pelo menos, $k + 1$ namoradas, (ii) para algum $k < m$, há um conjunto κ de k rapazes com exactamente k namoradas.

2.25 (a) Obtenha fórmulas logicamente equivalentes a

(i) $p \leftrightarrow q$; (ii) $p \rightarrow \neg q \vee r$; (iii) $p \rightarrow q \rightarrow r \rightarrow s$;

(iv) $p \wedge (\neg q \vee r)$; (v) $p \vee (q \wedge \neg(r \wedge s))$,

respectivamente, nas formas normal conjuntiva e disjuntiva.

(b) Determine equivalentes mais simples para as fórmulas (i) $(p \rightarrow q) \wedge p$; (ii) $(p \rightarrow q) \vee \neg p$; (iii) $(p \rightarrow q) \rightarrow q$; (iv) $p \rightarrow (p \wedge q)$; (v) $(p \wedge q) \vee p$.

(c) Aplique o algoritmo da pág. 90 para testar se as fórmulas de Horn seguintes são ou não compatíveis:

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

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

(d) Determine três interpoladoras (logicamente equivalentes entre si) entre $((q \rightarrow p) \vee r) \wedge ((r \rightarrow p) \vee \neg q)$ e $(\neg p \wedge \neg q) \vee (p \wedge \neg q) \vee (p \wedge q) \wedge s$.

2.26 (**Dualidade**) Seja Form$(\neg, \wedge, \vee)$ o conjunto das fórmulas sobre P contendo somente os conectivos indicados. Para cada fórmula ϕ em Form$(\neg, \wedge, \vee)$, seja ϕ^* a fórmula que se obtém de ϕ permutando $\wedge$ com $\vee$ e substituindo cada letra proposicional p_i em ϕ por $\neg p_i$. Por exemplo,

$$((p \wedge \neg q) \vee r)^* = (\neg p \vee \neg\neg q) \wedge \neg r.$$

Indutivamente, pode-se definir ϕ^* pelas regras: $p_i^* = \neg p_i$, $(\neg\psi)^* = \neg\psi^*$, $(\psi \wedge \theta)^* = \neg\psi \vee \neg\theta$ e analogamente permutando $\wedge$ com $\vee$. ϕ^* é chamada a **dual** de ϕ.

(a) Dê uma definição indutiva de ϕ^* e formule um princípio de indução na complexidade das fórmulas de Form$(\neg, \wedge, \vee)$.

(b) Prove que para toda a fórmula ϕ em Form$(\neg, \wedge, \vee)$, ϕ^* é uma fórmula do mesmo conjunto.

(c) Prove que para toda a fórmula ϕ de Form$(\neg, \wedge, \vee)$, ϕ e $\neg\phi^*$ são logicamente equivalentes.

§II.15

2.27 Mostre que a relação $\sim$ é uma congruência com respeito às operações $\wedge$, $\vee$, $\neg$ em F.

2.28 Demonstre o lema 15.2, o lema 15.4 e conclua as demonstrações do metateorema 15.1 e do teorema 15.5 da secção II.15.

2.29 Prove que numa álgebra de Boole $\mathfrak{B} = (B, +, \cdot, -, 0, 1)$:
(a) 0 e 1 são os únicos elementos tais que

$$a + 0 = a,\ a \cdot 1 = a, \text{ para todo } a \in B;$$

(b) $-a$ é o único elemento b tal que $a + b = 1$, $a \cdot b = 0$;

(c) $-(-a) = a$;

(d) $-0 = 1$, $-1 = 0$;

(e) $a + a = a = a \cdot a$;

(f) $a + 1 = 1$, $a \cdot 0 = 0$;

(g) $a + (a \cdot b) = a$, $a \cdot (a + b) = a$;

(h) $-(a + b) = (-a) \cdot (-b)$, $-(a \cdot b) = (-a) + (-b)$.

2.30 (a) Quais as equivalências lógicas na álgebra $\mathfrak{F}$ correspondentes às identidades (c)-(h) do exercício anterior? [Exemplo: $-(-a) = a$ corresponde a $\neg\neg\phi \sim \phi$].

(b) Mostre que a identidade $a \cdot (a + b) = a$ é válida na álgebra de Lindenbaum, e demonstre-a a partir dos axiomas das álgebras de Boole e das propriedades do exercício 2.28.

2.31 Numa álgebra de Boole $\mathfrak{B} = (B, ...)$, definindo

$$a \leq b \text{ sse } a + b = b \text{ (sse } a \cdot b = a),$$

prove que:

(a) $(B, \leq)$ é parcialmente ordenado (quer dizer: $\leq$ é reflexiva, anti-simétrica e transitiva) com elemento mínimo 0 e elemento máximo 1;

(b) para quaisquer elementos $a, b \in B$, $a + b = \sup\{a, b\}$ e $a \cdot b = \inf\{a, b\}$, onde $\sup\{a, b\}$ é o *supremo* de $\{a, b\}$, ou o menor dos majorantes de $\{a, b\}$, isto é, um elemento c tal que:

(i) $a \leq c$ e $b \leq c$ e

(ii) para qualquer elemento x, se $x \leq a$ e $x \leq b$, então $c \leq x$;

$\inf\{a, b\}$ é o *ínfimo* de $\{a, b\}$, ou o maior dos minorantes de $\{a, b\}$, e pode ser caracterizado por duas condições análogas a (i) e (ii) (a fazer!).

§II.16-II.17

2.32 O sistema dedutivo **MU** aparece no livro de HOFSTADTER, pp. 33-41, cuja leitura se recomenda. O problema seguinte foi retirado do livro de HODEL, um fabuloso manual moderno de lógica matemática. A linguagem do sistema tem somente os símbolos, M, I e U; toda a expressão é fórmula; o sistema tem um *axioma* (regra sem premissas) MI e as seguintes *regras de inferência*, onde σ e τ denotam expressões arbitrárias (possivelmente vazias):

$$(\mathrm{R}_1)\quad \frac{\sigma I}{\sigma IU};\quad (\mathrm{R}_2)\quad \frac{M\sigma}{M\sigma\sigma};\quad (\mathrm{R}_3)\quad \frac{\sigma III\tau}{\sigma U\tau};\quad (\mathrm{R}_4)\quad \frac{\sigma UU\tau}{\sigma\tau}.$$

Uma *dedução* no sistema é uma sequência finita de expressões σ_1, ..., σ_n ($n \geq 1$) tal que cada σ_i é um axioma ou é inferida de alguma σ_j com $j < i$ por uma regra de inferência. A última expressão de uma dedução é um *teorema* de **MU**. Mostre que:

(a) $MUII$ é teorema de **MU**;

(b) o número de I's de um teorema de **MU** nunca é múltiplo de 3 [Sugestão: indução completa no comprimento das deduções);

(c) para todo n, MI^{2^n} é teorema de **MU** onde, para qualquer k, $I^k = II\cdots I$ (k vezes);

(d) se σIII é teorema, então σ é teorema;

(e) se n é da forma $2^m - 3k$, com $k \geq 0$, então MI^n é teorema;

(f) para todo n que não é múltiplo de 3, MI^n é teorema [por (e), basta mostrar que todo n que não é múltiplo de 3 é da forma indicada: supondo m tal que $2^m \geq n$, ou $2^m - n$ ou $2^{m+1} - n$ é múltiplo de 2; note que não ser múltiplo de 3 é ser de uma das formas $3r + 1$ ou $3r + 2$];

(g) uma expressão σ é teorema de **MU** sse é da forma $M\tau$, onde τ é uma expressão só com I's e U's mas o número de I's não é múltiplo de 3. Conclua que **MU** é *decidível*, isto é, existe um algoritmo para decidir, para qualquer expressão σ, se σ é ou não teorema de **MU**.

***2.33** Construa derivações à Beth de diversas leis anteriormente estabelecidas no sistema **DN**.

***2.34** Mostre, utilizando as propriedades de validade e de completude semântica, que se $\vdash_{\mathbf{B}} \phi$ e $\vdash_{\mathbf{B}} \phi \rightarrow \psi$, então $\vdash_{\mathbf{B}} \psi$.

***2.35** Chama-se **peso** de uma fórmula ϕ ao número $\mathrm{peso}(\phi) = n(\phi) + 2c(\phi) + d(\phi) + 2i(\phi)$, onde $n(\phi)$, $c(\phi)$, $d(\phi)$ e $i(\phi)$ são os números de ocorrências dos conectivos $\neg$, $\wedge$, $\vee$, $\rightarrow$ em ϕ, respectivamente. Mostre que se uma fórmula é derivável em **G**, então ela é derivável em $\leq 2^{\mathrm{peso}(\phi)}$ linhas. Tente melhorar esta majoração.

2.36 Construa derivações em forma de árvore, em **G**, e converta-as na configuração linear vertical, das fórmulas:

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

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

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

2.37 Aplique o algoritmo descrito na pág. 122 aos sequentes

(a) $p \to q, q \to r, r \to p$;

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

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

2.38 (a) Mostre que se ψ é uma disjunção de $\{\phi_1, \phi_2, ..., \phi_n\}$, então, para cada i, $\phi_i \vdash_{\mathbf{DN}} \psi$.

(b) Chama-se **grau** de uma disjunção sobre $\{\phi_1, \phi_2, ..., \phi_n\}$ ao número natural definido pelas seguintes regras:

— o grau de cada ϕ_i é 0;

— se ψ, θ são disjunções sobre $\{\phi_1, \phi_2, ..., \phi_n\}$, então

$$\text{grau}(\psi \vee \theta) = 1 + \max\{\text{grau}(\psi), \text{grau}(\theta)\}.$$

Utilizando (a), demonstre o Metateorema da Subdisjunção (pág. 125), por indução completa (2ª forma, ver pág. 74) no grau m de $\{\phi_1, \phi_2, ..., \phi_n\}$.

***2.39** (**Compacidade do espaço de Cantor**) O espaço de Cantor $\mathsf{C} = {}^{\omega}2 = {}^{\mathbb{N}}\{0,1\}$ foi definido na pág. 46 (exercício 2.14), e é constituído por todas as sucessões infinitas de 0's e 1's. Ora, aparte a notação, uma sucessão infinita de 0's e 1's não é mais do que uma valoração simples $v : P \to \{0,1\}$, onde $P = \{p_0, p_1, ...\}$. Designamos por V o conjunto de todas as valorações, pelo que não advém grande mal se «identificarmos» C com o *espaço das valorações, V*, no que segue. Os *abertos básicos* deste espaço são, portanto, os conjuntos de valorações da forma $[u] = \{v : v \supseteq u\}$, onde u é uma função booleana (ou uma *valoração parcial* $u : \{p_0, ..., p_{n-1}\} \to \{0,1\}$ para algum $n \geq 0$).

Associamos a cada fórmula ϕ de $\mathcal{L}^0$ o conjunto de valorações o

$$\overline{\phi} = \{v : \widehat{v}(\phi) = 1\} \subseteq V,$$

e a cada conjunto Σ de fórmulas o conjunto $\overline{\Sigma} = \{v : \widehat{v}(\phi) = 1 \text{ para todo } \phi \in \Sigma\}$ (Recorde que toda a valoração simples v determina uma única valoração booleana $\widehat{v}$ — ver pág. 53 e a convenção feita na pág. 71). Mostre que:

(a) para cada fórmula ϕ, $\overline{\phi}$ é um aberto básico, e também é fechado;

(b) para quaisquer fórmulas ϕ e ψ, $\overline{\neg\phi} = V \setminus \overline{\phi}$, $\overline{\phi \wedge \psi} = \overline{\phi} \cap \overline{\psi}$, $\overline{\phi \vee \psi} = \overline{\phi} \cup \overline{\psi}$;

(c) para quaisquer fórmulas ϕ e ψ, $\vDash \phi$ sse $\overline{\phi} = V$, $\overline{\bot} = \emptyset$ (onde $\bot$ representa uma contradição qualquer), e $\vDash \phi \rightarrow \psi$ sse $\overline{\phi} \subseteq \overline{\psi}$;

(d) para qualquer fórmula ϕ e conjunto Σ de fórmulas, $\overline{\Sigma}$ é fechado e $\Sigma \vDash \phi$ sse $\overline{\Sigma} \subseteq \overline{\phi}$;

(e) o metateorema da compacidade, na forma (MC) (pág. 150) corresponde exactamente à compacidade do espaço das valorações [Sugestão: alínea (d) e formulação da compacidade em termos de fechados.]

§II.18

2.40 Mostre que são teoremas lógicos do sistema **H**, tendo em conta as definições dos conectivos $\wedge$, $\vee$ e $\leftrightarrow$:

(a) $\phi \rightarrow (\phi \vee \psi)$; (b) $\phi \vee \psi \rightarrow \psi \vee \phi$;

(c) $\phi \wedge \psi \rightarrow \phi$; (d) $(\phi \rightarrow \theta) \rightarrow ((\psi \rightarrow \theta) \rightarrow (\phi \vee \psi \rightarrow \theta))$;

(e) $((\phi \rightarrow \psi) \rightarrow \phi) \rightarrow \phi$;

(f) $\phi \rightarrow (\psi \rightarrow (\phi \wedge \psi))$; (g) $(\phi \rightarrow \psi) \leftrightarrow (\neg\psi \rightarrow \neg\phi)$.

§II.19

2.41 Obtenha a forma clausural de:

(a) $\neg(p \wedge q \wedge \neg r)$; (b) $p \leftrightarrow (\neg q \wedge \neg r)$.

2.42 Diga se são ou não compatíveis e, no caso afirmativo, indique um modelo da forma clausural:

(a) $\{\{p, q\}, \{\neg p, \neg q\}, \{\neg p, q\}$;

(b) $\{\{\neg p\}, \{p, \neg q\}, \{q\}\}$;

(c) $\{\{p\}, \square\}$.

2.43 Determine $R^*(\mathcal{C})$, onde $\mathcal{C} = \{\{p, \neg q\}, \{p, q\}, \{\neg p\}\}$.

2.44 Mostre, mediante o sistema de resolução, que os conjuntos de cláusulas seguintes são incompatíveis:

(a) $\{\{\neg p, q, s\}, \{\neg q, s, p\}, \{\neg s, r\}, \{\neg s, p\}, \{p, q\}, \{q, \neg r\}, \{\neg p, \neg q\}\}$;

(b) $\{\{\neg p, q\}, \{\neg q, r\}, \{\neg r, p\}, \{p, r\}, \{\neg p, \neg r\}\}$.

2.45 Complete a demonstração do lema 19.9 (pág. 143).

2.46 Justifique as afirmações seguintes:

(a) Para qualquer fórmula ϕ, ϕ é compatível sse $\square \notin R^*(\mathcal{C}_\phi)$;

(b) para qualquer fórmula ϕ, $\vDash \phi$ sse $\mathcal{C}_{\neg\phi} \vdash_{\mathbf{R}} \square$;

(c) o sistema de resolução constitui um método de decisão para a compatibilidade de fórmulas de $\mathcal{L}^0$.

2.47 Mostre, mediante o sistema de resolução [exercício anterior, (b)], que as fórmulas do exercício 2.40 são válidas.

Capítulo III

CÁLCULO DE PREDICADOS

III.1 As linguagens elementares: alfabeto

Vamos proceder, para o cálculo de predicados, de uma maneira semelhante à do capítulo anterior, mas tendo em conta as complicações inerentes a um formalismo mais rico, mais expressivo e poderoso.

Começamos por definir uma linguagem formal (ou melhor: *as* linguagens formais) $\mathcal{L}^1$ (ou $\mathcal{L}$), mais rica(s) que $\mathcal{L}^0$, no duplo sentido seguinte: mais símbolos no alfabeto e uma gramática mais complexa, que permite um maior poder expressivo. Uma tal linguagem diz-se **elementar** ou **de primeira ordem**, por razões que mais adiante serão explicadas (III.9).

Do alfabeto proposicional só aproveitaremos os conectivos proposicionais $\wedge$, $\vee$, $\neg$, $\rightarrow$ ($\leftrightarrow$ será definido como no Cap. II) e os parênteses formais $($, $)$, embora alguns autores incluam também letras proposicionais. Mais exactamente, o alfabeto de uma linguagem elementar $\mathcal{L}$ divide-se em dois subalfabetos, o **lógico** e o **não lógico** ou **específico**, o primeiro constituído pelos **símbolos lógicos** e o segundo pelos **símbolos não lógicos**. Os símbolos lógicos são *os mesmos* para todas as linguagens elementares, as quais só diferem entre si no que respeita aos símbolos não lógicos.

Como símbolos lógicos adoptamos os seguintes:

- conectivos proposicionais $\wedge$, $\vee$, $\neg$, $\rightarrow$;
- quantificadores $\forall$, $\exists$;
- parênteses $($, $)$;
- variáveis individuais x, y, z, ... (possivelmente com índices)[99];
- símbolo de igualdade $\doteq$,[100] e finalmente

---

[99] Quando tal for conveniente, consideram-se as variáveis individuais como sendo x_0, x_1, ... Analogamente para parâmetros.

[100] Afastando-nos da prática corrente no Cap. I, pensamos que é vantajoso, a partir desta altura, utilizar ' $\doteq$ ' como símbolo de igualdade de uma linguagem elementar (outros autores da mesma opinião utilizam ' $\equiv$ ', ' $\simeq$ ', ou até ' $\approx$ ') em vez de ' $=$ ', que denota a *relação de identidade* no universo de todas as coisas (e, em particular, em cada domínio interpretativo). É claro que a interpretação intencional de $\doteq$ é $=$, mas sobre isto convém ler, oportunamente, o que mais adiante se escreve a este respeito (pp. 187-187).

• parâmetros a, b, a', ... (possivelmente com índices).

Desta última categoria de símbolos (utilizados como *nomes indefinidos*) nunca se falou no Cap. I, e até podia ser dispensada, pois nada acrescenta ao poder expressivo das linguagens. Mas a sua utilização na formulação das regras de inferência e nas deduções traz grandes vantagens do ponto de vista didáctico, pelo menos, que, a nosso ver, justificam a complicação notacional resultante do seu uso. Os parâmetros serão utilizados primordialmente em deduções; deixamos a explicação do seu uso para mais adiante.

Os símbolos não lógicos podem ser de três categorias. Cada linguagem $\mathcal{L}$ terá um certo número (finito, possivelmente zero, ou infinito) de símbolos não lógicos de cada uma das categorias seguintes:

• símbolos predicativos ou relacionais;

• constantes individuais;

• símbolos funcionais ou operacionais.

Os símbolos predicativos denotam, intencionalmente, predicados e/ou relações e serão designados por letras, como P, Q, R, ... (possivelmente com índices); cada símbolo predicativo possui um **grau**, **peso** ou **aridade**, que é um número inteiro positivo e representa o número de «posições» que o símbolo abrange. Escreve-se, por vezes, P^n para indicar que P é n-ário (*unário* se $n = 1$, *binário* se $n = 2$, etc.). O símbolo de igualdade $\doteq$ pode ser considerado como um símbolo relacional binário, mas, atendendo ao tratamento especial que lhe é dado, é considerado como símbolo lógico. As constantes denotam, intencionalmente, objectos ou indivíduos fixos; usaremos as letras c, d, c', d', c_1, ..., como já fizemos no Cap. I, para esse fim. Finalmente, os símbolos funcionais ou operacionais denotam intencionalmente, como o nome indica, funções ou operações e são designados por letras, como f, g, h,... Cada símbolo funcional também possui um grau ou aridade, que é um número inteiro positivo. Os símbolos funcionais são teoricamente dispensáveis,[101] mas na prática são de grande utilidade. No entanto, para não complicar demasiadamente as coisas nesta fase inicial, lidaremos quase exclusivamente, no que segue, com linguagens sem símbolos funcionais. Mais adiante, no entanto, eles serão tidos em conta.

Nas primeiras duas edições deste livro não fizemos tal distinção notacional, mas nem por isso confundimos as duas coisas, deixando para o contexto, porém, a sua distinção. Convém referir, todavia, que em certos estudos lógicos, ou simplesmente por uma questão metodológica, se consideram amiúde linguagens *sem* o símbolo de igualdade, ou em que este é, inicialmente, tratado como um símbolo relacional binário qualquer, e só posteriormente é que se lhe dá um tratamento semântico ou dedutivo privilegiado. Além disso, em certas ocasiões e condições, $=$ é introduzido como símbolo definido (por exemplo, em MENDELSON).

[101] Isto advém do facto conhecido de que uma função ou operação de grau n (ou n-ária) é, tecnicamente (isto é, na teoria dos conjuntos) uma relação $n+1$-ária especial, como mais adiante se verá com mais pormenor.

Em aplicações ou áreas particulares poderão ser utilizados símbolos *especiais* ou *específicos* de cada uma das categorias anteriores. Assim, por exemplo, se quisermos uma linguagem para as *ordens,* é comum usar o símbolo predicativo binário $<$ (ou o símbolo $\leq$; variantes destes símbolos: $\prec$, $\preceq$, $\leqq$, $\precsim$, $\sqsubseteq$, etc.); numa linguagem para as relações de equivalência é costume usar um dos símbolos $\equiv$, $\sim$ ou a letra E; na linguagem da teoria dos conjuntos usam-se os símbolos $\in$, $\subset$, $\subseteq$, etc. Em linguagens para teorias algébricas usam-se os símbolos funcionais $+$, $\times$, $-$, $^{-1}$, $\oplus$, etc., as constantes 0, 1, e (para elemento neutro), $\vec{0}$ (vector nulo), etc. A **linguagem pura da igualdade**, como o nome indica, só tem o símbolo $\doteq$, além dos restantes símbolos lógicos. Vejamos agora a gramática das linguagens elementares $\mathcal{L}$.

III.2 Termos e fórmulas

Há duas espécies de «expressões bem formadas» que nos interessa considerar, os *termos* (tradicionalmente, *expressões designatórias, designações*) e as *fórmulas* (tradicionalmente, *expressões proposicionais, condições, proposições*), uns e outros definidos indutivamente.

Numa linguagem $\mathcal{L}$ sem símbolos funcionais os **termos** são simplesmente os parâmetros e as constantes (se algumas houver). Numa linguagem com símbolos funcionais há ainda a considerar os termos da forma

$$ft_1...t_n$$

em que f é um símbolo funcional n-ário de $\mathcal{L}$ e t_1, ..., t_n são termos. Nada mais é termo. Observe-se que a definição de termo é indutiva. Explicitando as regras de formação dos termos:

T_1. Os parâmetros e as constantes (que houver em $\mathcal{L}$) são termos;

T_2. Se f é um símbolo funcional n-ário de $\mathcal{L}$ e t_1, ..., t_n são termos, então $ft_1...t_n$ é um termo;

T_3. Nada mais é termo.

Se f é um símbolo funcional binário (por exemplo, $+$, ou $\times$) de $\mathcal{L}$, é usual escrever $t_1 f t_2$ [$(t_1 + t_2)$, $(t_1 \times t_2)$, respectivamente] em vez de ft_1t_2. Poderá escrever-se $f(t_1, ..., t_n)$ como abreviatura de $ft_1...t_n$.

As **fórmulas** são definidas indutivamente pelas seguintes regras de formação:

F_1. Se t_1, t_2 são termos, então $\doteq t_1t_2$ é uma fórmula; se P é um símbolo predicativo n-ário e t_1, ..., t_n são termos, então $Pt_1...t_n$ é uma fórmula.

F_2. Se ϕ é uma fórmula, então $\neg\phi$ é uma fórmula.

F_3. Se ϕ, ψ são fórmulas, então $(\phi \wedge \psi)$, $(\phi \vee \psi)$, $(\phi \rightarrow \psi)$ são fórmulas.

F_4. Se $\phi(a)$ é uma fórmula onde ocorre o parâmetro a e x é uma variável que não ocorre em $\phi(a)$, então $\forall x\,\phi(x)$, $\exists x\,\phi(x)$ são fórmulas, onde $\phi(x)$ é a expressão que resulta de $\phi(a)$ substituindo *todas* as ocorrências de a por x [$\phi(x)$ é $\phi(x/a)$, ver Nota 102].

F_5. Nada mais é fórmula.

As fórmulas do tipo F_1 são ditas **atómicas**; as restantes são **compostas**. As expressões '$\forall x$', '$\exists x$' são chamadas os **quantificadores em** x. Na cláusula F_4, e tendo em conta as passagens de $\phi(a)$ a $\forall x\,\phi(x)$ e a $\exists x\,\phi(x)$, o parâmetro a é chamado o **parâmetro da quantificação** em (ou parâmetro **associado** a) x.

Convencionamos escrever $(t_1 \doteq t_2)$ em vez de $\doteq t_1 t_2$, como é usual, e $(t_1 \neq t_2)$ em vez de $\neg(t_1 \doteq t_2)$, omitindo parenteses sempre que não houver perigo de confusão. Do mesmo modo, se P é binário (por exemplo, $<$), podemos escrever $t_1 P\, t_2$ (por exemplo, $t_1 < t_2$), em vez de $P\, t_1 t_2$.

As fórmulas bicondicionais $(\phi \leftrightarrow \psi)$ definem-se como no Cap. II. Além disso, adoptamos as mesmas convenções aí feitas (p. 48) para simplificação da escrita. Observações análogas às de II.3 podem fazer-se a propósito dos termos e fórmulas de uma linguagem elementar $\mathcal{L}$. Exemplos de fórmulas (abreviadas ou simplificadas na escrita, muitas delas) já foram dados no Cap. I, e muitos mais serão dados adiante.

2.1 Exemplo

Vejamos entretanto como se poderiam aplicar as regras F_1-F_4 para provar que a expressão

$$\forall x(\exists y Pxy \rightarrow \neg\exists u \forall y Quy)$$

é uma sentença (em notação abreviada). Se sentença, só poderia ter resultado por F_4 de uma fórmula como $\exists y Pay \rightarrow \neg\exists u \forall y Quy$, para certo parâmetro a, que por sua vez é uma condicional (F_3) com antecedente $\exists y Pay$ e consequente $\neg\exists u \forall y Quy$. O primeiro só pode ter resultado de uma fórmula atómica Pab (F_1), com um parâmetro b diferente de a (se b fosse a, de Paa teria resultado $\exists y Pyy$ e não $\exists y Pay$), e o segundo é a negação (F_2) de $\exists u \forall y Quy$. Isto só pode ter sifo formado aplicando F_4 duas vezes, digamos a partir de Qba, também com a, b distintos. Em cosequência, temos a seguinte sequência formativa (que não é a única possível) a partir de fórmulas atómicas:

$$Pab,\ Qba,\ \exists y Pay,\ \forall y Qby,\ \exists u \forall y Quy,\ \neg\exists u \forall y Quy,$$
$$\exists y Pay \rightarrow \neg\exists u \forall y Quy,\ \forall x(\exists y Pxy \rightarrow \neg\exists u \forall y Quy).$$

É importante observar que na definição de fórmula, regra F_4, há um passo intermédio entre $\phi(a)$ e $\forall x \phi(x)$ [ou $\exists x \phi(x)$] que consiste em substituir todas as ocorrências de 'a' por 'x' em $\phi(a)$, resultando a *expressão* $\phi(x)$, a qual *não é uma fórmula*. [A uma expressão como $\phi(x)$ ou $\phi(x_1, ..., x_n)$ podíamos chamar *pré-formula* e pode-se dar uma definição indutiva de tais expressões. Para isso teríamos

de começar por definir indutivamente os *pré-termos* $t(x_1, ..., x_n)$ imitando a definição de termo mas admitindo na cláusula T_1 que as variáveis individuais x_i, os parâmetros e as constantes são pré-termos].

$\forall x \forall y\, \phi$ pode-se abreviar $\forall x,y\, \phi$ ou $\forall xy\, \phi$, e analogamente com '$\exists$' no lugar de '$\forall$'. Numa fórmula da forma $\forall x\psi$, $\exists x\psi$, a fórmula ψ é o **alcance** ou **alçada** do quantificador em x respectivo. Todas as ocorrências numa fórmula ϕ de uma variável x que ocorrem num quantificador em x ou no alcance de um quantificador em x, dizem-se **mudas** ou **aparentes** (em ϕ): do ponto de vista do significado, é como se não estivessem lá. De facto, o seguinte exemplo explica porquê: a fórmula (da linguagem da aritmética) $\exists x(a \doteq x + x)$ exprime que «a é par», mas nada exprime acerca de x. Ela exprime acerca de a exactamente o mesmo que $\exists y(a \doteq y + y)$, mas nada exprime acerca de y. Uma fórmula ϕ na qual ocorrem os parâmetros a_1, ..., a_n também se diz uma **fórmula aberta**, uma **sentença aberta** ou uma **condição** nesses parâmetros, e é habitual empregar a notação

$$\phi(a_1, ..., a_n)$$

para assinalar tal facto, mas, por vezes, esta mesma notação emprega-se quando os parâmetros que ocorrem em ϕ estão entre a_1, ..., a_n; e se t_1, ..., t_n são termos, o resultado de substituir toda a ocorrência de a_i por t_i $(1 \leq i \leq n)$ na fórmula $\phi(a_1, ..., a_n)$ denota-se

$$\phi(t_1/a_1, ..., t_n/a_n), \text{ ou simplesmente } \phi(t_1, ..., t_n),^{102}$$

excepto se algo for dito em contrário. Se $\phi = \phi(a_1, ..., a_n)$, onde a_1, ..., a_n são exactamente os parâmetros que ocorrem em ϕ, denota-se por $\overline{\phi}$, ou Cl(ϕ), o *fecho universal* de ϕ, $\forall x_1 ... x_n \phi(x_1, ..., x_n)$, único a menos de uma permutação dos quantificadores universais iniciais, mas podemos convencionar que a quantificação se faz seguindo a ordem alfabética (indicada pelos índices) dos parâmetros.

2.2 Definição

Um **termo fechado** é um termo onde não ocorre nenhum parâmetro. Uma **fórmula fechada** ou **sentença** é uma fórmula sem parâmetros.

Observe-se que os termos fechados também podem ser definidos indutivamente (exercício), mas a definição de fórmula fechada *não* é indutiva. Note-se, além disso, que *somente as variáveis individuais x, y, z, ... podem ser quantificadas,* isto é, utilizadas como variáveis mudas, pois foram reservadas para esse fim. Por outras palavras, não é lícito quantificar parâmetros, os quais vão desempenhar o papel tradicionalmente reservado (quer dizer, na maioria dos livros de lógica matemática) às variáveis livres nas fórmulas, mas na prática, a sua utilização pode cingir-se às deduções.

---

[102] Uma outra notação mais explícita para o resultado de uma substituição simultânea das ocorrências de a_1,…, a_n por t_1,…, t_n em ϕ, respectivamente, é $\phi^{t_1,\ldots,t_n}_{a_1,\ldots,a_n}$.

III.3 Um sistema dedutivo: dedução natural

Adoptamos as regras de inferência [primitivas e derivadas, incluindo o princípio (T^+)] do sistema **DN** e as noções de derivação, dedutibilidade, etc., mas agora *somente para fórmulas* de $\mathcal{L}$, e acrescentaremos regras de eliminação e de introdução para os quantificadores. O sistema assim obtido designa-se por

DNQ (Dedução Natural Quantificacional)

Mais adiante acrescentamos regras para a igualdade, mas de momento $\doteq$ será tratado (dedutivamente) como um qualquer outro símbolo predicativo binário.

No que se segue supomos fixada ao arbítrio uma linguagem $\mathcal{L}$, cujos símbolos não lógicos serão especificados conforme seja conveniente. A mesma letra "P" poderá ser usada, porém, umas vezes como símbolo unário, outras como símbolo binário, etc. (mas não no mesmo contexto ou na mesma dedução!).

Eliminação universal	
$(\forall^-)$	$\dfrac{\forall x\,\phi(x)}{\phi(t)}$

onde t é um termo qualquer e $\phi(t)$ resulta de $\phi(x)$, substituindo *todas* as ocorrências livres de x por t.[103] Numa dedução em que se aplique esta regra, a conclusão depende das hipóteses de que depende a premissa.

Intuitivamente, a regra $(\forall^-)$ diz que «o que vale para todos vale para cada um», o que está de acordo com o significado intuitivo da expressão «para todo». Vejamos um primeiro exemplo de uma dedução com esta nova regra, precisamente a correspondente à formalização do argumento clássico (1) da pág. 15.

(101) $\forall x(Px \to Qx),\, Pa \vdash Qa.$

Dedução:

1	$\forall x(Px \to Qx)$	H
2	Pa	H
3	$Pa \to Qa$	1 $(\forall^-)$
4	Qa	2, 3 (MP).

Antes de prosseguir devemos chamar a atenção para um aspecto da regra $(\forall^-)$ a ter em conta em deduções: *deve-se aplicar a regra de maneira criteriosa, somente quando é manifestamente oportuno e conveniente fazê-lo*. Em raciocínios informais e em demonstrações matemáticas impera o bom senso nas utilizações desta e de outras regras dos quantificadores, mas em deduções formais é fácil ao

[103] Não perder de vista que a expressão $\phi(x)$ resultou de certa fórmula $\phi(a)$ nas condições da regra F_4, e bem podíamos ter dito, portanto, que $\phi(t)$ resulta de $\phi(a)$ substituindo todas as ocorrências de 'a' por 't': $\phi(x) = \phi(x/a)$.

iniciando esquecer o bom senso e tentar aplicar a regra só porque é possível aplicá-la em qualquer altura (por exemplo, logo à partida) sem ter em conta o objectivo último a atingir com a sua utilização, que é chegar à tese. No exemplo anterior também se pode obter $Pt \rightarrow Qt$ na linha 3 com qualquer termo fechado t distinto da constante a, mas isso tornaria impossível, logo de seguida, a conclusão que se pretende, que é Qa. *Em geral, há que ser sensato e objectivo na construção das deduções*, evitando a manipulação cega das regras de inferência, como quem movimenta as pedras de um jogo de damas ou de xadrez de acordo com as regras mas sem qualquer objectivo táctico ou estratégico.

(102) $\forall x\,(Px \rightarrow Qx),\ \neg Qa \vdash\ \neg Pa.$

Introdução universal
$(\forall^{+})$ $\quad \dfrac{\phi(a)}{\forall x\,\phi(x)}$,

desde que a fórmula $\phi(a)$ *não seja uma hipótese e não dependa de nenhuma hipótese em que '*a*' ocorra,* e $\phi(x)$ resulte de $\phi(a)$, substituindo *todas* as ocorrências de a por x. Também aqui, numa dedução, a conclusão depende das hipóteses de que depende a premissa.

Podemos agora explicar o papel dos parâmetros e ao mesmo tempo verificar que a regra $(\forall^{+})$ é intuitivamente válida. Intencionalmente, os parâmetros desempenham o papel de *nomes arbitrários*, isto é, nomes de indivíduos arbitrários (em cada domínio interpretativo), papel esse que também se poderia atribuir às variáveis livres x, ... numa dada fórmula ou condição (se as houvesse, isto é, se tivéssemos definido as fórmulas de outra maneira, de modo a permitir tal coisa), mas vamos reservar esse papel para os parâmetros. Ora, se $\phi(a)$ é verdadeira, quer dizer que um indivíduo ao arbítrio a tem a propriedade expressa por ϕ, donde se conclui legitimamente que $\forall x\,\phi(x)$ é verdadeira.

Mas atenção: a *não pode ocorrer em nenhuma hipótese de que a premissa dependa*; caso contrário, ficaria definitivamente condicionado (ou hipotecado) por essa hipótese, perdendo, assim, o carácter de *representante arbitrário* que se lhe deveria exigir.

Se, por exemplo, no domínio das pessoas, fazemos a hipótese de que «a não é membro de um conselho de administração», da fórmula «se a é deputado, então a é isento» não seria legítimo inferir que todos os deputados são isentos (mesmo que isto seja verdade), mas apenas seria legítimo inferir que são isentos aqueles deputados que não são membros de nenhum conselho de administração.

Reitera-se que, aqui e em qualquer outro lado neste capítulo só ocorrem sentenças (abertas ou fechadas).

(103) $\forall x\,(Px \rightarrow Qx),\ \forall x\,(Qx \rightarrow Rx) \vdash \forall x\,(Px \rightarrow Rx).$

Dedução:

1	$\forall x\,(Px \to Qx)$	H
2	$\forall x\,(Qx \to Rx)$	H
3	Pa	[H]
4	$Pa \to Qa$	1 ($\forall^-$)
5	Qa	3, 4 (MP)
6	$Qa \to Ra$	2 ($\forall^-$)
7	Ra	5, 6 (MP)
8	$Pa \to Ra$	3-7 ($\to^+$)
9	$\forall x\,(Px \to Rx)$	8 ($\forall^+$).

(104) $\forall x\,(Px \to Qx),\ \forall x\,Px \vdash \forall x\,Qx.$

(105) $\forall x\,(Px \wedge Qx) \vdash \forall x\,Px.$

(106) $\forall x\,(Px \wedge Qx) \dashv\vdash \forall x\,Px \wedge \forall x\,Qx.$

(107) $\forall x\,(Px \vee Qx),\ \forall x\,\neg Px \vdash \forall x\,Qx.$

Introdução existencial

$$(\exists^+) \qquad \frac{\phi(t)}{\exists x\,\phi(x)},$$

onde t é um termo e $\phi(x)$ resulta de $\phi(t)$, substituindo *algumas* (pelo menos uma, mas não necessariamente todas) ocorrências de t por x. Além disso, para obstar à alteração de significado (ver pág. 24) suporemos tacitamente que x não ocorre já em $\phi(t)$. A conclusão também depende das hipóteses de que depende a premissa numa aplicação desta regra no seio de uma dedução. De notar que, por exemplo,

$$\frac{Raa}{\exists x\,Rxx},\quad \frac{Raa}{\exists x\,Rax},\quad \frac{Raa}{\exists x\,Rxa},\quad \frac{\exists x\,Rxa}{\exists y \exists x\,Rxy},$$

são particularizações correctas desta última regra.

(108) $\forall x\,(Px \to Qx),\ Pa \vdash \exists x\ Qx$

Dedução: obtém-se da dedução de (101) acrescentando a linha

5 | $\exists x\ Qx$ 4 ($\exists^+$).

As restrições enunciadas juntamente com cada regra não são gratuitas: a sua violação pode conduzir a disparates (isto é, à dedução de falácias), como no

exemplo (pseudo-dedução) seguinte:

1	$\forall x(x \doteq x)$	H
2	$a \doteq a$	1 ($\forall^-$)
3	$\forall y(a \doteq y)$	2 ($\forall^+$)
4	$\forall xy\,(x \doteq y)$	3 ($\forall^+$).

Se esta dedução estivesse correcta, da hipótese (universalmente verdadeira) $\forall x(x \doteq x)$ deduzir-se-ia a tese $\forall xy\,(x \doteq y)$, obviamente falsa em domínios com mais de um elemento. Onde está o erro naquela «dedução»?

A nossa última regra quantificacional (eliminação existencial) é um pouco mais complicada do que as anteriores, mas corresponde a um método de uso frequente em demonstrações matemáticas, o chamado *método da constante auxiliar* ou, mais propriamente, no nosso formalismo, o *método do parâmetro auxiliar.*[104]

Quando, em matemática, de certa hipótese (entre outras) existencial $\exists x\phi(x)$ (por exemplo: o conjunto A é não vazio, isto é, $\exists x\, x \in A$) se pretende demonstrar certa tese ou teorema ψ, diz-se a determinada altura algo como «seja a_0 tal que $\phi(a_0)$» (: «seja a_0 um elemento de A»[105]), e a demonstração prossegue até se obter ψ. Em tal procedimento $\phi(a_0)$ é o que se chama uma **particularização** da sentença $\exists x\,\phi(x)$, particularização essa que é admitida temporariamente como nova hipótese, e a_0 é o **parâmetro da particularização**. Além disso, o bom senso recomenda que a_0 seja **típico**, isto é, sujeito à condição $\phi(a_0)$ e a mais nenhuma (hipótese), e neste caso falamos de uma **particularização típica**, e ainda que ψ nada deve dizer acerca de a_0 (obviamente, pois ψ foi enunciada antes de se ter escolhido um parâmetro de particularização). É isto tudo que a regra ($\exists^-$) formaliza.

Eliminação existencial			
		$\phi(a_0)$	[H]
		⋮	
	$\exists x\phi(x)$	ψ	
($\exists^-$)	ψ		

onde $\phi(a_0)$ resulta de $\phi(x)$, substituindo *todas* as ocorrências livres de x por a_0, a_0

---

[104] Em linguagens sem parâmetros utiliza-se uma nova constante, a juntar provisoriamente aos símbolos não lógicos da linguagem; daí a primeira designação do método.

[105] É evidente que a letra usada numa demonstração matemática pode não ser a_0. Na verdade, os matemáticos usam a mesma letra x da quantificação, a qual, entretanto, durante a demonstração, permanece com um estatuto especial: x denota um objecto arbitrário, mas *fixo*, sujeito apenas à condição $\phi(x)$.

não ocorre em ψ nem em hipóteses de que ψ depende na subderivação-premissa (excepto na própria particularização).[106]

Numa dedução, a conclusão depende das hipóteses de que dependem as premissas (exceptuando a particularização típica, que é descarregada ou eliminada aquando da aplicação da regra).

Estruturalmente, a regra ($\exists^-$) é semelhante à regra ($\vee^-$), de que se deve considerar uma generalização.[107]

(109) $\forall x\,(Px \to Qx),\ \exists x\,Px \vdash \exists x\,Qx$

Dedução:

1	$\forall x\,(Px \to Qx)$	H
2	$\exists x\,Px$	H
3	Pa_0	[H]
4	$Pa_0 \to Qa_0$	1 ($\forall^-$)
5	Qa_0	3, 4 (MP)
6	$\exists x\,Qx$	5 ($\exists^+$)
7	$\exists x\,Qx$	2, 3-6 ($\exists^-$).

Outro exemplo de uma pseudo-dedução, por violação de uma restrição da regra ($\exists^-$) que, se fosse correcta, permitiria deduzir da hipótese (verdadeira) «existe um cão raivoso» [$\exists x\,\phi(x)$] a conclusão (falsa) de que «todos os cães são raivosos» [$\forall x\,\phi(x)$]:

1	$\exists x\,\phi(x)$	H
2	Pa	[H]
3	Pa	1, 2-2 ($\exists^-$)
4	$\forall x\,\phi(x)$	3 ($\forall^+$).

Onde está o erro?

Vejamos mais alguns exemplos (outros tantos exercícios), que conduzem a diversas leis importantes (**mudança de variáveis mudas**, **permutabilidade de quantificadores da mesma espécie**):

(110) $\forall x\,Px \dashv\vdash \forall y\,Py.$

(111) $\exists x\,Px \dashv\vdash \exists y\,Py.$

(112) $\forall xy\,Qxy \dashv\vdash \forall yx\,Qxy.$

---

[106] Para evitar de todo a possibilidade de tais ocorrências a maneira mais prática é tomar para a_0 um parâmetro que nunca tenha ocorrido em linhas precedentes na dedução.

[107] Aliás, as regras dos quantificadores não são mais que generalizações das regras dos conectivos $\wedge$, $\vee$ necessárias para podermos lidar (dedutiva, ou semanticamente) com domínios infinitos. As regras dos quantificadores, e os próprios quantificadores, indispensáveis em matemática, seriam possivelmente dispensadas (em teoria) se apenas tivessemos de lidar com domínios finitos.

(113) $\exists xy\, Qxy \dashv\vdash \exists yx\, Qxy.$

(114) $\exists x\, Px \dashv\vdash \exists xy\, (Px \wedge Py).$

(115) $\exists x \forall y\, Rxy \vdash \forall y \exists x\, Rxy.$

Relativamente a este último exemplo, não é de esperar (se as nossas regras forem válidas, como o são de facto[108]) que da hipótese $\forall y \exists x\, Rxy$ se possa deduzir a tese $\exists x \forall y\, Rxy$, isto é, que

$$\forall y \exists x Rxy \rightarrow \exists x \forall y Rxy$$

seja uma lei lógica, como mostra o seguinte

3.1 Contra-exemplo

Suponhamos que o domínio é o conjunto $\mathbb{N}$ dos números naturais (0, 1, 2, ...) e que o símbolo predicativo R denota neste domínio a relação «maior que» (relação inversa da ordem usual em $\mathbb{N}$), e escrevamos $a > b$ em vez de Rab. Ora, para esta interpretação, a sentença antecedente $\forall y\, \exists x\, x > y$ («para todo o número existe um número maior») é verdadeira, mas a consequente $\exists x\, \forall y\, x > y$ («existe um número maior do que todos os números») é, obviamente, falsa.

Nos exemplos acima, onde está Pa pode estar uma condição em a, $\phi(a)$, onde está Qab pode estar uma condição em a e b, $\phi(a, b)$, etc., e analogamente nos exemplos seguintes [mas, ao fazer deduções com as regras ($\forall^+$), ($\exists^-$), devemos ter o cuidado de utilizar parâmetros que não ocorram naquelas condições].

Os dois exemplos seguintes dão origem [contrapondo, utilizando ($\rightarrow^+$) e as regras para $\leftrightarrow$, etc.] às chamadas *leis de De Morgan generalizadas*:

(116) $\forall x\, Px \dashv\vdash \neg\exists x \neg Px.$

(117) $\exists x\, Px \dashv\vdash \neg\forall x \neg Px.$

Também podemos, a partir dos dois exemplos anteriores [com $\phi(x)$ no lugar de Px], justificar as seguintes regras derivadas de De Morgan:

$$(\mathrm{DM}_1) \quad \frac{\neg\forall x\, \phi(x)}{\exists x\, \neg\phi(x)} \qquad (\mathrm{DM}_2) \quad \frac{\neg\exists x\, \phi(x)}{\forall x\, \neg\phi(x)},$$

onde o traço duplo significa que tanto se pode inferir de cima para baixo como de baixo para cima [ver solução de (116) no final do livro]. Estas regras são de grande utilidade, pois abreviam de maneira espectacular qualquer dedução onde sejam oportuno aplicá-las.

---

[108] O que está em causa é, obviamente, a propriedade de validade do sistema **DNQ**, cujo enunciado é exactamente o mesmo que para o sistema **DN**, com a diferença de dizer agora respeito a sentenças de $\mathcal{L}$ e à noção de consequência para $\mathcal{L}$, de que falaremos mais adiante.

Nos exemplos que seguem, que originam *leis de transporte* (ou de *importação* e *exportação*) dos quantificadores (para dentro e para fora de conjunções, etc.), θ é uma qualquer sentença onde não ocorre a variável x. Nas deduções, devem ter-se em conta os parâmetros que possam ocorrer em θ.

(118) $\forall x\,(\theta \rightarrow \phi(x)) \;\dashv\vdash\; \theta \rightarrow \forall x\,\phi(x)$

(119) $\forall x\,(\theta \wedge \phi(x)) \;\dashv\vdash\; \theta \wedge \forall x\,\phi(x)$

(120) $\forall x\,(\theta \vee \phi(x)) \;\dashv\vdash\; \theta \vee \forall x\,\phi(x)$

(121) $\exists x\,(\theta \vee \phi(x)) \;\dashv\vdash\; \theta \vee \exists x\,\phi(x)$

(122) $\exists x\,(\theta \wedge \phi(x)) \;\dashv\vdash\; \theta \wedge \exists x\,\phi(x)$

(123) $\exists x\,(\phi(x) \rightarrow \theta) \;\dashv\vdash\; \forall x\,\phi(x) \rightarrow \theta$

(124) $\forall x\,(\phi(x) \rightarrow \theta) \;\dashv\vdash\; \exists x\,\phi(x) \rightarrow \theta$.

III.4 Regras para a igualdade

O símbolo de igualdade é, formalmente, um símbolo predicativo binário como qualquer outro mas como, intencionalmente, tem uma interpretação fixa em cada domínio, como relação de identidade nesse domínio, recebe, por esse motivo, um tratamento privilegiado em termos dedutivos.

A primeira regra para a igualdade formaliza o clássico *princípio da identidade*, que afirma «qualquer coisa é igual a si mesma». É uma regra sem premissas, como que uma verdade incondicional, que pode ser introduzida em qualquer linha de uma dedução sem mais justificação.

Introdução da igualdade	
$(\doteq^{+})$	$t \doteq t$

onde t é um termo qualquer.

(125) $\vdash \exists x\,(x \doteq t)$, com t fechado.

Dedução:

1	$t \doteq t$	$(\doteq^{+})$
2	$\exists x\,(x \doteq t)$	1 $(\exists^{+})$.

Com uma dedução semelhante obtém-se a importante *lei de existência*, que implica que os domínios interpretativos (III.6 adiante) são sempre não vazios:

(126) $\vdash \exists x\,(x \doteq x)$.

Devemos observar que existem formalizações da lógica de primeira ordem com igualdade para ter em conta a possibilidade de interpretações vazias, possibilidade que alguns autores (por exemplo, JOHNSTONE) defendem com o fundamento da melhor adequação às interpretações concretas. Cremos que a complicação daí resultante não compensa a maior generalidade das regras e, em todo o caso, as interpretações matemáticas vazias são sempre situações de excepção.

A regra de eliminação da igualdade formaliza o *princípio da substituibilidade*, de que «coisas iguais têm as mesmas propriedades».

Eliminação da igualdade	
$(\doteq^{-})$	$\dfrac{t_1 \doteq t_2,\ \phi(t_1)}{\phi(t_2)}$

onde t_1, t_2 são termos e $\phi(t_2)$ resulta de $\phi(t_1)$, substituindo *algumas* ocorrências de t_1 por t_2.

Como é usual, a conclusão depende das hipóteses de que dependem as premissas. Das regras da igualdade facilmente se deduzem as propriedades familiares da igualdade.

(127) $\vdash \forall x\,(x \doteq x)$ [lei da *reflexidade*].

(128) $\vdash \forall xy(x \doteq y \to y \doteq x)$ [lei da *simetria*].

Dedução:

1	$a \doteq b$	[H]
2	$a \doteq a$	$(=^{+})$
3	$b \doteq a$	1, 2 $(=^{-})$
4	$a \doteq b \to b \doteq a$	1-3 $(\to^{+})$
5	$\forall y(a \doteq y \to y \doteq a)$	4 $(\forall^{+})$
6	$\forall x \forall y(x \doteq y \to y \doteq x)$	5 $(\forall^{+})$.

(129) $\vdash \forall xyz(x \doteq y \wedge y \doteq z \to x \doteq z)$ [lei da *transitividade*].

As leis da simetria e da transitividade da igualdade permitem justificar (o que deixamos como exercício) as regras derivadas seguintes, bastante mais convenientes na construção de deduções do que o recurso àquelas leis por invocação de (T^{+}):

$$\text{(Sim)}\quad \frac{s \doteq t}{t \doteq s}, \qquad \text{(Tran)}\quad \frac{r \doteq s,\ s \doteq t}{r \doteq t},$$

onde r, s, t são termos fechados quaisquer.

As duas leis seguintes são outras manifestações da substituibilidade da igualdade. Na terminologia algébrica usual, a igualdade é uma *congruência* com respeito às relações e operações.

(130) $\forall x\, y\, u\, v\, (x \doteq u \wedge y \doteq v \rightarrow (Rxy \leftrightarrow Ruv))$.

(131) $\forall x\, y\, u\, v\, (x \doteq u \wedge y \doteq v \rightarrow fxy \doteq fuv)$.

(132) $Pa \dashv\vdash \exists x\, (x \doteq a \wedge Px)$.

Deduções:

$\vdash$:	1	Pa	H
	2	$a \doteq a$	($=^+$)
	3	$a \doteq a \wedge Pa$	1, 2 ($\wedge^+$)
	4	$\exists x\, (x \doteq a \wedge Px)$	3 ($\exists^+$);

$\dashv$:	1	$\exists x\, (x \doteq a \wedge Px)$	H
	2	$b \doteq a \wedge Pb$	[H]
	3	$b \doteq a$	2 ($\wedge^-$)
	4	Pb	2 ($\wedge^-$)
	5	Pa	3, 4 ($\doteq^-$)
	6	Pa	1, 2-5 ($\exists^-$).

Observe-se, nesta última dedução, a utilização de um parâmetro b distinto do parâmetro a que ocorre na hipótese.

Recorde-se o argumento (11) da pág. 27. Mostramos agora que

(133) $\forall x(Px \rightarrow x \doteq c \vee x \doteq d), \exists x(Px \wedge Qx) \vdash Qc \vee Qd$.

Dedução:

1	$\forall x(Px \rightarrow x \doteq c \vee x \doteq d)$	H
2	$\exists x\,(Px \wedge Qx)$	H
3	$Pa_0 \wedge Qa_0$	[H]
4	Pa_0	3 ($\wedge^-$)
5	Qa_0	3 ($\wedge^-$)
6	$Pa_0 \rightarrow a_0 \doteq c \vee a_0 \doteq d$	1 ($\forall^-$)
7	$a_0 \doteq c \vee a_0 \doteq d$	4, 6 (MP)
8	$a_0 \doteq c$	[H_1]
9	Qc	5, 8 ($\doteq^-$)
10	$Qc \vee Qd$	9 ($\vee^+$)
11	$a_0 \doteq d$	[H_2]
12	Qd	5, 11 ($\doteq^-$)
13	$Qc \vee Qd$	12 ($\vee^+$)
14	$Qc \vee Qd$	7, 8-10, 11-13 ($\vee^-$)
15	$Qc \vee Qd$	2, 3-14 ($\exists^-$).

Relativamente a esta última dedução (ou a muitas outras, nomeadamente, aquelas que o leitor deve tentar fazer por si próprio), é instrutivo compará-la com uma dedução informal do mesmo resultado, tal como seria feita, por exemplo, num texto matemático comum.

4.1 Dedução informal

Seja a_0 um indivíduo tal que (1) Pa_0 e Qa_0, o que faz sentido em virtude da segunda hipótese. Particularizando $x = a_0$ na primeira hipótese, e atendendo a que Pa_0 é verdadeira, por (1), tem-se $a_0 = c$ ou $a_0 = d$. No primeiro caso, tem-se Qc, por causa de (1) e, analogamente, no segundo caso, tem-se Qd. Em qualquer dos casos tem-se Qc ou Qd, como se queria demonstrar.■

Tal como neste exemplo, as demonstrações matemáticas informais são, em regra, muito mais simples e curtas do que as correspondentes deduções formais num sistema como **DNQ** (ou em qualquer outro sistema dedutivo). Não temos a pretensão de afirmar que as deduções formais são, em algum sentido, «melhores» do que as informais, ou que estas, por informais, são menos correctas ou menos rigorosas. *O rigor não é incompatível com a informalidade.* O nosso objectivo tem sido tão-somente o de explicitar um sistema de regras de inferência que permitem analisar os passos lógicos implícitos nas demonstrações informais (e não só).

Por outro lado, é muitas vezes conveniente ter uma ideia intuitiva ou informal de como se demonstra determinada tese a partir de determinadas hipóteses antes de tentar construir uma dedução formal. A ideia intuitiva de uma demonstração fornece invariavelmente uma *estratégia* para a construção de uma dedução formal. Por outro lado, o leitor deve prevaver-se contra a tendência «natural» de aplicar mecanicamente as regras de inferência; deve, em vez disso, desenvolver a

«naturalidade» na argumentação informal, essa sim, útil para proceder depois a uma formalização no sistema dedutivo.

(134) $Pa \dashv\vdash \forall x\,(x \doteq a \rightarrow Px)$.

(135) $\vdash \forall xyz(x \doteq z \wedge y \doteq z \rightarrow x \doteq y)$ [*lei de Euclides*].

Esta última lei foi formulada por Euclides como uma das «Noções Comuns» da sua conhecida axiomatização da geometria.

III.5 Teorias elementares: introdução de símbolos definidos

O conceito de dedutibilidade pode-se alargar-se ao caso de um conjunto arbitrário (finito ou infinito) de hipóteses, como já se viu no capítulo anterior. Recordamos a definição:

5.1 Definição
Seja Γ um conjunto de sentenças, ψ uma sentença de $\mathcal{L}$. Dizemos que ψ é **dedutível de** Γ, ou que é **teorema de** Γ, e escreve-se

$$\Gamma \vdash \psi,$$

sse existe uma dedução (no sistema **DNQ**) de ψ com hipóteses em Γ.

Mesmo no caso de Γ ser finito, estamos admitindo a possibilidade de numa dedução de ψ com hipóteses em Γ não serem utilizadas todas as sentenças de Γ; é necessariamente assim, se Γ for infinito. Observe-se, por outro lado, que toda a lei lógica é automaticamente teorema de qualquer conjunto Γ, pois numa dedução de uma lei lógica nenhumas hipóteses em Γ são necessárias. Por outras palavras, as leis lógicas são os teoremas do conjunto vazio de sentenças, $\emptyset$. As leis lógicas também se chamam, por isso, **teoremas lógicos**.

5.2 Definição
Uma **teoria dedutiva** (ou simplesmente **teoria**, se não houver confusão possível[109]) **T** numa linguagem elementar $\mathcal{L}$ (abreviadamente: uma **teoria elementar**) é um conjunto de sentenças de $\mathcal{L}$ que é **dedutivamente fechado**, isto é, tal que todo o teorema de **T** pertence a **T**.

---

[109] Existem também teorias semânticas, ou teorias definidas semanticamente. Um exemplo muito importante de uma tal teoria é a chamada **aritmética verdadeira** (ou **aritmética completa**), constituída por todas as sentenças (sem parâmetros) da linguagem da aritmética que são verdadeiras na estrutura *standard* dos números naturais (ver definições pertinentes em III.6 e III.8 e também no capítulo IV).

Uma teoria elementar é, pois, essencialmente, um conjunto de teoremas (incluindo sempre os teoremas lógicos). Mas é claro que, sendo infinito um tal conjunto, não é possível dá-lo ou exibi-lo de uma só vez. O que se faz, normalmente, é fornecer um sistema (ou lista) de axiomas para a teoria, que são certas sentenças tais que todo o teorema da teoria já é dedutível delas: Σ é um **sistema de axiomas para a teoria T** sse os teoremas de Σ são exactamente os teoremas de **T**. Obviamente, **T** é um sistema de axiomas para si própria mas, em muitos casos, é possível encontrar um sistema de axiomas para **T** mais simples de descrever.

Um grande número de teorias de ordens (teoria elementar das ordens parciais, teoria elementar das ordens totais, teoria elementar dos reticulados) e algébricas (teoria elementar dos grupos, teoria elementar dos anéis, dos corpos, dos corpos ordenados, etc.) são definidas por meio de axiomas, em número finito, familiares a todo o estudante de matemáticas (ver exercícios). Uma teoria diz-se **axiomatizável** sse possui um sistema decidível de axiomas, e diz-se **finitamente axiomatizável** sse possui um sistema finito de axiomas. Algumas teorias matemáticas importantes, como a aritmética elementar e a teoria axiomática dos conjuntos, são definidas por sistemas infinitos mas decidíveis de axiomas (voltaremos a este assunto).

Veremos adiante (exercícios e Cap. IV) alguns exemplos de teorias elementares. Entretanto, completamos esta secção com algumas observações de natureza geral sobre a introdução de símbolos definidos e sobre a eliminação de símbolos funcionais ou operacionais.

Supomos fixada uma teoria **T** numa linguagem $\mathcal{L}$. Pode acontecer certa fórmula $\phi(a_1, ..., a_n)$ ocorrer tantas vezes no desenvolvimento de **T** que se torne conveniente abreviá-la de alguma maneira. Por exemplo, na teoria dos inteiros, a condição

$$\exists z\ y \doteq z \times x$$

abrevia-se

$$a \mid b \quad \text{(ler «}a \textit{ divide } b\text{»)},$$

onde $\mid$ é o símbolo definido de divisibilidade. No caso geral acima, introduz-se um novo símbolo relacional (isto é, um símbolo relacional que não está em $\mathcal{L}$) n-ário, digamos S, e juntamos a **T** o **axioma de definição** de S

Def(S) $$\forall x_1 ... x_n (S x_1 ... x_n \leftrightarrow \phi(x_1, ..., x_n)).$$

Se $\mathcal{L}'$ é a linguagem cujos símbolos são S e os símbolos de $\mathcal{L}$, e **T**′ é a teoria em $\mathcal{L}'$ cujos axiomas são Def(S) e os axiomas de **T**, só aparentemente $\mathcal{L}'$ tem mais poder expressivo que $\mathcal{L}$ e **T**′ é mais forte (tem mais teoremas) que **T**. Na realidade, a forma de Def(S) é tal, que tudo quanto se possa exprimir em $\mathcal{L}'$ também se pode exprimir em $\mathcal{L}$ (utilizando ϕ no lugar de S) e todo o teorema de **T**′ que não mencione S é já teorema de **T** (dizendo-se, por esta razão, que **T**′ é uma **extensão**

conservativa de **T**). Não demonstramos estas propriedades gerais das teorias mas, em todo o caso, elas devem parecer razoáveis.

Foi dito anteriormente que os símbolos funcionais são teoricamente dispensáveis. Justificaremos agora esta afirmação, exemplificando com o caso de um símbolo funcional binário, digamos $+$, para usar uma notação familiar. A ideia é simplesmente a de introduzir um novo símbolo relacional ternário, digamos S_+, ou simplesmente S, nesta discussão, por meio da definição

Def(S) $$\forall xyz(Sxyz \leftrightarrow x + y \doteq z).$$

À nossa teoria **T** juntaremos igualmente o **axioma de funcionalidade** de S

Fun(S) $$\forall xyz_1z_2\,(Sxyz_1 \wedge Sxyz_2 \rightarrow z_1 \doteq z_2)$$

que exprime que S é **funcional** no 3.º argumento (isto é, S «comporta-se» como uma função binária dos dois primeiros argumentos, ou seja $Saba'$ comporta-se como se a' fosse funcional em a, b). Também se prova, neste caso, que a nova teoria é extensão conservativa da teoria inicial e que tudo quanto se pode exprimir na linguagem original, com $+$, pode-se exprimir equivalentemente utilizando S. Por exemplo, para exprimir a comutatividade de $+$, expressa por

$$\forall x\,y\,(x + y \doteq y + x),$$

escrevemos primeiramente a sentença equivalente

$$\forall\, x\,y\,\exists\, u\,v\,(x + y \doteq u \ \wedge\ y + x \doteq v \wedge u \doteq v),$$

e finalmente:

$$\forall\, x\,y\,\exists\, u\,v\,(Sxyu \wedge Syxv \wedge u \doteq v).$$

Ao invés de eliminar um símbolo funcional a favor de um novo símbolo predicativo (de maior aridade), mostramos de seguida como se podem introduzir novos símbolos funcionais e constantes.

Comecemos pelas constantes. Suponhamos que na teoria **T** se demonstrou um teorema de existência e unicidade da forma

(1) $$\exists^1 x\,\phi(x)$$

É possível então introduzir uma nova constante, digamos c_0, que passará a designar o único a tal que $\phi(a)$. A sentença

Def(c_0) $$\phi(c_0)$$

é o **axioma de definição** de c_0, e dela, juntamente com (*), pode deduzir-se a sentença que define o predicado unário $c_0 \doteq a$:

(2) $$\forall x(c_0 \doteq x \leftrightarrow \phi(x)).$$

Por exemplo, na teoria dos conjuntos, depois de se demonstrar que existe um único conjunto sem elementos, introduz-se a constante $\emptyset$ para designar um tal conjunto. O axioma de definição de $\emptyset$ é $\forall x \neg (x \in \emptyset)$.

Mais geralmente,[110] suponhamos que na nossa teoria **T** se demonstrou um **teorema de existência e unicidade** da forma

(3) $$\forall x_1 ... \, x_n \exists^1 y \, \phi(x_1, ..., x_n, y).$$

É então possível introduzir um novo símbolo funcional n-ário, digamos h, de tal modo que para quaisquer a_1, ..., a_n, $ha_1...a_n$ designe o único b tal que $\phi(a_1, ..., a_n, b)$. A sentença

Def(h) $$\forall x_1 ... \, x_n \, \phi(x_1, ..., x_n, hx_1...x_n)$$

é o **axioma de definição** de h, e desta sentença, juntamente com o teorema (3), pode deduzir-se a definição do predicado $ha_1...a_n \doteq b$:

(4) $$\forall x_1 ... \, x_n \, y \, (hx_1 ... \, x_n \doteq y \leftrightarrow \phi(x_1, ..., x_n, y)).$$

Por exemplo, na teoria dos conjuntos (ver exercício 3.21), depois de demonstrar que para quaisquer conjuntos a_1, a_2 existe um único conjunto b cujos elementos são exactamente os elementos comuns a a_1 e a_2, introduz-se o símbolo operacional $\cap$, de tal modo que $a_1 \cap a_2$ designe esse único b. O axioma de definição de $\cap$ é

$$\forall x (x \in x_1 \cap x_2 \leftrightarrow x \in x_1 \wedge x \in x_2).$$

A importância das sentenças (2) e (4) reside no facto de permitirem *eliminar* os símbolos definidos das fórmulas da linguagem ampliada onde ocorram. Por outro lado, também se prova que as teorias com os axiomas de definição dos novos símbolos são extensões conservativas das teorias originais.

III.6 Semântica tarskiana

No Cap. I explicámos, em termos informais, a semântica do cálculo de predicados. Precisaremos agora um pouco mais o que então foi dito.

Como é de esperar, a semântica de uma linguagem elementar $\mathcal{L}$ é um tanto mais complicada do que a de uma linguagem proposicional $\mathcal{L}^0$, e envolve em maior grau noções e técnicas da teoria dos conjuntos. É claro que existe uma *semântica intuitiva* ou *informal,* já referida no Cap. I, mas insuficiente para poder estabelecer resultados metateóricos com rigor. Acontece, por outro lado, que, se nos restringirmos a uma semântica estritamente matemática [quer dizer, por exemplo, que *os domínios das interpretações são conjuntos* (abstractos ou concretos), no sentido matemático, e não meras colecções intuitivas, como a colecção dos seres

[110] Certos autores consideram as constantes como símbolos funcionais nulários ou 0-ários, o que tem a sua justificação na teoria dos conjuntos: uma função nulária com valores num conjunto não vazio «fixa» um elemento nesse conjunto.

humanos], nada de essencial se vai perder do ponto de vista lógico.[111] De facto, para a semântica quantificacional não bastam as valorações e as tabelas de verdade. Muitas mais noções estão envolvidas: conjuntos (possivelmente infinitos) como domínios interpretativos, relações definidas em conjuntos, operações definidas em conjuntos, etc.

Suponhamos, para facilitar a discussão, que a nossa linguagem (com igualdade) $\mathcal{L}$ tem somente como símbolos não lógicos um símbolo relacional binário P, um símbolo funcional binário f e uma constante c, o que indicaremos abreviadamente escrevendo:

$$\mathcal{L} = \{P, f, c\}.$$

Todavia, as definições que vamos dar generalizam-se imediatamente a qualquer linguagem elementar, com qualquer número e variedade de símbolos não lógicos.[112]

6.1 Definição

Uma **estrutura adequada** para a linguagem $\mathcal{L}$ acima (ou simplesmente: **estrutura**-$\mathcal{L}$) é um sistema (um «uplo» ordenado)

$$\mathfrak{M} = (M, P^{\mathfrak{M}}, f^{\mathfrak{M}}, c^{\mathfrak{M}}) = (M, P, f, c),$$

constituído por:

• Um conjunto (ou classe) não vazio M, chamado o **domínio**, **suporte** ou **universo** da estrutura $\mathfrak{M}$, o qual, por vezes, se designa por $|\mathfrak{M}|$;

• Uma relação binária $P^{\mathfrak{M}} = P$ em M, isto é, $P \subseteq M^2$, que se diz a relação em $\mathfrak{M}$ **correspondente** ao símbolo P, ou a **interpretação** de P em $\mathfrak{M}$, ou ainda a relação que P **denota** (ou **designa**) em $\mathfrak{M}$;

• Uma operação binária $f^{\mathfrak{M}} = f : M^2 \to M$, que se diz a operação em $\mathfrak{M}$ **correspondente** ao símbolo f, ou a **interpretação** de f em $\mathfrak{M}$, ou a operação que f **denota** (ou **designa**) em $\mathfrak{M}$;

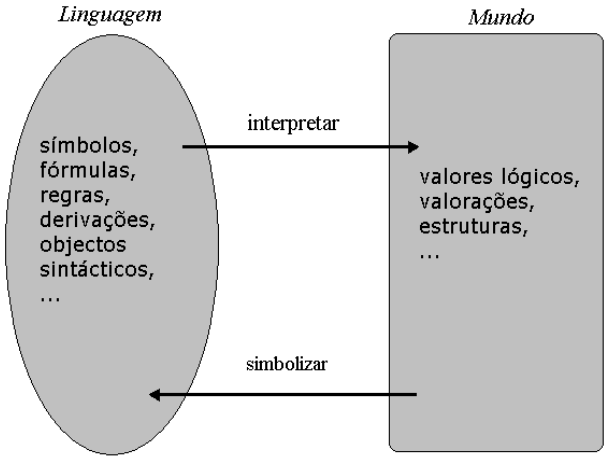
• Um elemento constante ou fixo $c^{\mathfrak{M}} = c \in M$, **correspondente** ao símbolo c, ou a **interpretação** de c em $\mathfrak{M}$, ou o elemento que a constante c **denota** (ou **designa**).

Duas estruturas para a mesma linguagem $\mathcal{L}$ dizem-se **semelhantes** ou **do mesmo tipo**.

---

[111] Esta afirmação é um pouco difícil de precisar de momento, pois apoia-se num resultado metateórico profundo. O que se quer dizer, informalmente, é que algumas noções semânticas, como a noção de fórmula válida, são as mesmas, quer se utilize a semântica intuitiva, quer se utilize a semântica matemática ou tarskiana, essencialmente conjuntista (ver III.11).

[112] É conveniente, por vezes, chamar *linguagem de* ϕ e representar por $\mathcal{L}_\phi$ o conjunto dos símbolos não lógicos que ocorrem em ϕ.



6.2 Exemplos

Eis três estruturas do mesmo tipo, para a linguagem $\mathcal{L} = \{P, f, c\}$ acima

$$\mathfrak{M}_1 = (M_1, P^{\mathfrak{M}_1}, f^{\mathfrak{M}_1}, c^{\mathfrak{M}_1}) = (M_1, P_1, f_1, c_1) = (\mathbb{N}, <, +, 0);$$
$$\mathfrak{M}_2 = (M_2, P^{\mathfrak{M}_2}, f^{\mathfrak{M}_2}, c^{\mathfrak{M}_2}) = (M_2, P_2, f_2, c_2) = (\{1\}, \emptyset, \{((1,1),1)\}, 1);$$
$$\mathfrak{M}_3 = (M_3, P^{\mathfrak{M}_3}, f^{\mathfrak{M}_3}, c^{\mathfrak{M}_3}) = (M_3, P_3, f_3, c_3)$$
$$= (\{1,2\}, \{(1,2),(2,2)\}, \{((1,1),1),((1,2),2),((2,1),1),((2,2),2)\}, 2).$$

No primeiro exemplo, $<$ é a relação de ordem (estrita) usual em $\mathbb{N}$ e $+$ é a operação de adição usual; no segundo exemplo, $f = \{((1,1),1)\}$ é a operação binária em $\{1\}$ tal que $f(1,1) = 1$ (não há mais nenhuma!) e, finalmente, no terceiro exemplo,

$$f_3 = \{((1,1),1),((1,2),2),((2,1),1),((2,2),2)\} : \{1,2\} \to \{1,2\}$$

é a operação binária em $\{1,2\}$ tal que $f_3(1,1) = f_3(2,1) = 1$, $f_3(1,2) = f_3(2,2) = 2$.[113]

Dissemos acima que o domínio M de uma estrutura $\mathfrak{M}$ pode ser uma *classe*. Digamos apenas, de momento, que a noção de classe é um pouco mais geral do que a noção de conjunto. Todo o conjunto é uma classe, mas não reciprocamente. Por

[113] Ilustra-se neste exemplo o facto de uma função ou aplicação $f : A \to B$ ser, do ponto de vista extensional ou conjuntista, um certo subconjunto do produto cartesiano $A \times B$ (isto é, uma relação de A para B). Mais geralmente, uma função ou operação n-ária é uma relação $(n+1)$-ária com o mesmo domínio e uma propriedade especial — a *funcionalidade*: para $n = 1$, uma relação F de A para B (isto é, $F \subseteq A \times B$) é uma função ou aplicação de A em B, e escreve-se $F : A \to B$, sse para todo $x \in A$ existe um único $y \in B$ tal que $(x, y) \in F$. Se F é função, dado x, o único y tal que $(x, y) \in F$ chama-se o *valor de F em x e designa-se por* $F(x)$ (ou, por vezes, Fx, ou ainda F_x). O conjunto A é o *domínio* de F: $A = \text{dom}(F)$.

exemplo, a classe de todos os conjuntos, a classe de todos os grupos, etc., não são conjuntos. A distinção conjunto/classe não foi feita por Cantor (nem por Frege), mas é necessária na moderna teoria axiomática (veja-se V.4), para evitar paradoxos.[114] Por outro lado, nada se disse sobre a interpretação do símbolo de igualdade $\doteq$ de $\mathcal{L}$, mas fica convencionado que $\doteq$ se interpreta como, denota ou corresponde à *relação de identidade em* M (usualmente: $=$).[115]

O leitor já conhece (presumivelmente) muitos exemplos de estruturas (grupos, grupos ordenados, álgebras de Boole, anéis, corpos, conjuntos parcialmente ordenados, estruturas relacionais e bases de dados, etc.), embora talvez nunca as tenha encarado sob o ponto de vista acima, isto é, cada estrutura dessas como uma estrutura para determinada linguagem (ver exercícios no final).

Suponhamos, para exemplificar, que a nossa linguagem é a linguagem dos grupos (estritamente) ordenados, em notação aditiva, $\mathcal{L}_{\text{gror}}$, com um símbolo predicativo binário $<$, um símbolo operacional binário $+$, e uma constante 0. Uma estrutura para $\mathcal{L}_{\text{gror}}$ é da forma

$$\mathfrak{G} = (G, +^{\mathfrak{G}}, <^{\mathfrak{G}}, 0^{\mathfrak{G}}) = (G, +, <, 0)$$

onde G é um conjunto não vazio, $+ : G \times G \to G$, $<$ é uma relação binária em G, e $0 \in G$. Mas atenção: uma tal estrutura *não é* necessariamente um grupo ordenado. Para ser grupo ordenado tem de ter certas propriedades (como: $+$ é associativa, 0 é elemento neutro para $+$, etc.). Diremos mais adiante que para ser grupo ordenado uma estrutura-$\mathcal{L}_{\text{gror}}$ $\mathfrak{G}$ tem de *satisfazer* ou realizar certas sentenças, quer dizer, ter as propriedades expressas por essas sentenças [os axiomas de grupo ordenado (ver exercício 3.17)].

Regressemos ao caso geral. O nosso objectivo é definir, para cada sentença ϕ de $\mathcal{L}$ e cada estrutura $\mathfrak{M}$,

«ϕ é **verdadeira** (ou **satisfeita**) em $\mathfrak{M}$»

(ou $\mathfrak{M}$ **satisfaz** ϕ, ou ainda $\mathfrak{M}$ é **modelo de** ϕ»). Intuitivamente, a ideia é simples: *ϕ é verdadeira em $\mathfrak{M}$ sse aquilo que ϕ exprime acerca dos elementos de M, incluindo c, da operação f e da relação P em M, acontece de facto.*[116] Mas, mesmo esta explicação intuitiva só faz sentido no caso de ϕ não ter parâmetros.

---

[114] O paradoxo mais famoso da teoria intuitiva dos conjuntos é, talvez, o *paradoxo de Russell*, que resulta da suposição de que a classe dos conjuntos X tais que $X \notin X$ é conjunto. Supondo, com vista a um absurdo, que tal classe era conjunto, digamos R (de Russell), ter-se-ia para qualquer X, $X \in R$ sse $X \notin X$ donde, em particular, para $X = R$, que $R \in R$ sse $R \notin R$, o que é contraditório [ver exercícios 2.11(b) e 5.6].

[115] Em rigor, esta é a relação de identidade universal, ou seja, no universo de todas as coisas, e a relação de identidade em M é o conjunto de pares ordenados $I_M = \Delta_M = \{(a, b) : a \in M \text{ e } b \in M \text{ e } a = b\}$, também chamado a **diagonal** de M — ver adiante, pp. 187-187.

[116] Recorde-se o exemplo não matemático do Cap. I: se ϕ é a proposição «a relva é verde», então ϕ é verdadeira sse a relva realmente é verde.

Não saberemos dizer de uma fórmula com parâmetros, por exemplo:

$$a + b \doteq 0,$$

da linguagem $\mathcal{L}_{\text{gror}}$, se é verdadeira ou falsa num dado grupo ordenado $\mathfrak{G}$, se não soubermos que *valores é que são dados aos parâmetros* a, b. No grupo ordenado dos inteiros, $\mathfrak{Z} = (\mathbb{Z}, +, <, 0)$, aquela sentença é verdadeira para atribuições em que $a \mapsto 2$, $b \mapsto -2$, mas é falsa para atribuições em que $a \mapsto 2$, $b \mapsto 3$.

No caso geral necessitamos, pois, de *atribuir valores* (no domínio M de uma estrutura $\mathfrak{M}$) *aos parâmetros de* $\mathcal{L}$ antes de podermos dizer se uma dada fórmula ϕ (possivelmente com parâmetros) é verdadeira ou falsa em $\mathfrak{M}$ com respeito a esses valores.

Dissemos no início do capítulo que os parâmetros seriam utilizados primordialmente em deduções e que nestas somente se utilizariam fórmulas (com ou sem parâmetros). Na definição geral de satisfação, teremos de atender também a fórmulas com parâmetros (sentenças abertas) para que seja possível, mais tarde, uma prova de que as regras são válidas. Convém não perder de vista, pois, que algumas sentenças sem parâmetros compostas só podem ser definidas (*não* indutivamente) a partir das fórmulas ou sentenças abertas (com parâmetros), e só para estas últimas é em princípio possível dar uma definição de satisfação por indução na complexidade. Para ajudar à formalização da definição de satisfação, vamos supor as variáveis individuais e os parâmetros indexados nos números naturais:

- variáveis individuais $x_0, x_1, x_2, ...$;
- parâmetros $a_0, a_1, a_2, ...$,

respectivamente.

6.3 Definição

Seja $\mathfrak{M} = (M, P, f, c)$ uma estrutura-$\mathcal{L}$. Chama-se **atribuição em** $\mathfrak{M}$ a toda a sucessão $\alpha = \langle \alpha_0, \alpha_1, ... \rangle = \langle \alpha_i \rangle_{i \geq 0}$, de elementos de M. A um par ordenado da forma $\mathfrak{I} = (\mathfrak{M}, \alpha)$ chamamos uma **interpretação de** $\mathcal{L}$.

Dada uma atribuição α em $\mathfrak{M}$, supomos tacitamente que a cada parâmetro a_i é atribuído o valor α_i, o que se indica escrevendo

$$a_i \mapsto \alpha_i \; [= \alpha(i), \text{para } i = 0, 1, 2, ...],$$

respectivamente. O domínio, as relações e operações de $\mathfrak{M}$ também se chamarão o domínio, as relações e operações da interpretação $\mathfrak{I}$.

Note-se que esta noção de interpretação é ligeiramente diferente da noção intuitiva dada no Cap. I, pois nessa altura não considerámos a possibilidade de atribuir valores aos parâmetros (variáveis livres) e é claro que estes ainda nem sequer tinham sido mencionados.

O nosso objectivo é, pois, definir a noção

«ϕ é verdadeira (ou satisfeita) na interpretação $\mathfrak{I}$»,

ou, sinonimamente,

«ϕ é verdadeira (ou satisfeita) em $\mathfrak{M}$ com respeito a α»,

o que se abrevia escrevendo

$$\mathfrak{I}(\phi) = 1, \text{ ou } \mathfrak{I} \vDash \phi, \text{ ou ainda } \mathfrak{M} \vDash \phi[\alpha].^{117}$$

Com esse objectivo em vista, definimos indutivamente (na complexidade dos termos e das fórmulas, respectivamente) as noções seguintes:

(1) **Valor de um termo** t **em** $\mathfrak{I}$, $\mathfrak{I}(t)$ [$= t_{\mathfrak{I}} = t^{\mathfrak{M}}[\alpha]$], também chamado o *valor de* t *em* $\mathfrak{M}$ *com respeito a* α;

(2) **valor lógico da fórmula** ϕ **em** $\mathfrak{I}$, $\mathfrak{I}(\phi)$ [$= \phi_{\mathfrak{I}} = \phi^{\mathfrak{M}}[\alpha]$], também chamado o *valor lógico de* ϕ *em* $\mathfrak{M}$ *com respeito a* α.

Definição de $\mathfrak{I}(t)$: — Se t é um parâmetro a_i, então $\mathfrak{I}(t)$ é α_i, isto é,

$$\mathfrak{I}(a_i) = \alpha_i;$$

— se t é a constante c, então $\mathfrak{I}(t)$ é o elemento $c^{\mathfrak{M}} = c$ que c denota em $\mathfrak{M}$, isto é,

$$\mathfrak{I}(c) = c;$$

— se t é da forma ft_1t_2, então $\mathfrak{I}(t)$ é $f(\mathfrak{I}(t_1), \mathfrak{I}(t_2))$, isto é,

$$\mathfrak{I}(ft_1t_2) = f(\mathfrak{I}(t_1), \mathfrak{I}(t_2)).$$

6.4 Exemplo

No grupo ordenado dos inteiros, $\mathfrak{Z} = (\mathbb{Z}, +, <, 0)$, se

$$\alpha = \langle 1, 3, 2, 3, ... \rangle,$$

$\mathfrak{I} = (\mathfrak{Z}, \alpha)$ e t é o termo $a_0 + (a_3 + 0)$, tem-se

$$\mathfrak{Z}(t) = 1 + (3 + 0) = 4.$$

---

[117] Estamos, por abuso, representando pelo mesmo símbolo '$\mathfrak{I}$' a interpretação $\mathfrak{I} = (\mathfrak{M}, \alpha)$ e a função que associa a cada ϕ um valor lógico $\mathfrak{I}(\phi)$. O símbolo '$\vDash$' também será utilizado mais adiante para designar a relação de consequência lógica ou semântica, mas evita-se a confusão prestando atenção ao contexto.

Em geral, $\mathfrak{I}(t)$ não é mais do que o elemento do domínio de $\mathfrak{I}$ que o termo t intencionalmente designa, quando se dão aos parâmetros em t os valores atribuídos por α.

6.5 Definição de $\mathfrak{I}(\phi)$: — Se ϕ é atómica, digamos uma igualdade $(t_1 \doteq t_2)$, então

$$\mathfrak{I}((t_1 \doteq t_2)) = 1 \text{ sse } \mathfrak{I}(t_1) = \mathfrak{I}(t_2),$$

isto é, sse t_1 e t_2 têm *o mesmo valor* em $\mathfrak{M}$ com respeito a α; e se ϕ é da forma Pt_1t_2, então

$$\mathfrak{I}(P\,t_1t_2) = 1 \text{ sse } (\mathfrak{I}(t_1), \mathfrak{I}(t_2)) \in P,$$

isto é, sse o par ordenado de valores de t_1 e de t_2 em $\mathfrak{M}$ com respeito a α está na relação que P designa em $\mathfrak{M}$;

— se ϕ é da forma $\neg\psi$, então

$$\mathfrak{I}(\neg\psi) = 1 \text{ sse } \mathfrak{I}(\psi) = 0;$$

— se ϕ é de uma das formas $\psi \wedge \theta$, $\psi \vee \theta$, $\psi \rightarrow \theta$, então

$$\begin{aligned}
&\mathfrak{I}(\psi \wedge \theta) = 1 \text{ sse } \mathfrak{I}(\psi) = 1 \text{ e } \mathfrak{I}(\theta) = 1,\\
&\mathfrak{I}(\psi \vee \theta) = 1 \text{ sse } \mathfrak{I}(\psi) = 1 \text{ ou } \mathfrak{I}(\theta) = 1,\\
&\mathfrak{I}(\psi \rightarrow \theta) = 1 \text{ sse } \mathfrak{I}(\psi) = 0 \text{ ou } \mathfrak{I}(\theta) = 1,
\end{aligned}$$

respectivamente;

— se ϕ é da forma $\forall x_k\psi = \forall x_k\psi(x_k/a_j)$, então

$$\mathfrak{I}(\forall x_k\psi) = 1 \text{ sse para todo o elemento } m \text{ de } M, \mathfrak{I}'(\psi) = 1,$$

onde $\mathfrak{I}' = (\mathfrak{M}, \alpha')$ e $\alpha' = \alpha(m/a_j) = \langle\alpha'_i\rangle_{i\geq 0}$ é em tudo como α, excepto possivelmente no valor em a_j, pois que $\alpha'_j = m$; e se ϕ é da forma $\exists x_k\psi(x_k/a_j)$, então

$$\mathfrak{I}(\exists x_k\psi) = 1 \text{ sse existe } m \in M \text{ tal que } \mathfrak{I}'(\psi) = 1,$$

sendo $\mathfrak{I}' = (\mathfrak{M}, \alpha') = (\mathfrak{M}, \alpha(m/a_j))$ como acima.[118]

---

[118] Estas definições são devidas essencialmente a A. Tarski (1936), e com elas se inaugurou a possibilidade de um tratamento matemático da semântica quantificacional. Elas são um pouco mais complexas que quaisquer outras neste livro, e podem ser omitidas numa primeira leitura, aceitando-se como suficiente o entendimento do seu significado intuitivo.

K. Gödel e A. Tarski
(Princeton, 1962)

Observe-se que as claúsulas proposicionais mostram que a determinação de um valor lógico $\mathfrak{I}(\phi)$, no que respeita aos conectivos $\neg$, $\wedge$, $\vee$, $\rightarrow$ se faz *exactamente como na lógica proposicional*; por outras palavras, uma interpretação $\mathfrak{I}$ determina uma valoração booleana $\widehat{v} = \widehat{v}_{\mathfrak{I}}$ definida no conjunto das fórmulas de $\mathcal{L}$, pondo

$$\widehat{v}(\phi) = \mathfrak{I}(\phi).$$

O conjunto das fórmulas de $\mathcal{L}$ é um conjunto da forma $\mathrm{Prop}(P_1)$ (p. 50), onde agora P_1 é o conjunto das fórmulas **primas** de $\mathcal{L}$, isto é, as fórmulas atómicas e as fórmulas da forma $\forall x_i \phi$, $\exists x_i \phi$.

As fórmulas primas desempenham, do ponto de vista «proposicional» relativamente a $\mathcal{L}$, o mesmo papel que as letras proposicionais desempenham relativamente a $\mathcal{L}^0$. Mas não devemos supor, por cautela, que a semântica das linguagens elementares se reduz à semântica proposicional.

Semelhantemente à propriedade enunciada no exercício 2.3(b), pode-se provar, por indução na complexidade dos termos e das fórmulas, que, no que respeita à atribuição α em $\mathfrak{M}$, e sendo $\mathfrak{I} = (\mathfrak{M}, \alpha)$, $\mathfrak{I}(t)$ *só depende da valores atribuídos aos parâmetros que ocorrem em* t e $\mathfrak{I}(\phi)$ *só depende dos valores atribuídos aos parâmetros que ocorrem em* ϕ. Em particular, se ϕ é uma sentença (fórmula *sem* parâmetros), $\mathfrak{I}(\phi)$ *não depende de* α (logo, só depende de $\mathfrak{M}$), e poderíamos designar o valor lógico $\mathfrak{I}(\phi)$ por $\mathfrak{M}(\phi)$, mas não usaremos esta notação.

6.6 Definição

Se $\mathfrak{I}(\phi) = 1$, dizemos que ϕ é **verdadeira** ou **satisfeita** em $\mathfrak{I}$, ou que $\mathfrak{I}$ **satisfaz** ϕ, ou ainda que ϕ é verdadeira ou satisfeita em $\mathfrak{M}$ com respeito a α, e escreve-se $\mathfrak{I} \vDash \phi$, ou $\mathfrak{M} \vDash \phi[\alpha]$. Se $\mathfrak{I}(\phi) = 0$, dizemos que ϕ é **falsa** em $\mathfrak{I}$, etc., e escreve-se $\mathfrak{I} \nvDash \phi$, ou $\mathfrak{M} \nvDash \phi[\alpha]$.

Da definição de satisfação resulta logo que para qualquer interpretação $\mathfrak{I}$ e qualquer fórmula ϕ, se tem $\mathfrak{I} \vDash \phi$ ou $\mathfrak{I} \vDash \neg\phi$. Já introduzimos a notação mais sugestiva

$$\mathfrak{M} \vDash \phi[\alpha], \quad \mathfrak{M} \nvDash \phi[\alpha], \qquad (*)$$

em vez de $\mathfrak{I}(\phi) = 1$, $\mathfrak{I}(\phi) = 0$, respectivamente, onde $\mathfrak{I} = (\mathfrak{M}, \alpha)$, podendo suprimir-se a parte "$[\alpha]$" no caso de uma sentença sem parâmetros ϕ pois, neste caso, $\mathfrak{I}(\phi)$ só depende de $\mathfrak{M}$. Neste caso, resulta logo da definição de satisfação que para qualquer estrutura $\mathfrak{M}$ e qualquer sentença sem parâmetros ϕ se tem $\mathfrak{M} \vDash \phi$ ou $\mathfrak{M} \vDash \neg\phi$.[119] (Veja-se, a propósito, a observação 2 da pág. 184.)

Pelas observações acima, se $\phi(a_0, a_1, ..., a_k)$ é uma fórmula nos parâmetros exibidos, e $a_0 \mapsto \alpha_0$, ..., $a_k \mapsto \alpha_k$, podemos simplificar as notações $(*)$ em

$$\mathfrak{M} \vDash \phi(a_0, a_1, ..., a_k)[\alpha_0, \alpha_1, ..., \alpha_k], \quad \mathfrak{M} \nvDash \phi(a_0, a_1, ..., a_k)[\alpha_0, \alpha_1, ..., \alpha_k],$$

respectivamente. Com esta notação, são mais fáceis de entender as últimas claúsulas da definição de satisfação.

Considerando a fórmula com parâmetros $\psi(a_0, a_1, ..., a_k)$, tem-se, de acordo com a definição,

$$\mathfrak{M} \vDash \forall x_0 \psi(x_0, a_1, ..., a_k)[\alpha_1, ..., \alpha_k] \text{ sse}$$
$$\text{para todo } m \in M, \mathfrak{M} \vDash \psi(a_0, a_1, ..., a_k)[m, \alpha_1, ..., \alpha_k],$$

onde supomos que $a_0 \mapsto m$, e analogamente

$$\mathfrak{M} \vDash \exists x_0 \psi(x_0, a_1, ..., a_k)\ [\alpha_1, ..., \alpha_k] \text{ sse}$$
$$\text{existe } m \in M \text{ tal que } \mathfrak{M} \vDash \psi(a_0, a_1, ..., a_k)[m, \alpha_1, ..., \alpha_k].^{120}$$

6.7 Exemplo

Consideremos, na linguagem dos grupos ordenados, a fórmula

$$\phi(a_1, a_3) : \ \exists x_0\, (x_0 < a_1 \wedge a_1 + a_3 < x_0 + 0).$$

Seja $\mathfrak{Z}$ (inteiros) como acima, α tal que $a_1 \mapsto 1$, $a_3 \mapsto -1$. Temos $\mathfrak{Z} \vDash \phi(a_1, a_3)$ $[1, -1]$ sse existe um inteiro m tal que

$$\mathfrak{Z} \vDash (a_0 < a_1 \wedge a_1 + a_3 < a_0 + 0)[m, 1, -1],$$

sse existe um inteiro m tal que

$$\mathfrak{Z} \vDash (a_0 < a_1)[m, 1] \text{ e } \mathfrak{Z} \vDash (a_1 + a_3 < a_0 + 0)[m, 1, -1],$$

sse existe um inteiro m tal que

$$m < 1 \text{ e } 1 + (-1) < m + 0, \text{ isto é, tal que } m < 1 \text{ e } 0 < m,$$

o que não acontece; portanto, $\mathfrak{Z} \nvDash \phi(a_1, a_3)[1, -1]$.

---

[119] Há uma razão «escondida» para a veracidade desta afirmação, nomeadamente, o facto de as nossas estruturas terem domínios não vazios e, portanto, existirem atribuições nelas.

[120] Abusando da notação: $\mathfrak{M} \vDash \forall x_0\, \psi(x_0, \alpha)$ sse para todo $m \in M$, $\mathfrak{M} \vDash \psi(m, \alpha)$, e $\mathfrak{M} \vDash \exists x_0 \psi(x_0, \alpha)$ sse existe $m \in M$ tal que $\mathfrak{M} \vDash \psi(m, \alpha)$, onde α abrevia $a_1, \ldots, a_k$.

Com a mesma fórmula $\phi(a_1, a_3)$ e a mesma atribuição, mas agora encarada como atribuição no grupo ordenado dos números racionais $\mathfrak{Q} = (\mathbb{Q}, +, <, 0)$ (o que faz sentido, pois $\mathbb{Z} \subseteq \mathbb{Q}$), tem-se analogamente

$$\mathfrak{Q} \vDash \phi(a_1, a_3)[1, -1] \text{ sse existe um racional } r \text{ tal que } r < 1 \text{ e } 0 < r,$$

o que é verdade, logo $\mathfrak{Q} \vDash \phi(a_1, a_3)[1, -1]$.

Outras noções semânticas importantes se podem agora definir em função da noção de satisfação, generalizando as noções correspondentes na lógica proposicional.

6.8 Definição

Dizemos que uma fórmula ϕ é **válida na estrutura** $\mathfrak{M}$ sse ϕ é verdadeira em $\mathfrak{M}$ com respeito a *todas* as atribuições α em $\mathfrak{M}$, e escreve-se

$$\mathfrak{M} \vDash \phi.$$

E diz-se que ϕ é **universalmente válida**, ou simplesmente **válida**, sse ϕ é válida em todas as estruturas, escrevendo-se então $\vDash \phi$.

6.9 Observações importantes

1) Para uma sentença sem parâmetros ϕ, são equivalentes as asserções «ϕ é verdadeira em $\mathfrak{M}$» e «ϕ é válida em $\mathfrak{M}$», pois ϕ é verdadeira em $\mathfrak{M}$ sse ϕ é verdadeira em $\mathfrak{I} = (\mathfrak{M}, \alpha)$, qualquer que seja a atribuição α em $\mathfrak{M}$.

2) Devemos ter um cuidado especial quando formulados a validade de um argumento (ou a mais geral relação de consequência lógica — ver adiante)

$$\frac{\phi_1, \phi_2, ..., \phi_n}{\psi},$$

no caso que alguma das premissas ϕ_i (ou a conclusão) é uma fórmula com parâmetros. Será conveniente, por razões óbvias, poder continuar a dizer que um tal argumento é válido sse todo o modelo das premissas é modelo da conclusão, mas temos de ter presentes que *um modelo de uma fórmula com parâmetros $\phi = \phi(a_1, ..., a_k)$ é uma estrutura $\mathfrak{M}$ que satisfaz ϕ com respeito a todas as atribuições α em $\mathfrak{M}$*. Quer dizer, para fórmulas com parâmetros (sentenças abertas) ϕ,

$$\mathfrak{M} \text{ é modelo de } \phi \text{ sse } \phi \text{ é válida em } \mathfrak{M}.$$

Tais preocupações com a terminologia são escusadas no caso de fórmulas sem parâmetros (sentenças fechadas) pois, neste caso, como já se referiu anteriormente (pág. 182), ϕ é válida em $\mathfrak{M}$ sse ϕ é verdadeira em ϕ.

As fórmulas universalmente válidas desempenham, relativamente a uma linguagem elementar $\mathcal{L}$, um papel semelhante ao desempenhado pelas tautologias relativamente à linguagem proposicional $\mathcal{L}^0$.

Exemplos de fórmulas válidas:

$$a \doteq a,\ \forall xy\,(Rxy \vee \neg Rxy),\ \exists x\,\forall y\,Rxy \rightarrow \forall y\,\exists x\,Rxy.$$

A sentença recíproca desta última não é válida — um contra-exemplo já foi dado anteriormente (com a relação $>$ em $\mathbb{N}$). Veremos adiante que, na realidade, todas as sentenças que são leis lógicas (ou teoremas lógicos) do sistema **DNQ**, e somente essas, são universalmente válidas.

6.10 Definição

Seja Σ um conjunto de sentenças, ou até de fórmulas. Σ é **compatível** sse tiver, pelo menos, um modelo. Uma fórmula ψ é **consequência lógica** de Σ e escreve-se

$$\Sigma \vDash \psi,$$

sse todo o modelo de Σ (isto é, modelo de todas as fórmulas de Σ) é modelo de ψ. Se Σ é finito, digamos $\Sigma = \{\phi_1, ..., \phi_n\}$, e $\Sigma \vDash \psi$, escrevemos simplesmente

$$\phi_1, ..., \phi_n \vDash \psi.$$

Tal como no caso proposicional, a validade universal não é mais do que um caso particular da noção de consequência:

$$\phi \text{ é válida sse } \emptyset \vDash \phi.$$

Como é bom de ver, as noções semânticas para uma linguagem elementar $\mathcal{L}$ são bem mais complicadas e abstractas do que as correspondentes para a lógica proposicional. A verificação de que certa fórmula é válida, ou que é consequência de certas outras, envolve a consideração de *todas* as estruturas-$\mathcal{L}$ e em cada estrutura dessas a consideração de *todas* as atribuições. Não é de esperar que tanta informação possa ser condensada numa tabela de verdade! Em regra, pois, a verificação de validade ou invalidade de uma dada fórmula (ou, mais geralmente, a verificação de satisfação, ou a verificação de consequência) é uma tarefa de natureza abstracta, envolvendo, em geral, raciocínios e técnicas matemáticas sofisticadas, excepto em casos particulares muito especiais.

Pode-se afirmar, no entanto, que uma das principais tarefas do matemático é a busca de consequências dos seus sistemas de axiomas, mas a (quase) única maneira de se certificar que certa proposição ou sentença é consequência de certos axiomas é por *via dedutiva* (num sistema como **DNQ**, ou outro), utilizando regras e princípios lógicos universalmente válidos (ver III.7 adiante).

Podemos verificar por tabelas, porém, uma noção *restrita* de validade, a n-**validade**, onde n é um inteiro positivo, isto é, a validade em estruturas com n elementos.

6.11 Exemplo

Exemplificamos a n-validade com a sentença deveras simples

$$Pc \to \exists x Px,$$

supondo que a nossa linguagem $\mathcal{L}$ tem somente o símbolo predicativo unário P e a constante c. Uma estrutura $\mathfrak{M}$ para tal linguagem $\mathcal{L}$ é da forma

$$\mathfrak{M} = (M, P^{\mathfrak{M}}, c^{\mathfrak{M}}) = (M, P, c),$$

onde $P = P^{\mathfrak{M}}$ é um subconjunto de M e $c = c^{\mathfrak{M}} \in M$. Para simplificar, vamos supor $n = 2$. Então M tem somente dois elementos, digamos $M = \{a, b\}$. Há exactamente 8 estruturas-$\mathcal{L}$ nestas condições, conforme as interpretações possíveis de P e de c, pois há exactamente quatro subconjuntos P de M, a saber,

$$P = \emptyset, \quad P = \{a\}, \quad P = \{b\}, \quad P = \{a, b\} = M,$$

e duas maneiras possíveis de interpretar c, a saber,

$$c = a, \text{ e } c = b.$$

Na tabela a seguir, na coluna da esquerda indicamos as 8 estruturas possíveis, e nas colunas seguintes os valores lógicos das fórmulas Pc, $\exists x\, Px$, $Pc \to \exists x\, Px$ em cada uma dessas oito estruturas, respectivamente. Após a tabela damos, em contrapartida, uma argumentação geral com vista a demonstrar a validade universal da mesma sentença, $Pc \to \exists x Px$.

ESTRUTURAS	**VALORES LÓGICOS**		
	Pc	$\exists x\, Px$	$Pc \to \exists x\, Px$
$(M, \emptyset, a)$	0	0	1
$(M, \emptyset, b)$	0	0	1
$(M, \{a\}, a)$	1	1	1
$(M, \{a\}, b)$	0	1	1
$(M, \{a\}, b)$	0	1	1
$(M, \{a\}, b)$	1	1	1
$(M, \{a, b\}, a)$	1	1	1
$(M, \{a, b\}, b)$	1	1	1

Demonstração informal da validade de $Pc \to \exists x Px$. Seja $\mathfrak{M} = (M, P, c)$ uma estrutura-$\mathcal{L}$ ao arbítrio, com vista a mostrar que $\mathfrak{M} \vDash Pc \to \exists x\, Px$. Se $\mathfrak{M} \nvDash Pc$, vem logo que $\mathfrak{M} \vDash Pc \to \exists x\, Px$, pela definição de satisfação; se, pelo contrário, $\mathfrak{M} \vDash Pc$, quer dizer que $c \in P$; logo, existe um elemento de M no conjunto P e, portanto, pela definição de satisfação, $\mathfrak{M} \vDash \exists x\, Px$, e novamente pela definição de satisfação vem que $\mathfrak{M} \vDash Pc \to \exists x\, Px$. Como $\mathfrak{M}$ era arbitrária, podemos concluir que $\vDash Pc \to \exists x\, Px$.■

6.12 Sobre a interpretação do símbolo de igualdade

A definição tarskiana de satisfação impõe, logo na primeira claúsula, que o símbolo de igualdade " $\doteq$ " seja interpretado como a identidade no domínio da estrutura. Não tem de ser necessariamente assim. Na verdade, nada impede, nas regras da igualdade ou suas consequências, que a interpretação do símbolo de igualdade seja uma *relação de congruência* no domínio interpretativo, diferente da identidade. Menos do que isso não pode ser, por causa de leis como (130) e (131). As estruturas e interpretações em que " $\doteq$ " é interpretado como a identidade são chamadas **normais**, as outras são **não normais**. É claro que na definição tarskiana nos restringimos desde logo às normais e não faria sentido, na altura, falar de outras já que, em todas as situações práticas, só interessam realmente as interpretações normais. A possibilidade de interpretações não normais tem, pois, interesse meramente teórico ou filosófico.

Damos a seguir um exemplo de uma interpretação não normal.

6.13 Exemplo

Consideremos a estrutura (para a linguagem dos grupos aditivos, ver exercício 3.17) $\mathfrak{M} = (\mathbb{Z}, \equiv_p, +, 0)$, onde p é um inteiro positivo fixo e $\equiv_p$ é a relação de congruência modulo p, definida por

$$m \equiv_p n \text{ sse } m - n \text{ é múltiplo de } p$$

Além disso, modificamos a definição de satisfação de modo que " $=$ " seja interpretado como a relação $\equiv_p$:

$$\mathfrak{I}(t_1 = t_2) = 1 \text{ sse } \mathfrak{I}(t_1) \equiv_p \mathfrak{I}(t_2)$$

Ora bem, com esta nova noção de interpretação (não normal), os axiomas de grupo G_1, G_2 e G_3 são verdadeiros em $\mathfrak{M}$, todavia $\mathfrak{M}$ não é um grupo (porquê?). Deve dizer-se, por outro lado, que existe um procedimento geral bem conhecido dos algebristas para, a partir de uma estrutura não normal, obter uma normal: é a chamada *passagem ao quociente*. No caso presente, o resultado de tal procedimento, aplicado a $\mathfrak{M}$, é o *grupo dos inteiros modulo p*, $\mathbb{Z}_p$ [ver exercício 3.17(c)].

III.7 Metateoria. Validade e completude semântica

Tendo esclarecido as principais noções semânticas relativas às linguagens elementares, podemos agora dizer algo sobre as relações entre os pontos de vista dedutivo e semântico. Temos em vista, é claro, certos resultados de natureza metamatemática (metateoremas), à semelhança do que se disse para a lógica proposicional.

Os resultados em causa são em tudo análogos aos correspondentes na lógica proposicional (ver II.11), excepto para o problema de decisão. As demonstrações,

porém, são bastante mais complicadas do que no caso proposicional e serão igualmente omitidas.[121]

Combinando os dois resultados num só, tem-se (para o sistema **DNQ**):

7.1 Metateorema da validade e completude semântica

Seja Σ um conjunto qualquer de sentenças de uma linguagem elementar $\mathcal{L}$, ψ uma sentença de $\mathcal{L}$. Então $\Sigma \vDash \psi$ sse $\Sigma \vdash \psi$. Em particular, ψ é válida sse ψ é um teorema lógico.

7.2 Corolário

O sistema **DNQ** *é* ***consistente****, isto é, não existe nenhuma sentença ϕ tal que $\vdash \phi \wedge \neg\phi$.*

Este corolário demonstra-se tal e qual como no caso proposicional. Outro corolário, que também pode ser demonstrado independentemente e tem muitas aplicações em lógica matemática, é o

7.3 Metateorema da compacidade

Um conjunto Σ de sentenças de $\mathcal{L}$ é compatível sse todo o subconjunto finito de Σ é compatível.

7.4 Corolário 1

Se um conjunto Σ de sentenças de $\mathcal{L}$ tem modelos finitos arbitrariamente grandes, então Σ tem, pelo menos, um modelo infinito.

Dem. Consideremos o conjunto (ver exercício 3.5)

$$\Sigma' = \Sigma \cup \{\exists^{\geq n} x\,(x = x) \,:\, n = 1, 2, 3, ...\}.$$

É óbvio que um modelo $\mathfrak{M}$ de Σ' é necessariamente infinito. Provamos que Σ' é compatível por compacidade. Seja Σ_0 uma parte finita qualquer de Σ'. Há, em Σ_0, quando muito um número finito de sentenças da forma $\exists^{\geq n} x\,(x = x)$, digamos

$$\exists^{\geq n_1} x\,(x = x),\ \exists^{\geq n_2} x\,(x = x),\ ...,\ \exists^{\geq n_k} x\,(x = x)$$

Para algum m suficientemente grande (maior do que n_1, ..., n_k), Σ tem um modelo com m elementos, que será também modelo de Σ_0, logo Σ_0 é compatível.■

---

[121] Os resultados em questão, para o sistema dedutivo dos *Principia Mathematica* de RUSSELL & WHITEHEAD, foram primeiramente demonstrados por K. Gödel (1930). Modernamente, porém, nas monografias de Lógica Matemática, é costume apresentar uma outra demonstração, devida a L. Henkin (1949). Esta demonstração pode ser consultada em várias das monografias indicadas na bibliografia, como Van DALEN, ENDERTON, HÖDEL, MENDELSON, etc.

Como aplicação deste corolário podemos provar que não é possível obter um sistema de axiomas numa linguagem de primeira ordem para a classe dos grupos finitos (ver exercício 3.17), quer dizer, mais exactamente:

7.5 Corolário 2

Não existe nenhum conjunto Σ *de sentenças de primeira ordem cujos modelos sejam exactamente os grupos finitos*.

Dem. Como se sabe, existem grupos finitos arbitrariamente grandes, nomeadamente, os grupos $(\mathbb{Z}_p, +_p, \overline{0})$ onde, para cada inteiro positivo p,

$$\mathbb{Z}_p = \{\overline{0}, \overline{1}, ..., \overline{n-1}\}$$

é o *conjunto dos inteiros modulo p:* cada elemento $\overline{m}$ é uma classe de congruência modulo p, isto é, $\overline{m} = \{m + kp : k \in \mathbb{Z}\}$, sendo $+_p$ definida por

$$\overline{m} +_p \overline{n} = \overline{m+n} \text{ [ver exercício 3.17(c)]}.$$

Se todos os grupos finitos são modelos de Σ, então Σ tem, pelo menos, um modelo infinito, pelo 7.4 Corolário.■

Em contrapartida, a classe dos grupos infinitos já pode ser axiomatizada por sentenças de primeira ordem, nomeadamente, os axiomas de grupo e todas as sentenças da forma $\exists^{\geq n} x\,(x = x)$, $n = 1, 2, ...$. Esta lista de sentenças é infinita mas decidível, e pode-se provar (por compacidade) que ela não é equivalente a nenhuma lista finita de axiomas ou, como se costuma dizer, que aquela classe não é finitamente axiomatizável (exercício 3.18).

Vem a propósito mencionar uma maneira alternativa à da definição 2 da pág. 172 para definir teorias.

7.6 Definição

Seja $\mathcal{L}$ uma linguagem elementar. Se $\mathfrak{M}$ é uma estrutura-$\mathcal{L}$, a **teoria de** $\mathfrak{M}$ é o conjunto de todas as sentenças (sem parâmetros) de $\mathcal{L}$ verdadeiras em $\mathfrak{M}$, e denota-se $\mathrm{Tr}(\mathfrak{M})$. Se $\mathcal{K}$ é uma classe de estruturas-$\mathcal{L}$, a **teoria de** $\mathcal{K}$ é o conjunto de todas as sentenças (sem parâmetros) de $\mathcal{L}$ verdadeiras em todas as estruturas de $\mathcal{K}$, e denota-se $\mathrm{Tr}(\mathcal{K})$.

As definições fazem sentido: $\mathrm{Tr}(\mathfrak{M})$ e $\mathrm{Tr}(\mathcal{K})$ são, de facto, dedutivamente fechados. Vejamos o caso de $\mathrm{Tr}(\mathfrak{M})$. Se ϕ é dedutível deste conjunto, então ϕ é consequência dele, isto é, ϕ é verdadeira em todos os modelos de $\mathrm{Tr}(\mathfrak{M})$, modelos esses onde são verdadeiras todas as sentenças verdadeiras em $\mathfrak{M}$, logo ϕ é verdadeira em $\mathfrak{M}$, isto é, $\phi \in \mathrm{Tr}(\mathfrak{M})$. Analogamente para $\mathrm{Tr}(\mathcal{K})$. Diz-se de teorias da forma $\mathrm{Tr}(\mathfrak{M})$ ou $\mathrm{Tr}(\mathcal{K})$ que são *definidas semanticamente*.

Assim, qualquer estrutura ou classe de estruturas semelhantes dá origem a uma teoria definida semanticamente, a teoria dessa estrutura ou dessa classe, respecti-

vamente. Questão importante que logo se coloca é a de saber se é possível obter um sistema de axiomas razoavelmente «simples» (finito ou, pelo menos, decidível, ver II.12) para uma teoria assim definida. Pela observação acima, a teoria dos grupos infinitos é axiomatizável, mas não finitamente.

Quanto ao *problema de decisão* no cálculo de predicados, prova-se que não existe nenhum algoritmo para decidir a questão (Q_1) enunciada na pág. 70, agora formulada para sentenças de $\mathcal{L}$. Este é um resultado profundo [devido a A. Church (1936)] da *teoria da computabilidade,* onde também se estudam problemas de decidibilidade em lógica e em matemática, com toda a generalidade (ver Cap. V.3).

III.8 Isomorfismos

É facto conhecido, em diferentes áreas matemáticas, que «estruturas isomorfas têm as mesmas propriedades». Embora as noções de estrutura e de isomorfismo sejam de natureza puramente algébrica, o tal facto já envolve a lógica através da noção de «propriedade» e, talvez por isso, não é objecto de demonstração geral nas disciplinas matemáticas das diferentes áreas. Quando muito, faz-se a demonstração directa de um ou dois casos particulares, por exemplo, de que se dois grupos são isomorfos e um deles é comutativo, então o outro também é comutativo. Nesta secção damos a definição geral de isomorfismo de estruturas semelhantes ou do mesmo tipo (isto é, estruturas para a mesma linguagem) e demonstramos que estruturas isomorfas satisfazem exactamente as mesmas sentenças da linguagem (elementar) respectiva.

Para simplificar as notações suporemos que a linguagem $\mathcal{L}$ tem somente um símbolo predicativo binário P, um símbolo funcional binário f e uma constante c. A adaptação a outras linguagens é exercício de rotina. As estruturas-$\mathcal{L}$ são, portanto, da forma $\mathfrak{M} = (M, P, f, c)$, $\mathfrak{M}' = (M', P', f', c')$, etc.

8.1 Definição. Sejam $\mathfrak{M} = (M, ...)$ e $\mathfrak{M}' = (M', ...)$ estruturas-$\mathcal{L}$. Uma aplicação $h : M \to M'$ diz-se um **isomorfismo de $\mathfrak{M}$ em $\mathfrak{M}'$** (ou **entre $\mathfrak{M}$ e $\mathfrak{M}'$**), e escreve-se $h : \mathfrak{M} \xrightarrow{\simeq} \mathfrak{M}'$ sse

(1) h é bijectiva;

(2) para quaisquer $m, n \in M$, $(m, n) \in P$ sse $(hm, hn) \in P'$;

(3) para quaisquer $m, n \in M$, $hf(m, n) = f(hm, hn)$, e

(4) $hc = c'$.

$\mathfrak{M}$ e $\mathfrak{M}'$ dizem-se **isomorfas**, e escreve-se $\mathfrak{M} \simeq \mathfrak{M}'$, sse existe um isomorfismo entre $\mathfrak{M}$ e $\mathfrak{M}'$. Um isomorfismo entre $\mathfrak{M}$ e $\mathfrak{M}$ diz-se um **automorfismo de $\mathfrak{M}$**.

8.2 Exemplo

Sejam $\mathfrak{M} = (\mathbb{N}, +, \cdot, <, 0)$, P o conjunto dos números naturais pares. É sabido que 0 é par e que P é fechado para a adição e a multiplicação (quer dizer, a

soma e o produto de números naturais pares são pares). Continuando a denotar por $+$, etc. as operações em P, temos, assim, outra estrutura $\mathfrak{M}' = (P, +, \cdot, <, 0)$ semelhante a $\mathfrak{M}$. A função $h : \mathbb{N} \to P$ definida por $h(n) = 2n$ é um isomorfismo entre $\mathfrak{M}$ e $\mathfrak{M}'$.

As condições (1) e (2) da definição podem ser enfraquecidas de diversas maneiras, obtendo-se noções mais gerais do que a de isomorfismo. Assim, omitindo (1) obtemos a noção de **homomorfismo (forte) de $\mathfrak{M}$ em $\mathfrak{M}'$** e se, além disso, enfraquecermos (2) em

(2′) para quaisquer $m, n \in M$, $(m, n) \in P \Rightarrow (hm, hn) \in P'$,

obtemos a noção de **homomorfismo fraco de $\mathfrak{M}$ em $\mathfrak{M}'$** e escreve-se $h : \mathfrak{M} \to \mathfrak{M}'$. Enfraquecendo (1) em

(1′) h é injectiva,

obtemos a noção de **monomorfismo** ou **mergulho de $\mathfrak{M}$ em $\mathfrak{M}'$**, e escreve-se $h : \mathfrak{M} \hookrightarrow \mathfrak{M}'$. Substituindo (1) por

(1″) h é sobrejectiva,

dizemos que h é um **epimorfismo de $\mathfrak{M}$ em $\mathfrak{M}'$** ou um **homomorfismo de $\mathfrak{M}$ sobre $\mathfrak{M}'$** e escrevemos $h : \mathfrak{M} \twoheadrightarrow \mathfrak{M}'$. Obviamente, h é um isomorfismo sse h é monomorfismo e epimorfismo. Facilmente se prova que

(i) $\mathfrak{M} \simeq \mathfrak{M}$,

(ii) $\mathfrak{M} \simeq \mathfrak{M}' \Rightarrow \mathfrak{M}' \simeq \mathfrak{M}$, e

(iii) $\mathfrak{M} \simeq \mathfrak{M}'$ e $\mathfrak{M}' \simeq \mathfrak{M}'' \Rightarrow \mathfrak{M} \simeq \mathfrak{M}''$.

O conjunto dos automorfismos de $\mathfrak{M}$, $\mathrm{Aut}(\mathfrak{M})$, é o suporte de um grupo para a composição (exercício): a aplicação composta $h_2 \circ h_1$ de dois automorfismos é um automorfismo, a aplicação inversa h^{-1} de um automorfismo h é um automorfismo, e o elemento neutro do grupo é a identidade: a aplicação $I : M \to M$ tal que $I(m) = m$ para todo $m \in M$.

8.3 Metateorema do isomorfismo

Sejam $\mathfrak{M}$ e $\mathfrak{M}'$ estruturas-$\mathcal{L}$, $h : \mathfrak{M} \xrightarrow{\simeq} \mathfrak{M}'$ um isomorfismo. Então, para qualquer sentença ϕ de $\mathcal{L}$, tem-se

$$\mathfrak{M} \vDash \phi \text{ sse } \mathfrak{M}' \vDash \phi.$$

Dem. Visto que não é permitido fazer indução na complexidade das sentenças (pois estas, ao contrário das fórmulas, não são definidas indutivamente), demonstramos um pouco mais do que se pretende no enunciado. Mostramos que para qualquer fórmula (sem parâmetros) ϕ e qualquer atribuição $\alpha = \langle \alpha_i \rangle_{i \geq 0}$ em $\mathfrak{M}$,

$$\mathfrak{M} \vDash \phi\ [\alpha] \text{ sse } \mathfrak{M} \vDash \phi\ [h \circ \alpha],$$

onde $h \circ \alpha = \langle h\alpha_i \rangle_{i \geq 0}$ é a atribuição correspondente em $\mathfrak{M}'$. Note-se que simplificámos a noção de atribuição, já que não intervêm parâmetros. Para seguir a demonstração é talvez mais conveniente utilizarmos a notação simplificada para a satisfação,

$$\mathfrak{M} \vDash \phi(a_1, ..., a_n)\ [\alpha_1, ..., \alpha_n] \text{ sse } \mathfrak{M} \vDash \phi(a_1, ..., a_n)\ [h\alpha_1, ..., h\alpha_n],$$

onde $x_i \mapsto \alpha_i$ para $i = 1, ..., n$, supondo que $\phi(a_1, ..., a_n)$ é uma condição nos parâmetros $a_1, ..., a_n$. Abreviadamente,

$$(*) \qquad \mathfrak{M} \vDash \phi(\overline{a})\ [\overline{\alpha}] \text{ sse } \mathfrak{M} \vDash \phi(\overline{a})\ [h\overline{\alpha}].$$

Antes da demonstração disto, por indução na complexidade das fórmulas, há que fazer uma outra, por indução na complexidade dos termos.

8.4 Lema

Para qualquer termo t (sem parâmetros), a imagem por h do valor de t em $\mathfrak{M}$ com respeito a α é o valor de t em $\mathfrak{M}'$ com respeito a $h\alpha$, isto é

$$h(\mathfrak{I}(t)) = \mathfrak{I}'(t),$$

onde $\mathfrak{I}' = (\mathfrak{M}', h\alpha)$.

Deixamos a demonstração deste lema como exercício, e prosseguimos com a demonstração por indução de (*):

— se ϕ é atómica, digamos da forma $(t_1 \doteq t_2)$, tem-se

$$\begin{aligned} \mathfrak{M} \vDash (t_1 \doteq t_2)\ [\overline{\alpha}] &\Leftrightarrow \mathfrak{I}(t_1) = \mathfrak{I}(t_2) \\ &\Leftrightarrow h\mathfrak{I}(t_1) = h\mathfrak{I}(t_2), \text{ por } h \text{ ser injectiva} \\ &\Leftrightarrow \mathfrak{I}'(t_1) = \mathfrak{I}'(t_2), \text{ pelo lema} \\ &\Leftrightarrow \mathfrak{M}' \vDash (t_1 \doteq t_2)\ [h\overline{\alpha}], \end{aligned}$$

e se ϕ é da forma Pt_1t_2 tem-se

$$\begin{aligned} \mathfrak{M} \vDash Pt_1t_2\ [\overline{\alpha}] &\Leftrightarrow (\mathfrak{I}(t_1), \mathfrak{I}(t_2)) \in P \\ &\Leftrightarrow (h\mathfrak{I}(t_1), h\mathfrak{I}(t_2)) \in P' \\ &\Leftrightarrow (\mathfrak{I}'(t_1), \mathfrak{I}'(t_2)), \text{ pelo lema} \\ &\Leftrightarrow \mathfrak{M}' \vDash Pt_1t_2\ [h\overline{\alpha}]; \end{aligned}$$

— se ϕ é da forma $\neg\psi$ tem-se

$$\begin{aligned}\mathfrak{M} \vDash \neg\psi\ [\overline{\alpha}] &\Leftrightarrow \mathfrak{M} \nvDash \psi\ [\overline{\alpha}] \\ &\Leftrightarrow \mathfrak{M}' \nvDash \psi\ [h\overline{\alpha}], \text{ por hipótese de indução} \\ &\Leftrightarrow \mathfrak{M}' \vDash \neg\psi\ [h\overline{\alpha}];\end{aligned}$$

— se ϕ é da forma $\psi \wedge \theta$ tem-se

$$\begin{aligned}\mathfrak{M} \vDash \psi \wedge \theta\ [\overline{\alpha}] &\Leftrightarrow \mathfrak{M} \vDash \psi\ [\overline{\alpha}] \text{ e } \mathfrak{M} \vDash \theta\ [\overline{\alpha}] \\ &\Leftrightarrow \mathfrak{M}' \vDash \psi\ [h\overline{\alpha}] \text{ e } \mathfrak{M}' \vDash \theta\ [h\overline{\alpha}] \\ &\Leftrightarrow \mathfrak{M}' \vDash \psi \wedge \theta\ [h\overline{\alpha}],\end{aligned}$$

e analogamente para ϕ da forma $\psi \vee \theta$ ou $\psi \rightarrow \theta$;

— se $\phi = \phi(\overline{x})$ é da forma $\forall x_0 \psi(x_0, \overline{x})$ tem-se

$$\begin{aligned}\mathfrak{M} \vDash \forall x_0\psi(x_0, \overline{x})\ [\overline{\alpha}] &\Leftrightarrow \text{para todo } m \in M, \mathfrak{M} \vDash \psi(x_0, \overline{x})\ [m, \overline{\alpha}] \\ &\Leftrightarrow \text{para todo } m \in M, \mathfrak{M}' \vDash \psi(x_0, \overline{x})\ [hm, h\overline{\alpha}] \\ &\Rightarrow \text{para todo } m' \in M', \mathfrak{M}' \vDash \psi(x_0, \overline{x})\ [m', h\overline{\alpha}],\end{aligned}$$

por h ser sobrejectiva, donde, por definição de satisfação,

$$\mathfrak{M}' \vDash \forall x_0\psi(x_0, \overline{x})\ [h\overline{\alpha}];$$

reciprocamente, se isto se dá tem-se

$$\text{para todo } m' \in M', \mathfrak{M}' \vDash \psi(x_0, \overline{x})\ [m', h\overline{\alpha}]$$

donde resulta, por h ser função, que

$$\text{para todo } m \in M', \mathfrak{M}' \vDash \psi(x_0, \overline{x})\ [hm, h\overline{\alpha}];$$

— o caso de ϕ ser da forma $\exists x_0\psi(x_0, \overline{x})$ é análogo fica como exercício.■

8.5 Isomorfismo e equivalência elementar

O conceito de estrutura que definimos e temos utilizado não tem a generalidade que é comum encontrar no universo matemático, pois as nossas estruturas são somente as estruturas para linguagens de primeira ordem (ditas, por isso, *estruturas de primeira ordem* — ficam de fora, por exemplo, as estruturas topológicas), mas outras linguagens existem para além das de primeira ordem. Todavia, não é ainda inteiramente claro o que se deva entender por «estrutura» no sentido mais geral possível. Bourbaki propôs uma definição muito geral no primeiro volume (*Théorie des Ensembles*) do seu imenso tratado *Éléments de Mathématique*, mas alguns matemáticos e lógicos estão procurando melhorar sob diversos aspectos a definição bourbakista. Por outro lado, é ideia corrente entre muitos matemáticos que a noção de isomorfismo deveria significar ou ser sinónima de «ter as mesmas propriedades». Se é verdade que, relativamente a todas as linguagens e lógicas conhecidas,

se pode demonstrar o correspondente metateorema de isomorfismo, de que

($*$) *estruturas isomorfas têm as mesmas propriedades,*

enquanto propriedades expressas na linguagem, estamos ainda muito longe de poder garantir que se duas estruturas semelhantes tiverem as mesmas propriedades, no sentido mais geral possível de «propriedade», então elas são isomorfas (para a noção apropriada de isomorfismo). A dificuldade do problema é de natureza lógica: saber *o que é uma propriedade nesse sentido mais geral possível*. Em todo o caso, podemos garantir que para linguagens e estruturas de primeira ordem não é assim, quer dizer, a comunhão de propriedades de primeira ordem não garante o isomorfismo. O exemplo canónico citado nos manuais é o das estruturas ordenadas usuais $(\mathbb{Q},\ <)$ e $(\mathbb{R},\ <)$, que têm as mesmas propriedades de primeira ordem (na linguagem $\mathcal{L} = \{\ <\ \}$), mas não são isomorfas (por uma questão de cardinalidade: não existe bijecção entre $\mathbb{Q}$ e $\mathbb{R}$).

A noção

$$\textit{para qualquer sentença } \phi \textit{ de } \mathcal{L},\ \mathfrak{M} \vDash \phi \ \textit{ sse } \ \mathfrak{M}' \vDash \phi,$$

exprime-se abreviadamente por

$$\mathfrak{M} \equiv_{\mathcal{L}} \mathfrak{M}',$$

e diz-se que $\mathfrak{M}$ e $\mathfrak{M}'$ são **equivalentes-$\mathcal{L}$** (ou **elementarmente equivalentes** com respeito a $\mathcal{L}$). O metateorema do isomorfismo diz-nos, pois, que para qualquer linguagem elementar $\mathcal{L}$ e quaisquer estruturas-$\mathcal{L}$ $\mathfrak{M}$ e $\mathfrak{M}'$,

$$\mathfrak{M} \equiv_{\mathcal{L}} \mathfrak{M}' \Rightarrow \mathfrak{M} \simeq \mathfrak{M}',$$

mas, como acima se disse, a implicação recíproca é falsa, em geral.

*III.9 Completude Definicional

Na secção III.5 definimos a noção de teoria elementar e indicámos o procedimento para enriquecer a linguagem da teoria com símbolos definidos (relacionais, operacionais ou constantes). Estudamos agora, com maior profundidade, a noção de definibilidade de um conceito numa teoria.

Supomos fixada uma linguagem elementar $\mathcal{L}$ (com alfabeto numerável). Denotaremos por $\mathcal{L}'$ ou $\mathcal{L}(\Theta)$ uma linguagem cujo alfabeto não lógico se obtém do alfabeto de $\mathcal{L}$ juntando um novo símbolo Θ, que pode ser relacional, operacional ou constante, e por $\mathbf{T}'$ uma teoria na linguagem $\mathcal{L}'$. Por exemplo, $\mathbf{T}'$ poderá ser a teoria que se obtém de uma teoria $\mathbf{T}$ em $\mathcal{L}$ juntando o axioma de definição de Θ, se Θ foi introduzido como se explicou em III.5. Começamos por definir a noção «Θ é definível em $\mathbf{T}'$» considerando separadamente três casos, conforme a categoria de Θ. No que segue, salvo menção em contrário, consideramos apenas sentenças.

9.1 Definição

Seja $\mathcal{L}' = \mathcal{L}(P)$, onde P é um símbolo relacional n-ário ($n \geq 1$). Dizemos que P é **definível em** $\mathbf{T}'$ sse existe uma fórmula $\phi(a_1, ..., a_n)$ de $\mathcal{L}$ com exactamente os parâmetros a_1, ..., a_n tal que

(1) $$\mathbf{T}' \vdash \forall x_1 ... \forall x_n \, (Px_1...x_n \leftrightarrow \phi(x_1, ..., x_n)).$$

Sendo $\mathcal{L}' = \mathcal{L}(f)$, onde f é um símbolo operacional m-ário ($m \geq 1$), dizemos que f é **definível em** $\mathbf{T}'$ sse existe uma fórmula $\psi(a_1, ..., a_m, b)$ de $\mathcal{L}$ com exactamente os parâmetros a_1, ..., a_m, b tal que

(2) $$\mathbf{T}' \vdash \forall x_1 ... x_m \, y \, (fx_1...x_m \doteq y \leftrightarrow \psi(x_1, ...x_m, y)).$$

Finalmente, se $\mathcal{L}' = \mathcal{L}(c)$, a constante c é **definível em** $\mathbf{T}'$ sse existe uma fórmula $\psi(b)$ com um único parâmetro b tal que

(3) $$\mathbf{T}' \vdash \forall y \, (c \doteq y \leftrightarrow \psi(y)).$$

A fórmula $\phi(a_1, ..., a_n)$ tal que (1) diz-se uma **definidora de** P **em** $\mathbf{T}'$; $\psi(b_1, ..., b_m, b)$ tal que (2) diz-se uma **definidora de** f **em** $\mathbf{T}'$, e $\psi(b)$ tal que (3) é uma **definidora de** c **em** $\mathbf{T}'$. Em todos estes casos a fórmula definidora de Θ ($= P$, f ou c) em $\mathbf{T}'$ *não contém o símbolo* Θ — é uma fórmula da linguagem primitiva $\mathcal{L}$. Para chamar a atenção para este facto poderiámos dizer que Θ é **definível-**$\mathcal{L}$ **em** $\mathbf{T}'$. Além disso, facilmente se conclui, no caso de um símbolo funcional f, que

$$\mathbf{T}' \vdash \forall x_1 ... x_m \, \exists^1 y \psi(x_1, ..., x_m, y),$$

se $\psi(a_1, ..., a_m, b)$ é uma definidora de f em $\mathbf{T}'$, e que

$$\mathbf{T}' \vdash \exists^1 y \psi(y),$$

se $\psi(b)$ é uma definidora de c em $\mathbf{T}'$. Poderíamos ter poupado algumas linhas nas definições acima, considerando as constantes como símbolos funcionais 0-ários ($m = 0$).

9.2 Exemplos

1) Sendo $\mathcal{L}_{\text{gr}}$ a linguagem aditiva dos grupos (ver exercício 3.14), $\mathbf{T}' = \mathbf{T}_{\text{gr}}$, a constante 0 é definível em $\mathbf{T}'$, pois

$$\mathbf{T}_{\text{gr}} \vdash \forall x\,(0 \doteq x \leftrightarrow \forall z\,(x + z \doteq z \wedge z + x \doteq z)).$$

2) Seja $\mathcal{L}' = \mathcal{L}_{\text{ar}}(<)$ a linguagem da aritmética (ver exercício 3.16) com um símbolo predicativo binário adicional $<$ denotando a ordem usual (estrita) em $\mathbb{N}$, $\mathbf{T}' = \mathbf{AP}$ (aritmética de Peano, ver Cap. IV). Então $<$ é definível em $\mathbf{T}'$, pois

$$\mathbf{AP} \vdash \forall xy\,(x < y \leftrightarrow \exists z\,(y \doteq x + z)).$$

3) Seja $\mathcal{L}' = \mathcal{L}(\Theta)$, sendo Θ um símbolo definido como se explicou na secção III.5, $\mathbf{T}$ uma teoria qualquer na linguagem $\mathcal{L}$, $\mathbf{T}' = \mathbf{T}$ + axioma de dedinição de Θ. Então Θ é definível em $\mathbf{T}'$.

No final de III.5 falou-se da possibilidade de eliminar símbolos definidos. Tratamos seguidamente da eliminibilidade de símbolos definíveis. Será conveniente introduzir as convenções de abreviatura de escrita seguintes: $\phi(x_1, ..., x_n)$ abrevia-se $\phi(\overline{x})$ e $\forall x_1 ... x_n$ abrevia-se $\forall \overline{x}$.

9.3 Definição

Sejam $\mathcal{L}' = \mathcal{L}(\Theta)$, Θ não em $\mathcal{L}$, $\mathbf{T}'$ uma teoria em $\mathcal{L}'$. Diz-se que $\mathbf{T}'$ **elimina** Θ sse para toda a fórmula $\phi(\overline{a})$ de $\mathcal{L}'$ existe, pelo menos, uma fórmula $\psi(\overline{b})$ de $\mathcal{L}$ tal que

$$\mathbf{T}' \vdash \forall \overline{x}\,\overline{y}\,(\phi(\overline{x}) \leftrightarrow \psi(\overline{y})).$$

9.4 Lema

Se $\mathbf{T}'$ *elimina* Θ*, então* Θ *é definível em* $\mathbf{T}'$.

Dem. Fazemos a demonstração para $\Theta = P$, símbolo predicativo n-ário. Por hipótese, existe uma fórmula de $\mathcal{L}$ (quer dizer, sem P) $\phi(\overline{a}, \overline{b})$ tal que

$$\mathbf{T}' \vdash \forall \overline{x}\,\overline{y}\,(P\overline{x} \leftrightarrow \phi(\overline{x}, \overline{y})),$$

onde $\overline{y} = y_1, ..., y_m$. Então $\mathbf{T}' \vdash \forall \overline{x}\,\overline{y}\,(P\overline{x} \rightarrow \phi(\overline{x}, \overline{y}))$ e $\mathbf{T}' \vdash \forall \overline{x}\,\overline{y}\,(\phi(\overline{x}, \overline{y}) \rightarrow P\overline{x})$, donde

$$\mathbf{T}' \vdash \forall \overline{x}\,(\exists \overline{y}\,\phi(\overline{x},\overline{y}) \rightarrow P\overline{x}) \text{ e } \mathbf{T}' \vdash \forall \overline{x}\,(P\overline{x} \rightarrow \forall \overline{y}\,\phi(\overline{x},\overline{y})),$$

mas $\mathbf{T}' \vdash \forall \overline{x}\,(\forall \overline{y}\,\phi(\overline{x},\overline{y}) \rightarrow \exists \overline{y}\,\phi(\overline{x},\overline{y}))$, logo

$$\mathbf{T}' \vdash \forall \overline{x}\,(P\overline{x} \rightarrow \exists \overline{y}\,\phi(\overline{x},\overline{y})).$$

Portanto,

$$\mathbf{T}' \vdash \forall \overline{x}\,(P\overline{x} \leftrightarrow \exists \overline{y}\,\phi(\overline{x},\overline{y})),$$

o que mostra que $\exists \overline{y}\,\phi(\overline{a},\overline{y})$ é uma definidora de P em $\mathbf{T}'$.

Os outros casos tratam-se de maneira análoga.■

Mais importante e interessante é o resultado recíproco de anterior, contido no enunciado seguinte:

9.5 Metateorema de Beth

As proposições seguintes são equivalentes:

(a) *Toda a estrutura-$\mathcal{L}$ possui, quando muito, uma expansão a um modelo de $\mathbf{T}'$;*

(b) $\mathbf{T}'$ *elimina* Θ;

(c) Θ *é definível em* $\mathbf{T}'$.

A parte «difícil» da demonstração é a da implicação (a) $\Rightarrow$ (b), que não fazemos por transcender o âmbito deste livro. A implicação (b) $\Rightarrow$ (c) é o lema 9.4. Quanto a (c) $\Rightarrow$ (a), é necessária uma explicação prévia.

Se $\mathfrak{M} = (M, ...)$ é uma estrutura-$\mathcal{L}$, uma **expansão de $\mathfrak{M}$ a** $\mathcal{L}'$ é uma estrutura-$\mathcal{L}'$ da forma $\mathfrak{M}' = (M, ..., \boldsymbol{\Theta})$ onde $\boldsymbol{\Theta}$ é a interpretação de Θ em $\mathfrak{M}'$. Se $\mathfrak{M}' = (M, ..., \boldsymbol{\Theta})$ é uma estrutura-$\mathcal{L}'$, então a estrutura-$\mathcal{L}$ $\mathfrak{M} = (M, ...)$ diz-se o **reduto** de $\mathfrak{M}'$ a $\mathcal{L}$ e denota-se $\mathfrak{M}'|\mathcal{L}$. Admitindo (c), e dada $\mathfrak{M}$ para $\mathcal{L}$, pode haver ou não expansões de $\mathfrak{M}$ a $\mathcal{L}'$ que sejam modelos de $\mathbf{T}'$, mas não haverá mais de uma:

(a′) se $\mathfrak{M}' = (M, ..., \boldsymbol{\Theta}')$ e $\mathfrak{M}'' = (M, ..., \boldsymbol{\Theta}'')$ são modelos de $\mathbf{T}'$, então $\boldsymbol{\Theta}' = \boldsymbol{\Theta}''$,

e, portanto, $\mathfrak{M}' = \mathfrak{M}''$. Com efeito, as interpretações de Θ em $\mathfrak{M}'$ e em $\mathfrak{M}''$ são determinadas pela definição de Θ em $\mathbf{T}'$, que existe por hipótese (c), e é feita mediante uma fórmula $\psi(\overline{b})$ *da linguagem* $\mathcal{L}$ (definição 9.1), cujo significado é necessariamente o mesmo em $\mathfrak{M}'$ e $\mathfrak{M}''$ visto que estas estruturas são ambas expansões de $\mathfrak{M}$. Portanto, $\boldsymbol{\Theta}' = \boldsymbol{\Theta}''$.■

A propriedade (a), na formulação (a′) exprime que Θ é **implicitamente definível em T′**, enquanto a definibilade referida em (c) é chamada a definibilidade **explícita** de Θ em **T′**. Tem-se, pois, o

9.6 Corolário

Θ é (explicitamente) definível em **T′** *sse Θ é implicitamente definível em* **T′**.

9.7 *Mais exemplos

4) Seja $\mathcal{L}_{\text{cp}}$ a linguagem dos corpos nos primitivos $+$, $\cdot$, 0, 1, $\mathcal{L}' = \mathcal{L}_{\text{cp}}(i)$ onde i é uma nova constante, **T** a teoria (elementar) dos corpos e **T′** a teoria que se obtém juntando aos axiomas de **T** o axioma

$$i^2 + 1 = 0$$

A constante i não é definível em **T**, pois não é implicitamente definível em **T′**: i pode ser interpretado no corpo dos números complexos $(\mathbb{C}, ...)$ de duas maneiras diferentes, ora como uma ora como a outra raiz quadrada de -1. De facto, se $\sqrt{-1}$ é uma das raízes quadradas de -1, então $(\mathbb{C}, ..., \sqrt{-1})$ e $(\mathbb{C}, ..., -\sqrt{-1})$ são ambos modelos de **T**.

5) Seja $\mathbf{T}_{\text{co}}$ a teoria dos corpos ordenados na linguagem $\mathcal{L}_{\text{co}} = \mathcal{L}_{\text{cp}}(<)$ e seja $\mathfrak{Q}(\sqrt{2}) = (\mathbb{Q}(\sqrt{2}), ...)$ o corpo de decomposição de $x^2 - 2$ sobre $\mathbb{Q}$, que pode ser encarado como o conjunto (subcorpo) de todos os números reais da forma

$$a + b\sqrt{2}, \text{ com } a, b \in \mathbb{Q}.$$

$\mathfrak{Q}' = (\mathbb{Q}(\sqrt{2}), ..., <)$ é um corpo ordenado, com a ordem $<$ induzida pela ordem usual em $\mathbb{R}$. A aplicação $h : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$ definida por

$$h(a + b\sqrt{2}) = a - b\sqrt{2}$$

é um automorfismo do corpo $\mathfrak{Q}$, e podemos definir em $\mathbb{Q}(\sqrt{2})$ outra relação de ordem (compatível com as operações) $<'$ por

$$a <' b \text{ sse } h(a) < h(b)$$

Assim, os corpos ordenados $\mathfrak{Q}'$ e $\mathfrak{Q}'' = (\mathbb{Q}(\sqrt{2}), ..., <')$ são isomorfos (isomorfismo h), logo

$$h[<] = h[<_{\mathfrak{Q}'}] = <_{\mathfrak{Q}''} = <',$$

por definição de isomorfismo, onde

$$h[<] = \{(h(a), h(b)) : (a, b) \in <\}.$$

Se $<$ fosse definível em $\mathbf{T}_{\text{co}}$ teria de ser $< = <'$, pois os corpos $\mathfrak{Q}'$ e $\mathfrak{Q}''$ têm as mesmas propriedades expressas em $\mathcal{L}_{\text{co}}$, mas não é: por exemplo,

$$1+\sqrt{2}<1+2\sqrt{2},$$
$$h(1+\sqrt{2})=1-\sqrt{2},\ h(1+2\sqrt{2})=1-2\sqrt{2},$$

logo

$$h(1+2\sqrt{2})<h(1-\sqrt{2}),$$

isto é, por definição de $<'$,

$$1+2\sqrt{2}<'1-\sqrt{2},$$

o que mostra que $<\ \neq\ <'$.

6) Seja $\mathbf{T}'$ a extensão de $\mathbf{T}_{\text{co}}$ que se obtém juntando o axioma

$$\forall x\,(0<x\rightarrow\exists y\,(x\doteq y^2)),$$

e seja $\mathfrak{M}$ um modelo qualquer de $\mathbf{T}'$. Se $a<b$ em $\mathfrak{M}$, isto é, $0<b-a$, então existe $c\neq 0$ tal que $b-a=c^2$; reciprocamente, se $b-a=c^2$ para algum $c\neq 0$, então $0<b-a$, logo $a<b$ em $\mathfrak{M}$. Isto mostra que

$$\mathfrak{M}\vDash\forall xy(x<y\leftrightarrow\exists z\,(z\neq 0\wedge y\doteq x+z^2)).$$

Como $\mathfrak{M}$ é um modelo arbitrário de $\mathbf{T}'$, podemos concluir que

$$\mathbf{T}'\ \vDash\ \forall xy(x<y\leftrightarrow\exists z\,(z\neq 0\wedge y\doteq x+z^2)),$$

donde

$$\mathbf{T}'\vdash\forall xy(x<y\leftrightarrow\exists z\,(z\neq 0\wedge y\doteq x+z^2)),$$

pelo metateorema da completude semântica. Isto mostra que $<$ é definível em $\mathbf{T}'$.

Os exemplos 4 e 5 acima mostram como tirar partido (por contraposição) da implicação (c) ⇒ (a) no metateorema de Beth para mostrar que certo conceito *não é definível* em certa teoria. Estamos em presença de um *critério de não definibilidade* de conceitos:

9.8 Corolário 2 (Método de Padoa[122])

Se Θ não é implicitamente definível em $\mathbf{T}'$, *então Θ não é definível em* $\mathbf{T}'$.■

---

[122] Alessandro Padoa foi um discípulo de Giuseppe Peano que utilizou pela primeira vez, de forma explícita, o corolário anterior em questões de geometria, daí a designação de *método de Padoa*, embora a ideia possa ter previamente ocorrido a outros matemáticos. As aplicações que Padoa fez do método com o seu nome datam do princípio do século, mas o metateorema de Beth que o justifica é relativamente recente (1955).

A não definibilidade de um conceito numa teoria pode-se encarar como a *independência* desse conceito relativamente aos restantes conceitos da teoria. Pelo metateorema de Beth, se Θ é independente (isto é, não definível), então existem sempre dois modelos $\mathfrak{M}$ e $\mathfrak{M}'$ da teoria com

$$\Theta^{\mathfrak{M}} \neq \Theta_{\mathfrak{M}'}.$$

A situação é semelhante à da independência de sentenças: ϕ é **independente de T** (no sentido forte) sse $\mathbf{T} \nvdash \phi$ e $\mathbf{T} \nvdash \neg\phi$. Para mostrar que assim é, basta, pelo metateorema de completude semântica, mostrar que existem dois modelos $\mathfrak{M}$ e $\mathfrak{M}'$ de **T** tais que $\mathfrak{M} \vDash \neg\phi$ e $\mathfrak{M}' \vDash \phi$ (donde $\mathbf{T} \nvDash \phi$ e $\mathbf{T} \nvDash \neg\phi$). Por virtude desta analogia o metateorema de Beth pode ser encarado como um metateorema de *completude definicional*, daí o título desta secção.

III.10 Sobre os conceitos de «elementar» e de «validade universal»

O termo «elementar» é utilizado pelos matemáticos e pelos lógicos com significados diferentes. Os primeiros dizem «elementar» como quem diz «simples», «acessível», ou «básico». Na chamada *teoria dos números* o termo «elementar» tem um significado um pouco mais preciso quando aplicado a certas demonstrações. De facto, nessa teoria matemática, altamente sofisticada e desenvolvida, utilizam-se, além da aritmética dos números (inteiros), outros conhecimentos e métodos, ora algébricos, ora analíticos (daí também as ramificações conhecidas por *teoria algébrica dos números* e *teoria analítica dos números*), e é somente quando se restringem tais métodos, de modo a não ultrapassar a força dedutiva da aritmética dos inteiros, que se fala em demonstrações «elementares», em regra, bastante mais difíceis e trabalhosas do que as «habituais» que utilizem tais resultados e métodos não aritméticos. Quanto mais rudimentar o instrumento, mais difícil é a execução do trabalho. Para os lógicos, porém, o termo «elementar» é quase sempre sinónimo de «de primeira ordem» e tem mais a ver com o poder expressivo de uma linguagem. Numa linguagem elementar $\mathcal{L}$ só podemos quantificar variáveis individuais [para «elementos» do(s) domínio(s) interpretativo(s)] x, y, z, ...

A lógica *elementar* (ou: *de 1.ª ordem*) compreende ainda linguagens com várias espécies de variáveis individuais, de que não falámos neste livro. Para uma linguagem elementar com duas espécies de variáveis individuais, digamos x^0, y^0, z^0, ... e x^1, y^1, z^1, ..., uma estrutura terá dois domínios em vez de um só: um domínio M_0 para os «indivíduos da primeira espécie» e outro domínio M_1 para os «indivíduos da segunda espécie». Todavia, podemos sempre transformar uma tal linguagem numa linguagem com variáveis de uma única espécie mediante um artifício conhecido por «unificação dos domínios»: introduzimos dois símbolos predicativos unários, M_0 e M_1 e convencionamos escrever $\forall x(M_0x \rightarrow \phi(x, ...))$ em vez de $\forall x^0\phi(x^0, ...)$, $\forall x(M_1x \rightarrow \phi(x, ...))$ em vez de $\forall x^1\phi(x^1, ...)$, etc.

Outras linguagens há, de *segunda ordem*, por exemplo, de que também não falámos neste livro. As mais simples são as linguagens de segunda ordem *monádicas*, que possuem variáveis X, Y, Z, ... para «conjuntos de indivíduos», quantificáveis tal como as variáveis individuais (e possivelmente também variáveis para relações e para funções). Para uma tal linguagem $\mathcal{L}^2$ uma estrutura terá dois domínios em vez de um só: um domínio M_0 para os «indivíduos» e outro domínio M_1 para os «conjuntos de indivíduos», contido no conjunto dos subconjuntos de M_0.[123] Se, nas interpretações semânticas, nos restringirmos a estruturas $(M_0, M_1, ...)$ em que M_1 é o conjunto de todos os subconjuntos de M_0, isto é, $M_1 = \mathcal{P}(M_0)$ e, portanto, $\forall X$ significa «para todo o subconjunto X do conjunto de indivíduos», então $\mathcal{L}^2$ é uma linguagem de segunda ordem *forte* ou genuína com maior poder expressivo do que uma linguagem de primeira ordem mas, em contrapartida, perde-se a possibilidade de encontrar um sistema dedutivo semanticamente completo. Se, porém, admitirmos que M_1 possa ser uma parte arbitrária de $\mathcal{P}(M_0)$ e $\forall X$ signifique «para todo o conjunto X em M_1», então $\mathcal{L}^2$ é uma linguagem de segunda ordem *fraca*, o que quer dizer que é essencialmente uma linguagem de primeira ordem disfarçada (com duas espécies de variáveis individuais).

É claro que aquilo que decidimos considerar como «indivíduo», «elemento» ou «objecto» susceptível de ser constitutivo de um domínio interpretativo (um domínio para as variáveis x, y, z, ...) é, em boa medida, fruto do nosso livre arbítrio [na teoria axiomática de conjuntos, os «indivíduos» são chamados **conjuntos**; um domínio interpretativo é um **universo de conjuntos** (ver exercício 3.21)], mas, uma vez fixado um domínio ou domínios intencionais e escolhida a linguagem, não pode haver confusão sobre os objectos ou indivíduos referentes das variáveis.

As linguagens elementares ou de 1.ª ordem têm, portanto, um poder expressivo limitado. Nelas não se pode escrever uma expressão (de 2.ª ordem) da forma

$$\forall X \exists y \phi(X, y),$$

onde X é uma variável para conjuntos de indivíduos e y uma variável para indivíduos (sejam estes o que forem), ou exprimir algo como

«existe uma operação unária injectiva (do domínio em si mesmo».

Pode-se exprimir que f é injectiva (sendo f um símbolo funcional unário primitivo ou definido) por

$$\forall x \forall y (fx \doteq fy \rightarrow x \doteq y),$$

mas não se pode quantificar "f".

---

[123] Para as linguagens de segunda ordem gerais, em que também estão presentes variáveis para relações entre indivíduos e para funções (de argumentos e valores que são indivíduos), haverá, em cada estrutura interpretativa, também um domínio para as relações em M_0, etc.

Esta limitação do poder expressivo não é, todavia, tão limitativa quanto poderia parecer. Por um lado, há as opções da escolha do domínio de indivíduos, há a possibilidade de várias espécies de variáveis e a correspondente «unificação dos domínios», e há também a possibilidade de, para certos conceitos matemáticos, utilizar não uma mas uma infinidade de fórmulas ou sentenças de 1.ª ordem. Por exemplo, se Σ é o conjunto das sentenças (sem parâmetros) da forma

$(\exists^{\geq n})$ $\qquad \exists x_1, x_2, ..., x_n (x_1 \neq x_2 \wedge x_1 \neq x_3 \wedge ... \wedge x_{n-1} \neq x_n),$

para $n = 1, 2, 3, ...$ (veja-se o exercício 3.5), então, para qualquer linguagem $\mathcal{L}$ e estrutura-$\mathcal{L}$ $\mathfrak{M} = (M, ...)$, tem-se

$$\mathfrak{M} \vDash \Sigma \text{ sse } M \text{ é infinito.}$$

*
* *

Precisando a Nota 70 (p. 139) acima: se ϕ é **intuitivamente válida**, isto é, é válida em *todas* as interpretações, matemáticas e extramatemáticas, em particular ϕ é universalmente válida, portanto, é um teorema lógico (propriedade de completude semântica); sendo ϕ um teorema lógico e sendo as regras do sistema **DNQ** intuitivamente válidas (além de «matematicamente» válidas ou válidas para a semântica tarskiana), ϕ é também intuitivamente válida. Em notação óbvia, temos, portanto, as seguintes inclusões entre conjuntos de sentenças de $\mathcal{L}$:

$$\text{Val}_{\text{intuitiva}} \subseteq \text{Val}_{\text{universal}} \subseteq \text{Teor}_{\mathbf{DNQ}} \subseteq \text{Val}_{\text{intuitiva}},$$

donde se conclui, um tanto surpreendentemente, que

$$\text{Val}_{\text{intuitiva}} = \text{Val}_{\text{universal}} !$$

A possível surpresa advém do facto de o primeiro conjunto, o do lado esquerdo da igualdade, ser definido apenas intuitiva ou informalmente, quer dizer, não possui, em princípio, estatuto matemático, enquanto o conjunto do lado direito da mesma igualdade é definido com precisão matemática. Por outro lado, das inclusões acima também se infere que o conjunto dos teoremas lógicos de $\mathcal{L}$, no sistema **DNQ**, é igual ao conjunto das sentenças universalmente válidas de $\mathcal{L}$. Ora, sabendo-se que existem muitos sistemas dedutivos para $\mathcal{L}$, de que **DNQ** é apenas um exemplo, e sendo a noção de validade universal uma noção semântica independente de qualquer sistema dedutivo somos levados a concluir que *a noção de teorema lógico é, também ela, independente do sistema dedutivo utilizado*. Por outras palavras, *há essencialmente uma única noção de teorema lógico* para uma linguagem elementar, mas diversas as maneiras de caracterizar essa noção.

III.11 Formas normais, rectificação e skolemização

A noção de *equivalência lógica* para linguagens elementares é uma generalização «natural» (mas com cautelas adicionais) da correspondente noção proposicional, e representa-se pelo mesmo símbolo $\sim$: se ϕ, ψ são fórmulas da mesma linguagem $\mathcal{L}$, tem-se $\phi \sim \psi$ sse cada uma das fórmulas ϕ, ψ é consequência lógica da outra, o que acontece sse têm exactamente os mesmos modelos (ver pág. 184): para qualquer $\mathfrak{M}$ para $\mathcal{L}$,

$$\mathfrak{M} \vDash \phi \text{ sse } \mathfrak{M} \vDash \psi.$$

Para obter fórmulas logicamente equivalentes a fórmulas dadas e, em particular, com certa forma especial, há que saber lidar com os quantificadores, o que quer dizer, nomeadamente, ter em conta os resultados seguintes, os quais já foram estabelecidos dedutivamente (sistema **DNQ**) mas serão aqui estabelecidos novamente por via semântica:

11.1 Metateorema (Equivalências lógicas notáveis)
(a) De Morgan: *para qualquer fórmula* $\phi(a, ...)$,

$$\neg\forall x\phi \sim \exists x\neg\phi, \quad \neg\exists x\phi \sim \forall x\neg\phi;$$

(b) Importação/exportação dos quantificadores: *para quaisquer fórmulas* $\phi(a, ...)$ *e* $\psi(a, ...)$,

(b_1) $$(\forall x\phi \wedge \forall x\psi) \sim \forall x(\phi \wedge \psi); \quad (\exists x\phi \vee \exists x\psi) \sim \exists x(\phi \vee \psi);$$

para quaisquer fórmulas $\phi(a, ...)$ *e* ψ, *onde o parâmetro* a *não ocorre em* ψ,

(b_2) $$\begin{array}{ll} (\forall x\phi \wedge \psi) \sim \forall x(\phi \wedge \psi); & (\forall x\phi \vee \psi) \sim \forall x(\phi \vee \psi); \\ (\exists x\phi \wedge \psi) \sim \exists x(\phi \wedge \psi); & (\exists x\phi \vee \psi) \sim \exists x(\phi \vee \psi); \end{array}$$

(c) Permutação de quantificadores da mesma natureza: *para qualquer fórmula* $\phi(a, b, ...)$,

$$\forall x\forall y\phi \sim \forall y\forall x\phi; \quad \exists x\exists y\phi \sim \exists y\exists x\phi.$$

Vistas da direita para a esquerda, as equivalências acima podem ser encaradas como regras para «puxar os quantificadores para fora».

Dem. Estabelecemos apenas algumas equivalências lógicas — as restantes, ficam para o leitor, como exercícios.

(a) Sejam $\mathfrak{I} = (\mathfrak{M}, \alpha)$ ao arbítrio [sempre subentendido: $\mathfrak{M} = (M, ...)$ para a linguagem $\mathcal{L}$ de $\phi(a, ...)$, $\alpha = \langle \alpha_i : i \geq 0 \rangle$ uma atribuição em $\mathfrak{M}$]; então, pela

definição semântica básica, nas notações introduzidas nas págs. 181-184,

$$\begin{array}{lll} \mathfrak{M} \vDash \neg\forall x\phi[\alpha] & \text{sse} & \mathfrak{M} \nvDash \forall x\phi \\ & \text{sse} & \text{não se tem, para todo } m \in M,\ \mathfrak{M} \vDash \phi[\alpha(m/a)] \\ & \text{sse} & \text{para algum } m \in M,\ \mathfrak{M} \nvDash \phi[\alpha(m/a)] \\ & \text{sse} & \text{para algum } m \in M,\ \mathfrak{M} \vDash \neg\phi[\alpha(m/a)] \\ & \text{sse} & \mathfrak{M} \vDash \exists x\neg\phi[\alpha]; \end{array}$$

(b) sendo $\mathfrak{M}$, α ao arbítrio, como acima, $\phi(a, ...)$ onde ocorre a, ψ onde a não ocorre,

$$\begin{array}{lll} \mathfrak{M} \vDash \forall x\phi \wedge \psi[\alpha] & \text{sse} & \mathfrak{M} \vDash \forall x\phi[\alpha] \text{ e } \mathfrak{M} \vDash \psi[\alpha] \\ & \text{sse} & \text{para todo } m \in M,\ \mathfrak{M} \vDash \phi[\alpha(m/a)] \text{ , e } \mathfrak{M} \vDash \psi[\alpha] \\ & \text{sse} & \text{para todo } m \in M,\ \mathfrak{M} \vDash \phi[\alpha(m/a)] \text{ e } \mathfrak{M} \vDash \psi\phi[\alpha(m/a)], \\ & & \qquad\qquad \text{pois } a \text{ não ocorre em } \psi, \\ & \text{sse} & \mathfrak{M} \vDash \forall x(\phi \wedge \psi)[\alpha]. \blacksquare \end{array}$$

De notar que as equivalências «similares» não exibidas são, em geral, inválidas, por exemplo:

$$\forall x\phi \vee \forall x\psi \not\sim \forall x(\phi \vee \psi), \quad \exists x\phi \wedge \exists x\psi \not\sim \exists x(\phi \vee \psi).$$

A *propriedade de substituição de equivalentes* [(3), pág. 135] estende-se sem dificuldade à lógica de 1.ª ordem, e na justificação respectiva, por indução na complexidade das fórmulas, apenas se tem de considerar adicionalmente as alíneas correspondentes aos quantificadores $\forall x\psi$, $\exists x\psi$, pois no resto é análoga. No que segue, designamos esta propriedade abreviadamente por «sub.».

11.2 Exemplo

Aplicamos as «regras» (a)-(c) do metateorema e a propriedade de substituição acima, além das equivalências correspondentes às leis da associatividade («ass.») e da comutatividade («com.») dos conectivos, entre outras, para «puxar os quantificadores para fora», ao mesmo tempo que «empurramos as negações para dentro» na fórmula seguinte (onde P e Q são unários, f é unário e R é binário)

$$\neg\forall y(\exists xPxy \vee \forall zQz) \wedge \exists wRfcw):$$

$$\begin{array}{lcll} \exists y\neg(\exists xPxy \vee \forall zQz) \wedge \exists wRfcw) & \sim & \exists y(\neg\exists xPxy \wedge \neg\forall zQz) \wedge \exists wRfcw) & \text{(a)} \\ & \sim & \exists y(\forall x\neg Pxy \wedge \exists z\neg Qz) \wedge \exists wRfcw & \text{(a), sub.} \\ & \sim & \exists y\exists w((\forall x\neg Pxy \wedge \exists z\neg Qz) \wedge Rfcw) & \text{com., sub.} \\ & \sim & \exists y\exists w(\forall x\exists z(\neg Pxy \wedge \neg Qz) \wedge Rfcw) & \text{(b), sub.} \\ & \sim & \exists y\exists w\forall x\exists z((\neg Pxy \wedge \neg Qz) \wedge Rfcw)) & \text{(b).} \end{array}$$

Estes procedimentos não são, em geral, únicos, quer dizer, a ordem dos quantificadores iniciais obtida não é bem determinada pela fórmula inicial, o que não quer dizer que seja arbitrária, mas apenas que outras «combinações» são amiúde possíveis, e não apenas por causa da permutabilidade (c). Algo se poderia fazer no sentido de uma maior determinação do resultado final, mas não necessitamos disso neste livro.

11.3 Mudança de variáveis mudas

A exportação (b_2) nem sempre é possível, por causa da restrição de o parâmetro a da quantificação em x não ocorrer em ψ, mas até esta impossibilidade é mais aparente do que real, atendendo a que se pode efectuar, sempre que necessário, uma *mudança de variáveis mudas,* como explicaremos a seguir a alguns preliminares.

Recorde-se (nota 102, pág. 161) que se ϕ é uma fórmula, a um parâmetro, e t um termo qualquer, designa-se por ϕ_a^t, ou por $\phi(t/a)$, ou simplesmente por $\phi(t)$, se não houver confusão possível, a fórmula que resulta de substituir todas as ocorrências de a em ϕ por t.[124] Por exemplo, de substituir a por $a+b$ em $\phi(a) = \forall x(b < a + x)$ resulta a fórmula

$$\phi(a+b) = \phi(a)_a^{a+b} = \forall x(b < (a+b) + x).$$

11.4 Propriedade de substituição de parâmetros por termos

Para quaisquer fórmula $\phi(a)$ onde ocorre o parâmetro a, termo fechado t e interpretação $\mathfrak{I} = (\mathfrak{M}, \alpha)$, tem-se

$$\mathfrak{M} \vDash \phi(t/a)[\alpha] \ \textit{ sse } \ \mathfrak{M} \vDash \phi[\alpha(t^{\mathfrak{M}}/a)].\blacksquare$$

Este resultado estende-se imediatamente a várias substituições simultâneas. A demonstração é por indução nas fórmulas e fica como exercício.

Por palavras, a propriedade anterior significa, abreviadamente, que «tanto faz substituir na fórmula como na atribuição». Observe-se que, sendo t um termo fechado (isto é, sem parâmetros), o valor de t em $\mathfrak{I}$ só depende de $\mathfrak{M}$ e não de α. Utilizando a definição semântica básica, também se prova facilmente a seguinte

11.5 Propriedade da mudança de variáveis mudas

Se $\psi = \psi(a)$ é uma fórmula, $\phi = Qx\psi(x/a)$, onde Q é $\forall$ ou $\exists$, e y é uma variável que não ocorre em ψ, então

$$\phi \sim Qy\psi(y/a).\blacksquare$$

---

[124] Devemos acrescentar: se algumas houver, caso contrário $\phi_a^t = \phi$. Por outro lado, deve observar-se que o resultado de uma tal substituição é ainda, de facto, uma fórmula. Isto mesmo pode provar-se por indução nas fórmulas.

Iterando a aplicação desta propriedade quantas vezes forem necessárias, vê-se que podemos sempre encontrar uma fórmula ψ logicamente equivalente a uma fórmula dada ϕ, com os mesmos parâmetros que ϕ, mas variáveis mudas diferentes e de modo que em ψ *não ocorra nenhum parâmetro associado a uma quantificação numa variável que nela ocorra*.[125] Observe-se, por exemplo, que

$$a < b,\ \exists x(x \doteq b),\ a < b \wedge \exists x(x \doteq b),\ \exists x(x < b) \text{ e } \exists x(x < b) \wedge \exists x(x \doteq b)$$

são fórmulas, na última das quais a variável x foi quantificada duas vezes, mas a terceira das regras (b_2) não permite «puxar $\exists x$ para fora» nessa última; todavia, $\exists x(x \doteq b) \sim \exists y(y \doteq b)$ e

$$\exists x(x < b) \wedge \exists x(x \doteq b) \sim \exists x(x < b) \wedge \exists y(y \doteq b) \sim \exists x(x < b \wedge \exists y(y \doteq b)).$$

Uma fórmula onde não ocorre nenhum parâmetro associado a uma quantificação (nessa mesma fórmula) diz-se **rectificada**. Tem-se então o seguinte

11.6 Lema da rectificação

Toda a fórmula é logicamente equivalente a uma fórmula rectificada com os mesmos parâmetros.■

11.7 Definição

Diz-se que uma fómula está na **forma normal prenexada** (FNP) sse tiver a forma

$$Q_1 y_1 Q_2 y_2 \cdots Q_n y_n \psi \ \ (n \geq 0),$$

onde cada Q_i é $\forall$ ou $\exists$ e a fórmula ψ não tem quantificadores. ψ é chamada a **matriz.** Diz-se que ϕ está na **forma normal rectificada** (FNR) sse está rectificada e na forma FNP.

---

[125] Para linguagens sem parâmetros (em que o papel dos parâmetros é desempenhados por variáveis com ocorrências *livres*), esta propriedade corresponde à seguinte: nenhuma variável tem simultaneamente ocorrências mudas e livres na fórmula.

11.8 Metateorema (Forma normal prenexada)

Toda a fórmula é logicamente equivalente a uma fórmula rectificada na FNP com os mesmos parâmetros.

Dem. Por indução na complexidade das fórmulas.

Se ϕ é atómica não há nada mais a fazer, pois já está na FNR.

Se $\phi = \neg\psi$ com ψ na FNR (hipótese de indução), digamos

$$\psi = Q_1 y_1 Q_2 y_2 \cdots Q_n y_n \psi',$$

então, pelas regras de De Morgan (pág. 203),

$$\phi = \neg Q_1 y_1 Q_2 y_2 \cdots Q_n y_n \psi' \sim \overline{Q}_1 y_1 \overline{Q}_2 y_2 \cdots \overline{Q}_n y_n \neg\psi',$$

que está na FNR, onde $\overline{Q}$ é $\exists$, $\forall$ se Q é $\forall$, $\exists$, respectivamente.

Se $\phi = \psi \diamond \theta$, onde $\diamond$ é $\wedge$ ou $\vee$, então, por hipótese de indução, ψ e θ são logicamente equivalentes a fórmulas na FNR ψ_1 e θ_1, respectivamente. Por mudança de variáveis mudas (por exemplo, em ψ_1), se necessário, podemos supor que as variáveis mudas em ψ_1 são distintas das variáveis mudas em θ_1, digamos

$$\psi_1 \sim Q_1 y_1 Q_2 y_2 \cdots Q_m y_m \psi_1', \quad \theta_1 \sim Q_1' z_1 Q_2' z_2 \cdots Q_n' z_n \theta_1',$$

donde, passando os quantificadores para fora,

$$\phi = \psi \diamond \theta \sim Q_1 y_1 Q_2 y_2 \cdots Q_m y_m Q_1' z_1 Q_2' z_2 \cdots Q_n' z_n (\psi_1' \diamond \theta_1'),$$

que está na FNR.

Se $\phi = Qx\psi$, onde Q é $\forall$ ou $\exists$, e $\psi \sim Q_1 y_1 Q_2 y_2 \cdots Q_n y_n \psi'$ na FNR, por hipótese de indução, por mudança de variáveis mudas, se necessário, podemos supor que x é distinta de y_1, ..., y_n. Então

$$\phi \sim Qx Q_1 y_1 Q_2 y_2 \cdots Q_n y_n \psi',$$

a qual está na FNR.■

A demonstração anterior tem implícito um *procedimento de conversão*[126] de qualquer fórmula numa fórmula logicamente equivalente na FNR.

11.9 Exemplo

Convertendo $\phi = \forall x \exists y \neg \exists z P x y z \rightarrow \exists y \forall z \neg R y z$ na FNR: primeiro, rectifica-se ϕ, obtendo, por exemplo,

$$\phi' = \forall x \exists v \neg \exists w P x v w \rightarrow \exists y \forall z \neg R y z.$$

---

[126] O resultado é único, a menos de equivalência lógica. As «instruções» para o dito procedimento podem ser ligeiramente modificadas de modo a ficarem deterministas e podermos falar de um *algoritmo de conversão* no sentido estrito.

Prosseguindo na conversão:

$$\begin{aligned}\phi &\sim \phi' \\ &\sim \forall x\exists v\forall w\neg Pxvw \rightarrow \exists y\forall z\neg Ryz \\ &\sim \exists y\forall z(\forall x\exists v\forall w\neg Pxvw \rightarrow \neg Ryz) \\ &\sim \exists y\forall z\exists x\forall v\exists w(\neg Pxvw \rightarrow \neg Ryz) \\ &\sim \exists y\forall z\exists x\forall v\exists w(Ryz \rightarrow Pxvw).\end{aligned}$$

Apenas por razão estética levámos o procedimento um passo mais adiante do que o mínimo necessário, mas ainda seria possível continuar, nomeadamente, convertendo a matriz numa das formas normais proposicionais (FNC ou FND). Outra fórmula logicamente equivalente à dada na FNR é

$$\exists x\forall v\exists w\exists y\forall z(Ryz \rightarrow Pxvw).$$

11.10 Skolemização[127]

Uma maneira sintáctica de medir a «complexidade» lógica (não confundir com a complexidade computacional) das noções matemáticas é através da presença e alternância dos quantificadores $\forall$, $\exists$ nas definições. Tal medida parece estar associada ao nível médio de compreensão daquelas noções. Assim, por exemplo, estima-se que as conhecidas definições de limite e de continuidade de uma função num ponto, digamos, para fixar ideias, de uma função real de variável real $f : \mathbb{R} \rightarrow \mathbb{R}$, tipifique o nível médio máximo de complexidade de uma noção matemática intuitivamente compreensível. Utilizando as «variáveis limitadas» δ, ε para números reais positivos, e x para variável limitada aos números reais, uma definição comum (dita «à Cauchy») de $\lim_{x\rightarrow a} f(x) = f(a)$ é

$$\forall\delta\exists\varepsilon\forall x(|x - a| < \varepsilon \rightarrow |f(x) - f(a)| < \delta),$$

a qual é do tipo $\forall\exists\forall$ de complexidade sintáctica.[128]

---

[127] Procedimento introduzido pelo matemático e lógico de origem norueguesa, Albert Thoralf Skolem (1887-1963).

[128] Parece pouco, mas não esqueçamos que, para poder compreender intuitivamente bem as noções de complexidade superior os matemáticos introduzem *novos objectos e classes de objectos* de tipo superior, precisamente para que as noções acerca deles fiquem com menor complexidade. Assim por exemplo, se admitirmos lidar com sucessões arbitrárias de números reais, podemos reduzir drasticamente a complexidade sintáctica da definição de continuidade pontual, como se sabe, obtendo uma definição de complexidade sintáctica $\forall$ (definição «à Heine»): para toda a sucessão de números reais $s = \langle a_n\rangle_{n\in\mathbb{N}}$ que converge para a, a sucessão $f \circ s = \langle f(a_n)\rangle_{n\in\mathbb{N}}$ converge para $f(a)$. Não esqueçamos, todavia, que as duas definições só são equivalentes mediante o axioma da escolha para famílias numeráveis de conjuntos (nomeadamente, para a prova de que as noções à Heine implicam as correspondentes noções à Cauchy.

Bem mais simples de compreender são, portanto, as fórmulas ou sentenças *universais*

$$\forall y_1 \forall y_2 \cdots \forall y_n \psi,$$

com ψ sem quantificadores.

Mediante um certo preço a pagar, podemos associar a cada fórmula ou sentença ϕ uma fórmula ou sentença universal ϕ_s, respectivamente, em geral *não equivalente* a ϕ, mas sempre *equicompatível* com ϕ.

A primeira coisa a fazer é converter ϕ na FNR. Suponhamos que isto já está feito, digamos

(S) $$\phi = \forall y_1 \forall y_2 \cdots \forall y_k \exists z \psi(y_1, y_2, ..., y_k, z)$$

com $k \geq 0$ e $\psi(a_1, a_2, ..., a_k, b)$ ainda na FNR mas contendo, possivelmente, alguns quantificadores no início (onde $\overline{a} = a_1, ..., a_k$ são os parâmetros associados às quantificações em $\overline{y} = y_1, ..., y_k$ e b é associado à quantificação em z). Introduzimos na linguagem $\mathcal{L}$ um *novo símbolo operacional k-ário g* (ou uma nova constante, d, se for $k = 0$) e definimos

(S′) $$\phi' = \forall y_1 \forall y_2 \cdots \forall y_k \psi(y_1, y_2, ..., y_k, g y_1 y_2 ... y_k / z).$$

Note que se ϕ é fórmula na linguagem $\mathcal{L}$, então ϕ' é fórmula na linguagem $\mathcal{L}' = \mathcal{L} \cup \{g\}$ (mas não é fórmula em $\mathcal{L}$).

É óbvio que ϕ' continua na FNR, mas já tem menos um quantificador existencial do que ϕ. O procedimento anterior pode-se repetir, aplicado a ϕ', e assim sucessivamente até serem eliminados a favor de novos símbolos operacionais todos os quantificadores existenciais, obtendo no final uma fórmula ϕ_s que sa chama uma **skolemizada** de ϕ.

11.11 Exemplo

Skolemizando a fórmula $\exists y \forall z \exists x \forall v \exists w((R(y, z) \rightarrow P(x, v, w))$ do exemplo anterior, após conversão na FNR, obtemos sucessivamente (trabalhando os quantificadores da esquerda para a direita):

1. $\exists y \forall z \exists x \forall v \exists w(R(y, z) \rightarrow P(x, v, w))$
2. $\forall z \exists x \forall v \exists w(R(c_1, z) \rightarrow P(x, v, w))$
3. $\forall z \forall v \exists w(R(c_1, z) \rightarrow P(g_1(z), v, w))$
4. $\forall z \forall v(R(c_1, z) \rightarrow P(g_1(z), v, g_2(z, v))$.

11.12 Metateorema da skolemização

Toda a fórmula ϕ na FNR é equicompatível a qualquer sua skolemizada.

Por outro lado, não se deve confundir o conceito lógico de *complexidade sintáctica* com o conceito informático de *complexidade computacional*.

***Dem.** Basta ver que cada em cada passo da skolemização [passagem de (S) a (S′) como acima] se obtém uma fórmula equicompatível com a fórmula que precede.

Sejam ϕ como em (S), abreviadamente $\phi = \forall\overline{y}\exists z\psi(\overline{y}, z) = \forall\overline{y}\exists z\psi(\overline{y}/\overline{a}, z/b)$ e ϕ' como em (S′), abreviadamente $\phi' = \forall\overline{y}\psi(\overline{y}, g\overline{y}/b)$.

Se ϕ' é compatível, então existem $\mathfrak{M}'$, α tais que $\mathfrak{M}' \vDash \phi'[\alpha]$, com $\mathfrak{M}' = (M, ..., g_{\mathfrak{M}'})$ adequada para a linguagem $\mathcal{L}'$ de ϕ', onde $\mathcal{L}' = \mathcal{L} \cup \{g\}$ e $\mathcal{L}$ é a linguagem de ϕ. É claro que em $\mathfrak{M}'$ também podemos interpretar todos os símbolos de $\mathcal{L}$ (pois $\mathcal{L} \subset \mathcal{L}'$), e, em notação abreviada,

$$\text{para todo } \overline{m} \in M^k,\ \mathfrak{M}' \vDash \psi(\overline{a}, g\overline{a}/b)[\alpha(\overline{m}/\overline{a})].$$

Pela propriedade de substituição de parâmetros por termos (pág. 205), tem-se

$$\text{para todo } \overline{m} \in M^k,\ \mathfrak{M}' \vDash \psi(\overline{a}, b)[\alpha(\overline{m}/\overline{a})(n/b)],$$

onde $n = g^{\mathfrak{M}}(\overline{m})$. Quer dizer, portanto, que

$$\text{para todo } \overline{m} \in M^k \text{ existe } k \in M \text{ tal que } \mathfrak{M}' \vDash \psi(\overline{a}, b)[\alpha(\overline{m}/\overline{a})(k/b)],$$

ou seja, que

$$\mathfrak{M}' \vDash \forall\overline{y}\exists z\psi(\overline{y}, z).$$

Viu-se, portanto, que todo o modelo de ϕ' é também modelo de ϕ.

Reciprocamente, se $\mathfrak{M} = (M, ...)$ e $\mathfrak{I} = (\mathfrak{M}, \alpha) \vDash \phi$, $\mathfrak{I}$ ainda não interpreta o novo símbolo operacional k-ário g que foi introduzido na passagem de ϕ a ϕ', mas sabemos que

$(*)$ para todo $\overline{m} \in M^k$ existe $k \in M$ tal que $\mathfrak{M} \vDash \psi(\overline{a}, b)[\alpha(\overline{m}/\overline{a})(k/b)]$.

Trata-se, agora, de obter a partir de $\mathfrak{I}$ um modelo conveniente de ϕ', que terá de ser, antes de mais, uma interpretação adequada para $\mathcal{L}'$. Precisamos, pois, de uma função conveniente $g : M^k \to M$ para interpretar o símbolo g. $(*)$ dá-nos uma ideia de como definir uma tal função: para cada $\overline{m}$ em M^k *escolhemos* um k em M, como em $(*)$, para valor da função, isto é, pômos, por definição, $g(\overline{m}) = k$. Mas o conjunto M pode ser infinito e, por conseguinte, para definir g, podemos ter de efectuar uma *infinidade de escolhas arbitrárias*. Ora, em matemática, há uma única maneira de justificar tais escolhas, que é o chamado *Princípio (ou Axioma) da Escolha de Zermelo*, que é vulgarmente designado pela sigla (AC) e que se pode enunciar da seguinte maneira:

11.13 Axioma da escolha (AC)

Se $\mathcal{F}$ é um conjunto (ou família) de conjuntos não vazios, então existe uma função S definida em $\mathcal{F}$ tal que, para cada $X \in \mathcal{F}$, $S(X) \in X$.

Uma função S como acima chama-se um *selector* para $\mathcal{F}$. No caso que se nos apresenta, podemos tomar para $\mathcal{F}$ o conjunto de todos os subconjuntos não vazios de M da forma

$$X_{\overline{m}} = \{k \in M : \mathfrak{M} \vDash \psi(\overline{a}, b)[\alpha(\overline{m}/\overline{a})(k/b)]\}, \text{ com } \overline{m} \in M^k,$$[129]

e definir a função g pondo, para cada $\overline{m} \in M^k$,

$$g(\overline{m}) = S(X_{\overline{m}}) \in M.$$

Tendo definido g desta maneira, e pondo $\mathfrak{M}' = (M, ..., g)$, prosseguimos, observando, a partir de $(*)$, que

$$\text{para todo } \overline{m} \in M^k, \mathfrak{M}' \vDash \psi(\overline{a}, b)[\alpha(\overline{m}/\overline{a})(g(\overline{m})/b)].$$

Pela propriedade de substituição dos parâmetros por termos (pág. 205), tem-se

$$\text{para todo } \overline{m} \in M^k, \mathfrak{M}' \vDash \psi(\overline{a}, g(\overline{a})/b)[\alpha(\overline{m}/\overline{a})],$$

donde

$$\mathfrak{M}' \vDash \forall \overline{y} \psi(\overline{y}, g(\overline{y})/b)[\alpha],$$

isto é, $\mathfrak{M}' \vDash \phi'[\alpha]$, como queríamos demonstrar.■

O resultado estende-se imediatamente a qualquer conjunto Σ de fórmulas ou sentenças, procedendo para cada uma delas como na demonstração e, no fim, expandindo a linguagem com todos os novos símbolos operacionais introduzidos. Se Σ' é o conjunto das skolemizadas das fórmulas de Σ, então é fácil concluir que Σ é compatível sse Σ' é compatível.

Essencialmente por causa dos novos símbolos operacionais (incluindo, eventualmente, algumas constantes), uma fórmula ϕ e uma sua skolemizada ψ não são logicamente equivalentes, mas são, como se demonstrou, *equicompatíveis,* e a partir de um modelo de uma delas pode-se obter um modelo da outra. Escrevemos

$$\phi \overset{\text{S}}{\leftrightsquigarrow} \psi$$

para representar a passagem de ϕ à skolemizada ψ e, também, para exprimir que ϕ e ψ são equicompatíveis, e dizemos, um tanto abusivamente, que elas são *s-equivalentes*.[130]

Para algumas aplicações, nomeadamente, relacionadas com o método de *resolução* (ver adiante), é conveniente seguir a seguinte lista de procedimentos, a aplicar a uma fórmula arbitrária $\phi = \phi(a_1, ..., a_n)$:

1) rectificar ϕ, se necessário, obtendo $\phi_1 = \phi_1(a_1, ..., a_n) \sim \phi$;

---

[129] No caso $k = 0$, toma-se $X_{\overline{m}} = M$.

[130] Não perder de vista, todavia, que a relação $\overset{\text{S}}{\leftrightsquigarrow}$ assim definida, *não é simétrica*.

2) substituir ϕ_1 pela s-equivalente $\phi_2 = \exists y_1 ... \exists y_n \phi_1(y_1/a_1, ..., y_1/a_1)$;

3) converter ϕ_2 na FNR, obtendo $\phi_3 \sim \phi_2$;

4) skolemizar ϕ_3, obtendo uma s-equivalente ϕ_4;

5) converter a matriz de ϕ_4 na FNC, obtendo $\phi_5 \sim \phi_4$;

6) reescrever a matriz de ϕ_5 na forma clausural, obtendo $\phi_6 \sim \phi_5$.

Por *cláusula* ou fórmula na *forma clausural* entende-se uma sentença (sem parâmetros) na FNP cuja matriz é uma disjunção de literais, isto é, de fórmulas atómicas ou suas negações. Por exemplo,

$$\forall x \forall y (Px \vee Qxy \vee \neg Ry),$$

é uma cláusula. Uma vez que as cláusulas só possuem quantificadores universais no início, é possível representar as cláusulas na lógica de 1ª ordem sob a forma de conjuntos de literais, tal como se fez na lógica proposicional. No exemplo acima obtemos, por exemplo, a representação cláusural

$$\{Pa, Qab, \neg Rb\}.$$

III.12 Outros sistemas dedutivos (I): *tableaux* semânticos

Nesta secção estendemos o sistema dedutivo dos *tableaux* semânticos de Beth à lógica de 1.ª ordem, que designamos por **BQ**, ou simplesmente por **B**. As derivações neste sistema são árvores binárias, tal como no sistema proposicional dos *tableaux* (II.12, pág. 106), mas agora os nós das árvores serão preenchidos por fórmulas valoradas da forma $V\phi$ ou $F\phi$, onde ϕ é uma fórmula de uma linguagem de 1.ª ordem dada, digamos $\mathcal{L}$. Aqui, o papel que as letras proposicionais desempenham na lógica proposicional será desempenhado pelas fórmulas ou sentenças atómicas, e haverá novas regras (*tableaux* atómicos) para lidar com os quantificadores e a igualdade ($\doteq$). Mas haverá também outra modificação importante a ter em conta, como explicamos a seguir.

Consideremos, por exemplo, a sentença valorada $V\exists x \phi(x)$ que exprime, intuitivamente, que $\exists x \phi(x)$ é verdadeira, o que quererá dizer que algum sucessor imediato do nó $V\exists x \phi(x)$ é da forma $V\phi(t)$, para algum termo fechado (isto é, sem parâmetros — um termo que designe um indivíduo ou objecto bem determinado) t.[131] Um tal t é o que se chama uma *testemunha* para a sentença existencial $\exists x \phi(x)$. Mas pode bem acontecer que a linguagem $\mathcal{L}$ não disponha de termos em quantidade e variedade suficientes para servir de testemunhas: $\mathcal{L}$ até pode não conter constantes e não haver, portanto, termos fechados em $\mathcal{L}$!

---

[131] Como já foi explicado anteriormente, $\forall x \phi(x) = \forall x \phi(x/a)$, onde é suposto que a ocorre em ϕ e é o parâmetro da quantificação em x na formação de $\forall x \phi(x/a)$. Então $\phi(t)$ não é mais do que $\phi(t/a)$.

Para obviar ao problema anterior vamos expandir a linguagem $\mathcal{L}$ com uma lista infinita numerável de constantes *adicionais* (isto é, não em $\mathcal{L}$)

$$c_0,\ c_1,\ c_2,\ c_3,\ \ldots\ .$$

Ponhamos $C = \{c_0, c_1, ...\}$ e seja $\mathcal{L}_C = \mathcal{L} \cup C$ a nova linguagem expandida de $\mathcal{L}$ com as constantes em C. Os nós das derivações no sistema de *tableaux* para a linguagem $\mathcal{L}$ serão sentenças de $\mathcal{L}_C$. Nesta secção, e até aviso em contrário, o símbolo de igualdade $\doteq$ será tratado como qualquer outro símbolo relacional binário.

Os *tableaux* atómicos de **B** são os *tableaux* proposicionais 1-6 da pág. 107, com as seguintes diferenças e acrescentos:

• os *tableaux*

1a. $V\phi$	1b. $F\phi$

,

para sentenças atómicas de $\mathcal{L}_C$;

• os *tableaux* 2–6 para sentenças ϕ, ψ de $\mathcal{L}_C$;

• os *tableaux* quantificacionais seguintes:

7a.	$V\forall x\phi(x)$ | $V\phi(t)$	onde t é um termo fechado qualquer de $\mathcal{L}_C$	7b.	$F\forall x\phi(x)$ | $F\phi(c)$	onde $c \in C$ e c não ocorre em $\phi(x)$ [ver 12.1(ii) adiante]
8a.	$V\exists x\phi(x)$ | $V\phi(c)$	onde $c \in C$ e c não ocorre em $\phi(x)$ [ver 12.1(ii) adiante]	8b.	$F\exists x\phi(x)$ | $F\phi(t)$	onde t é um termo fechado qualquer de $\mathcal{L}_C$.

Damos a seguir a definição (indutiva) precisa de *tableaux* no sistema **BQ**, recordando, a propósito, o que se disse na Nota 81, pág. 109.

12.1 Definição

Um *tableau* é uma árvore binária, finita ou infinita, cujos nós são sentenças valoradas de $\mathcal{L}_C$, definido indutivamente pelas regras seguintes:

(i) os *tableaux* atómicos são *tableaux*;

(ii) se T é um *tableau* finito, κ é um ramo de T e X é uma entrada de T que ocorre em κ, e T' obtém-se de T apensando um *tableau* atómico com raiz X no término de κ, então T' é um *tableau*; além disso, nos casos dos *tableaux* atómicos 7b e 8a, é exigido que c seja *nova com respeito a todas as entradas em* κ e não apenas com respeito a X;

(iii) se T_0 é um *tableau* finito e T_0, T_1, T_2, ... é uma sequência de *tableaux* tais que, para cada n, T_{n+1} é construído a partir de T_n como em (ii), então $T = \bigcup_{n=0}^{\infty} T_n$ é um *tableau*.

A exigência em (ii) é fundamental. Na prática, o melhor é utilizar uma c_i que ainda não tenha ocorrido anteriormente no *tableau.* Além disso, é crucial que a entrada X seja repetida como raiz do *tableau* atómico que apensa ao término de κ mas, tal como no caso proposicional, esta repetição pode-se omitir relativamente aos outros *tableaux* atómicos. Quer dizer, portanto, que uma mesma fórmula valorada por ocorrer em diferentes nós do *tableau.*

Tal como no caso proposicional (pág. 115), também admitiremos *tableaux* com hipóteses, isto é, *tableaux* em que, em certos nós, se possam introduzir fórmulas valoradas $V\phi_i$ com ϕ_i num conjunto dado (finito ou infinito) de sentenças na linguagem original $\mathcal{L}$ $\Sigma = \{\phi_1, \phi_2, ...\}$. A estas chamamos *hipóteses.*

12.2 Definição

Se $\Sigma = \{\phi_1, \phi_2, ...\}$ é um conjunto de sentenças de $\mathcal{L}$ (a que chamamos *hipóteses*), um *tableau com hipóteses em* Σ define-se tal e qual como um tableau ordinário (12.1), com a cláusula adicional seguinte:

(ii′) Se T é um *tableau* finito com hipóteses em Σ, κ é um ramo em T e T' obtém-se de T apensando $T\phi$, com $\phi \in \Sigma$, no término de T, então T' é um *tableau* com hipóteses em Σ.

Quer por Σ ser infinito, quer por (ii) ou (iii), é claro que um *tableau*, com ou sem hipóteses, é sempre uma união de uma sequência finita ou infinita de *tableaux* com ou sem hipóteses T_0, T_1, ..., T_n, ..., em que T_0 é um *tableau* atómico e, para cada n, T_{n+1} é obtido de T_n por (ii) ou (ii′): basta pensar nos diferentes níveis. No que segue suporemos tacitamente que um *tableau* (com ou sem hipóteses) se apresenta sempre como uma tal união.

12.3 Definição

Seja T um *tableau* (com ou sem hipóteses), κ um ramo de T.

(a) κ é **contraditório** sse contém as entradas $V\phi$ e $F\phi$ para alguma ϕ;

(b) T é **contraditório** sse todo o ramo κ em T é contraditório;

(c) T é uma **derivação**-B (com hipóteses em Σ) de ϕ sse T é um *tableau* (com hipóteses em Σ) finito e contraditório com raiz $F\phi$;

(d) ϕ é **derivável**-B (com hipóteses em Σ) sse existe uma derivação-B de ϕ (com hipóteses em Σ), e neste caso escreve-se

$$\vdash_{\mathrm{B}} \phi \quad (\Sigma \vdash_{\mathrm{B}} \phi, \text{ respectivamente});$$

(e) Σ é **inconsistente** sse $\Sigma \vdash_{\mathrm{B}} \phi \wedge \neg\phi$ para alguma ϕ.

12.4 Exemplos

1) $\vdash_{\mathrm{B}} \forall x\phi(x) \rightarrow \exists x\phi(x)$ (omitindo os traços verticais "|"):

$$
\begin{array}{l}
F\forall x\phi(x)\rightarrow\exists x\phi(x)\\
V\forall x\phi(x)\\
F\exists x\phi(x)\\
\quad\mid\text{(8b)}\\
F\phi(c)\ \ (c\text{ nova})\\
V\forall x\phi(x)\ \ \text{(entrada repetida)}\\
V\phi(c)\\
\otimes\,.
\end{array}
$$

Note-se que a *mesma* constante c que era nova [no sentido de (ii)] na entrada n.º 4 (contando de cima para baixo) foi utilizada na entrada n.º 6 (aqui já não tem que ser nova no mesmo sentido), a fim de obter um ramo contraditório.

2) $\vdash_{\mathrm{B}}\forall x(Px\rightarrow Qx)\rightarrow(\forall xPx\rightarrow\forall xQx)$:

$$
\begin{array}{ll}
F\forall x(Px\rightarrow Qx)\rightarrow(\forall xPx\rightarrow\forall xQx)\\
V\forall x(Px\rightarrow Qx)\\
F\forall xPx\rightarrow\forall xQx\\
V\forall xPx\\
F\forall xQx\\
FQc\ \ (c\text{ nova})\\
V\forall xPx\ \ \text{(rep.)}\\
VPc\\
V\forall x(Px\rightarrow Qx)\ \ \text{(rep.)}\\
VPc\rightarrow Qc\\
FPc\qquad\qquad VQc\\
\otimes\qquad\qquad\otimes\,,
\end{array}
$$

onde omitimos os traços verticais '|'. Na prática, tal como neste exemplo, é conveniente estender um *tableau* estendendo primeiramente o *tableau* atómico que requer a introdução de constante nova, e só depois aqueles que envolvem a introdução de um termo fechado arbitrário. Resumindo: em geral, é conveniente introduzir *primeiro,* 7b ou 8a, e só *depois* introduzir 7a ou 8b. Chamemos a isto os *preceitos do bom senso* (vejam-se as observações na pág. 163). Os exemplos seguintes também são ilustrativos da pertinência destes preceitos.

3) $\vdash_{\mathrm{B}} \forall x(\phi(x) \wedge \psi(x)) \longleftrightarrow (\forall x\phi(x) \wedge \forall x\psi(x))$, onde $\phi(x) = \phi(x/a)$ e $\psi(x) = \psi(x/a)$:

$$
\begin{array}{cccc}
F\forall x(\phi(x) \wedge \psi(x)) \longleftrightarrow (\forall x\phi(x) \wedge \forall x\psi(x)) & & & \\
V\forall x(\phi(x) \wedge \psi(x)) & & F\forall x(\phi(x) \wedge \psi(x)) & \\
F\forall x\phi(x) \wedge \forall x\psi(x) & & V\forall x\phi(x) \wedge \forall x\psi(x) & \\
F\forall x\phi(x) & F\forall x\psi(x) & V\forall x\phi(x) & \\
F\phi(c) & F\psi(d) & V\forall x\psi(x) & \\
V\forall x(\phi(x) \wedge \psi(x)) & V\forall x(\phi(x) \wedge \psi(x)) & F\phi(e) \wedge \psi(e) & \\
V\phi(c) \wedge \psi(d) & V\phi(c) \wedge \psi(d) & F\phi(e) & F\psi(e) \\
V\phi(c) & V\phi(d) & V\forall x\phi(x) & V\forall x\psi(x) \\
V\psi(c) & V\psi(d) & V\phi(e) & V\psi(e) \\
\otimes & \otimes & \otimes & \otimes
\end{array}
$$

As constantes c, d, e é suposto serem novas no sentido de (ii).

Note-se que os *tableaux* atómicos para $V\forall x\phi(x)$ (7a) e para $F\exists x\phi(x)$ (8b) dizem-nos que podemos introduzir $V\phi(t)$ e $F\phi(t)$, respectivamente, *para qualquer termo* t, mas este «qualquer» significa na prática «aquele t que é mais conveniente e oportuno para o objectivo a atingir, nas circunstâncias dadas». Por outro lado, o *tableau* atómico para $V\exists x\phi(x)$ (8a) permite-nos declarar $V\phi(t)$ *somente para* t *que seja uma das constantes novas* c_i *que ainda não tenha ocorrido anteriormente na derivação* [de acordo com o requisito em (ii)]. O exemplo seguinte mostra como pode ser insensato não ter em conta estes preceitos.

4) A sentença $\exists x\phi(x) \rightarrow \forall x\phi(x)$ é obviamente falsa em domínios com mais de um elemento, e desde que o antecedente não seja falso. Mas se não tivermos na devida conta os preceitos acima quanto à introdução de constantes novas, obtém-se a «pseudo-derivação» seguinte que, se estivesse correcta, atestaria que a sentença acima é derivável-B:

$$
\begin{array}{c}
F\exists x\phi(x) \rightarrow \forall x\phi(x) \\
V\exists x\phi(x) \\
F\forall x\phi(x) \\
V\phi(c) \\
F\phi(c) \\
\otimes .
\end{array}
$$

Observe que a entrada n.º 3 foi desenvolvida incorrectamente na entrada n.º 5, uma vez que c, nesta última, não é nova no sentido de (ii) da definição 12.1.

12.5 Axiomas da igualdade

A razão pela qual não introduzimos regras para lidar com a igualdade $\doteq$ é que parece tecnicamente mais conveniente distinguir o tratamento dado a $\doteq$ do tratamento dado a outros símbolos relacionais (se os houver) através de hipóteses

especiais (chamadas os *axiomas lógicos da igualdade*), que são precisamente todas as fórmulas das formas seguintes:

E_1. $\forall x(x \doteq x)$;

E_2. $\forall x_1 ... x_n y_1 ... y_n (x_1 \doteq y_1 \wedge ... \wedge x_n \doteq y_n \rightarrow (Rx_1 ... x_n \rightarrow Ry_1 ... y_n))$, se R é um símbolo relacional n-ário de $\mathcal{L}$, incluindo o caso em que R é $\doteq$;

E_3. $\forall x_1 ... x_m y_1 ... y_m (x_1 \doteq y_1 \wedge ... \wedge x_m \doteq y_m \rightarrow (fx_1 ... x_m \doteq fy_1 ... y_m))$, se f é um símbolo operacional m-ário de $\mathcal{L}$.

Os axiomas do tipo E_2 e E_3 exprimem, em terminologia algébrica, que a interpretação normal de $\doteq$ é uma *congruência* com respeito às «relações» R e às «operações» f correspondentes aos símbolos não lógicos de $\mathcal{L}$.

O caso especial de E_2 é:

E_2'. $\forall x_1 x_2 y_1 y_2 (x_1 \doteq y_1 \wedge x_2 \doteq y_2 \rightarrow (x_1 \doteq x_2 \rightarrow y_1 \doteq y_2))$.

12.6 Exemplos

Pode-se provar, por exemplo, que $\doteq$ é *simétrica,* ou mais precisamente, que a simetria de $\doteq$ é derivável-B dos axiomas da igualdade E_1 e E_2,

$$\mathrm{E}_1, \mathrm{E}_2 \vdash_{\mathrm{B}} \forall xy(x \doteq y \rightarrow y \doteq x),$$

mas em vez de construirmos uma derivação-B mostramos apenas, informalmente, que a simetria é consequência daqueles dois axiomas. O nosso esquema de raciocínio pode depois ser traduzido numa derivação-B, o que deixamos como exercício. As nossas hipóteses são, pois, E_1 e E_2. Sejam c, d ao arbítrio tais que $c \doteq d$, com vista a provar que $d \doteq c$; particularizando E_1 e E_2 convenientemente obtemos $c \doteq c$ e $c \doteq d \wedge c \doteq c \rightarrow (c \doteq c \rightarrow d \doteq c)$, respectivamente, donde facilmente concluimos que $d \doteq c$. Na derivação-B a efectuar, constrói-se um *tableau* contraditório com raiz $F \forall xy(x \doteq y \rightarrow y \doteq x)$ e as duas hipóteses E_1 e E_2', tomando esta última na forma $\forall xy(x \doteq y \wedge x \doteq x \rightarrow (x \doteq x \rightarrow y \doteq x)$. Analogamente para a *transitividade* da igualdade:

$$\mathrm{E}_1, \mathrm{E}_2 \vdash_{\mathrm{B}} \forall xyz(x \doteq y \wedge y \doteq z \rightarrow x \doteq z),$$

mas, desta vez, é mais conveniente utilizar E_2' na forma $\forall xyz(x \doteq x \wedge y \doteq z \rightarrow (x \doteq y \rightarrow x \doteq z))$.

Como já se disse, a construção passo a passo de um *tableau* pode não terminar nunca (enquanto houver ramos não contraditórios). Põe-se a questão de saber em que condições podemos dizer que uma dada fórmula valorada num nó de um *tableau* é ou pode ser «reduzida», isto é, a informação que ela contém ou transporta foi extraída na totalidade, e dizer em que condições um *tableau* é ou pode ser considerado «terminado» num sentido análogo.

Para motivar as definições que seguem, consideremos os *tableaux* atómicos dos quantificadores e a maneira como são utilizados na construção de *tableaux*.

No caso de $V\exists x\phi(x)$ ou $F\forall x\phi(x)$ (8a, 7b) o desenvolvimento dedutivo consiste em introduzir $V\phi(c/x)$ ou $F\phi(c/x)$, respectivamente, para alguma constante $c \in C$ que seja *nova* no ramo considerado. A sentença existencial original $\exists x\phi(x)$ não contém mais informação do que $\phi(c)$ e podemos considerar que estamos terminados com ela (dizemos que foi *reduzida*).

Por outro lado, se estamos a lidar com $V\forall x\phi(x)$ ou $F\exists x\phi(x)$ (7a, 8b), a situação é muito diferente. Aqui podemos introduzir $V\phi(t/x)$ ou $F\phi(t/x)$, respectivamente, *para qualquer termo fechado* t, e é claro que $\phi(t)$ é apenas *uma particularização* em t das muitas possíveis (eventualmente) e já não podemos dizer que toda a informação foi extraída das sentenças em questão (dizemos que ainda não foram reduzidas).

O objectivo das definições seguintes é descrever um procedimento sistemático (algoritmo) para produzir uma derivação de ϕ com hipóteses em Σ dado, se alguma existe, o que é exactamente o caso quando ϕ é consequência lógica de Σ. Este é o conteúdo do importante

12.7 Metateorema da completude semântica do sistema dos *tableaux*

Se $\Sigma \vDash \phi$, *então* $\Sigma \vdash_{\mathrm{B}} \phi$. *Em particular, se* $\vDash \phi$, *então* $\vdash_{\mathrm{B}} \phi$.

À semelhança do que acontece na lógica proposicional, também vale o resultado recíproco (e mais fácil de demonstrar), o qual garante a *consistência* do sistema:

12.8 Metateorema da validade do sistema dos *tableaux*

Se $\Sigma \vdash_{\mathrm{B}} \phi$, *então* $\Sigma \vDash \phi$. *Em particular, se* $\vdash_{\mathrm{B}} \phi$, *então* $\vDash \phi$.

Faremos adiante a demonstração destes dois resultados.

Seja

$(*)$ $$t_0, t_1, ..., t_n, ...$$

uma enumeração, fixada uma vez por todas, de todos os termos fechados da linguagem com as constantes novas, $\mathcal{L}_C$. Existe uma tal enumeração porque o alfabeto de $\mathcal{L}_C$ é infinito numerável, e até podem ser dados exemplos concretos de tais enumerações. (Sugere algum?)

12.9 Definição

Seja $T = \bigcup_{n=0}^{\infty} T_n$ um *tableau* (possivelmente, com hipóteses em Σ), κ um ramo em T, X uma entrada em κ, e $Y = X^{(i)}$ a i-ésima ocorrência de X em κ (contando de cima para baixo ao longo de κ).[132]

(1) Y diz-se **reduzida em** κ sse

(a) X não é de nenhuma das formas $V\forall x\phi(x)$, $F\exists x\phi(x)$ e, para algum j, T_{j+1} é obtido de T_j aplicando a regra 12.1(ii) a X e a um ramo em T_j que seja um segmento inicial de κ, ou

(b) X é da forma $V\forall x\phi(x)$ ou $F\exists x\phi(x)$, $V\phi(t_{i-1})$ é uma entrada em κ e existe uma $(j+1)$-ésima ocorrência de X em κ.

(2) T está **terminado** sse toda a ocorrência de toda a entrada em T está reduzida em todo o ramo não contraditório que a contém (e, para qualquer hipótese ϕ em Σ, $V\phi$ ocorre em todo o ramo não contraditório de T); T diz-se **não terminado**, no caso contrário.

Dizemos, no caso (1)(a), que X ocorre em κ como raiz de um *tableau* atómico.

A ideia da redução é que as fórmulas valoradas como $V\forall x\phi(x)$ tenham de ser particularizadas em cada termo fechado t_i da nossa linguagem expandida antes de podermos afirmar que terminámos com elas (por já não haver mais informação para extrair). Podemos mostrar, de seguida, que existe um *tableau* terminado (com hipóteses em Σ), qualquer que seja a entrada na raiz, construindo um *tableau* completo (noção a definir) por um procedimento sistemático (algoritmo) que reduz todas as entradas até se chegar a um *tableau* terminado. Para esse fim, convém considerar uma ordenação especial dos nós de um *tableau*, que é uma variante da conhecida ordenação lexicográfica (ou alfabética) dos nomes de uma lista telefónica. Esta ordenação, aliás, já foi utilizada implicitamente na secção relativa aos *tableaux* proposicionais (pág. 109).

12.10 Definição

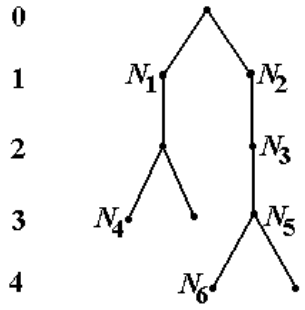
Seja T uma árvore com uma ordenação esquerda-direita dos nós em cada nível. A ordenação **lexicográfica nivelada** $\leq_{\text{ln}}$ dos nós de T é definida por:

$$N \leq_{\text{ln}} M \text{ sse } \begin{cases} \text{o nível de } \kappa \text{ em } T \text{ é menor que o nível de } M, \text{ ou } N \text{ e } M \\ \text{estão no mesmo nível e } N \text{ está à esquerda de } M. \end{cases}$$

O esquema seguinte ilustra esta ordenação numa árvore com cinco níveis (o nível 0 é o nível da raiz, como é usual):

---

[132] No sistema dos *tableaux* para a lógica proposicional podemos identificar cada entrada (fórmula valorada) com o nó onde ela ocorre, como sabemos (ver Nota 81, pág. 109), mas aqui não podemos fazer essa identificação, por razões já explicadas.



Neste exemplo tem-se, em particular:

$$N_1 <_{\text{ln}} N_2 <_{\text{ln}} N_3 <_{\text{ln}} N_5 <_{\text{ln}} N_6,$$
$$N_3 <_{\text{ln}} N_4 <_{\text{ln}} N_5 <_{\text{ln}} N_6,$$

onde, é claro, $M <_{\text{ln}} N$ significa $M \leq_{\text{ln}} N$ e $M \neq N$.

Um *tableau completo* é um *tableau* $T = \bigcup_{n=0}^{\infty} T_n$ construído de acordo com as instruções seguintes.

12.11 Algoritmo de construção de *tableaux* completos

Constrói-se (indutivamento) um *tableau completo* tendo qualquer sentença valorada como raiz, mediante o seguinte procedimento sistemático:

Etapa 0*:* começa-se com um *tableau* atómico T_0, com raiz $V\phi$ ou $F\phi$ (ϕ uma sentença de $\mathcal{L}_C$), sendo T_0 bem determinado, além disso, nos casos $\phi = \forall x\psi(x)$ ou $\phi = \exists x\psi(x)$, pela restrição de que nos casos 7a e 8b utilizamos o termo t_0 da enumeração $(*)$ acima e, nos casos 7b e 8a, utilizamos a constante adicional c_i onde i é o mínimo possível.

Etapa $n+1$*:* Suponhamos já obtido o *tableau* T_n na etapa n, que é finito e está munido da ordenação $\leq_{\text{ln}}$. Se todas as ocorrências de entradas em T_n estão reduzidas, nada mais há a fazer. No caso contrário, seja N o menor nó de T_n com respeito a $\leq_{\text{ln}}$ que contém uma entrada X não reduzida em algum ramo não contraditório κ de T_n. Há dois casos a considerar:

(a) Se X não é de nenhuma das formas $V\forall x\phi(x)$ ou $F\exists x\phi(x)$, apensa-se o *tableau* atómico com raiz X no término de todo o ramo não contraditório que contém N; e se X é de uma das formas $V\exists x\phi(x)$ ou $F\forall x\phi(x)$, utiliza-se a constante adicional c_j com j mínimo tal que c_j ainda não ocorreu no *tableau*;

(b) Se X é de uma das formas $V\forall x\phi(x)$ ou $F\exists x\phi(x)$ e N é o nó da i-ésima ($i \geq 1$) ocorrência de X em κ apensa-se

$$\begin{array}{ccc} X & & X \\ | & & | \\ V\phi(t_{i-1}) & \text{ou} & F\phi(t_{i-1}), \end{array}$$

respectivamente, no término de todo o ramo não contraditório que contém N.

Para *tableaux* com hipóteses (sentenças de $\mathcal{L}$ num conjunto dado, finito ou infinito, $\Sigma = \{\phi_1, \phi_2, ...\}$) o procedimento é análogo, apenas com as alterações seguintes para a introdução de hipóteses em etapas intercalares:

— nas etapas pares ($n = 2m$, onde $m \geq 0$) procede-se como acima, conforme o caso;

— em cada etapa ímpar ($n = 2m + 1$) apensa-se $V\phi_m$, onde $\phi_m \in \Sigma$, a todo o ramo não contraditório em T_{2m}, enquanto houver hipóteses para introduzir.

Não se dá por concluída a construção enquanto não tiverem sido introduzidas todas as hipóteses (se as houver) nos ramos não contraditórios ou houver ocorrências não reduzidas de entradas.

O resultado final da construção é o *tableau* $T = \bigcup_{n=0}^{\infty} T_n$, que se diz um *tableau completo* e que poderá ser infinito, mesmo que Σ seja finito. Mas o mais importante é que este *tableau* está terminado:

12.12 Metateorema

O tableau *completo* $T = \bigcup_{n=0}^{\infty} T_n$ *que resulta por aplicação do algoritmo 12.11 está terminado.*

Dem. Supondo primeiro que não há hipóteses, seja N o nó de uma ocorrência não reduzida de uma entrada X nalgum $T_k \subseteq T$ que está num ramo não contraditório κ do *tableau* completo T, e suponhamos que há n nós em T que estão na relação $<_{\text{ln}}$ com N; então, por definição de *tableau* completo, X já estará reduzida em κ quando construirmos T_{k+n+1}. Assim, toda a ocorrência de toda a entrada num ramo não contraditório em T está reduzida.

No caso de haver hipóteses em Σ o argumento é análogo, apenas com a diferença de envolver o dobro dos passos. O facto de introduzir a hipótese ϕ_m na etapa $2m + 1$ garante que todo a hipótese em Σ é introduzida em todo o ramo não contraditório de T.■

12.13 Exemplos

1) O *tableau* seguinte está terminado, como se pode verificar directamente, embora seja infinito. As colunas da esquerda e da direita são facultativas

(numeração e comentários):

0	$V\exists y(\neg Py \vee Qy) \wedge \forall x Px$		
1	$V\exists y(\neg Py \vee Qy)$		
2	$V\forall x Px$		1.ª oc.
3	$V\neg Pc_0 \vee Qc_0$		
4	$V\forall x Px$		2.ª oc.
5	VPc_0		tomou-se $t_0 = c_0$
6	$V\neg Pc_0$	VQc_0	
7	FPc_0	$V\forall x Px$	3.ª oc.
8	$\otimes$	VPt_1	
9		$V\forall x Px$	4.ª oc.
10		VPt_2	
$\vdots$		$\vdots$	

Note que a sentença $\exists y(\neg Py \vee Qy) \wedge \forall x Px$ é, antes de mais, uma conjunção, o que explica o *tableau* atómico com os níveis 1, 2 e 3.

Note, além disso, que o nível 5 resultou de aplicar um *tableau* atómico com raiz $V\forall x Px$ no nível 2 no término do (único) ramo que termina no nível 3, tendo sido necessário repetir aquela raiz no nível 4. A escolha de c_0 como termo de particularização é apenas por conveniência, para obter um ramo contraditório, face às entradas que precedem [mas não foi uma escolha feita de acordo com o algoritmo 12.11, excepto se, por um feliz acaso, a enumeração $(*)$ começasse realmente por c_0].

Este *tableau* não é contraditório, pois tem um ramo (infinito) não contraditório, o que significa que a sentença dada $\exists y(\neg Py \vee Qy) \wedge \forall x Px$ é compatível [como, aliás, é facil verificar semanticamente: pense-se na estrutura (M, P, Q) onde $M = P = \{1, 2\}, Q = \{1\}$].

2) O *tableau* completo e contraditório seguinte mostra que

$$\forall x\exists y\exists z\neg Pxyz \vdash_{\mathrm{B}} \forall x\exists y\neg\forall zPxyz:$$

0	F	$\forall x\exists y\neg\forall zPxyz$	✓	raiz
1	F	$\exists y\neg\forall zPc_0yz$	✓	reduz 0 (1ª oc.)
2	V	$\forall x\exists y\exists z\neg Pxyz$	✓	Hipótese (1ª)
3	F	$\exists y\neg\forall zPc_0yz$	✓	repete 1 (2ª)
4	F	$\neg\forall zPc_0t_0z$	✓	reduz 1 (1ª)
5	V	$\forall x\exists y\exists z\neg Pxyz$	✓	repete 2 (2ª)
6	V	$\exists y\exists z\neg Pt_0yz$	✓	reduz 2 (1ª)
7	F	$\exists y\neg\forall zPc_0yz$	✓	repete 3 (3ª)
8	F	$\neg\forall zPc_0t_1z$	✓	reduz 3 (1ª)
9	F	$\neg\forall zPc_0t_0z$		repete 4 (2ª)
10	V	$\forall zPc_0t_0z$		reduz 4 (1ª)
11	V	$\forall x\exists y\exists z\neg Pxyz$		repete 5 (3ª)
12	V	$\exists y\exists z\neg Pt_1yz$		reduz 5 (1ª)
13	V	$\exists y\exists z\neg Pt_0yz$		repete 6 (2ª)
14	V	$\exists z\neg Pt_0c_1z$		reduz 6 (1ª)
15	F	$\exists y\neg\forall zPc_0yz$		repete 7 (4ª)
16	F	$\neg\forall zPc_0t_2z$		reduz 7 (1ª)
17	F	$\neg\forall zPc_0t_1z$		repete 8 (2ª)
18	V	$\forall zPc_0t_1z$		reduz 8 (1ª)
		$\otimes$		

Acrescentaram-se colunas informativas à direita e fez-se uma disposição adequada à melhor compreensão da construção. Note que, por exemplo, a raiz só é reduzida no nível 1, e só então se coloca o símbolo '✓' ao lado da raiz, a hipótese só é reduzida no nível 6, etc.

Podemos agora avançar no caminho das demonstrações dos metateoremas referidos na pág. 218. Recorde-se que uma estrutura concorda com uma sentença valorada $V\phi$ sse é modelo de ϕ.

12.14 Lema

Se $T = \bigcup_{n\geq 0} T_n$ é um tableau com hipóteses num conjunto de sentenças Σ de $\mathcal{L}$ com raiz $F\phi$, então todo o modelo $\mathfrak{A}$ de $\Sigma \cup \{\phi\}$ pode-se expandir a um modelo $\mathfrak{A}'$ para $\mathcal{L}_C$ que concorda com com todas as entradas de algum ramo κ em T.

Dem. Seja $\mathfrak{A}$ um modelo de $\Sigma \cup \{\phi\}$. A expansão a considerar há-de ter interpretações para todas as novas constantes de $\mathcal{L}_C$, mas, para o efeito pretendido, só interessam as interpretações das novas constantes que ocorrem nas sentenças valoradas do *tableau* T que estão em κ, para κ conveniente.

Definimos κ e $c_{i\mathfrak{A}'}$

III.13 Teoria de Herbrand e unificação

A introdução de funções de Skolem e a consequente equicompatibilidade de fórmulas arbitrárias com fórmulas universais permite uma abordagem mais concreta, diremos mesmo, *canónica,* da questão de existência de modelos. A ideia remonta à tese de doutoramento (1930) de J. Herbrand (1930).[133]

Consideremos um conjunto Σ de sentenças universais de uma linguagem $\mathcal{L}$, com símbolos para todas as funções de Skolem já introduzidos e com, pelo menos, uma constante. Mostramos que Σ ou é incompatível, ou possui um modelo cujos elementos são os termos fechados de $\mathcal{L}$! Visto que tais termos têm interpretações em qualquer estrutura-$\mathcal{L}$, vê-se que em certo sentido um tal modelo de Σ é *minimal* entre os modelos de Σ. Recorde-se a definição indutiva de termo e a definição de termo fechado de $\mathcal{L}$ (pág. 161). Note que os termos fechados de $\mathcal{L}$ também podem ser definidos indutivamente: as constantes são termos fechados; se f é n-ário e t_1, ..., t_n são termos fechados, então $ft_1...t_n$ é termo fechado; nada mais é termo fechado. Os termos fechados também podem ser chamados os *termos base* de $\mathcal{L}$.

13.1 Definição

Chama-se **universo de Herbrand** de uma linguagem $\mathcal{L}$ como acima ao conjunto de todos termos fechados de $\mathcal{L}$. Chama-se **estrutura de Herbrand** para $\mathcal{L}$ a uma estrutura-$\mathcal{L}$ $\mathfrak{H}$ cujo universo ou domínio é o conjunto dos termos fechados de $\mathcal{L}$ e tal que, para toda a constante c de $\mathcal{L}$, $c_{\mathfrak{H}} = c$ e para todo o termo fechado $ft_1...t_n$ de $\mathcal{L}$, $f_{\mathfrak{H}}(t_1, ..., t_n) = ft_1...t_n$. Se Σ é um conjunto de sentenças de $\mathcal{L}$, chama-se **modelo de Herbrand** de Σ a toda a estrutura de Herbrand para $\mathcal{L}$ que é modelo de Σ.

Observe-se que nada é exigido quanto à interpretação dos símbolos predicativos de $\mathcal{L}$ (se alguns houver), pelo que, em geral, haverá muitas estruturas e modelos de Herbrand que só diferem entre si na interpretação dos símbolos predicativos.

13.2 Exemplo

Suponhamos que $\mathcal{L} = \{P, c, d, f, g\}$ com P binário, f unário e g binário. O universo de Herbrand para $\mathcal{L}$ tem como elementos, entre outros:

$$c, d, fc, fd, ffc, ffd, gcc, gcd, gfcfd, ...$$

No que segue, se $\phi(a_1,...,a_n)$ é uma fórmula com parâmetros como exibidos, chamamos particularização de ϕ a termos base ao resultado de substituir cada a_i em ϕ por um termo base t_i: $\phi(t_1/a_1, ..., t_n/a_n)$.

---

[133] O Cap. V da tese, que contém os resultados historicamente mais importantes e pertinentes para esta secção foram traduzidos (com correcções e notas) em inglês: "Investigations in proof theory: The properties of true propositions", em VAN HEIJENOORT, PP. 525-581.

13.3 Metateorema de Herbrand

Seja $\Sigma = \{\phi_i(a_1, ..., a_{n_i}) : i \in I\}$ *um conjunto (finito ou infinito) de fórmulas de uma linguagem* $\mathcal{L}$*, com parâmetros como exibidos. Então, ou*

(i) Σ *possui um modelo de Herbrand, ou*

(ii) Σ *é incompatível e, em particular, existe um número finito de particularizações a termos base de fórmulas de* Σ *cuja conjunção é incompatível.*

Em virtude das leis de De Morgan, a parte (ii) equivale a dizer que *há um número finito de particularizações a termos base de negações de fórmulas de* Σ *cuja disjunção é válida.*

Dem. Seja Σ' o conjunto de todas as particularizações a termos base de $\mathcal{L}$ de fórmulas de Σ, e construamos o *tableau* completo (12.11) com hipóteses em Σ' e raiz $F\phi \wedge \neg\phi$, onde ϕ é uma sentença qualquer. Há dois resultados possíveis:

(1) Há um ramo (possivelmente infinito) não contraditório no *tableau*

III.16 Indecidibilidade na lógica elementar

Contrariamente ao que sucede na lógica proposicional, os *problemas de decisão* para a compatibilidade e para a validade na lógica de 1.ª ordem são algoritmicamente insolúveis. Quer dizer, não existe nenhum algoritmo que permita decidir, para qualquer fórmula dada, se ela é ou não compatível, ou se ela é ou não válida.

III.17 Exercícios e Complementos

§III.1-III.5

3.1 Efectue todas as derivações (no sistema **DNQ**) indicadas no texto, exibindo as dependências de hipóteses.

3.2 Mostre que:

(a) $\forall x(Px \rightarrow Qx) \vdash \forall xPx \rightarrow \forall xQx.$

(b) $\forall x(Px \rightarrow Qx) \vdash \exists xPx \rightarrow \exists xQx.$

(c) $\forall x(Px \wedge Qx) \dashv\vdash \forall xPx \wedge \forall xQx.$

(d) $\exists x(Px \vee Qx) \dashv\vdash \exists xPx \vee \exists xQx.$

(e) $\exists x(Px \wedge Qx) \vdash \exists xPx \wedge \exists xQx.$

(f) $\forall xPx \vee \forall xQx \vdash \forall x(Px \vee Qx).$[134]

3.3 Mostre, por meio de contra-exemplos, que não se pode substituir ' $\vdash$ ' por ' $\dashv$ ' nas alíneas (a), (b), (e) e (f) acima.

3.4 Mostre que as sentenças seguintes são interderiváveis:

$$\exists x(Px \wedge \forall y(Py \rightarrow x \doteq y)),\ \exists xPx \wedge \forall xy(Px \wedge Py \rightarrow x \doteq y).$$

3.5 (a) Simbolize, em linguagens elementares apropriadas, os argumentos seguintes relativos ao domínio das pessoas:

(1) «Os únicos candidatos são Alberto e João. Alberto e João são idiotas. Portanto, todo o candidato é idiota.»;

(2) «Todo o barbeiro faz a barba a todas as pessoas que não se barbeiam a si próprias. Nenhum barbeiro faz a barba às pessoas que se barbeiam a si próprias. Portanto, não existem barbeiros.»

(b) Mostre (informalmente) que os argumentos são válidos.

---

[134] No lugar de Pa e Qa podem estar fórmulas arbitrárias, somente com a, $\phi(a)$ e $\psi(a)$, respectivamente, mas nas deduções há que ter em conta a possibilidade de ocorrências de parâmetros nessas fórmulas.

(c) Para cada argumento, deduza a conclusão a partir das premissas no sistema **DNQ**.

(d) Simbolize numa linguagem elementar com igualdade e com um símbolo predicativo unário P:

(1) Há, quando muito, dois objectos com a propriedade P [abreviatura: $\exists^{\leq 2} x Px$];

(2) Há, pelo menos, três objectos com a propriedade P [abreviatura: $\exists^{\geq 3} x\ Px$];

(3) Há, pelo menos, três objectos [$\exists^{\geq 3} x(x \doteq x)$, ou simplesmente ($\exists^{\geq 3}$)]

(4) Há exactamente três objectos [$\exists^{3} x(x \doteq x)$, ou simplesmente ($\exists^{3}$)];

(5) Há exactamente três objectos com a propriedade P [$\exists^{3} x\ Px$].

3.6 Designa-se por Par(t) o conjunto dos parâmetros que ocorrem no termo t, e por Par(ϕ) o conjunto dos parâmetros que ocorrem na fórmula ϕ.

(a) Dê uma definição indutiva de Par(ϕ);

(b) explique, utilizando as regras de formação de termos e de fórmulas, como foi construida a fórmula da linguagem $\mathcal{L} = \{P, Q, f, g, h, c\}$:

$$(\exists x Pxfa \vee \neg \forall y Qygchb),$$

onde P e Q são binários, f e h são unários e g é binário.

(c) Diga quais são os parâmetros e os termos da fórmula na alínea anterior.

§III.6-III.10

3.7 Recorde as diversas espécies de relações binárias definidas no exercício 1.5.

(a) Faça demonstrações informais, primeiro, e depois construa deduções no sistema **DNQ**, dos seguintes factos:

(i) R é anti-simétrica $\dashv\vdash \forall xy(x \neq y \wedge Rxy \rightarrow \neg Ryx)$;

(ii) R é não simétrica $\dashv\vdash \exists xy(Rxy\ \wedge\ \neg Ryx)$;

(iii) R é simétrica e assimétrica $\dashv\vdash$ R é vazia [a *assimetria* formula-se assim: $\forall xy(Rxy \rightarrow \neg Ryx)$];

(iv) R é irreflexiva e transitiva $\vdash$ R é assimétrica.

(b) Dê exemplos de estruturas (M, R) em que R é uma relação binária em M, com as propriedades seguintes:

(i) Nem simétrica nem anti-simétrica;

(ii) Intransitiva e simétrica [a *intransitividade* formula-se assim:

$$\forall xyz\,(Rxy \wedge Ryz \rightarrow \neg Rxz)];$$

(iii) Intransitiva, mas não simétrica;

(iv) Nem transitiva nem intransitiva;

(v) Nem reflexiva nem irreflexiva.

3.8 Uma ordem parcial num conjunto M é uma relação binária $\leq$ em M com as propriedades seguintes, também chamadas os *axiomas das ordens parciais*, formulados na linguagem $\mathcal{L}_{\text{or}}$ com um único símbolo predicativo binário $\leq$, chamada *linguagem das ordens:*

OP_1. $\forall x\ (x \leq x)$ [$\leq$ é *reflexiva*];

OP_2. $\forall xy(x \leq y \wedge y \leq x \to x \doteq y)$ [$\leq$ é *anti-simétrica*];

OP_3. $\forall xyz(x \leq y \wedge y \leq z \to x \leq z)$ [$\leq$ é *transitiva*].

Um **conjunto parcialmente ordenado** é um modelo $(M, \leq)$ destes axiomas, e a *teoria das ordens parciais* é a teoria $\mathbf{T}_{\text{op}}$ na linguagem $\mathcal{L}_{\text{or}}$, cujos axiomas são OP_1-OP_3. Define-se o símbolo de **ordem estrita** $<$ por

Def($<$) $\qquad\qquad \forall xy(x < y \leftrightarrow x \leq y \wedge x \neq y)$.

(a) Deduza (no sistema **DNQ**) os seguintes teoremas de $\mathbf{T}_{\text{op}}$:

T_1. $\forall x\, \neg(x < x)$ [abreviadamente, $\forall x\, x \not< x$: $<$ é *irreflexiva*].

T_2. $\forall xyz(x < y \wedge y < z \to x < z)$ [$<$ é *transitiva*].

Seja agora $\mathcal{L}_{\text{oe}}$ a *linguagem das ordens estritas*, com um único símbolo predicativo binário $<$, e $\mathbf{T}_{\text{ope}}$ a teoria cujos axiomas são exactamente as sentenças OPE_1=T_1, OPE_2=T_2 do exercício anterior. Define-se $\leq$ por

Def($\leq$) $\qquad\qquad \forall xy(x \leq y \leftrightarrow x < y \vee x \doteq y)$.

(b) Deduza, como teoremas de $\mathbf{T}_{\text{ope}}$, as sentenças OP_1-OP_3.

3.9 A *teoria das ordens totais*, $\mathbf{T}_{\text{ot}}$, é a teoria na linguagem $\mathcal{L}_{\text{or}}$ cujos axiomas são $\text{OT}_1 = \text{OP}_1$, $\text{OT}_2 = \text{OP}_2$, $\text{OT}_3 = \text{OP}_3$ e ainda o axioma

OT_4. $\forall xy(x \leq y \vee y \leq x)$ [$\leq$ é *dicotómica*].

A teoria das *ordens totais estritas* é a teoria $\mathbf{T}_{\text{ote}}$ na linguagem $\mathcal{L}_{\text{oe}}$ cujos axiomas são $\text{OTE}_1 = \text{OPE}_1$, $\text{OTE}_2 = \text{OPE}_2$ e ainda o axioma

OTE_3. $\forall xy(x \neq y \to x < y \vee y < x)$ [$<$ é *conexa*] ou, equivalentemente, o axioma

OTE_3'. $\forall xy(x < y \vee x \doteq y \vee y < x)$ [$<$ é *tricotómica (fraca)*[135]].

(a) Tendo em conta a definição de $<$ acima, deduza OTE_3 em $\mathbf{T}_{\text{ot}}$.

---

[135] A *tricotomia forte* é a propriedade de, para quaisquer a, b, ter lugar uma e uma só das condições $a < b$, $a = b$, $a < b$, e é consequência das propriedades que definem as ordens totais (ou ordens totais estritas) — exercício!

(b) Tendo em conta a definição de $\leq$ acima, deduza OT_4 em $\mathbf{T}_{\mathrm{ote}}$.

3.10 Mostre que a sentença $\forall x \exists y Rxy \rightarrow \exists y \forall x Rxy$ é 1-válida mas não é 2-válida.

3.11 Mostre, por meio de contra-exemplos, que as sentenças seguintes não são universalmente válidas:

(a) $\exists xy Rxy \rightarrow \exists x Rxx$; (b) $\exists x Px \wedge \exists x Qx \rightarrow \exists x(Px \wedge Qx)$.

3.12 Mostre, construindo uma tabela, que a sentença $\forall x Px \rightarrow Pc$ é 2-válida e argumente, abstractamente, para mostrar que ela é universalmente válida.

3.13 Seja $\mathcal{L}$ uma linguagem com um símbolo predicativo unário P, um símbolo funcional binário f e uma constante c, $\mathfrak{M} = (M, P, f, c)$ uma estrutura para $\mathcal{L}$.

(a) Exprima por sentenças de $\mathcal{L}$ que:

(i) P é fechado para f; (ii) f é injectiva; (iii) f não é sobrejectiva.

(b) Dê um exemplo de uma estrutura $\mathfrak{M}$ tal que $P \neq M$, $c \in P$ e $\mathfrak{M}$ satisfaça as sentenças (i) e (ii) da alínea anterior.

(c) Descreva o conjunto dos termos fechados (sem parâmetros) de $\mathcal{L}$.

(d) Prove directamente (isto é, sem invocar o metateorema de isomorfismo) que se $h : \mathfrak{M}_1 \simeq \mathfrak{M}_2$ é um isomorfismo e $\mathfrak{M}_1$ tem a propriedade expressa pela sentença (i) acima, então $\mathfrak{M}_2$ possui também esta propriedade.

(e) A sentença que exprime a propriedade (i) acima é 2-válida? Justifique a resposta.

3.14 Mostre, no sistema **DNQ**, que

(a) $\vdash \exists x(Px \vee Qx) \rightarrow (\forall x \neg Px \rightarrow \exists x Qx)$;

(b) $\forall x(Px \rightarrow \exists y Qxy), \neg \exists x Qxx \vdash Pa \rightarrow \exists y(Qay \wedge a \neq y)$.

3.15 Uma teoria **T** diz-se **completa** sse para qualquer sentença (sem parâmetros) ϕ, $\mathbf{T} \vdash \phi$ ou $\mathbf{T} \vdash \neg\phi$. Prove que são equivalentes, para **T** compatível:

(1) **T** é completa;

(2) quaisquer dois modelos de **T** satisfazem exactamente as mesmas sentenças (sem parâmetros) da linguagem de **T** [*Nota.* Dois modelos $\mathfrak{M}$ e $\mathfrak{M}'$ nestas condições dizem-se **elementarmente equivalentes**, e escreve-se $\mathfrak{M} \equiv \mathfrak{M}'$.]

(3) $\mathbf{T} = \mathrm{Tr}(\mathfrak{M})$ para algum modelo $\mathfrak{M}$ de **T**.

3.16 A linguagem da aritmética elementar[136] $\mathcal{L}_{\mathrm{ar}}$, tem dois símbolos funcionais binários $+$ (adição), $\times$ (multiplicação), um símbolo funcional unário $'$

[136] A escolha desta linguagem é meramente acidental, para o fim em vista. No entanto, ela é uma linguagem bastante importante em Lógica Matemática e em questões de Fundamentos, muito embora, do ponto de vista estritamente matemático, seja mais usual considerar a

(sucessor), e uma constante 0 (zero). Escrevemos xy como abreviatura de $x \times y$. Os termos

$$0,\ 0',\ 0'',\ 0''',\ ...$$

são chamados **numerais**, e é costume designar 0, $0'$, $0''$, $0'''$, ... por $\overline{1}$, $\overline{2}$, $\overline{3}$, ..., respectivamente. A estrutura

$$\mathfrak{N} = (\mathbb{N},\ +\ ,\ \times\ ,'\ , 0)$$

é chamada a **estrutura *standard*** para $\mathcal{L}_{\text{ar}}$. Considerando a atribuição em $\mathfrak{N}$

$$\alpha = (\langle 1, 3, 2, 1, 3, ...\rangle, \langle 2, 1, 3, 2, 1, ...\rangle),$$

determine em $(\mathfrak{N}, \alpha)$ o valor do termo $0' + \alpha_2$ e o valor lógico da sentença aberta

$$\exists x(x + a_1 \doteq 0' + a_2).$$

3.17 A *teoria elementar dos grupos*, $\mathbf{T}_{\text{gr}}$, em notação aditiva, é a teoria na linguagem $\mathcal{L}_{\text{gr}}$ (símbolo operacional binário $+$, constante 0) com axiomas:

G_1. $\forall x\, y\, z\, (x + (y + z) \doteq (x + y) + z)$ [*associatividade de* $+$].

G_2. $\forall x\, (x + 0 \doteq x)$ [0 *é elemento neutro à direita*].

G_3. $\forall x\, \exists y\, (x + y \doteq 0)$ [*Todo o elemento tem oposto à direita*].[137]

Juntando a estes o axioma seguinte, obtém-se a *teoria elementar dos grupos abelianos* (ou *comutativos*), $\mathbf{T}_{\text{grab}}$:

G_4. $\forall x\, y\, (x + y \doteq y + x)$.

Finalmente, a *teoria elementar dos grupos ordenados*, $\mathbf{T}_{\text{gror}}$, é a teoria na linguagem $\mathcal{L}_{\text{gror}}$ cujos axiomas são G_1-G_4, OT_1-OT_3 e ainda o axioma seguinte, chamado *axioma de compatibilidade* (ou de *monotonia*):

GO. $\forall x\, y\, z\, (x < y \rightarrow x + z < y + z)$.

(a) Demonstre, informalmente, os seguintes teoremas[138] de $\mathbf{T}_{\text{gr}}$:

T_1. $\forall x\, y\, z\, (x \doteq y \rightarrow x + z \doteq y + z)$.

T_2. $\forall x\, y\, z (x \doteq y \rightarrow z + x \doteq z + y)$.

T_3. $\forall x\, y\, z (x + z \doteq y + z \rightarrow x \doteq y)$ [*lei do corte à direita*].

(mais forte) aritmética conjuntista (isto é, «mergulhada» na teoria dos conjuntos). V. Cap. IV adiante.

[137] Há outras axiomáticas diferentes para esta teoria, quer por escolha de axiomas, quer por escolha de linguagem, quer por ambas as coisas, mas todas elas «equivalentes» em certo sentido.

[138] Na demonstração do teorema T_n, pode usar os teoremas T_m com $1 \leq m < n$.

T_4. $\forall x \exists y\,(x + y \doteq 0 \wedge y + x \doteq 0)$ [*todo o elemento tem oposto à esquerda:* um oposto à direita também é oposto à esquerda].

T_5. $\forall x\,(0 + x \doteq x)$ [0 é *neutro à esquerda*].

T_6. *Lei do corte à esquerda.*

T_7. $\forall x \exists^1 y\,(x + y \doteq 0)$ [*unicidade do oposto à direita*].

Este último teorema justifica a seguinte definição:

Def(–) $\qquad\qquad \forall x\,(x + (-x) \doteq 0).$

O elemento $-x$ tal que $x + (-x) \doteq 0$ é chamado o **simétrico** de x[139].

T_8. $\forall x\,((-x) + x \doteq 0)$.

(b) Um **grupo** (**grupo abeliano**, **grupo ordenado**) é um modelo de $\mathbf{T}_{\text{gr}}$ ($\mathbf{T}_{\text{grab}}$, $\mathbf{T}_{\text{gror}}$, respectivamente). Um grupo é *finito* ou *infinito* conforme o conjunto suporte é finito ou infinito, respectivamente.

Construa todos os grupos com suporte $G = \{0, a, b, c\}$ tendo 0 como elemento neutro. Quais deles são comutativos? E quais são isomorfos?

(c) Reportando-se à demonstração do corolário 2 do metateorema da compacidade, mostre que

(i) a operação $(\overline{m}, \overline{n}) \mapsto \overline{m + n}$ está bem definida, isto é, só depende de $\overline{m}$ e $\overline{n}$ e não dos representantes m, n: se $\overline{m} = \overline{j}$ e $\overline{n} = \overline{k}$, então $\overline{m + n} = \overline{j + k}$;

(ii) $(\mathbb{Z}_p,\ +_p, \overline{0})$ é, de facto, um grupo comutativo.

(d) Mostre que $\mathbf{T}_{\text{gr}} = \text{Tr}(\mathcal{G})$, onde $\mathcal{G}$ é a classe dos grupos.

(e) Mostre (sem utilizar o teorema de isomorfismo) que se dois grupos são isomorfos e um é comutativo, então o outro também é.

3.18 Mostre, por compacidade, que a classe dos grupos infinitos não é finitamente axiomatizável na linguagem dos grupos. [*Sugestão:* suponha que existia um sistema finito de axiomas na linguagem dos grupos cujos modelos são exactamente os grupos infinitos, digamos $\Sigma = \{\phi_1, ..., \phi_n\}$. Seja $\phi = \phi_1 \wedge ... \wedge \phi_n$, $\Sigma' = \{\text{G}_1, \text{G}_2, \text{G}_3, \neg\phi\}$. Mostre que Σ' tem modelos finitos arbitrariamente grandes.]

3.19 Demonstre o lema que antecede o metateorema do isomorfismo e complete a demonstração deste.

---

[139] Quando se utiliza a notação multiplicativa, o oposto de um elemento a é habitualmente chamado o seu **inverso**, e denota-se a^{-1}.

***3.20** (a) Mostre que todo o grupo abeliano $(G, +, 0)$ pode ser expandido a um anel comutativo. [*Sugestão:* defina $a * b = 0$, para todo a, $b \in G$, sendo $*$ a multiplicação no anel .]

(b) Seja $\mathbf{T}_{\text{an}}$ a teoria dos anéis (axiomas usuais na linguagem $\mathcal{L}_{\text{an}}$ com primitivos $+$, $\cdot$, 0). Mostre que $\cdot$ não é definível em $\mathbf{T}_{\text{an}}$.

***3.21** Seja $\mathcal{L}_{\text{tc}}$ a linguagem com um único símbolo predicativo binário, $\in$. Chamemos **conjuntos** às variáveis x, y, z, ... Uma fórmula atómica da forma $\in st$ escreve-se $s \in t$ e lê-se «s é *elemento* (ou *membro*) de t»; $\neg(s \in t)$ abrevia-se $s \notin t$. Define-se o símbolo predicativo binário $\subseteq$ por

Def($\subseteq$) $\qquad \forall xy(x \subseteq y \leftrightarrow \forall z(z \in x \rightarrow z \in y))$.

$s \subseteq t$ lê-se «s é *subconjunto* de t», ou «s *está contido em* t», ou «s é uma *parte* de t».

Seja $\mathbf{T}_{\text{fin}}$ a teoria cujos axiomas são:

A_1. $\forall xy(\forall z(z \in x \leftrightarrow z \in y) \rightarrow x \doteq y)$ [*extensionalidade*].

A_2. $\forall xy \exists z \forall u(u \in z \leftrightarrow u \doteq x \vee u \doteq y)$ [*pares não ordenados*].

A_3. $\exists x \forall y\ y \notin x$ [*conjunto vazio*].

A_4. $\forall xy \exists z \forall u(u \in z \leftrightarrow u \in x \vee u \in y)$ [*união finita*].

A_5. $\forall xy \exists z \forall u(u \in z \leftrightarrow u \in x \wedge u \in y)$ [*intersecção finita*].

A_6. $\forall xy \exists z \forall u(u \in z \leftrightarrow u \in x \wedge u \notin y)$ [*complemento relativo*].

Os últimos axiomas a enunciar requerem algumas definições e observações prévias. Entretanto:

(a) Simbolize na linguagem $\mathcal{L}_{\text{tc}}$ as sentenças:

(i) Existe um conjunto ao qual pertencem todos os conjuntos;

(ii) Dois conjuntos iguais têm os mesmos elementos.

(b) Demonstre, informalmente, os seguintes teoremas de $\mathbf{T}_{\text{fin}}$:

T_1. $\forall xy(x \doteq y \rightarrow \forall z(z \in x \leftrightarrow z \in y))$.

T_2. $\forall xy \exists^1 z \forall u(u \in z \leftrightarrow u \doteq x \vee u \doteq y)$.

Def($\{\ ,\ \}$) $\qquad \forall xyu(u \in \{x, y\} \leftrightarrow u \doteq x \vee u \doteq y)$.

Define-se ainda $\{x\} \doteq \{x, x\}$ [*singular de* x].

T_3. $\exists^1 x \forall y\ y \notin x$.

T_4. $\forall xy \exists^1 z \forall u(u \in z \leftrightarrow u \in x \vee u \in y)$.

T_5. $\forall xy \exists^1 z \forall u(u \in z \leftrightarrow u \in x \wedge u \in y)$.

T_6. $\forall xy\exists^1 z\forall u(u \in z \leftrightarrow u \in x \wedge u \notin y)$.

(c) Defina a constante $\emptyset$, e as operações $\cup$, $\cap$, $-$ entre conjuntos.

Define-se ainda $\mathcal{S}x \doteq x \cup \{x\}$ [*sucessor de* x], $(x, y) \doteq \{\{x\}, \{x, y\}\}$ [*par ordenado com* 1ª componente x e 2ª componente y].

(d) Formule e deduza leis associativas, comutativas, distributivas, idempotentes, de De Morgan, etc., para as operações conjuntistas $\cup$, $\cap$, $-$ (complementação relativa, também designada por $\setminus$).

(e) Prove que $\forall xyuv\,((x, y) \doteq (u, v) \leftrightarrow x \doteq u \wedge y \doteq v)$.

A teoria $\mathbf{T}_{\text{fin}}$ é (uma versão de) a *teoria dos conjuntos finitos* [ver (h)] e constitui uma formalização possível da teoria elementar dos números (no Cap. IV veremos uma outra) numa linguagem somente com o símbolo predicativo $\in$. Mostramos, apenas, como se definem os números naturais nesta teoria.

Os **numerais** (conjuntistas) são os conjuntos

$$0 \doteq \emptyset,\ 1 \doteq \mathcal{S}0 \doteq \{\emptyset\} \doteq \{0\},\ 2 \doteq \mathcal{S}1 \doteq \{\emptyset, \{\emptyset\}\} \doteq \{0, 1\},\ \text{etc.},$$

sendo cada um deles o conjunto dos «precedentes» no sentido de $\in$, mas não há nenhuma razão para supor que a colecção intuitiva dos numerais constitui (é) um conjunto. No entanto, podemos definir o conceito de *número natural* nesta teoria: «a é um número natural» abrevia-se $N(a)$, e a definição é

Def(N) $$\forall x\,(N(x) \leftrightarrow \mathit{Tric}(x) \wedge \mathit{Tran}(x)),$$

onde $\mathit{Tric}(a)$ abrevia $\forall yz\,(y \in a \wedge z \in a \rightarrow y \in z \vee y \doteq z \vee z \in y)$ [$\in$ *é tricotómica em* a] e $\mathit{Tran}(a)$ abrevia $\forall y(y \in a \rightarrow y \subseteq a)$ [a é *transitivo*].

Definimos ainda

Def($<$) $$\forall xy(x < y :\leftrightarrow N(x) \wedge N(y) \wedge x \in y).$$

(f) Prove que o sucessor de um número natural é um número natural, isto é, que $\forall x(N(x) \rightarrow N(\mathcal{S}x))$.

(g) Prove que para todo o número natural a, $<$ é transitiva em a, e que todo o elemento de um número natural é um número natural.

Abreviemos $\phi(a, b_1, ..., b_n)$ em $\phi(a, \overline{b})$ e $\forall y_1 ... y_n\,\phi$ em $\forall \overline{y}\,\phi$ no que se segue. Admitimos aqui a possibilidade $n = 0$, caso em que somente a está presente. Para cada fórmula $\phi(a, \overline{b})$ com parâmetros como indicados, a sentença seguinte é um *axioma de indução:*

A_ϕ. $$\forall \overline{y}\big(\phi(0, \overline{y}) \wedge \forall x(N(x) \wedge \phi(x, \overline{y}) \rightarrow \phi(\mathcal{S}x, \overline{y})) \rightarrow \forall x(N(x) \rightarrow \phi(x, \overline{y}))\big).$$

São estes axiomas que permitem desenvolver a parte propriamente aritmética da teoria, mas não faremos aqui esse desenvolvimento.

(h) Seja $M_0 = \emptyset$, e, para cada natural n, seja

$$M_{n+1} = M_n \cup \mathcal{P}(M_n),$$

onde $\mathcal{P}(M_n)$ é o conjunto dos subconjuntos de M_n. Seja ainda $M = \bigcup_{n=0}^{\infty} M_n$ o conjunto união de todos os M_n, isto é, para qualquer x, $x \in M$ sse $x \in M_n$ para algum n. Note que $M_n \subseteq M_{n+1}$, para todo n, e que cada M_n, tal como M, é um conjunto de conjuntos finitos.

Prove que $(M, \in)$ é um modelo dos axiomas A_1-A_6.[140]

§III.11

3.22 Dê contra-exemplos para as não equivalências da pág. 204:

$$\forall x\phi \vee \forall x\psi \not\sim \forall x(\phi \vee \psi), \quad \exists x\phi \wedge \exists x\psi \not\sim \exists x(\phi \vee \psi).$$

3.23 Mostre que, dadas $\phi(a, ...)$ e ψ onde não ocorre a,

(a) $\forall x(\phi \rightarrow \psi) \sim (\exists x\phi \rightarrow \psi)$; (b) $\forall x(\phi \rightarrow \psi) \sim (\phi \rightarrow \forall x\psi)$;

(c) $\exists x(\phi \rightarrow \psi) \sim (\forall x\phi \rightarrow \psi)$; (d) $\exists x(\phi \rightarrow \psi) \sim (\phi \rightarrow \exists x\psi)$.

3.24 Sendo R um símbolo relacional binário, mostre que

$$\exists y\forall x Rxy \vDash \forall x\exists y Rxy,$$

mas

$$\forall x\exists y Rxy \nvDash \exists y\forall x Rxy.$$

3.25 Converta na FNR as fórmulas

(a) $\forall x\exists y Pxfy \wedge \forall y(Qxy \vee Rz)$;

(b) $(\forall x\exists y Pxgyfx \vee \neg Qz) \vee \neg\forall x Rxy$.

3.26 Skolemize de $\forall x\exists y\forall z\exists w(\neg P(a, w) \vee Q(f(x), y))$.

3.27 Obtenha uma equivalente na FNR e skolemize a fórmula

$$\forall x\exists y(P(x, f(y), a) \vee \neg\forall x Qx) \wedge \neg\forall x\exists z\neg R(g(x, z), z).$$

---

[140] Esta construção mostra que o *axioma do infinito*

$$\exists x\,(\emptyset \in x \wedge \forall y\,(y \in x \rightarrow \mathcal{S}y \in x))$$

não é consequência dos axiomas A_1-A_6. V. secção 5.4 para uma descrição informal da teoria axiomática dos conjuntos.

3.28 Aplique os procedimentos da pág. 211 à fórmula

$$\neg\exists x(Pxa \vee \forall yQ(b, fy)) \vee \forall yP(g(b, y), a)),$$

e obtenha uma cláusula como conjunto.

§III.12

3.29 Nas alíneas que seguem estão fórmulas fechadas ou sentenças (de alguma linguagem de 1.ª ordem $\mathcal{L}$ que não interessa especificar) para derivar no sistema dos *tableaux*, onde $\phi(x) = \phi(x/a)$, $\psi(x) = \psi(x/a)$ para algum parâmetro a, e θ uma sentença (fórmula sem parâmetros).

(a) $\exists x(\phi(x) \vee \psi(x)) \longleftrightarrow \exists x\phi(x) \vee \exists x\psi(x)$;

(b) $\forall x(\phi(x) \wedge \psi(x)) \longleftrightarrow \forall x\phi(x) \wedge \forall x\psi(x)$;

(c) $\theta \vee \forall x\phi(x) \rightarrow \forall x(\theta \vee \phi(x))$;

(d) $\theta \wedge \exists x\phi(x) \rightarrow \exists x(\theta \wedge \phi(x))$;

(e) $\exists x(\theta \rightarrow \phi(x)) \rightarrow (\theta \rightarrow \exists x\psi(x))$;

(f) $\exists x(\theta \wedge \phi(x)) \rightarrow (\theta \wedge \exists x\phi(x))$;

(g) $\neg\exists x\phi(x) \rightarrow \forall x\neg\phi(x)$;

(h) $\forall x\neg\phi(x) \rightarrow \neg\exists x\phi(x)$;

(i) $\exists x\neg\phi(x) \rightarrow \neg\forall x\phi(x)$;

(j) $\exists x(\phi(x) \rightarrow \theta) \rightarrow (\forall x\phi(x) \rightarrow \theta)$;

(k) $(\exists x\phi(x) \rightarrow \theta) \rightarrow \forall x(\phi(x) \rightarrow \theta)$.

Capítulo IV

ARITMÉTICA DE PEANO

IV.1 Linguagem e axiomas

Já anteriormente definimos a linguagem da aritmética, $\mathcal{L}_{\text{ar}}$ (exercício 3.16), com símbolos não lógicos primitivos $+, \times, ', 0$, e os numerais $\overline{1}, \overline{2}, \ldots$ Na verdade, o símbolo $<$ pode ser definido a partir de $+$, 0 e demonstradas as propriedades pertinentes, mas preferimos juntá-lo como primitivo para, assim, facilitar o desenvolvimento da aritmética elementar, pagando embora o preço de um maior número de axiomas. Analogamente, é possível, após um considerável desenvolvimento da teoria, justificar a introdução de um símbolo operacional binário $\uparrow$ ou exp (de *exponenciação*) e demonstrar as propriedades pertinentes, mas encurtamos caminho [para abreviar o tratamento da divisibilidade (IV.5)] admitindo desde logo exp (ou seja, $\uparrow$) entre os primitivos, e admitindo alguns axiomas a seu respeito.

Portanto, considera-se a linguagem da aritmética $\mathcal{L}_{\text{ar}}$, daqui em diante, como tendo os seguintes símbolos específicos primitivos:

$$+, \times, \uparrow, ', <, 0$$

A **aritmética elementar** (ou **aritmética de Peano**, como já foi dito) é a teoria **AP** na linguagem $\mathcal{L}_{\text{ar}}$, cujos axiomas indicamos mais adiante. De momento, porém, faremos algumas convenções e enunciaremos alguns teoremas lógicos a respeito da igualdade e dos símbolos primitivos de $\mathcal{L}_{\text{ar}}$, todos eles fáceis de deduzir.

Convenções de escrita 1. Usaremos as letras *r*, *s*, *t*, ... (possivelmente com índices) para termos arbitrários de $\mathcal{L}_{\text{ar}}$, e ϕ, ψ, θ, ... para fórmulas de $\mathcal{L}_{\text{ar}}$, como vimos fazendo.

2. Usaremos as seguintes abreviaturas:

Expressão	*Abreviatura*
$\neg(s = t)$	$s \neq t$
$\neg(s < t)$	$s \not< t$
$s < t \vee s = t$	$s \leq t$
$\forall x(x < y \rightarrow \phi)$	$\forall x < y\ \phi$
$\exists x(x < y \wedge \phi)$	$\exists x < y\ \phi$

$+\,st$	$(s+t)$, ou $s+t$
$\times\, st$	$(s\times t)$, $s\times t$, $(s\cdot t)$, $s\cdot t$, (st) ou st
$s\uparrow t$	s^t,

e analogamente com $\leq$ no lugar de $<$ nas definições de $\forall x\leq y\,\phi$, $\exists x\leq y\,\phi$.

3. As expressões $t>s$, $t\geq s$ consideram-se sinónimas de $s<t$, $s\leq t$, respectivamente.

Teoremas lógicos da igualdade. Utilizaremos amiúde, sem menção especial, os seguintes teoremas lógicos da igualdade na linguagem $\mathcal{L}_{\text{ar}}$, onde r, s, t são termos fechados quaisquer [ver (130) e (131), p. 170]:

E_1. $r=s\to r+t=s+t$.

E_2. $r=s\to t+r=t+s$.

E_3. $r=s\to rt=st$.

E_4. $r=s\to tr=ts$.

E_5. $r=s\to t^r=t^s$.

E_6. $r=s\to r^t=s^t$.

E_7. $r=s\to r'=s'$.

E_8. $r=s\to(r<t\ \Leftrightarrow\ s<t)$.

E_9. $r=s\to(t<r\ \Leftrightarrow\ t<s)$.

Utilizando E_1-E_7, pode-se justificar a seguinte regra derivada, que corresponde à regra de substituibilidade ($\doteq^-$) para termos:

$$(=^*)\qquad \frac{r=s}{t=t^*}$$

onde r, s, t são termos fechados e t^* é o resultado de substituir *uma* ocorrência de r em t por s. Se r não ocorre em t, t^* é o próprio t, mas neste caso convencionamos que a regra se identifica com ($\doteq^+$).

A justificação da regra ($=^*$) (supondo que r tem, pelo menos, uma ocorrência em t, caso contrário, não há nada a demonstrar) consiste em mostrar que

$$(*)\qquad r=s\vdash t=t^*,$$

e faz-se por indução matemática no número n de operadores $+$, $\times$, $\uparrow$, $'$ que se aplicam a r na ocorrência dada de r em t, chamado *ordem* dessa ocorrência. Se $n=0$ é imediato, pois neste caso t é r e t^* é s, e $r=s\vdash r=s$ trivialmente. Admitindo ($*$) para $n=k$, suponhamos $n=k+1$; ora t é necessariamente de uma das formas $u+v$, $v+u$, uv, vu, u^v, v^u, u', em que a ordem da ocorrência de r, digamos em u, é k. Por hipótese de indução, $r=s\vdash u=u^*$, e pela propriedade

E_i correspondente tem-se $u = u^* \vdash t = t^*$, donde facilmente se obtém, por transitividade de $=$, $r = s \vdash t = t^*$.[141]

Por exemplo, se t é o termo $ab' + b''$, r é b', s é $0 + c$, e decidimos substituir a segunda ocorrência (contando da esquerda para a direita) de r por s em t, então t^* é o termo $ab' + (0 + c)'$.

Observe-se que a notação "t^*" é ambígua, mas na prática a regra (=*) aplica-se sem qualquer problema.

Enunciemos então alguns axiomas de **AP**. Os primeiros oito axiomas formalizam propriedades básicas de $+$, $\times$, $\uparrow$, $'$, 0. Outras propriedades terão de ser deduzidas delas, o que faremos mais adiante.

AXIOMAS DA ARITMÉTICA DE PEANO

AP_1. $\forall x\,(x' \neq 0)$.

AP_2. $\forall xy\,(x' = y' \to x = y)$.

AP_3. $\forall x\,(x + 0 = x)$.

AP_4. $\forall xy\,(x + y' = (x + y)')$.

AP_5. $\forall x\,(x \cdot 0 = 0)$.

AP_6. $\forall x\,(x \cdot y' = xy + x)$.

AP_7. $\forall x\,(x^0 = \overline{1})$.

AP_8. $\forall xy\,(x^{y'} = x^y \cdot x)$.

Enunciamos a seguir os axiomas da ordem e os axiomas de indução.

AP_9. $\forall x\; x \not< 0$.

AP_{10}. $\forall xy\,(x < y' \leftrightarrow x \leq y)$.

Abreviemos em $\phi(x, \overline{y})$ uma fórmula $\phi(x, y_1, ..., y_n)$ cujas variáveis livres são exactamente x, y_1, ..., y_n; admite-se aqui o caso $n = 0$, em que somente x é livre; "$\forall \overline{y}$" abrevia "$\forall y_1 ... y_n$", omitindo-se naturalmente no caso $n = 0$.

Os *axiomas de indução* de **AP** são todas as sentenças da forma

(Ind) $$\forall \overline{y}\,(\phi(0) \wedge \forall x\,(\phi(x, \overline{y}) \to \phi(x', \overline{y})) \to \forall x\,\phi(x, \overline{y})),$$

---

[141] Esta indução não é feita, obviamente, «dentro» da teoria **AP** mas é, sim, uma indução metamatemática relativamente a esta teoria, que pressupõe os números naturais e a sua estrutura e propriedades habituais, tal como se definem e estudam em matemática (na teoria dos conjuntos). Não querendo fazer tal suposição de momento, pois estamos, afinal, a formalizar uma teoria elementar para os números naturais (**AP**), renunciaríamos a demonstrar aquela regra com r, s, t arbitrários, e em cada caso particular deduziríamos $r = t \vdash t = t^*$ (ver também a secção IV.2).

onde $\phi(x, \overline{y})$ é uma fórmula como acima. (Ind) é o que se chama um *axioma-esquema*, ou *esquema de axiomas*, pois corresponde, na verdade, a uma infinidade de axiomas particulares, um para cada fórmula $\phi(x, \overline{y})$, como indicada. A teoria **AP** possui, portanto, uma infinidade de axiomas. Os teoremas de **AP** são todas as sentenças na linguagem $\mathcal{L}_{\text{ar}}$ que se podem deduzir (no sistema **DNQ**) a partir de hipóteses que sejam axiomas de **AP**, incluindo, como sempre, os teoremas lógicos.

O **modelo standard** de **AP** é a estrutura dos números naturais

$$\mathfrak{N} = (\mathbb{N},\ +\ ,\ \times\ ,\ \uparrow\ ,'\ ,\ <\ , 0)$$

mas não temos nenhuma razão para supor que esta estrutura é o único modelo de **AP**, ou até para supor que é único, a menos de isomorfismo,[142] embora seja, por certo, o modelo *intencional* da mesma: quer dizer, pretende-se, com **AP**, axiomatizar elementarmente as **verdades aritméticas**, que são todas as sentenças na linguagem $\mathcal{L}_{\text{ar}}$ verdadeiras na estrutura $\mathfrak{N}$. A teoria definida semanticamente $\text{Tr}(\mathfrak{N})$ é chamada a **aritmética verdadeira** ou **aritmética completa** (ver exercício 3.15). Em que medida é essa pretensão conseguida é outra questão bem diversa: será que

(**Q**) Toda a sentença verdadeira em $\mathfrak{N}$ é consequência (ou: é teorema) de **AP** ?

Diremos algo mais adiante sobre esta importante questão. Entretanto, façamos uma pequena digressão histórica sobre as origens das primeiras axiomáticas para os números naturais.

IV.2 Sobre a axiomática de Dedekind-Peano

Nas últimas décadas do século XIX teve lugar a chamada *aritmetização da Análise*, que consistiu essencialmente numa revisão dos fundamentos da Análise Infinitesimal, passando por uma construção rigorosa da estrutura dos números reais a partir dos números naturais (as construções dos inteiros e dos racionais nunca foi problemática) e por uma fundamentação dos conceitos básicos da Análise (continuidade, diferenciabilidade, integrabilidade, etc.) em termos do conceito de *limite* (de uma sucessão, de uma função, etc.). Tais construções basearam-se, em boa medida, numa nova teoria que estava a dar os primeiros passos, a teoria dos conjuntos, desenvolvida parcialmente por Richard Dedekind[143] e mais folgadamente por Georg Cantor[144] a partir dos anos setenta (ver secção V.4).

---

[142] A noção de isomorfismo entre duas estruturas para a mesma linguagem foi definida em III.8. A expressão «a menos de isomorfismo» significa «quaisquer dois são isomorfos».

[143] V. o artigo "Continuity and the irrational numbers" (tradução do original alemão de 1872) de R. DEDEKIND em *Essays on the Theory of Numbers*, Dover, 1963. Trad. port. "Continuidade e números irracionais" no *Bol. da SPM,* N. 40, 1999.

[144] *Contributions to the Founding of the Theory of Transfinite Numbers* (tradução e prefácio de P. E. B. JOURDAIN dos originais em alemão de 1895-1897), Dover, 1952.

Dedekind é, talvez, o primeiro matemático a chamar a atenção para a necessidade de, por seu turno, se fundamentar rigorosamente a teoria dos números naturais, cujo estatuto permanecia essencialmente informal ou intuitivo. Não parecendo possível, na altura, *definir* ou *construir* os números naturais a partir de entidades mais simples ou primitivas (a primeira construção de um conjunto de números naturais na teoria dos conjuntos é de origem mais recente, por E. Zermelo, por volta de 1908), restaria a via *axiomática* para caracterizar, por meio de axiomas, a progressão dos naturais intuitivos

(*) 0, 1, 2, 3, ...

Os factos considerados por Dedekind como relevantes para uma tal axiomatização são a *estrutura indutiva* da progressão (*), quer dizer:

(1) A existência de um «primeiro elemento» ou **zero**;[145]

(2) Uma operação injectiva que associa a cada elemento um outro, o seu **sucessor** ; e finalmente

(3) O facto de cada elemento da progressão (*) se poder obter a partir do primeiro (0), iterando a operação *sucessor* um número finito qualquer de vezes.

Há uma dificuldade fundamental com a formulação do facto (3), pois nele se refere o conceito de «número finito», conceito esse que, a ser definido como é habitual, requeriria o conceito de «número natural» (ou conceito equivalente), que se está querendo caracterizar pelos axiomas! Dedekind[146] consegue contornar esta dificuldade, mas a sua axiomática é mais conhecida e citada na literatura como *axiomática de Peano*, por ter sido popularizada por G. Peano num trabalho historicamente muito importante publicado em 1889.[147] Por uma questão de justiça histórica, designamos essa axiomática por *axiomática de Dedekind-Peano*.

---

[145] Na realidade, Dedekind chamou **um** (1) ao primeiro elemento, mas estamos chamando **zero** (0) ao primeiro elemento para facilitar a comparação com as axiomáticas modernas. É talvez por esta razão que no ensino liceal tem perdurado a ideia de que 0 não é número natural, o que se nos afigura absurdo. Os autores dos manuais conhecem provalvelmente a axiomática de (Dedekind)-Peano, mas parecem desconhecer os desenvolvimentos modernos. É de referir, nomeadamente, que no *Formulaire Mathématique* de 1894, G. Peano já toma o zero como primeiro elemento. Por outro lado, se é certo que o *zero* fez uma entrada tardia no idéario matemático ocidental, não é menos certa a utilização do *zero* e da numeração posicional hindu-árabe no ensino primário. Que sentido faz negar mais tarde o que já foi definitivamente adquirido no ensino básico? Igualmente simplificamos a apresentação da axiomática de Dedekind-Peano em alguns outros aspectos de pormenor, essencialmente de natureza notacional.

[146] V. o artigo "The nature and meaning of numbers" (1888) na referência indicada na Nota 143.

[147] *Arithmetices principia, nova methodo exposita*, parcialmente traduzido na colectânea de Van HEIJENOORT, pp. 85-97. Ver também o artigo de H. WANG, "The axiomatization of

Os axiomas de Dedekind-Peano são formulados de modo informal, pois na época não se conhecia ainda o conceito de linguagem formal (que haveria de ser formulado por G. Frege), nem tão-pouco a distinção entre linguagem elementar e não elementar.

É uma axiomática nos conceitos primitivos **zero** (*0*) e **sucessor**. Usaremos variáveis a, b, c, ... para «números», X, Y, Z, ... para conjuntos;[148] o sucessor de a denota-se Sa. Um modelo intencional da axiomática é uma estrutura $(N, \mathsf{S}, 0)$, onde N é o domínio dos «números» (intencionalmente: números naturais), 0 é um elemento de N, e S é uma aplicação de N em N. Os axiomas são:

DP_1. $\forall a\ Sa \neq 0$.

DP_2. $\forall a \forall b\,(Sa = Sb \rightarrow a = b)$.

DP_3. $\forall X\,(0 \in X \wedge \forall a\,(a \in X \rightarrow Sa \in X) \rightarrow N \subseteq X)$.

Os dois primeiros axiomas são claramente elementares (comparar com AP_1, AP_2, respectivamente), mas o último axioma, o *axioma de indução*, é um axioma «conjuntista» que nos envolve directamente com a teoria dos conjuntos, não tanto por causa do símbolo $\in$,[149] mas por causa do quantificador de 2ª ordem "$\forall X$".

A maneira como DP_3 contorna a dificuldade mencionada de formulação de (3) é a seguinte, que é deveras genial: um conjunto X que tenha 0 como elemento e seja fechado para S (e que, portanto, também tem $\mathsf{S}0$, $\mathsf{SS}0$, $\mathsf{SSS}0$, ... como elementos, podendo ter ou não outros elementos «estranhos») tem todos os «números» (isto é, $N \subseteq X$); ora o próprio conjunto N está nessas condições (pois, como acima se disse, $0 \in N$ e $\mathsf{S} : N \rightarrow N$) e, por conseguinte, N será *o mais pequeno conjunto* que tem 0 como elemento e é fechado para S, isto é, o mais pequeno conjunto que tem os elementos 0, $\mathsf{S}0$, $\mathsf{SS}0$, ..., da mesma maneira que a «colecção» dos naturais intuitivos (*) é a mais pequena colecção que tem como elementos 0, 1, 2, ... e se pretendia dizer, por palavras diferentes, em (3) (mas não se sabia como, antes de Dedekind).[150]

---

arithmetic", *Journal of Symbolic Logic* **22**, (1957), 145-158. Sob certos aspectos, Peano também se baseia num trabalho de H. Grassmann (1861).

[148] Diga-se, de passagem, que o conceito de conjunto em uso na época é um conceito intuitivo ou ingénuo: para Cantor, qualquer colecção, intuída ou pensada de alguma maneira e concebida como um todo, é um conjunto. Somente alguns anos mais tarde se descobriu que esta concepção intuitiva é liberal em demasia, tornando-se necessário substituí-la por outra mais restrita (axiomática), deixando os termos «conjunto» e «colecção» de ser considerados sinónimos. V. secção 5.4.

[149] Se X fosse uma variável predicativa unária, poderíamos escrever «Xa» em vez de «$a \in X$».

[150] *Durante quase cem anos parece ter passado despercebida a possibilidade de Dedekind ter-se, afinal, enganado na sua pretensão de captar axiomaticamente os naturais intuitivos, quer dizer, a possibilidade de N ter, além de todos os elementos da forma 0, $\mathsf{S}0$, $\mathsf{SS}0$, … *outros* elementos que não possam escrever-se na forma $\mathsf{S}\cdots\mathsf{S}0$ e que não correspondem,

Note-se que Dedekind (e Peano, depois dele) não pretendeu, com a sua axiomática, *definir* o que é *número natural* (por isso, escrevemos acima que N é o conjunto dos «números»), mas sim caracterizar axiomaticamente certa estrutura matemática a que *posteriormente* pudesse chamar **estrutura dos números naturais**.

Ora «caracterizar axiomaticamente» certa estrutura $\mathfrak{M}$ quer dizer exactamente o seguinte: dar um sistema de axiomas, digamos Σ, tal que $\mathfrak{M}$ seja modelo de Σ e qualquer outro modelo $\mathfrak{M}'$ de Σ seja isomorfo a $\mathfrak{M}$, podendo-se afirmar neste caso que $\mathfrak{M}$ é o único modelo de Σ (a menos de isomorfismo). E de uma teoria com um tal sistema de axiomas Σ, ou até do próprio sistema Σ, se dirá que é **categórica**(**o**).

Três questões metateóricas se podem então colocar a respeito dos axiomas de Dedekind-Peano:

(4) **Compatibilidade**: existe alguma estrutura matemática $(N, \mathsf{S}, 0)$ com as propriedades expressas pelos axiomas DP_1-DP_3, isto é, um modelo destes axiomas?

(5) **Categoricidade**: quaisquer dois modelos dos axiomas, digamos $(N_1, \mathsf{S}_1, 0_1)$ e $(N_2, \mathsf{S}_2, 0_2)$, são isomorfos?

(6) Até que ponto é que os axiomas DP_1-DP_3 constituem um fundamento (axiomático) adequado da aritmética dos naturais?

Nem Dedekind nem Peano responderam satisfatoriamente à primeira destas questões, mas as respostas dadas a (5) e (6) podem considerar-se satisfatórias. Note-se que a questão (6) é, de facto, pertinente. Os naturais intuitivos (*) não possuem estatuto matemático, nem tão-pouco podemos falar, formalmente, do conceito de natural intuitivo. Uma possível definição do tipo

$$x \text{ é um natural intuitivo } \Leftrightarrow\ x = 0 \vee x = 1 \vee x = 2 \vee ...$$

esbarra com a impossibilidade (na lógica clássica) de uma disjunção infinita. Embora seja comum escrever-se $\mathbb{N} = \{0, 1, 2, ...\}$, isto *não é uma definição matemática de* $\mathbb{N}$; quando muito, o lado direito da igualdade é uma abreviatura do símbolo '$\mathbb{N}$', e não ao contrário!

---

portanto, a naturais intuitivos. Tais outros elementos «estranhos» seriam «infinitamente grandes» relativamente aos primeiros. Como é isto possível? Simplesmente se for o caso de *todo e qualquer conjunto* X *que tenha* 0 *como elemento e seja fechado para* S *tenha também tais outros elementos* «*estranhos*»... De facto, esta é uma possibilidade imprevista a ter em conta que não invalida a teoria feita mas tardou em ser reconhecida. Mas uma coisa é reconhecer a possibilidade, outra é tirar partido dela... No quadro da axiomática para a teoria dos conjuntos aquela possibilidade mantém-se. Para tirar partido dela, porém, há que *ampliar conceptualmente* o quadro da matemática tradicional com um *novo conceito primitivo* que permita fazer distinções entre diferentes espécies de números naturais. Mais sobre isto no final da secção 5.4.

Algo, matematicamente bem definido, deverá tomar o lugar da colecção dos naturais intuitivos na prova de compatibilidade (4).[151]

A solução proposta por Dedekind é basicamente a seguinte. Considere-se a colecção infinita M_0, a totalidade das «coisas pensáveis» (ou «objectos do pensamento»). Tal colecção é infinita pelo facto de nela estar definida uma operação S que associa a cada elemento a de M_0 o pensamento de que a é uma coisa pensável, pensamento esse que se denota $\mathsf{S}a$ e que é distinto de a; ora, a operação S é, obviamente, injectiva (quer dizer, «números» diferentes têm sucessores diferentes) mas não sobrejectiva (o meu *ego* é elemento de M_0, mas não é da forma $\mathsf{S}a$), donde resulta que M_0 é equipotente a uma parte de si própria, sendo, por isso, infinita.[152] Seja agora 0 uma coisa pensável que não seja da forma $\mathsf{S}a$ (o meu *ego*, por exemplo). Assim, há, pelo menos, uma colecção que contém 0 e fechada para S, a colecção M_0, e o axioma DP_3 mais não faz do que determinar N como *a mais pequena colecção X que contém* 0 *e é fechada para* S. Esta solução de Dedekind é insatisfatória na medida em que faz depender a existência de um modelo dos axiomas DP_1-DP_3 de actos psíquicos (ainda que supostamente intersubjectivos) e de colecções intuitivas sem estatuto matemático.

Mas, se M_0 fosse um conjunto «respeitável», matematicamente falando, a ideia de Dedekind teria possibilidades de vingar. De facto, na teoria axiomática dos conjuntos é adoptado um axioma especial, o *axioma do infinito*, que postula a existência de, pelo menos, um conjunto X tal que

$$\emptyset \in X \wedge \forall x\,(x \in X \rightarrow \mathcal{S}x \in X)$$

onde $\mathcal{S}x = x \cup \{x\}$ (comparar com o exercício 3.21) é o **sucessor** (conjuntista) de x. Um conjunto X nestas condições diz-se **indutivo**. Pode-se então provar que existe o mais pequeno conjunto indutivo, conjunto este que se designa por $\mathbb{N}$ e cujos elementos são chamados **números naturais**. [Tecnicamente, $\mathbb{N}$ é a intersecção de todos os conjuntos indutivos,

---

[151] Do mesmo modo, a axiomática de Euclides para a geometria tinha como modelo intencional o «espaço físico ordinário», um modelo intuitivo. No final do século passado, e após a revisão dos fundamentos da geometria levada a cabo por Pasch, Pieri, Peano e Hilbert, entre outros, demonstrou-se a compatibilidade da geometria euclidiana (reformulada), utilizando o espaço euclidiano tridimensional (definido analiticamente) $\mathbb{R}^3$ como modelo.

[152] Dois conjuntos dizem-se **equipotentes** (**equinumerosos**, ou **equicardinais**) sse existir entre eles uma bijecção. A propriedade referida, de um conjunto ser equipotente a uma sua parte própria, foi considerada por Dedekind como característica dos conjuntos infinitos. Modernamente, tais conjuntos dizem-se **infinitos à Dedekind**, ou **Dedekind-infinitos**. Por exclusão de partes, um conjunto é **Dedekind-finito** sse não é equipotente a nenhuma sua parte própria. Pode-se provar, na teoria dos conjuntos, que um conjunto é Dedekind-finito sse é vazio ou é equipotente a um segmento $\{0, \ldots, n\}$ de $\mathbb{N}$, mas a prova deste facto (mais exactamente, da implicação $\Rightarrow$) utiliza uma forma fraca do axioma da escolha, mais precisamente, o axioma da escolha para famílias numeráveis de conjuntos.

$$\mathbb{N} = \{x : \forall X(X \text{ é indutivo} \rightarrow x \in X)\}.]$$

Observe-se que $0 = \emptyset$, $1 = \{\emptyset\}$, $2 = \{\emptyset, \{\emptyset\}\}$, ... são elementos de $\mathbb{N}$, sendo fácil provar que $\mathbb{N}$ é fechado para $\mathcal{S}$. Designando por σ a restrição a $\mathbb{N}$ da operação (no universo dos conjuntos) $\mathcal{S}$, quer dizer,

$$\sigma = \{(n, \mathcal{S}n) : n \in \mathbb{N}\},$$

prova-se que a estrutura $(\mathbb{N}, \sigma, \emptyset)$ é um modelo dos axiomas de Dedekind-Peano e que, além disso, é o único modelo destes axiomas, a menos de isomorfismo.[153] As questões (4) e (5) são, portanto, respondidas afirmativamente na teoria (axiomática) dos conjuntos.

A resposta a (5) segue, essencialmente, as linhas que o próprio Dedekind delineou, e com base na unicidade a menos de isomorfismo Dedekind chamou **sistema de números naturais** a *uma qualquer* estrutura $(N, \mathsf{S}, 0)$ que satisfizesse os seus axiomas (uma é tão boa como qualquer outra, pois são todas isomorfas entre si). Na teoria dos conjuntos vai-se um pouco mais longe, ao ponto de se poder indicar uma especial — $(\mathbb{N}, \sigma, \emptyset)$.

Quanto à questão (6), a resposta moderna também é essencialmente a que Dedekind delineou. É um facto notável que, na teoria dos conjuntos, é possível *definir* (por recorrência) as operações de adição, multiplicação, exponenciação, etc., e demonstrar as propriedades habituais destas operações em $\mathbb{N}$. Tal não se pode fazer em **AP**, porém, pela razão que a seguir explicamos, pelo que se torna necessário admitir aquelas operações como primitivas sujeitas aos axiomas indicados.

Pelo menos aparentemente, e de facto, a aritmética elementar, formalizada em **AP**, é (estritamente) mais fraca do que a aritmética conjuntista, embora não seja nada fácil demonstrar esta afirmação. Por outras palavras, há sentenças de $\mathcal{L}_{\text{ar}}$ verdadeiras em $\mathfrak{N}$, cuja veracidade se pode estabelecer na teoria dos conjuntos (não esqueçamos que o conceito semântico de satisfação é um conceito essencialmente conjuntista), que não são teoremas de **AP**.

Para já, tentamos explicar por que razão os axiomas de indução (Ind) não podem captar toda a potência dedutiva do axioma conjuntista de indução de Dedekind, DP_3.

Demonstremos primeiramente que os axiomas de indução de **AP** são, todos eles, verdadeiros em $(\mathbb{N}, ...)$, admitindo DP_3 nesta estrutura. Seja $\phi(x)$ uma condição qualquer em x que, para simplificar a discussão, supomos não conter outras variáveis livres nem parâmetros. Suponhamos que

(**) $$(\mathbb{N}, ...) \vDash \phi(0) \wedge \forall x\, (\phi(x) \rightarrow \phi(x')).$$

---

153 Ver o nosso livro *Teoria dos Conjuntos, Intuitiva e Axiomática (ZFC)*, Escolar Editora, 1982.

Seja X o conjunto que $\phi(x)$ define em $(\mathbb{N}, ...)$, isto é,

$$X = \{n \in \mathbb{N} \ : \ (\mathbb{N}, ...) \vDash \phi(x)\ [n]\}.$$

Atendendo à hipótese (**), tem-se

$$0 \in X, \text{ e para todo } n \in X, \sigma n \in X.$$

Por DP_3 [interpretado em $(\mathbb{N}, ...)$] podemos concluir que $\mathbb{N} \subseteq X$ e, portanto, que para todo $n \in \mathbb{N}$, $(\mathbb{N}, ...) \vDash \phi(x)\ [n]$, isto é, que $(\mathbb{N}, ...) \vDash \forall x \phi(x)$. Mostrámos, assim, que

$$(\mathbb{N}, ...) \vDash \phi(0) \wedge \forall x\, (\phi(x) \rightarrow \phi(x')) \rightarrow \forall x \phi(x)).$$

Tentemos agora, reciprocamente, demonstrar que o axioma DP_3 é verdadeiro em $(\mathbb{N}, ...)$, admitindo, como hipótese, que os axiomas de indução (Ind) são todos verdadeiros nessa mesma estrutura. Seja então X um conjunto tal que $\emptyset = 0 \in X$ e X é fechado para σ, com vista a mostrar que $\mathbb{N} \subseteq X$. Se existir uma fórmula $\phi(x)$ tal que X é o conjunto que essa fórmula define em $(\mathbb{N}, ...)$, tudo bem: por hipótese sobre X, $\phi(0) \wedge \forall x\, (\phi(x) \rightarrow \phi(x'))$ será verdadeira em $(\mathbb{N}, ...)$, portanto, por (Ind) (e *modus ponens*), $\forall x\, \phi(x)$ é verdadeira em $(\mathbb{N}, ...)$, e por conseguinte $\mathbb{N} \subseteq X$. Mas, *se não existir uma tal fórmula* $\phi(x)$, o argumento não pode prosseguir, e não se vê maneira de contorná-lo. E, de facto, pode bem não existir uma tal fórmula.

Para justificar esta última observação recorremos a um *argumento de cardinalidade* (utilizando alguns conhecimentos básicos da teoria dos cardinais infinitos). Por um lado, é sabido que o conjunto das partes de $\mathbb{N}$, $\mathcal{P}(\mathbb{N})$, tem cardinal superior ao cardinal de $\mathbb{N}$ (este é um famoso teorema devido a Cantor, ver Nota 165), e na formulação de DP_3 a variável X é uma variável para conjuntos, em particular para subconjuntos de $\mathbb{N}$, podendo, assim, «variar» em $\mathcal{P}(\mathbb{N})$. Mas, por outro lado, a linguagem $\mathcal{L}_{ar}$ tem uma infinidade numerável de símbolos e, por conseguinte, uma infinidade numerável de fórmulas (pois cada fórmula é uma sequência finita de símbolos), ou seja, tantas as fórmulas quantos os números naturais ($\mathbb{N}$ é infinito numerável). Vê-se, pois, que pode bem haver subconjuntos de $\mathbb{N}$ que não são definíveis em $(\mathbb{N}, ...)$ por nenhuma fórmula de $\mathcal{L}_{ar}$, pois há «mais» (cardinal maior) subconjuntos de $\mathbb{N}$ do que fórmulas de $\mathcal{L}_{ar}$. O argumento está concluído.

Mais uma vez, porém, dar um exemplo concreto de um conjunto contido em $\mathbb{N}$, mas não definível aritmeticamente, é tarefa muito complicada, nos seus pressupostos e pormenores técnicos, que estão para além do âmbito deste livro. Mas daremos uma ideia no final deste capítulo.

IV.3 Desenvolvimento de AP

Enumeramos os teoremas T_1, T_2, etc., que nesta secção exprimem propriedades fundamentais dos conceitos primitivos. Apenas demonstramos (cada vez mais informalmente) alguns teoremas, deixando os restantes como outros tantos exercícios. Querendo, tais demonstrações facilmente se convertem em deduções no sistema **DNQ**, em geral, porém, bastante mais longas.

T_1. $\forall x\,(0 + x = x)$.

Dem. (Informal, no estilo matemático usual, sem mencionar regras lógicas). Por virtude de (Ind), aplicado à fórmula $0 + x = x$, basta demonstrar que

(i) $0 + 0 = 0$, e

(ii) $\forall x\,(0 + x = x \rightarrow 0 + x' = x')$.

Quanto a (i), é imediato por AP_3. Quanto a (ii), basta demonstrar

(ii′) $0 + a = a \rightarrow 0 + a' = a'$.

Suponhamos que se tem $0 + a = a$ (hipótese de indução), com vista a demonstrar $0 + a' = a'$; da hipótese de indução resulta $(0 + a)' = a'$, mas, por outro lado, particularizando AP_4, $0 + a' = (0 + a)'$, donde $0 + a' = a'$ por transitividade de $=$, como se queria.■

A título de exemplo, fazemos também uma dedução formal (em **DNQ**).

1	$0 + 0 = 0 \wedge \forall x(0 + x = x \rightarrow 0 + x' = x') \rightarrow \forall x(0 + x = x)$	H (Ind)
2	$\forall x\,(x + 0 = x)$	H (AP_3)
3	$\forall xy\,(x + y' = (x + y)')$	H (AP_4)
4	$0 + 0 = 0$	2 ($\forall^-$) (base)
5	$0 + a = a$	[H] (HI)
6	$0 + a = a \rightarrow (0 + a)' = a'$	T^+ (E_7)
7	$(0 + a)' = a'$	5, 6 (MP)
8	$\forall y(0 + y' = (0 + y)')$	3 ($\forall^-$)
9	$0 + a' = (0 + a)'$	3 ($\forall^-$)
10	$0 + a' = a'$	9, 7 (Tran)
11	$0 + a = a \rightarrow 0 + a' = a'$	5-10 ($\rightarrow^+$)
12	$\forall x(0 + x = x \rightarrow 0 + x' = x')$	11 ($\forall^+$)
13	$0 + 0 = 0 \wedge \forall x(0 + x = x \rightarrow 0 + x' = x')$	4, 12 ($\wedge^+$)
14	$\forall x(0 + x = x)$	1, 13 (MP).

Em geral, para demonstrar, por indução, certa sentença $\forall x\,\phi(x, \overline{b})$ (onde $\overline{b}$ abrevia $b_1, ..., b_n$), basta demonstrar as duas sentenças seguintes [sendo a um parâmetro que não ocorre em $\phi(x, \overline{b})$]:

(i) $\phi(0, \overline{b})$, chamada a **base** da indução, e

(ii) $\phi(a,\overline{b}) \rightarrow \phi(a',\overline{b})$.

A dedução de $\phi(a',\overline{b})$ com hipótese $\phi(a,\overline{b})$ é o **passo de indução**, a referida hipótese é, naturalmente, a **hipótese de indução** (abreviadamente HI), enquanto a tese $\phi(a',\overline{b})$ é a **tese de indução**. Dizemos ainda que, por este processo, se deduziu $\phi(a,\overline{b})$ por *indução em* a, ou que se deduziu $\forall x \phi(x,\overline{b})$ por *indução.*

T_2. $\forall xyz\,((x+y)+z = x+(y+z))$ [*associatividade de* $+$].

Dem. Demonstre-se $(a+b)+c = a+(b+c)$ por indução em c.■

T_3. $\forall xy\,(x'+y = (x+y)')$.

T_4. $\forall xy\,(x+y = y+x)$ [*comutatividade de* $+$].

Dem. Provar $a+b = b+a$ (indução em a) utilizando T_1 e T_3.■

T_5. $\forall xyz\,(x(y+z) = xy+xz)$ [*distributividade à esquerda*].

T_6. $\forall xyz\,((xy)z = x(yz))$ [*associatividade de* $\times$].

T_7. $\forall x\,(0 \cdot x = 0)$.

T_8. $\forall xy\,(x' \cdot y = xy + y)$.

T_9. $\forall xy\,(xy = yx)$ [*comutatividade de* $\times$].

Dem. Provar $ab = ba$ por indução em a, utilizando T_7 e T_8.■

Todos os teoremas anteriores se demonstram por indução, em geral na variável «mais à direita» da fórmula respectiva.

T_{10}. $\forall xyz\,((x+y)z = xz+yz)$ [*distributividade à direita*].

Por comutatividade da multiplicação, facilmente se obtém a *distributividade à esquerda*, cujo enunciado omitimos. Propriedades como a associatividade, a comutatividade e a distributividade das operações $+$, $\times$ serão usadas, de futuro, sem menção especial.

T_{11}. $\forall x\,(x+\overline{1} = x')$.

Dem. $a+\overline{1} = a+0' = (a+0)' = a'$.■

Este último resultado permite escrever $t + \overline{1}$, em vez de t', para qualquer termo t, o que faremos algumas vezes. Vejamos mais alguns resultados de natureza geral.

T_{12}. $\forall x\,(x \cdot \overline{1} = x)$.

T_{13}. $\forall x\,(x \cdot \overline{2} = x + x)$.

T_{14}. $\forall xy\,(x + y = 0 \rightarrow x = 0 \wedge y = 0)$.

Dem. Provemos $a + b = 0 \rightarrow a = 0 \wedge b = 0$ por indução em b. *Base:* $a + 0 = 0 \rightarrow a = 0 \wedge 0 = 0$, imediato, utilizando AP_3.

HI: $a + b = 0 \rightarrow a = 0 \wedge b = 0$. *Tese:* $a + b' = 0 \rightarrow a = 0 \wedge b' = 0$. Esta implicação até se prova sem utilizar a HI, pois $a + b' = (a + b)' \neq 0$, por virtude de AP_4 e AP_1, bastando então utilizar o paradoxo da implicação material $\neg\phi \rightarrow (\phi \rightarrow \psi)$, onde ϕ é $a + b' = 0$ e ψ é $a = 0 \wedge b = 0$.■

Os três primeiros resultados seguintes são as chamadas **regras das potências**.

T_{15}. $\forall xyz\,(x^{y+z} = x^y \cdot x^z)$ [*potências da mesma base*].

T_{16}. $\forall xyz\,((xy)^z = x^z \cdot y^z)$ [*potências do mesmo expoente*].

T_{17}. $\forall xyz\,((x^y)^z = x^{yz})$ [*potência da potência*].

T_{18}. $\forall xy\,(x \neq 0 \wedge xy = 0 \rightarrow y = 0)$.

T_{19}. $\forall xy\,(x + y = \overline{1} \rightarrow (x = 0 \wedge y = \overline{1}) \vee (x = \overline{1} \wedge y = 0))$.

Dem. Prove-se $a + b = \overline{1} \rightarrow (a = 0 \wedge b = \overline{1}) \vee (a = \overline{1} \wedge b = 0)$ por indução em b.■

T_{20}. $\forall xy\,(x \cdot y = \overline{1} \rightarrow\ x = \overline{1} \wedge y = \overline{1})$.

T_{21}. $\forall xyz\,(x + z = y + z \rightarrow x = y)$ [*lei do corte à direita para* $+$].

Por comutatividade de $+$ obtém-se facilmente a lei do corte *à esquerda*, que nos abstemos de enunciar. De futuro, diremos apenas *lei do corte* (para $+$), respeitando a um qualquer dos lados.

Dem. Prove-se $a + c = b + c \rightarrow a = b$ por indução em c. Pela primeira vez, relativamente a demonstrações de teoremas anteriores, é necessário utilizar AP_2 no passo de indução.■

T_{22}. $\forall x\,(x \neq 0 \rightarrow \exists^1 y\,(x = y'))$.

Dem. Prove-se $a \neq 0 \rightarrow \exists y\,(a = y')$ por indução em a. No que respeita à unicidade, prove-se, utilizando AP_2, que

$$\forall uv\,(a = u' \wedge a = v' \rightarrow u = v).\blacksquare$$

T_{23}. $\forall xyz\,(x \neq 0 \wedge z \cdot x = y \cdot x \rightarrow z = y)$ [*lei do corte à direita para* $\times$].

Valem observações análogas às que se fizeram relativamente à lei do corte para a adição.

Dem. Demonstramos $\forall z\,(a \neq 0 \wedge z \cdot a = b \cdot a \rightarrow z = b)$ por indução em b. *Base:* $\forall z\,(a \neq 0 \wedge z \cdot a = 0 \cdot a \rightarrow z = 0)$. Tomando c ao arbítrio, e supondo $a \neq 0$ e $ca = 0a$, obtemos $ca = 0$, por T_7, donde $c = 0$, utilizando T_{18} e a comutatividade de $\times$.

HI: $\forall z\,(a \neq 0 \wedge z \cdot a = b \cdot a \rightarrow z = b)$.

Tese: $\forall z\,(a \neq 0 \wedge z \cdot a = b' \cdot a \rightarrow z = b')$.

Tomemos c ao arbítrio e suponhamos $a \neq 0$ e $c \cdot a = b' \cdot a$, com vista a mostrar que $c = b'$. Ora $b' \neq 0$ (AP_1), e como também $a \neq 0$, por hipótese, vem $b' \cdot a \neq 0$, por virtude do T_{18}, donde $c \cdot a \neq 0$, e portanto $c \neq 0$. Sendo pois $c \neq 0$, é $c = d'$ para algum d, por T_{22}, donde, substituindo c por d' na segunda hipótese, $d' \cdot a = b' \cdot a$. Por T_8, isto quer dizer que $d \cdot a + a = b \cdot a + a$, donde $da = ba$, pela lei do corte. Particularizando HI, concluimos que $d = b$, logo $d' = b'$, e portanto $c = b'$, como se queria.$\blacksquare$

T_{24}. $\forall x\,(x \neq 0 \wedge x \neq \overline{1} \rightarrow \exists y\,(x = y''))$.

Vejamos agora algumas propriedades de $<$, $\leq$ e seu relacionamento com as operações aritméticas.

IV.4 Propriedades da ordem. Outras formas de indução

T_{25}. $\forall x\,(0 \leq x)$ [0 *é elemento mínimo*].

Dem. Provamos $0 \leq a$ por indução em a. *Base:* $0 \leq 0$, isto é, $0 < 0 \vee 0 = 0$, o que é trivial, por $(=^+)$ e $(\vee^+)$.

HI: $0 \leq a$. *Tese:* $0 \leq a'$. Por AP_{10}, a hipótese de indução equivale a $0 < a'$, donde imediatamente se conclui $0 \leq a'$, como se queria.$\blacksquare$

Utilizando a definição de $\leq$, facilmente se conclui que a operação de sucessão $'$ também é monótona com respeito a $\leq$.

T_{26}. $\forall xy\,(x < y \rightarrow x' < y')$ [*monotonia de* $'$].

Dem. Provar $a < b \rightarrow a' < b'$ por indução em b, utilizando AP_9 e T_{25}.■

T_{27}. $\forall xyz\,(x < y \wedge y < z \rightarrow x < z)$ [*transitividade de* $<$].

Dem. Prove-se $a < b \wedge b < c \rightarrow a < c$ por indução em c.■

Usando a definição de $\leq$, facilmente se conclui (discutindo os diferentes casos possíveis) que $\leq$ também é transitiva. Aliás, resultados deste tipo, que relacionam algumas propriedades de $<$ com as de $\leq$, já foram discutidos nos exercícios 3.8 e 3.9.

T_{28}. $\forall xy\,(x < y \vee x = y \vee y < x)$ [*tricotomia (fraca)*].

Dem. Provamos $a < b \vee a = b \vee b < a$ por indução em a. *Base:* $0 < b \vee 0 = b \vee b < 0$, o que é imediato pois, por T_{25}, $0 \leq b$.

HI: $a < b \vee a = b \vee b < a$. *Tese:* $a' < b \vee a' = b \vee b < a'$. Desdobremos a HI nos casos (i) $a < b$ e (ij) $a = b \vee b < a$. No caso (i), obtemos, por T_{26}, $a' < b'$, ou seja, por AP_{10}, $a' < b \vee a' = b$ e no caso (ij) obtemos, novamente por AP_{10}, $b < a'$.■

Para se poder afirmar que $<$ tem as propriedades das ordens totais estritas falta demonstrar a propriedade de irreflexividade. Antes de demonstrar esta propriedade, porém, convém demonstrar algumas outras formas de indução, consequências dos axiomas de indução (Ind).

PRINCÍPIO DE INDUCÃO COMPLETA [1.ª forma, (IC_1)]

Seja $\phi(a, \overline{b})$ *uma condição nos parâmetros a,* $\overline{b}$*, e* z *uma variável que não ocorre em* ϕ*. Então*

(IC_1) $$\forall \overline{y}\left(\forall x\,(\forall z < x\ \phi(z, \overline{y}) \rightarrow \phi(x, \overline{y})) \rightarrow \forall x\ \phi(x, \overline{y})\right).$$

Dem. Fixemos $\overline{b}$ ao arbítrio; para simplificar a notação, escrevemos simplesmente $\phi(x)$, em vez de $\phi(x, \overline{b})$. Denotemos também por $\psi(x)$ a fórmula $\forall z < x\ \phi(z)$, abreviatura de $\forall z\,(z < x \rightarrow \phi(z))$. Temos então que demonstrar a sentença $\forall x\,(\psi(x) \rightarrow \phi(x)) \rightarrow \forall x \phi(x)$. Se demonstrarmos

$$\forall x\,(\psi(x) \rightarrow \phi(x)) \rightarrow \phi(0) \wedge \forall x\,(\phi(x) \rightarrow \phi(x')),$$

poderemos concluir $\forall x \phi(x)$, por (Ind).

Admitamos, pois,

(*) $$\forall x\,(\psi(x) \rightarrow \phi(x))$$

donde, em particular, $\psi(0) \rightarrow \phi(0)$, isto é, $\forall z\,(z < 0 \rightarrow \phi(z)) \rightarrow \phi(0)$. O antecedente desta implicação resulta trivialmente de AP_9, donde $\phi(0)$, por *modus ponens*.

Mostramos agora que $\phi(a) \rightarrow \phi(a')$, com a arbitrário. Admitamos o antecedente desta implicação com vista a demonstrar o consequente. Sabendo que $y < a' \leftrightarrow y < a \vee y = a$ (AP_{10}) e efectuando algumas manipulações lógicas, facilmente se constata que

$$\psi(a') \leftrightarrow \psi(a) \vee \phi(a),$$

isto é, que

$$\forall y\,(y < a' \rightarrow \phi(y)) \leftrightarrow \forall y\,(y < a \rightarrow \phi(y)) \vee \phi(a)$$

Tendo admitido $\phi(a)$, podemos concluir $\psi(a')$; mas, particularizando (*) acima, obtemos $\psi(a') \rightarrow \phi(a')$, donde $\phi(a')$, por *modus ponens*, como se queria.■

A 2.ª forma deste princípio é (utilizando as mesmas notações que acima)

(IC_2) $\quad \forall \overline{y}\,\big(\phi(0,\overline{y}) \wedge \forall x\,(\forall z \leq x\ \phi(z,\overline{y}) \rightarrow \phi(x',\overline{y})) \rightarrow \forall x\,\phi(x,\overline{y})\big)$.

A equivalência entre as duas formas do princípio de indução completa será deixada para um exercício (4.6). Outro princípio muito importante e de grande utilidade em certas demonstrações é o chamado

PRINCÍPIO DE MÍNIMO

Seja $\phi(x,\overline{y})$ uma condição nas variáveis x, $\overline{y}$, e z uma variável que não ocorre em ϕ. Então

(Min) $\qquad \forall \overline{y}\,\big(\exists x\,\phi(x,\overline{y}) \rightarrow \exists x\,(\phi(x,\overline{y}) \wedge \forall z < x\,\neg\phi(z,\overline{y}))\big)$.[154]

Dem. Resulta facilmente de (IC_1), substituindo ϕ por $\neg\phi$ e efectuando algumas transformações lógicas simples [contrapondo, utilizando as leis de conversão e as regras de De Morgan (DM_i) do Cap. III.3, etc.].■

Retomemos a discussão de algumas propriedades de $<$.

T_{29}. $\forall x\,(x \not< x)$ [*irreflexividade*].

---

[154] Este princípio corresponde, na teoria **AP**, à conhecida propriedade de boa ordenação da relação de ordem em $\mathbb{N}$: a propriedade de que *todo o subconjunto não vazio de* $\mathbb{N}$ *tem elemento mínimo*. Formulada desta maneira, esta propriedade é de segunda ordem relativamente aos números naturais (por virtude do quantificador «para todo o subconjunto…»), não podendo por isso ser formulada directamente na linguagem elementar $\mathcal{L}_{\mathrm{ar}}$. Indirectamente, porém, podemos formalizar que todo o conjunto *definível* e não vazio de «números» tem mínimo, e é isto precisamente que diz o princípio de mínimo.

Dem. Por indução completa, 1ª forma, e *modus ponens*, basta provar que $\forall x\,(\forall y < x\ y \not< y \to x \not< x)$, ou seja, que $\forall y < a\ y \not< y \to a \not< a$, com a arbitrário. Admitindo o antecedente, que abrevia $\forall y\,(y < a \to y \not< y)$, obtemos $a < a \to a \not< a$, donde $a \not< a$ [utilizando a lei $(\phi \to \neg\phi) \to \neg\phi$)].■

T_{30}. $\forall xy\,(x < y \to y \not< x)$ [*assimetria*].

Em resumo, demonstrámos que $<$ tem as propriedades das ordens totais (estritas), com elemento mínimo 0, satisfazendo, além disso, o princípio de mínimo. Nas propriedades seguintes relaciona-se $<$, $\leq$ com $+$, $\times$, $'$. Algumas outras propriedades podem-se encontrar nos exercícios 4.7 e seguintes.

T_{31}. $\forall xy\,(x \leq x + y)$.

T_{32}. $\forall xy\,(y \neq 0 \to x < x + y)$.

T_{33}. $\forall xy\,(x < y \leftrightarrow \exists^1 z\,(z \neq 0 \wedge x + z = y))$.

Dem. Demonstrar $a < b \leftrightarrow \exists z\,(z \neq 0 \wedge a + z = b)$ por indução em b. A unicidade de c tal que $a + c = b$ resulta imediatamente da lei do corte para a adição.■

No caso de não termos considerado $<$ como primitivo, teríamos definido $<$ pela sentença deste último teorema. Claro está que algumas demonstrações de teoremas já enunciados seriam diferentes das apresentadass ou sugeridas. A irreflexividade de $<$ (T_{29}), por exemplo, resultaria facilmente da lei do corte para $+$ (T_{21}).

T_{34}. $\forall xy\,(x \leq y \leftrightarrow \exists^1 z\,(x + z = y))$.

Dados a, b tais que $a \leq b$, o único c tal que $a + c = b$ chama-se a **diferença** entre a e b, e denota-se $b - a$; $b - \overline{1}$ é o **predecessor** de b ($b \neq 0$). Sem exigir que $a \leq b$, pode-se definir a **diferença cortada**

$$b \dot{-} a = \begin{cases} 0 & \text{se } b \leq a \\ b - a & \text{se } a < b. \end{cases}$$

T_{35}. $\forall xy\,(0 < y \to x \leq xy)$.

T_{36}. $\forall xy\,(0 < x \wedge \overline{1} < y \to x < xy)$.

T_{37}. $\forall xy\,(0 < y \to x < x'y)$.

T_{38}. $\forall xyz\,(x < y \to x + z < y + z)$ [*compatibilidade de* $<$ *com* $+$].

T_{39}. $\forall xyz\,(x \leq y \rightarrow x + z \leq y + z)$ [*compatibilidade de* $\leq$ *com* $+$].

T_{40}. $\forall xyz\,(0 < z \rightarrow (x < y \leftrightarrow xz < yz))$ [*compatibilidade de* $<$ *com* $\times$].

T_{41}. $\forall xyz\,(0 < z \rightarrow (x \leq y \leftrightarrow xz \leq yz))$ [*compatibilidade de* $\leq$ *com* $\times$].

Outras propriedades dos primitivos serão deixadas para os exercícios.

IV.5 Divisibilidade

A título ilustrativo, enunciamos e demonstramos alguns resultados básicos sobre a noção de divisibilidade e noções afins. Primeiramente definimos:

Def($\mid$) $\qquad\qquad \forall xy\,(x \mid y \leftrightarrow \exists z\; y = xz).$

«$x \mid y$» lê-se «x **divide** y», ou «y **é divisível por** x», ou «x **é divisor de** y», ou ainda «y **é multiplo de** x».

De agora em diante seremos ainda mais informais nos enunciados e nas demonstrações. Às variáveis e parâmetros chamaremos **números** (intencionalmente: *números naturais*[155]), e usaremos uma grande variedade de letras (k, m, p, q, r, ...) como parâmetros.

T_{42}. Para quaisquer números a, b, c:

(i) $a \mid a$; (ii) $\overline{1} \mid a$; (iii) $a \mid 0$;

(iv) $a \mid b \wedge b \mid c \to a \mid c$;

(v) $b \neq 0 \wedge a \mid b \to a \leq b$;

(vi) $a \mid b \wedge b \mid a \to a = b$;

(vii) $a \mid b \to a \mid (bc)$;

(viii) $a \mid b \wedge a \mid c \to a \mid (b + c)$;

(ix) $a \mid b \to ac \mid bc$;

(x) $a > \overline{1} \to \neg(a \mid b \wedge a \mid (b + \overline{1}))$.

Dem. (iv) Suponhamos que $a \mid b$ e $b \mid c$, isto é, que $ak_1 = b$ e $bk_2 = c$ para certos números k_1, k_2, donde $(ak_1)k_2 = c$, ou seja, por associatividade, $a(k_1k_2) = c$, o que mostra que $\exists z(az = c)$, isto é, que $a \mid c$.

(v) Suponhamos que $b \neq 0$ e $a \mid b$, digamos que $ak = b$; não pode ser $k = 0$, caso contrário viria $b = 0$, contra a hipótese; então $k \neq 0$, logo $k = m'$ para algum m, donde $b = ak = am' = am + a \geq a$.

(x) Suponhamos $a > \overline{1}$ e que $a \mid b$ e $a \mid (b + \overline{1})$, com vista a um absurdo; digamos que $ak = b$ e $am = b + \overline{1}$, donde $am = ak + \overline{1}$. Por tricotomia, tem-se $m < k$ ou $m = k$ ou $k < m$, mas qualquer destes casos conduz a um absurdo, como facilmente se verifica. Só para exemplificar: se fosse $k < m$, digamos $k + j = m$, viria $a(k + j) = ak + \overline{1}$, donde $aj = \overline{1}$, o que é impossível.■

---

[155] Mas tenha-se em conta que $(\mathbb{N}, \dots)$ não é o único modelo de **AP** (nem a menos de isomorfismo) e que um teorema de **AP** exprime uma propriedade verdadeira em todos os seus modelos, e não somente acerca dos números naturais (elementos do modelo *standard*), ver IV.6.

O teorema seguinte estabelece a existência e unicidade do quociente e do resto da divisão inteira (ou divisão com resto) de dois números.

T_{43}. TEOREMA DA DIVISÃO INTEIRA

Para quaisquer números a, b, com $b > 0$, existem e são únicos números q, r tais que

$$a = bq + r,\ r < b.$$

O número q é chamado o **quociente** da divisão inteira de a (o **dividendo**) por b (o **divisor**) e r é o respectivo **resto**.

Dem. Demonstramos primeiramente a *existência* de números q, r tais que $a = bq + r$ e $0 \leq r < b$. Isto é, demonstramos (com b fixado ao arbítrio)

$$\phi(a, b): \quad 0 < b \rightarrow \exists xy\,(a = bx + y \wedge y < b)$$

por indução em a.

Base: supondo $0 < b$, é óbvio que $0 = b \cdot 0 + 0 \wedge 0 < b$, logo $\exists xy$ $(0 = bx + y \wedge y < b)$, o que prova $\phi(0, b)$.

HI: $0 < b \rightarrow \exists xy\,(a = bx + y \wedge y < b)$. *Tese:* $\phi(a + \overline{1}, b)$. Suponhamos $0 < b$, com vista a demonstrar que $\exists xy\,(a + \overline{1} = bx + y \wedge y < b)$. Da hipótese de indução sabemos que para certos números $q,\ r$ se tem $a = bq + r$ e $r < b$, donde $r + \overline{1} \leq b$ (por T_{26} e AP_{10}); no caso $r + \overline{1} < b$ obtemos

$$a + \overline{1} = (bq + r) + \overline{1} = bq + (r + \overline{1}),$$

portanto $\exists xy(a + \overline{1} = bx + y \wedge y < b)$; e no caso $r + \overline{1} = b$ obtemos

$$\begin{aligned} a + \overline{1} = (bq + r) + \overline{1} \quad &= bq + (r + \overline{1}) = bq + b \\ &= bq + b \cdot \overline{1} = b(q + \overline{1}) + 0, \end{aligned}$$

donde, também neste caso, $\exists xy\,(a + \overline{1} = bx + y \wedge y < b)$.

Demonstremos agora a *unicidade* do quociente e do resto:

$$\begin{aligned} 0 < b \wedge a = bq_1 + r_1 \wedge r_1 < b \wedge a = bq_2 + r_2 \wedge r_2 < b \\ \rightarrow q_1 = q_2 \wedge r_1 = r_2. \end{aligned}$$

Admitido o antecedente desta implicação, tem-se, por tricotomia, $q_1 < q_2 \vee q_1 = q_2 \vee q_2 < q_1$. Mostramos que as desigualdades conduzem a absurdos, restando, assim, a igualdade como única possibilidade.

Se fosse $q_1 < q_2$, por exemplo, teríamos, para certo $w > 0$, $q_2 = q_1 + w$, donde $bq_2 = bq_1 + bw$, e portanto, atendendo a que por hipótese se tem $a = bq_1 + r_1 = bq_2 + r_2$,

$$bq_2 + r_1 = bq_1 + bw + r_1 = bq_1 + r_1 + bw = bq_2 + r_2 + bw,$$

donde finalmente (cortando bq_2 no primeiro e último membro), $r_1 = r_2 + bw$. Mas

$0 < b$, por hipótese, e, além disso, também $0 < w$, logo $b \leq bw$, donde

$$r_1 = r_2 + bw \geq r_2 + b \geq b,$$

contradizendo a hipótese $r_1 < b$. Analogamente se prova que não pode ser $q_2 < q_1$. Tem-se, portanto, $q_1 = q_2$, o que prova a unicidade do quociente, donde

$$bq_1 + r_1 = bq_2 + r_2 = bq_1 + r_2,$$

e, finalmente, $r_1 = r_2$, pela lei do corte da adição, o que prova a unicidade do resto.■

No estudo da divisibilidade em $\mathbb{N}$, os números primos ocupam um lugar de relevo. Daremos a sua definição e demonstraremos, em **AP**, algumas das suas propriedades.

Definição. Um número p diz-se **primo** sse $p > \overline{1}$ e p só é divisível por si próprio e por $\overline{1}$. Formalmente:

$$p \text{ é primo} \leftrightarrow p > \overline{1} \wedge \forall x\,(x \mid p \rightarrow x = \overline{1} \vee x = p)$$

Um número maior do que $\overline{1}$ que não é primo diz-se **composto**.

Os dois primeiros primos, em $\mathbb{N}$, são 2 e 3, e o primeiro composto é $4 = 2 \times 2$. A razão pela qual não se considera 1 como primo prende-se com a unicidade de que fala o chamado *Teorema Fundamental da Aritmética*, que adiante formulamos e demonstramos em **AP**.

Muito cedo se construíram tabelas de primos, que os modernos computadores vão estendendo sem cessar.[156] Na antiguidade, já Euclides de Alexandria demonstrou haver uma infinidade de primos.[157] Em **AP** podemos demonstrar a seguinte versão deste facto:

---

[156] Diversas equipas de matemáticos, pelo mundo fora, investigam os números primos produzidos por potentes computadores e, ao mesmo tempo, vão calculando determinadas funções e testando diversas hipóteses sobre a distribuição dos primos, etc., como suporte de estudos teóricos de grande complexidade mas com aplicações práticas, nomeadamente, à criptografia.

[157] Pode-se consultar a demonstração de Euclides no nosso artigo "Sobre a teoria dos números (I). Breve introdução histórica a alguns problemas e conjecturas", in *Boletim da S.P.M.* N. 6, Outubro de 1983, pp. 49-64. Para uma introdução «elementar», no melhor sentido, à teoria dos números, ver o livrinho de A. A. MONTEIRO e J. SILVA PAULO *Aritmética Racional*, 1945 (procurar nos alfarrabistas); para um estudo mais profundo mas ainda muito acessível recomendamos os livros de N. H. McCOY, H. M. EDGAR ou W. J. LeVEQUE indicados na Bibliografia, e só depois um tratado clássico como o de G. H. HARDY e E. M. WRIGHT *An Introduction to the Theory of Numbers*, Fifth edition, Oxford UP, 1979.

T_{44}. SEGUNDO TEOREMA DE EUCLIDES

$$\forall x\, \exists y\, (y \text{ é primo} \wedge y > x).$$

Dem. A demonstração, mesmo informal, é relativamente longa, em virtude do grande número de propriedades que pressupõe ou utiliza. Limitamo-nos aos passos principais, deixando alguns detalhes como outros tantos exercícios. Note-se, desde já, que $0 < \overline{1} < \overline{2}$. Em primeiro lugar:

(1) Todo o número maior do que $\overline{1}$ possui um divisor mínimo maior do que $\overline{1}$: $a > \overline{1} \rightarrow \exists y \psi(a, y)$, onde $\psi(a, y)$ abrevia

$$y > \overline{1} \wedge y \mid a \wedge \forall z < y\, \neg(z > \overline{1} \wedge z \mid a)$$

Pois, supondo $a > \overline{1}$, existe, pelo menos, um divisor de a maior do que $\overline{1}$, nomeadamente o próprio a; assim sendo, existe o menor de tais divisores, por (Min). Em segundo lugar:

(2) Um divisor mínimo maior do que $\overline{1}$ de um número maior do que $\overline{1}$ é primo: $\psi(a, b) \rightarrow b$ é primo, onde ψ é como acima.

Pois $\psi(a, b)$ exprime que $b > \overline{1}$ e b é um divisor mínimo de a; para provar que b é primo só falta provar que $\neg\exists z\, (\overline{1} < z < b \wedge z \mid b)$. Suponhamos, com vista a um absurdo, que existia c tal que $\overline{1} < c < b$ e $c \mid b$; visto que $b \mid a$, também $c \mid a$, logo c é um divisor de a maior do que $\overline{1}$ e menor do que b, contrariando a minimalidade de b. De seguida:

(3) Se $a > \overline{1}$, então existe um número $d > 0$ que divide todos os números y tais que $0 < y \leq a$.

Prova-se $a > \overline{1} \rightarrow \exists x\, (0 < x \wedge \forall y\, (0 < y \leq a \rightarrow y \mid x)$ por indução em a, o que deixamos como exercício. Finalmente:

(4) Se $a > \overline{1}$ e d é como em (3), então o divisor mínimo maior do que $\overline{1}$ de $d + \overline{1}$ é um primo maior do que a.

Um tal d é $\geq \overline{2}$, donde $d + \overline{1} > \overline{1}$; por (1), com $d + \overline{1}$ no lugar de a, tem-se $\psi(d + \overline{1}, b)$ para algum b, e por (2) um tal b é primo, só faltando ver que $b > a$. Ora $\psi(d + \overline{1}, b)$ implica $b \mid (d + \overline{1})$ e $b > \overline{1}$, logo b não divide d [T_{42} (x)]. Por outro lado, por hipótese sobre d,

$$\forall y\, (0 < y \leq a \rightarrow y \mid d),$$

donde, em particular, $0 < b \leq a \rightarrow b \mid d$, mas, como b não divide d, tem de ser $b > a$, por tricotomia.■

Terminamos esta secção com um importante resultado acerca da representação dos números como produtos de primos.

T_{45}. LEMA DA DECOMPOSIÇÃO

Todo o número maior do que $\overline{1}$ é primo ou um produto de primos.

Dem. Demonstramos

$$\phi(a): \quad a > \overline{1} \rightarrow a \text{ é primo ou um produto de primos}$$

por indução completa (IC_1) em a. Suponhamos que (HI) $\forall x < a\, \phi(x)$ com vista a mostrar que $\phi(a)$. Supondo então $a > \overline{1}$, tem-se $a = \overline{2}$ ou $a > \overline{2}$; no primeiro caso, a é primo, e nada mais há a fazer; no segundo caso, se a é primo, nada mais há a fazer, e se a é composto, digamos $a = bc$, com b, c ambos menores do que a, então, pela hipótese de indução b e c são primos ou produtos de primos, donde se conclui, em qualquer dos casos, que $a = bc$ é um produto de primos.■

Este resultado estabelece a *existência* de uma decomposição (ou factorização) em factores primos de qualquer número composto maior do que $\overline{1}$. Em $\mathbb{N}$ os primos de uma tal decomposição de um número $n \geq 2$, digamos

$$n = p_1 \times p_2 \times \cdots \times p_r \tag{1}$$

não são necessariamente distintos, mas primos iguais podem ser agrupados em potências de expoentes positivos, e ordenados por ordem crescente, digamos

$$n = p_1^{e_1} \times p_2^{e_2} \times \cdots \times p_k^{e_k} \tag{2}$$

com $e_i > 0$ ($i = 1, ..., k$) e $p_1 < p_2 < ... < p_k$. Uma decomposição desta forma diz-se **canónica**. Nada assegura, por enquanto, que uma decomposição canónica de um número n seja *única.* A *unicidade* de uma decomposição canónica em factores primos de um número natural $n \geq 2$ é um resultado tão importante para a teoria dos números que tem o nome de *teorema fundamental.* Há várias maneiras de obter este resultado de unicidade da decomposição em factores primos. Aquela que preferimos baseia-se no chamado *algoritmo de Euclides (das divisões sucessivas)* para determinação do *máximo divisor comum* de dois números naturais não ambos nulos (ver exercícios 4.20, 4.21). É possível, por certos artifícios, e desenvolvendo um tanto mais a teoria, obter uma demonstração do algoritmo de Euclides na teoria **AP**. Em todo o caso, só necessitamos, para as aplicações que temos em vista, do resultado seguinte, igualmente atribuído a Euclides, o qual pode ser demonstrado em **AP** sem passar pelo Algoritmo de Euclides.

T_{46}. Se um primo p divide um produto ab, então $p \mid a$ ou $p \mid b$.

Deixamos a demonstração para o exercício 4.19(b). Uma consequência (quase) imediata [4.19(d)] é:

T_{47}. COROLÁRIO

Se um primo p divide um produto de primos $p_1 \cdots p_k$, então $p = p_i$ para algum i.

T_{48}. TEOREMA FUNDAMENTAL DA ARITMÉTICA

A decomposição em factores primos de $n \geq \overline{2}$ é única, a menos da ordem dos mesmos. Em particular, a decomposição canónica é única.[158]

Dem. Chamemos *anormais* aos números $n \geq \overline{2}$ que possuem mais de uma decomposição e suponhamos, com vista a um absurdo, que existe, pelo menos, um número anormal. Então existe o menor desses números, digamos n_0. Um mesmo primo p não pode ocorrer em duas decomposições canónicas de n_0, pois, caso contrário, n_0/p[159] seria anormal e menor do que n_0, contrariando a minimalidade de n_0. Temos, pois

$$n_0 = p_1 \times p_2 \times p_3 \times \cdots \times p_r = q_1 \times q_2 \times \cdots \times q_s$$

em que os p_i e os q_j são primos, e nenhuma igualdade $p_i = q_j$ tem lugar. Sem perda de generalidade podemos supor que p_1 é o menor dos p_i, e analogamente q_1 o menor dos q_j. Como n_0 é composto, tem-se

$$p_1 \cdot p_1 \leq n_0 \text{ e } q_1 \cdot q_1 \leq n_0$$

donde $p_1 \cdot q_1 < n_0$, visto que $p_1 \neq q_1$. Sendo m tal que $p_1 \cdot q_1 + m = n_0$, tem-se $0 < m < n_0$ e m não é anormal. Ora, $p_1 \mid n_0$, logo $p_1 \mid m$, e analogamente $q_1 \mid m$, o que significa que, quer p_1, quer q_1, ocorrem na decomposição (única) de m, e, além disso, $p_1 \cdot q_1$ divide m, donde se conclui que $p_1 \cdot q_1$ divide n_0 e, portanto, que q_1 divide

$$\frac{n_0}{p_1} = p_2 \times \cdots \times p_r$$

Esta factorização é única (àparte a ordem dos factores), pois n_0/p_1 é menor do que n_0, o que significa, pelo corolário T_{47} acima, que q_1 é igual a um dos p_i ($i = 2$, ..., r), o que é impossível, como acima se viu.■

IV.6 Modelos de AP

Como já se disse, a estrutura $\mathfrak{N} = (\mathbb{N}, +, \times, \uparrow, ', <, 0)$ é um modelo de **AP**, chamado o **modelo standard** desta teoria. A existência deste modelo prova que a teoria **AP** é **consistente** (ou **não contraditória**), no sentido de que não existe nenhuma sentença ϕ de $\mathcal{L}_{\text{ar}}$ tal que $\mathbf{AP} \vdash \phi \wedge \neg\phi$. Mas não se deve perder de vista que a prova de que $\mathfrak{N}$ é modelo de **AP** é de natureza abstracta, por fazer uso de noções semânticas conjuntistas («infinitárias») que transcendem o aparato

---

[158] A demonstração é adaptada de HARDY & WRIGHT, *op. cit.*, p. 21, mas é devida a E. Zermelo.

[159] A notação n/p pressupõe, como é óbvio, a unicidade de z tal que $pz = n$. Um tal z denota-se n/p, ou $n \div p$.

puramente aritmético. Pelo menos na aparência, a afirmação «**AP** é consistente» é mais fraca do que a afirmação «$\mathfrak{N}$ é um modelo de **AP**», no sentido de ser talvez possível demonstrá-la de maneira mais «elementar» ou «finitária». Assim se pensava nos anos vinte deste século, e toda uma escola de eminentes matemáticos e lógicos dirigida por David Hilbert elaborou um ambicioso programa que incluía, como componente fundamental, a busca de uma demonstração «finitária» ou «finitista» da consistência de **AP**, primeiro passo para voos mais altos (consistência da teoria axiomática dos conjuntos). Cedo se descobriu, porém, que tal empreendimento estava destinado ao fracasso. Mais diremos sobre esta questão nas secções seguintes.

Provaremos nesta secção que existem modelos **não-standard** de **AP**, isto é, modelos não isomorfos a $\mathfrak{N}$. Isto é já uma indicação de que os axiomas de **AP** não caracterizam axiomaticamente (a menos de isomorfismo) o modelo intencional $\mathfrak{N}$, o que, por sua vez, sugere logo outra questão: será possível acrescentar alguns axiomas de modo a caracterizar $\mathfrak{N}$? A resposta a esta questão também é negativa, como veremos, se exigirmos que o novo sistema de axiomas (contendo os axiomas de **AP**) seja «razoável» (em sentido a precisar).

Seja $\mathcal{L}'$ a linguagem que se obtém de $\mathcal{L}_{\text{ar}}$ juntando uma nova constante c e consideremos o conjunto Σ de sentenças de $\mathcal{L}'$ constituído por:

- todas as sentenças de $\mathcal{L}_{\text{ar}}$ verdadeiras em $\mathfrak{N}$,[160] e
- todas as sentenças de $\mathcal{L}'$ da forma $\overline{n} < c$, com n em $\mathbb{N}$.

Aplicaremos o metateorema da compacidade (ver pág. 94) para mostrar que Σ é compatível, isto é, possui um modelo. Pois seja Σ_0 um subconjunto finito ao arbítrio de Σ. Em Σ_0 há, quando muito, um número finito de sentenças da forma $\overline{n} < c$, digamos

$$\overline{n}_1 < c, \overline{n}_2 < c, ..., \overline{n}_k < c$$

Σ_0 possui um modelo: basta pensar na estrutura $\mathfrak{N}' = (\mathbb{N}, ..., m)$, onde m é a interpretação de c, e é um qualquer número natural maior do que n_1, n_2, ..., n_k, o que é possível fazer-se, pois estes são em número finito. Portanto, Σ_0 é compatível. Pelo metateorema da compacidade, o conjunto Σ é compatível, isto é, possui, pelo menos, um modelo. Seja

$$\mathfrak{M}' = (M, +, ..., 0, m)$$

um modelo de Σ, onde $+$, ..., 0 são as interpretações dos símbolos $+$, ..., $<$ de $\mathcal{L}_{\text{ar}}$, respectivamente, e m é a interpretação da constante c. É claro que $\mathfrak{M}'$ é uma estrutura para $\mathcal{L}'$, logo o reduto $\mathfrak{M} = (M, +, ..., 0)$ é uma estrutura para $\mathcal{L}_{\text{ar}}$. Em

---

[160] O conjunto de todas estas sentenças chama-se **teoria de** $\mathfrak{N}$, **aritmética verdadeira**, ou **aritmética completa**, e denota-se Th($\mathfrak{N}$) (ver final de III.7 e exercício 3.17). Pelo que acima se disse, todos os axiomas de **AP**, portanto também os teoremas de **AP**, estão em Th($\mathfrak{N}$).

todo o caso, $\mathfrak{M}$ é um modelo de **AP** (por ser modelo das sentenças de $\mathcal{L}_{\text{ar}}$ verdadeiras em $\mathfrak{N}$, incluídas em Σ), e há em M um elemento m com uma propriedade muito especial:

(*) $$\text{para todo } n \in \mathbb{N},\ \overline{n}^{\mathfrak{M}} < m,$$

pois $\mathfrak{M}'$ é modelo de todas as sentenças da forma $\overline{n} < c$ ($n \in \mathbb{N}$), e as interpretações de $\overline{n}$ em $\mathfrak{M}'$ e em $\mathfrak{M}$ são idênticas. Tal estrutura $\mathfrak{M}$ não pode ser isomorfa a $\mathfrak{N}$: um isomorfismo h de $\mathfrak{N}$ em $\mathfrak{M}$ teria de aplicar os números naturais nas interpretações em $\mathfrak{M}$ dos numerais, isto é,

$$n = \overline{n}^{\mathfrak{N}} \ \mapsto\ h(n) = \overline{n}^{\mathfrak{M}}$$

mas então nunca o elemento m de M poderia ser imagem por meio de h de um elemento de $\mathbb{N}$, pois, como acima se viu (*), é $h(n) < m$ para todo $n \in \mathbb{N}$.■

Os elementos de um modelo não-standard $\mathfrak{M}$ de **AP** da forma $\overline{n}^{\mathfrak{M}}$, com $n \in \mathbb{N}$, dizem-se **standard**, dizendo-se **não-standard** (ou **infinitamente grandes**) todos os restantes.[161]

IV.7 Metateoria. Os metateoremas de Gödel e Tarski

Concluimos este capítulo dando uma (assaz grosseira) ideia de alguns dos resultados mais profundos da lógica matemática obtidos neste século, precisamente a propósito da teoria **AP** e de teorias nas quais se possa «mergulhar» a aritmética de Peano (como a teoria axiomática dos conjuntos). Os pormenores mais «dolorosos» serão omitidos pois excedem o âmbito introdutório deste livro.

Idealmente, uma teoria formal é consistente, completa e decidível. Expliquemos estes conceitos a propósito de **AP**. A *consistência* já foi definida anteriormente: somente verdades são demonstráveis. A *completude* de **AP** significaria: toda a sentença aritmética verdadeira (subentende-se sempre: em $\mathfrak{N}$) é teorema, isto é, todas as verdades são demonstráveis. Finalmente, a *decidibilidade* é um conceito muito geral, aplicável a conjuntos e relações de números naturais, ou de outras entidades, como símbolos, termos, fórmulas e sentenças, e em particular a teorias (em linguagens numeráveis).

---

[161] O estudo de modelos *não standard* de **AP** é um tema «quente» em lógica matemática. V., por exemplo, o artigo de C. SMORYNSKI "Lectures on non-standard models of arithmetic", *in* G. LOLLI, G. LONGO & A. MARCJA (editors), *Logic Colloquium '82,* North-Holland, 1984. Fazendo para a estrutura dos números reais $(\mathbb{R},\dots)$ algo semelhante ao que acima se fez para $(\mathbb{N},\dots)$ resulta um **modelo não standard da Análise**, base de um importante novo método em análise (a chamada *análise não standard*), criada a partir dos anos sessenta pelo matemático ameriano de origem judaica A. Robinson. Para uma introdução, ver o nosso livrinho *Infinitesimais: Passado, Presente e Futuro*, Dep. Mat. Un. Évora, 1987. A monografia de ROBINSON é já um clássico, mas um pouco «duro» de roer. Ver também o final da secção 5.4.

Recorde-se (II.12) que um conjunto S é *decidível* sse existe um método ou processo de decisão para o conjunto: um algoritmo que permite decidir, num número finito de passos, para cada entidade $\boldsymbol{s}$, se $\boldsymbol{s}$ é ou não elemento de S. Dizer que **AP** é decidível é dizer que existe um algoritmo que permite decidir (num número finito de passos), para cada sentença (sem parâmetros) ϕ de $\mathcal{L}_{\text{ar}}$, se ϕ é ou não teorema de **AP**. Na verdade, o conjunto dos axiomas de **AP**, embora infinito, é decidível, mas pode-se provar que o conjunto dos teoremas de **AP** não é decidível.[162]

No final do Cap. II foi referido que o sistema **DN** é consistente. Visto de outro modo, o conjunto das leis ou teoremas lógicos proposicionais é consistente; este mesmo conjunto é completo, considerando como verdades exactamente as fórmulas válidas ou tautologias (em virtude do metateorema de completude semântica); e é decidível, pois a construção de uma tabela de verdade é um procedimento algorítmico que, aplicado a qualquer fórmula proposicional ϕ, permite decidir ao fim de um número finito de passos se ϕ é ou não válida (e, portanto, se ϕ é ou não teorema lógico). Analogamente (final do Cap. III), o sistema **DNQ** é consistente e completo (considerando como verdades as sentenças universalmente válidas), mas já não é de esperar que seja decidível, e pode-se demonstrar que, de facto, não o é.

Podemos mesmo dizer que as noções sintáticas relativas a uma teoria **T** numa linguagem elementar $\mathcal{L}$ são, em regra, decidíveis, desde que o conjunto dos símbolos seja decidível. E, relativamente a **AP** na linguagem $\mathcal{L}_{\text{ar}}$, mediante um elaborado processo de codificação e representação, tais noções podem ser expressas na própria linguagem $\mathcal{L}_{\text{ar}}$ (convenientemente ampliada com os símbolos definidos pertinentes).

Em primeiro lugar, a *codificação* (ou *godelização*) consiste em associar números naturais aos símbolos, expressões (termos e fórmulas) e sequências finitas de expressões (deduções) de $\mathcal{L}_{\text{ar}}$. Aos símbolos

$$\neg,\ \wedge,\ \vee,\ \rightarrow,\ (,\ ),\ \forall,\ \exists,\ =,\ 0,\ ',\ +,\ \times,\ \uparrow,\ <$$

associamos os números 1, 2, 3, ..., 15, respectivamente; às variáveis x_i ($i \geq 0$), associamos os números $17 + 2i$, e aos parâmetros a_j ($j \geq 0$) associamos os números $17 + (2j + 1)$.

Seja $\#s$ o número associado ao símbolo s, também chamado o *código* de s. De seguida, a cada expressão $s_1\ s_2\ ...\ s_k$ associamos o número

$$2^{\#s_1} \times 3^{\#s_2} \times \cdots \times p_k^{\#s_k}$$

onde p_k é o $(k + 1)$-ésimo número primo ($p_0 = 2$, $p_1 = 3$, $p_2 = 5$, etc.).

Denotemos por $\#\xi$ o número associado ou código da expressão ξ.

---

[162] Só é possível estabelecer a impossibilidade de um algoritmo de decisão utilizando noções matematicamente precisas de algoritmo, conjunto decidível, etc., formuladas no ramo da lógica matemática conhecido por teoria da computabilidade.

Finalmente, a cada sequência finita de expressões (como uma dedução) ξ_1, ξ_2, ..., ξ_m associamos o código

$$3^{\#\xi_1} \times 5^{\#\xi_2} \times \cdots \times p_{m+1}^{\#\xi_m}$$

Certas relações entre objectos sintácticos, como, por exemplo, «ϕ é uma fórmula e a é um parâmetro e a ocorre em ϕ» irão ser traduzidas em relações numéricas entre os respectivos números de código, e, por sua vez, representadas na teoria **AP** por fórmulas de $\mathcal{L}_{\text{ar}}$, no sentido da definição seguinte:

Definição. Uma relação $R \subseteq \mathbb{N}^k$ ($k \geq 1$) diz-se **representável** numa teoria **T** (na linguagem $\mathcal{L}_{\text{ar}}$) sse existe uma sentença $\phi(a_1, ..., a_k)$ com exactamente k parâmetros como exibidos tal que, para quaisquer números naturais n_1, ..., $n_k \in \mathbb{N}$,

(i) Se $(n_1, ..., n_k) \in R$, então $\mathbf{T} \vdash \phi(\overline{n}_1, ..., \overline{n}_k)$; e

(ii) Se $(n_1, ..., n_k) \notin R$, então $\mathbf{T} \vdash \neg\phi(\overline{n}_1, ..., \overline{n}_k)$.

De imediato se conclui que, se **T** é um modelo de $\mathfrak{N}$ e a relação R é representável em **T**, então R é definível em $\mathfrak{N}$ por qualquer fórmula que a represente em **T**. Isto acontece, em particular, quando **T** é a teoria **AP**. Pode-se provar, por outro lado, que as relações numéricas representáveis em **AP** são exactamente as relações decidíveis.

O resultado final de todos estes procedimentos[163] é a obtenção de uma sentença com um só parâmetro a:

$$\mathit{Teor}(a)$$

que representa o conjunto dos códigos dos teoremas de **AP**, isto é, que exprime (interpretada em $\mathfrak{N}$) que

«a é o número de um teorema de **AP**»

Vamos então supor, com vista a obter uma contradição, que

(1) Os teoremas de **AP** são exactamente as verdades aritméticas, isto é, as sentenças de $\mathcal{L}_{\text{ar}}$ verdadeiras no modelo *standard* $\mathfrak{N}$.

Chamemos **sentença número** n, e denotemos por ϕ_n, a sentença de $\mathcal{L}_{\text{ar}}$ cujo código é n, se existe alguma tal contendo o parâmetro a e nenhum outro, e a sentença $a \neq a$ no caso contrário. Seja ainda Φ_n o conjunto dos números $m \in \mathbb{N}$ que satisfazem ϕ_n em $\mathfrak{N}$:

---

[163] Em qualquer compêndio de lógica matemática os pormenores da codificação e representação ocupa uma dezena de páginas. V., por exemplo, o nosso *Lógica e Fundamentos II,* embora pressupondo uma formalização da lógica diferente da apresentada no presente livro.

(2) $\Phi_n = \{m \in \mathbb{N} : \mathfrak{N} \vDash \phi_n(a)[m]\} = \{m \in \mathbb{N} : \mathfrak{N} \vDash \phi_n(\overline{m})\}$

Note-se que, se ϕ_n é $a \neq a$, então $\Phi_n = \emptyset$. Em qualquer dos casos, para cada $m \in \mathbb{N}$,

$m \in \Phi_n$ sse (*) { n é o código de uma sentença na qual ocorre o parâmetro a e nenhum outro, e a sentença que resulta substituindo toda a ocorrência de a pelo numeral de m é verdadeira em $\mathfrak{N}$, ou seja, por (1), é teorema de **AP**

sse $\mathfrak{N} \vDash \phi_n(\overline{m})$, por definição de ϕ_n,
sse **AP** $\vdash \phi_n(\overline{m})$, por (1).

Mas todos os conceitos e predicados utilizados em (*) são decidíveis (por exemplo, «ψ é uma sentença», «n é o código de uma sentença», «o parâmetro a ocorre na sentença ψ», «ψ é um teorema de **AP**»,[164] etc.), de modo que também o predicado ou relação binária «$m \in \Phi_n$» é representável em **AP** por uma sentença com dois parâmetros apenas, digamos *Dem*(a, b), que exprime (informalmente) «a satisfaz a fórmula número b», tal que, para quaisquer m, $n \in \mathbb{N}$,

(3) $m \in \Phi_n$ sse $\mathfrak{N} \vDash$ *Dem*(a, b) $[m, n]$ sse $\mathfrak{N} \vDash$ *Dem*$(\overline{m}, \overline{n})$
sse **AP** $\vdash$ *Dem*$(\overline{m}, \overline{n})$.

Consideremos agora a sentença $\neg$*Dem*(a, a), que designamos por $\gamma(a)$. Esta passagem é reminiscente do **método de diagonalização** inventado por G. Cantor, e podemos mesmo chamar a $\gamma(a)$ a diagonalizada de *Dem*(a, a).[165] Esta sentença

---

[164] Chama-se a atenção para o facto de «ψ é um teorema de **AP**» ser decidível somente na hipótese muito especial (1) que se fez na página anterior, de que os teoremas de **AP** são exactamente as sentenças verdadeiras no modelo standard. Sob esta hipótese, obtém-se um método de decisão para os teoremas através de uma simples enumeração dos mesmos: para qualquer sentença ψ, como ψ ou é verdadeira ou é falsa (e, portanto, $\neg\psi$ é verdadeira), uma das sentenças ψ, $\neg\psi$ há-de ocorrer mais tarde ou mais cedo na enumeração. Sem aquela hipótese, porém, aquele predicado não é decidível, como foi dito, aliás, na pág. 263.

[165] Recorde-se, para efeitos comparativos, a demonstração de Cantor de que o cardinal de um conjunto M é menor do que o cardinal do conjunto das partes de M, $\mathcal{P}(M)$. O passo relevante desta demonstração consiste em provar que não existe nenhuma aplicação sobrejectiva de M no conjunto $\mathcal{P}(M)$: para qualquer aplicação $f : M \to \mathcal{P}(M)$, denotando o valor de f em $a \in M$ por X_a, defina-se (por «diagonalização») o conjunto

$$Y = \{a \in M : a \notin X_a\} \in \mathcal{P}(M).$$

Imediatamente se conclui que, para qualquer $m \in M$, $Y \neq X_m$ (pois $m \in Y$ sse $m \notin X_m$), o que prova que f não é sobrejectiva.

$\gamma(a)$ tem um código, digamos $k = \#\neg Dem(a, a) = \#\gamma(a)$, e é, portanto, a sentença $\phi_k(a)$, na enumeração das sentenças de $\mathcal{L}_{\text{ar}}$ acima definida. Atendendo às definições e a (1), tem-se:

$$\begin{aligned} k \in \Phi_k \quad &\text{sse} \quad \mathbf{AP} \vdash \phi_k(\overline{k}) \\ &\text{sse} \quad \mathbf{AP} \vdash \neg Dem(\overline{k}, \overline{k}) \\ &\text{sse} \quad \mathfrak{N} \vDash \neg Dem(\overline{k}, \overline{k}) \\ &\text{sse} \quad k \notin \Phi_k, \end{aligned}$$

o que é absurdo. O absurdo resultou da suposição (1), mais particularmente da suposição de que todas as sentenças aritméticas verdadeiras são teoremas de **AP**. Podemos concluir, portanto, que existem sentenças aritméticas verdadeiras que não são teoremas de **AP**. Esta conclusão constitui uma forma fraca do chamado

Iº METATEOREMA DE INCOMPLETUDE DE GÖDEL

Se os axiomas de **AP** *são verdadeiros, então existem verdades que não são teoremas.*

Por outras palavras, se os teoremas de **AP** são verdadeiros, então **AP** é incompleta. Podemos mesmo indicar uma sentença verdadeira que não é teorema de **AP**: a sentença que exprime que $k \notin \Phi_k$, $\gamma(\overline{k})$, a que chamaremos **sentença de Gödel**. Com efeito, esta sentença é verdadeira se e somente se $\gamma(\overline{k})$ não é teorema de **AP**; portanto, se $\gamma(\overline{k})$ fosse teorema, $\gamma(\overline{k})$ seria falsa, contrariando a suposição de que os teoremas são verdadeiros, logo $\gamma(\overline{k})$ não é teorema, e por conseguinte $\gamma(\overline{k})$ é verdadeira. Além disso, sendo $\gamma(\overline{k})$ verdadeira, $\neg\gamma(\overline{k})$ é falsa, e portanto $\neg\gamma(\overline{k})$ também não pode ser teorema.

A sentença de Gödel $\gamma(\overline{k})$ é, pois, um exemplo de *uma sentença aritmética (verdadeira) que não é teorema,* e a sua negação tão-pouco é teorema. Dizemos, por isso, que é uma sentença **formalmente indecidível** na teoria **AP**. De notar que a veracidade desta sentença aritmética foi estabelecida por raciocínio metamatemático (relativamente à «matemática» em **AP**), método inteiramente novo, portanto, embora se possa dizer, com alguma razão, que uma tal sentença tem muito pouco interesse do ponto de vista matemático comum. Desde 1976, porém, são conhecidas diversas proposições aritméticas verdadeiras (demonstradas na teoria dos conjuntos), de cariz matemático, que não são teoremas de **AP**.[166]

Refinando o argumento acima, obtém-se a incompletude de **AP** na mera suposição de consistência de **AP**. Diversos outros refinamentos são possíveis, e até a teoria **AP** pode ser modificada em diferentes sentidos, continuando-se a verificar o fenómeno de incompletude. Nomeadamente, poderá enriquecer-se a linguagem, e até a lógica subjacente, poderão juntar-se novos axiomas (lista decidível), mas continuará a manifestar-se o fenómeno de incompletude, desde que os conceitos

[166] V. o artigo de J. PARIS & L. HARRINGTON "A mathematical incompleteness in Peano Arithmetic", incluído na colectânea editada por J. BARWISE (ver bibliografia), pp. 1133-1142.

sintácticos pertinentes continuem decidíveis e representáveis. **AP** é não apenas incompleta, é *incompletável,* desde que se mantenham certos requisitos naturais (como a decidibilidade da lista de axiomas, entre outros).

Num outro sentido mais dramático, por ter maiores implicações para os fundamentos da matemática, obtém-se o

IIº METATEOREMA DE INCOMPLETUDE DE GÖDEL

Se **T** *é uma teoria com um sistema decidível de axiomas, contendo a aritmética de Peano, e consistente, então existe uma sentença aritmética,* $Cons_{\mathbf{T}}$, *que exprime* «**T** *é consistente*», *mas que não é teorema de* **T**.

«Conter» a aritmética de Peano significa aqui que, ou a linguagem $\mathcal{L}$ de **T** é uma extensão da linguagem $\mathcal{L}_{\text{ar}}$ e os axiomas de **AP** são axiomas ou teoremas de **T**, ou é possível «traduzir» o formalismo de **AP** no formalismo de **T** de tal modo que os axiomas de **AP** sejam traduzidos em axiomas ou teoremas de **T** (na terminologia da lógica, está em jogo uma **interpretação sintática** de **AP** em **T**). Tal é o caso, por exemplo, relativamente às modernas teorias axiomáticas de conjuntos ou de classes (Zermelo-Fraenkel, Bourbaki, ou Von-Neumann-Gödel-Bernays, ver MENDELSON, HATCHER).

Mas regressemos à nossa modesta digressão, rematando com outro facto interessante acerca de **AP**.

Dissemos atrás que dar um exemplo de um subconjunto de $\mathbb{N}$ não definível em $\mathfrak{N}$ não é tarefa fácil. Pois podemos agora indicar um tal exemplo: o conjunto $V^{\mathfrak{N}}$ dos códigos das sentenças sem parâmetros verdadeiras no modelo standard $\mathfrak{N}$ [isto é, membros de $\text{Tr}(\mathfrak{N})$].

Com efeito, suponhamos, com vista a um absurdo, que tal conjunto é definível, digamos por uma sentença com um único parâmetro

$$\mathit{Verd}(a)$$

Definamos, à semelhança do que se fez acima, para cada natural n, o conjunto Ψ_n dos naturais m que satisfazem ϕ_n em $\mathfrak{N}$; quer dizer, para todo m,

$$m \in \Psi_n \text{ sse } \begin{cases} n \text{ é o código de uma sentença onde ocorre o parâmetro} \\ a \text{ e nenhum outro, e a sentença que dela resulta, substi-} \\ \text{tuindo } a \text{ por } \overline{m}, \text{ é verdadeira em } \mathfrak{N}. \end{cases}$$

Então a relação «$m \in \Psi_n$» é definível em $\mathfrak{N}$, digamos, por uma sentença com dois parâmetros $\mathit{Sat}(a, b)$. Seja $\tau(a)$ a sentença

$$\neg \mathit{Sat}(a, a),$$

e seja k o seu código,

$$k = \#\tau(a).$$

Tem-se, pois, em particular,

$$\begin{array}{lll} k \in \Psi_k & \text{sse} & \phi_k(\overline{k}) \text{ é verdadeira} \\ & \text{sse} & \tau(\overline{k}) \text{ é verdadeira} \\ & \text{sse} & k \notin \Psi_k, \end{array}$$

o que é, mais uma vez, absurdo. Concluindo:

METATEOREMA DE TARSKI
O conjunto das verdades aritméticas não é aritmeticamente definível.■

IV.8 Exercícios e Complementos

4.1 Demonstre os teoremas T_2 a T_{10}.

4.2 Demonstre os teoremas T_{12} e T_{13} e as regras das potências T_{15} e T_{16}.

4.3 Demonstre os teoremas T_{18} a T_{22} e T_{24}.

4.4 Demonstre os teoremas T_{26} e T_{27}.

4.5 Demonstre a equivalência entre a 1ª e a 2ª formas do princípio de indução completa.

4.6 Demonstre os teoremas T_{30} a T_{32} e T_{35} a T_{41}.

4.7 Demonstre os seguintes teoremas de **AP**:

(a) $\forall xy(xy = 0 \rightarrow x = 0 \vee y = 0)$;

(b) $\forall x(x < x')$;

(c) $\forall xy(x \leq y \vee y \leq x)$;

(d) $\forall x(x \neq 0 \leftrightarrow x > 0)$;

(e) $\forall xy(x > 0 \wedge y > 0 \rightarrow xy > 0)$;

(f) $\forall xy(x \leq y \wedge y \leq x \rightarrow x = y)$.

4.8 Demonstre a seguinte *propriedade de Arquimedes*: para quaisquer números a, b, tais que $\overline{1} \leq a < b$ existe um número n tal que $b < na$.

4.9 Prove que para quaisquer números a, b, c,

(a) Se $a = bc$ e $a < b$, então $a = 0$;

(b) Se $a = bc$ e $a \neq 0$, então $b \leq a$ e $c \leq a$.

4.10 Prove que para qualquer número n,

$$\overline{1}^n = \overline{1}, \text{ e } n > 0 \to 0^n = 0.$$

4.11 Prove que para quaisquer números a, n

(a) $a \neq 0 \to a^n \neq 0$;

(b) $a > \overline{1} \ \wedge a^n = \overline{1} \to n = 0$;

(c) $a \geq \overline{1} \wedge n \geq \overline{2} \to (\overline{1} + a)^n > \overline{1} + na$.

4.12 Prove que, sob hipóteses convenientes [por exemplo, $a \geq b$ em (b), para que $a - b$ faça sentido]:

(a) $(n + \overline{1})(n - \overline{1}) + \overline{1} = n^{\overline{2}}$; (b) $(a + b)(a - b) = a^{\overline{2}} - b^{\overline{2}}$;

(c) $(a \pm b)^{\overline{2}} = a^{\overline{2}} \pm \overline{2}ab + b^{\overline{2}}$; (d) $(\overline{2}n + \overline{1})(\overline{2}n - \overline{1}) + \overline{1} = (\overline{2}n)^{\overline{2}}$;

(e) Se $a \neq b$, $(a + b)^{\overline{2}} > \overline{4}ab$; (f) $a \geq \overline{2} \ \wedge \ m < n \to a^m < a^n$;

(g) $a \geq \overline{2} \wedge a^m = a^n \to m = n$; (h) $a < b \wedge n > 0 \leftrightarrow a^n < b^n$;

(i) $n > 0 \ \wedge a^n = b^n \to a = b$;

(j) Se a, m, não são ambos nulos, $a < b$ e $m < n$, então $a^m < b^n$.

4.13 Complete a demonstração do teorema T_{42}.

4.14 Prove que a relação de divisibilidade $\mid$ é reflexiva, simétrica e transitiva.

4.15 Sendo a, b números, com $b > 0$, represente-se por $\text{qt}(a, b)$ e $\text{rt}(a, b)$ o quociente e o resto da divisão inteira de a por b, respectivamente. Supondo $a = bq + r$ e $r < b$, prove que

(a) $n > 0 \to (\text{qt}(na, nb) = q \wedge \text{rt}(na, nb) = nr)$;

(b) $\text{qt}(a + bm, b) = q + m \wedge \text{rt}(a + bm, b) = r$;

(c) $a \geq q$; (d) $b > \overline{1} \to a > q$; (e) $a \geq \overline{2}r$;

(f) Todo o número que divide a e b divide r e todo o número que divide b e r divide a.

4.16 Seja $\phi(x)$ uma fórmula somente com x livre (e possivelmente com parâmetros) tal que:

(i) $\exists x \, \phi(x)$,

(ii) $\forall x \, y \, (\phi(x) \wedge \phi(y) \to \phi(x + y))$, e

(iii) $\forall x \, y \, (x \geq y \wedge \phi(x) \wedge \phi(y) \to \phi(x - y))$.

Prove que $\exists z \, (\, \forall x \, (\, \phi(x) \leftrightarrow x \mid z))$.

4.17 Dados a, $b \in \mathbb{N}$ não ambos nulos, um número natural $d > 0$ diz-se **um máximo divisor comum** de a e b sse

(i) $d \mid a \wedge d \mid b$; e

(ii) $\forall c\,(c \mid a \wedge c \mid b \rightarrow c \mid d)$.

Prove que um máximo divisor comum de a e b, se existir, é único, e é $\geq$ que qualquer divisor comum de a e b.

NOTA. No exercício a seguir prova-se (em **AP**) que existe sempre **o** máximo divisor comum de dois números não ambos nulos. Mais adiante, outro exercício (ALGORITMO DE EUCLIDES) fornece também um método para calcular (em $\mathbb{N}$) o máximo divisor comum de dois números naturais não ambos nulos. O máximo divisor comum de a e b denota-se $D(a,b)$ [ou mdc(a,b)]. Note-se desde já que $D(a,b) = D(b,a)$ e $D(a,0) = a$.

4.18 Sejam a, b, números não ambos nulos e $\phi(x)$ a fórmula (com parâmetros a, b) $\exists m\, n(x = am - bn \vee x = bn - am)$.

(a) Prove que $\exists x(x > 0 \wedge \phi(x))$;

(b) Sendo d o número mínimo tal que $\phi(d)$ [que existe pelo princípio de mínimo (Min)], prove que $d = D(a,b)$ [isto é, que d tem as propriedades (i) e (ii) da definição acima].

4.19 Dois números a, b tais que $D(a,b) = \overline{1}$ dizem-se **primos entre si** [ou a (b) diz-se **primo com** b (a, respectivamente)]:

(a) Prove que os números a, b são primos entre si sse existem naturais m, n tais que $\overline{1} = ma - nb$ ou $\overline{1} = nb - ma$.

(b) Prove que se um número a divide um produto bc e é primo com um dos factores, então divide o outro factor. [Use (a)]

(c) Prove que se um primo p divide um produto de primos $q_1 q_2$, então $p = q_1$ ou $p = q_2$.

(d) Generalize o resultado anterior (por indução metamatemática) a um produto de mais de dois factores primos.

NB. Os exercícios seguintes dizem respeito à estrutura $(\mathbb{N}, ...)$.

4.20 (ALGORITMO DE EUCLIDES) Prove que para quaisquer números naturais a, b não ambos nulos existe o máximo divisor comum de a e b. [V. indicações nas Soluções.]

4.21 (REPRESENTAÇÃO DO MDC) Prove, utilizando a demonstração do algoritmo de Euclides, que para quaisquer naturais a, b, não ambos nulos, existem naturais m, n tais que (i) $D(a,b) = ma - nb$ ou (ii) $D(a,b) = nb - ma$.

4.22 Prove, utilizando a demonstração do algoritmo de Euclides, que se $d = D(a,b)$, então $dc = D(ac,bc)$.

4.23 (a) Prove que os naturais a, b são primos entre si sse existem naturais m, n tais que $1 = ma - nb$ ou $1 = nb - ma$.

(b) Prove que se um natural a divide um produto bc e é primo com um dos factores, então divide o outro factor. [Use (a)]

(c) Prove que se um primo p divide um produto de primos $q_1 q_2$, então $p = q_1$ ou $p = q_2$.

(d) Generalize o resultado anterior (por indução) a um produto de mais de dois factores primos.

4.24 (CRIVO DE ERATÓSTENES) Prove que, se $1 \neq p < n^2$ e p não é divisível por nenhum natural q tal que $1 < q < n$, então p é primo.

4.25 Calcule os códigos de alguns termos e sentenças de $\mathcal{L}_{\text{ar}}$.

Capítulo V

O QUE É A LÓGICA MATEMÁTICA?

V.1 Explicação prévia

A questão que dá o título a este capítulo seria normalmente respondida (tentativamente) no início do livro. Não o fiz por diversas razões. A primeira, meramente circunstancial, deve-se ao facto de não ter planeado inicialmente um capítulo como este para o início do livro. Tendo sido persuadido a escrevê-lo (ou, melhor dizendo, a adaptar para ele um texto escrito anteriormente), e pondo-se novamente a questão do local da sua inserção no livro, concluiu-se que seria mais apropriada e natural a sua colocação no fim, por duas outras razões, uma de natureza editorial e outra mais difícil de explicar.

Por um lado, a natureza informal e amena dos capítulos inicial e final, contrastando com a maior exigência ou dificuldade de leitura dos capítulos intermédios, define um perfil original e interessante para a série de publicações que ora se inicia. Por outro lado, é agora, e não antes, que o leitor pode apreciar melhor a razão de certos desenvolvimentos em lógica. Com efeito, supondo que já «sujou as mãos» tentando perceber o conteúdo dos capítulos II a IV, dispõe agora de um precioso idéario terminológico e informativo sem o qual uma discussão, mesmo não técnica, de algumas questões de fundamentos que estiveram na origem dos principais desenvolvimentos da lógica moderna não fariam sequer sentido. E se, porventura, ainda tem as mãos limpas, poderá talvez encontrar aqui uma boa razão para pegar no lápis, na borracha e no papel e aventurar-se pelos capítulos intermédios.

V.2 Sobre a natureza da matemática

Debrucemo-nos um pouco sobre a natureza e métodos da matemática em geral, antes de tentar responder à questão do título deste capítulo.

Muita gente tem tentado caracterizar a matemática ao longo dos tempos, quer quanto ao seu conteúdo, quer quanto à sua forma e métodos. Acontece que a matemática está constantemente a ser enriquecida com novos conhecimentos e disciplinas, o que torna inútil uma sua enumeração, sendo, porém, mais proveitoso tentar caracterizar as teorias matemáticas quanto à natureza do seu conteúdo.

Assim, por exemplo, no século XIX tentou-se caracterizar a matemática como a *ciência da quantidade*. Embora esta impressão ainda perdure na mente de muita gente, com exclusão, tantas vezes ostensiva, de qualquer outra concepção,

devemos observar que ela se afigura demasiado estreita e limitativa, pois não tem em conta importantes ideias e desenvolvimentos como os contidos nas modernas teorias algébricas ou de ordens, na topologia geral e suas aplicações à análise infinitesimal, na moderna teoria da medida e da integração e na utilização generalizada da linguagem da teoria dos conjuntos e do método axiomático, em geral. Estas novas ideias foram-se impondo progressivamente com tanta força e naturalidade como as sucessivas generalizações da noção de *número*, pois, longe de gratuitas, tinham na maioria dos casos por finalidade essencial a resolução de problemas clássicos[167]. Somente desde o final do séc. XIX é que as atenções se concentraram em certas estruturas fundamentais, na sua forma mais pura ou abstracta. Como resultado, muitas disciplinas matemáticas (e a própria lógica) são ainda hoje dominadas pela ideia de *estrutura*, de tal modo que, para muitos (em particular desde que Bourbaki começou a publicar o seu tratado *Éléments de Mathématique*, em 1939) a matemática é concebida como a *ciência das estruturas*. Não temos a certeza de quanto tempo ainda continuará a ser aceite esta caracterização da natureza do conteúdo das disciplinas matemáticas, sendo certo que ela foi e continua a ser contestada por alguns matemáticos de tendências filosóficas diversas[168]. Por outro lado, a opinião dos matemáticos sobre quais as estruturas que se devem considerar como fundamentais tem sofrido alguma mudança com o tempo e as inovações. Todavia, parece que as opiniões da grande maioria dos matemáticos sobre os métodos da sua ciência (da sua arte?) têm permanecido razoavelmente estáveis ao longo dos séculos, desde há pouco mais de dois mil anos. Estes métodos podem caracterizar-se em poucas palavras, pois reduzem-se essencialmente a um só, o *método hipotético-dedutivo*: «Quem diz matemática diz demonstração» (Bourbaki). Com efeito, ao matemático é normalmente exigido que *demonstre* as asserções, leis ou teoremas da sua disciplina (qualquer que tenha sido a maneira como as descobriu ou intuiu). Esta exigência permite distinguir claramente a matemática das chamadas ciências da natureza ou das ciências sociais, em que as respectivas «leis» também podem ser estabelecidas por via experimental, ou estatística.

Além da natureza do conteúdo dos conhecimentos matemáticos e do método de organização ou sistematização desses conhecimentos há outro aspecto da

---

[167] Lembremos, também, as palavras de Bento de Jesus CARAÇA no seu livro *Conceitos Fundamentais da Matemática* (2.ª edição, Gradiva), capítulo I.10: «Verifiquemos, no entanto, como um dado real que não pode ser posto de lado, que o homem tem tendência a generalizar e estender todas as aquisições do seu pensamento, seja qual for o caminho pelo qual essas aquisições se obtêm, e a procurar o maior rendimento possível dessas generalizações, pela exploração metódica de todas as suas consequências» (*princípio de extensão dos conhecimentos*).

[168] Relevantes para esta questão são o volume *Structures in Mathematical Theories* (editores A. DÍAZ, J. ECHEVERRIA e A. IBARRA), Reports of the San Sebastian International Symposium, Sept. 25-29, 1990, Servicio Editorial de la Univ. del País Vasco, e o número especial da revista *Philosophia Mathematica*, series III, Vol. 4, Special Issue (*Mathematical Structuralism*), May 1996.

matemática ou, antes, da actividade dos matemáticos, que para muitos é igual ou mais fundamental ainda que os anteriores: a matemática como actividade criativa do pensamento virada (implícita ou explicitamente) para a formulação e resolução de problemas concretos (os quais podem ter relevância prática imediata ou pressupor já um maior ou menor grau de teorização abstracta). Sem dúvida, muitas disciplinas matemáticas começaram assim mesmo, na antiguidade, com a invenção dos sistemas de numeração, a descrição de órbitas e movimentos celestes, a medição de distâncias terrestres e astrais, a planificação de construções e estruturas arquitectónicas diversas, etc. Por outro lado, muitas disciplinas modernas cuja utilidade não é posta em causa nasceram da pura especulação (o «sonho» que pula e avança como uma bola colorida nas mãos de uma criança ...). Mais geralmente, está em causa o papel da *intuição* na aquisição de conhecimentos, como actividade distinta (mas, complementar) da de sistematização de conhecimentos adquiridos. Numa posição filosófica extrema, a este respeito, temos os matemáticos intuicionistas ou construtivistas, para os quais as noções básicas da matemática são (devem ser) tão simples e intuitivas que nenhum sistema lógico ou filosófico abstracto as pode anteceder ou explicar[169]. Não cabe aqui desenvolver estas questões, mais apropriadas para um livro de filosofia da matemática, pelo que as deixamos de lado por agora.

Regressando ao tema anterior, uma demonstração de uma proposição matemática consiste em grande parte num texto ou discurso bem definido e organizado de referenciação a teoremas ou resultados previamente demonstrados ou reconhecidos como verdadeiros [ou aceites como tal à partida, sem discussão (ver adiante)], de tal modo que se visualize[170] que o dito teorema é consequência desses resultados prévios. Estes, por sua vez, poderão necessitar para sua justificação de ser referenciados a outros resultados ainda, e assim sucessivamente. Mas é evidente que este processo regressivo não pode continuar indefinidamente, e que se devem evitar os círculos viciosos; caso contrário, cada asserção se justificaria a si mesma, em última análise. *Tem de haver um ponto de partida*.

Em geral, um matemático interessado em construir ou desenvolver determinada teoria toma como ponto de partida certas asserções que constituem a base da sua teoria, e que são estipuladas sem demonstração, isto é, sem referenciação justificativa a outras asserções precedentes. Aquelas primeiras asserções constituem os chamados *axiomas* (ou *postulados*) da teoria em causa[171]. Desde a

---

169 Terá sido, pois, com algum desencanto que foi encarada pelos intuicionistas a axiomatização feita por Heyting em 1931 da lógica intuicionista. Ver as monografias de HEYTING e de DUMMETT indicadas na bibliografia e secção 5.5. O livro de Van STIGT, muito informativo, é sobretudo biográfico e filosófico.

170 Ultimamente, algumas demonstrações assistidas por computador, que envolvem dezenas ou centenas de horas de computação, parecem pôr em causa a concepção clássica de demonstração «visualizável». A questão está a ser debatida no seio da comunidade lógica e matemática internacional.

171 Hoje em dia os termos «axioma» e «postulado» consideram-se sinónimos, mas, na terminologia da época de Euclides os axiomas eram as proposições primitivas universais de

época de Euclides de Alexandria (300-283 a. C., em que Euclides ensinava geometria no reino de Ptolomeu I) que a ideia de organizar as disciplinas matemáticas axiomaticamente domina a actividade neste ramo do saber, embora se possam situar em meados do século VI a. C. as primeiras ideias e tentativas de organização dedutiva, por parte de Tales de Mileto.[172] Um sistema de axiomas (numa certa linguagem) define uma teoria (lógica, ou matemática) cujos teoremas são todas as asserções (nessa linguagem) que são consequências desses axiomas, isto é, que são verdadeiras sempre que os axiomas são verdadeiros.[173] A maneira usual de estabelecer que certa proposição é consequência dos axiomas (e é, portanto, um teorema da teoria) é construir uma demonstração da mesma. Dizemos que o teorema se *reduz* aos axiomas, ou que é *deduzido*, *demonstrado*, *derivado* ou *inferido* dos mesmos, ou ainda que os axiomas *implicam* o teorema. Tornar preciso o conceito de demonstração matemática é uma das tarefas principais da lógica matemática, embora não exista uma só maneira de o fazer. Nos capítulos II e III vimos uma maneira de precisar esse conceito. Visto serem as demonstrações matemáticas os locais privilegiados onde se manifesta a relação de consequência entre axiomas e teoremas, também se pode dizer que uma das tarefas da lógica matemática é investigar a natureza das demonstrações matemáticas. Compreende-se, por isso, que os estudos lógicos sejam um requisito essencial para melhor se entender a metodologia da matemática como ciência dedutiva. Nesta perspectiva, a lógica é uma ciência *aplicada* ao estudo da prática dedutiva em matemática. Veremos, na secção seguinte, outro sentido possível do termo «lógica matemática».

V.3 O universo da lógica matemática

Se é verdade que os raciocínios e argumentos matemáticos (e não só) utilizam alguma lógica ou regras lógicas de inferência (uma boa parte deste livro centra-se

---

aceitação geral (como «o todo é maior do que a parte») e os postulados eram proposições primitivas propriamente geométricas que o autor pede para serem aceites como verdadeiras. Se há alguma distinção a fazer actualmente é entre axiomas lógicos e axiomas não lógicos ou específicos (isto é, matemáticos).

[172] A primeira exposição sistemática (em estilo informal) completa da geometria euclidiana foi feita em 1882 por M. Pasch, embora seja mais conhecida a axiomatização de D. Hilbert publicada em 1899 (*Fundamentos da Geometria*), que muito contribuiu para o aperfeiçoamento do método axiomático e a sua expansão a praticamente todas as áreas da matemática.

[173] Não vamos discutir aqui como se chega à formulação de um sistema de axiomas para uma dada disciplina ou corpo de conhecimentos, mas, nos capítulos III e IV já foram apresentados alguns critérios gerais a seguir numa escolha de (conceitos primitivos e) axiomas de uma teoria informal ou formal, ditados por exigências de natureza lógica ou metodológica (por exemplo, a consistência ou não contradição) ou resultantes da prática adquirida na formulação dos modernos sistemas axiomáticos. Sobre as bases do método axiomático ver, por exemplo, as monografias de BETH, EVES, HATCHER, KNEEBONE, TARSKI ou WILDER indicados na bibliografia.

em tais aspectos), não é este o aspecto mais desenvolvido do que modernamente se entende por lógica matemática. Com efeito, a lógica matemática tem vindo progressivamente a assumir também o cariz de uma disciplina matemática à qual não são estranhas, portanto, as técnicas abstractas da matemática dos nossos dias (ver semântica e metateoria das linguagens elementares, capítulos II e III), sendo talvez mais próximo da verdade dizer que a lógica matemática é mais uma *matemática da lógica* do que a *lógica da matemática*. Melhor dizendo, estes dois aspectos complementam-se e enriquecem-se constantemente. Acontece assim porque as investigações lógicas, desde finais do séc. XIX, inicialmente motivadas por questões de fundamentos, levaram à concepção de novos tipos de «estrutura», as chamadas *linguagens formais*, que, como objectos de estudo (tal como os grupos, os espaços lineares, as álgebras de Boole, os grafos, as geometrias finitas, etc.) despertaram a curiosidade dos matemáticos e permitiram, até, dar à matemática tradicional uma nova dimensão.

Poderá o leitor, nesta altura, começar a ficar um pouco inquieto (se ainda não se inquietou com o estudo dos capítulos precedentes). Pois, se a lógica se aplica (ou «precede») à matemática e esta por sua vez à lógica, não estaremos complacendo num grande círculo vicioso? Lembra a velha questão da galinha e do ovo ...

Podemos, desde já, esclarecer o seguinte: *uma* das utilizações da lógica consiste em fornecer as linguagens formais, os conceitos lógicos e as técnicas de inferência com os quais se formalizam as disciplinas matemáticas em teorias formais. Estas disciplinas continuam a ser desenvolvidas e aplicadas pelos matemáticos profissionais, e a serem ensinadas nas escolas e universidades, tudo informalmente e independentemente da formalização. Ora, enquanto a *definição* de uma linguagem ou teoria formal é tarefa bastante simples e rudimentar (trata-se de manipular símbolos e sequências finitas de símbolos), o *estudo matemático* (diremos, também, *metamatemático*) das diferentes linguagens e teorias formais, dos problemas de decisão e de completude semântica, do problema da consistência ou não contradição, da construção de modelos, etc., requer técnicas matemáticas (por exemplo, de natureza conjuntista) que em muito ultrapassam as simples ideias e manipulações envolvidas na sua definição formal[174]. Justifica-se, assim, a designação de *lógica matemática* para a disciplina onde tudo isto se estuda. Perceber os limites da aparente circularidade é coisa que se vai aprendendo com o tempo e neste livro se inicia, mas longe fica de esgotar-se.

Os lógicos profissionais preferem desenvolver e aplicar a lógica matemática a defini-la mas, quando instados, encaram a sua actividade como dizendo respeito essencialmente a um ou outro (ou ambos) dos aspectos seguintes:

(i) Aspecto *explicativo*, segundo o qual a lógica é um sofisticado instrumento de análise e ulterior formalização de fragmentos dos discursos coloquiais nas ciências e, em particular, na matemática (competindo parcialmente com a linguística geral);

---

[174] Que requer mesmo técnicas abstractas poderosas, é o que nos diz o segundo metateorema de incompletude de Gödel (ver final do Cap. IV).

(ii) Aspecto *calculativo*, operativo ou algoritmico, segundo o qual a lógica é considerada um instrumento de cálculo formal destinado a substituir a argumentação intuitiva e informal dos cientistas e matemáticos profissionais, e a responder a certas questões como:

(Q_1) Em que consiste a demonstrabilidade de uma proposição ϕ a partir de (certas hipóteses) **T**?;

(Q_2) Em que consiste a não demonstrabilidade de ϕ a partir de **T**?;

(Q_3) Em que consiste a indecidibilidade do problema da demonstrabilidade de ϕ a partir de **T**?

Os ramos da lógica matemática organizam-se *grosso modo* em torno das tentativas de resposta às questões anteriores. Em síntese, diremos que a lógica matemática comporta quatro ou cinco grandes ramos, cada um com especificidade própria, mas todos eles interligados e interactuantes entre si e com outras disciplinas matemáticas, a saber:

(a) Teoria da Demonstração;

(b) Teoria dos Modelos;

(c) Teoria da Computabilidade;

(d) Teoria dos Conjuntos;

(e) Lógica e matemática intuicionista/construtivista.

A Teoria da Demonstração é, talvez, o ramo mais nobre da lógica matemática. É o mais antigo, pois remonta às origens do método axiomático e à silogística de Aristóteles. Após algumas tentativas infrutíferas de criação de uma nova lógica adaptada às necessidades modernas, como, por exemplo, a tentativa de Leibniz (1646-1716), cujos manuscritos permaneceram em grande parte desconhecidos até quase aos nossos dias, somente em meados do séc. XIX se avançou sensivelmente neste domínio, sob o impulso decisivo de Georg Boole[175]. Anos mais tarde, no famoso *Begriffsschrift*[176] de Gottlob Frege aparece pela primeira vez o conceito de *linguagem formal* como instrumento adequado para formalizar as leis da lógica. Boole tentou introduzir uma notação algébrica para formalizar as leis da lógica, chamando *soma* ($+$) e *produto* ($\cdot$) lógicos ao que hoje em dia chamamos *disjunção* e *conjunção* de proposições, respectivamente. A notação algébrica caiu em desuso, mas, em contrapartida, o estudo algébrico da lógica não tem esmorecido até ao presente (álgebras de Boole, álgebras poliádicas e cilindricas, álgebras de Heyting, álgebras modais, etc.). A simbologia de Frege aproxima-se

---

[175] Na sua obra *An investigation of the laws of thought, on which are founded the mathematical theories of logic and probabilities* (1854), reeditada pela Dover.

[176] *A formula language, modeled upon that of arithmetic, for pure thought*, tradução do original alemão de 1879, *in* Van HEIJENOORT, pp. 1-82.

mais da linguagem matemática comum, mas peca igualmente por certas características bidimensionais da notação para deduções. Em 1894 o matemático italiano Giuseppe Peano criou, no seu *Formulaire de mathématique*, um simbolismo mais natural que é também, na essência, o simbolismo utilizado por Russell e Whitehead no tratado *Principia mathematica* (1910-1913). Estes autores tentaram concretizar um ambicioso programa de redução da matemática à lógica (iniciado por Frege, mas com uma grave deficiência estrutural descoberta por Russell em 1902), chamado *logicismo*. Pela mesma época (1908) E. Zermelo propunha uma axiomática para a teoria dos conjuntos, dando uma base sólida à teoria intuitiva de Cantor e removendo algumas dificuldades (paradoxos) que esta vinha enfrentando sem sucesso, e o matemático holandês L.E.J. Brouwer propunha uma fundamentação radical da matemática em bases construtivistas (o *intuicionismo*, parcialmente antecipado pelo matemático alemão Kronecker), quebrando, assim, a tradição de uma única matemática de tradição clássica.

Estes grandes projectos e sistemas fundacionais trouxeram consigo problemas igualmente grandes, nomeadamente o *problema da consistência ou não contradição*, para além de uma divisão marcada entre os estilos clássico e construtivista de fazer matemática. Uma segunda fase da teoria da demonstração é iniciada por David Hilbert, tendo precisamente como objectivo o estabelecimento da consistência de teorias formais que formalizam uma parte substancial da matemática clássica e, simultaneamente, a prova de que tais teorias são extensões conservativas da matemática finitária ou elementar (digamos, a teoria elementar dos números). Deste modo, ficaria inteiramente validada ou justificada a matemática clássica (infinitária, abstracta), codificada ou formalizada num grande sistema formal **T** (é isto o *formalismo* de Hilbert), e refutadas as principais objecções intuicionistas.

Hilbert acreditava que seria possível estabelecer a não contradição de uma tal teoria **T** por meio de uma análise profunda de estrutura dedutiva de **T**, que evidenciasse, entre outras coisas, que nenhuma dedução de uma contradição podia ser efectuada em **T**. Naturalmente, uma tal análise deveria ser conduzida numa teoria $\mathbf{T}'$, metateoria relativamente a **T**, a qual, para a demonstração de consistência de **T** estar acima de qualquer suspeita, teria de ser bem mais modesta do que **T**. Na realidade, a metateoria $\mathbf{T}'$ teria de ser «finitista» (elementar, combinatorial, construtiva) no sentido mais estrito.

A teoria da demonstração (ou *metamatemática*) de Hilbert falhou nos seus propósitos de justificação da matemática formal através de demonstrações finitistas de conservação e consistência, como veio a ser evidenciado pelos metateoremas de incompletude de Gödel (ver final do Cap. IV). Mas, como método de análise da estrutura dedutiva dos sitemas logico-matemáticos, deu origem a um dos principais e mais sofisticados ramos da lógica matemática.

A parte da lógica matemática que estuda a questão (Q_2) é a chamada *teoria dos modelos*, que compreende a moderna semântica e constitui uma extensão natural da teoria da demonstração. Nela se estudam, fundamentalmente, as relações entre os aspectos sintácticos e os aspectos semânticos de uma teoria, entre a teoria e as suas

interpretações ou modelos, questões como a independência e consistência relativa (de uma dada proposição ou axioma relativamente a outras proposições ou outros axiomas).

Os antecedentes da teoria dos modelos situam-se no periodo 1870-1930, caracterizado por intensa discussão e actividade nos fundamentos, e culminam, pode dizer-se, no metateorema de completude semântica de Gödel (1930) e algumas das suas consequências. O grande impulso deu-se, todavia, a partir dos anos quarenta e cinquenta, com importantes ligações (quer em termos de motivação quer em termos de aplicações) à Topologia e à Álgebra. No início da década de sessenta A. Robinson descobre importantes aplicações dos modelos não standard à aritmética e à Análise, com a criação da chamada *análise não standard*, e P. Cohen estabelece, construindo modelos especiais da teoria axiomática dos conjuntos, a independência relativa do Axioma da Escolha e da Hipótese do Contínuo de Cantor. Esta hipótese afirma que não existe nenhum cardinal estritamente compreendido entre o cardinal de $\mathbb{N}$ e o cardinal de $\mathbb{R}$.

Embora a teoria dos modelos seja hoje considerada uma disciplina matemática e tenha, desde sempre, ligações profundas com disciplinas matemáticas tradicionais, é curioso observar que, por outro lado, a prática matemática usual não dá nem deu indicação alguma do possível interesse (para a própria matemática) da consideração de sistemas arbitrários de axiomas. São inúmeros, porém, os resultados da teoria dos modelos com aplicações matemáticas não triviais que resultaram da consideração de teorias arbitrárias e seus modelos. É o caso, por exemplo, de diversos teoremas da teoria dos modelos conhecidos por *teoremas de preservação*. Damos apenas um exemplo, dos mais simples de entre os diversos metateoremas deste tipo conhecidos em lógica matemática.[177]

É sabido que uma subestrutura arbitrária de um grupo $(G, +, 0)$, isto é, uma estrutura da forma $(H, +, 0)$, onde H é um subconjunto de G fechado para $+$ e contendo o elemento 0, pode não ser um grupo. Por exemplo a estrutura dos números naturais $(\mathbb{N}, +, 0)$ é subestrutura do grupo aditivo dos inteiros $(\mathbb{Z}, +, 0)$, mas não é grupo (não é subgrupo). Em contrapartida, se a noção de grupo for formulada com a operação unária primitiva de inversão ou simetria (na notação aditiva), já toda a subestrutura de um grupo $(G, +, -, 0)$ é também um grupo (subgrupo), pois é fechado para $+$, $-$, e tem lá o elemento neutro.[178] A explicação deste fenómeno pode ser dada em termos muito gerais, pelo

---

[177] Para desenvolvimento da perspectiva histórica na teoria dos modelos, e sua relação com a matemática, de 1945 até aos nossos dias, ver o artigo de A. MACINTYRE "Model theory", em AGAZZI, pp. 45-65.

[178] Nesta nova formulação o axioma G_3 da pág. 231, que tem um quantificador universal e um existencial, é substituido pelo axioma G_3' seguinte, que só tem um quantificador universal: $\forall x(x + (-x)) = 0$.

Metateorema de Łós-Tarski

*Toda a subestrutura de um modelo de uma teoria **T** é ainda um modelo de **T** se e somente se **T** pode ser axiomatizada por sentenças universais, isto é, por sentenças da forma* $\forall x_1 \cdots \forall x_n \, \phi(x_1, \cdots, x_n)$*, em que* ϕ *é uma fórmula sem quantificadores.*

Esta explicação não lembraria a um matemático, pois envolve, de maneira essencial, a consideração da *forma sintáctica* dos axiomas.

O mesmo teorema explica, também, que a classe dos corpos algebricamente fechados não pode ser axiomatizada por (isto é, não é a classe dos modelos de uma teoria cujos axiomas são) sentenças universais na linguagem dos corpos, pois uma subestrutura e, até, um subcorpo de um corpo algebricamente fechado pode não ser algebricamente fechado.[179]

A teoria dos modelos é muito rica em resultados como o teorema de Łós-Tarski e suas aplicações mas, actualmente, não se limita às linguagens e teorias de primeira ordem e seus modelos. De facto, desde há algumas décadas que vêm sendo estudadas linguagens com maior poder expressivo que as de primeira ordem (linguagens de ordem superior à primeira, linguagens infinitárias, linguagens com quantificadores generalizados, linguagens modais, etc.) ou com semânticas alternativas à semântica tarskiana (valores lógicos numa álgebra de Boole, semântica dos «mundos possíveis» de Kripke, etc.), ou ambas as coisas, e para todas elas tem sido desenvolvida a respectiva «teoria de modelos».[180]

As respostas a questões do tipo (Q_3) cabem, naturalmente, na teoria da computabilidade, também chamada teoria das funções recursivas. Esta teoria teve origem nos estudos dos anos trinta em torno de certos problemas de decisão formulados em décadas anteriores que aguardavam solução. Para entender tais problemas convém recuar um pouco no tempo.

Pode-se dizer que a busca de algoritmos (procedimentos mecânicos ou computacionais, *calculæ*) para resolver problemas matemáticos os mais diversos é tão antiga como a própria matemática. Durante muito tempo pensou-se que para cada classe de problemas matemáticos semelhantes haveria de ser encontrado um algoritmo capaz de os resolver. Diversos algoritmos aritméticos são conhecidos na antiguidade grega, e a própria geometria de Euclides tem uma forte componente

---

[179] Os corpos algebricamente fechados são os corpos em que toda a equação algébrica com coeficientes no corpo, digamos $a_n x^n + \cdots + a_1 x + a_0 = 0 \;\; (n \geq 1, \;\; a_n \neq 0)$, tem pelo menos uma solução no corpo. O corpo dos números complexos é algebricamente fechado, mas o subcorpo dos números reais não é algebricamente fechado (por exemplo, a equação $x^2 + 1 = 0$ não tem soluções reais).

[180] José Sebastião e Silva (1914-1972), antigo professor na Faculdade de Ciências de Lisboa, mundialmente conhecido pelos seus trabalhos em análise funcional e na teoria das distribuições, redigiu nos anos 40 diversos trabalhos pioneiros no campo da lógica e da teoria dos modelos de ordem superior. V. "On the automorphisms of arbitrary mathematical systems", *in History and Philosophy of Logic*, vol. 6, 1985, pp. 91-116 (tradução por A. J. F. OLIVEIRA do original italiano de 1945).

algoritmica, na medida em que depende de construções com régua e compasso. O termo «algoritmo», porém, é de origem mais recente, e parece ter resultado da fusão dos termos «algorismo» e «aritmética». O primeiro destes termos designou, na europa ocidental, em meados do século XVI, o sistema de numeração árabe, e tem origem no nome de um célebre matemático árabe do século IX, Mohamed Al-Khuarismi. O lógico e filósofo R. Lull publicou em 1273 um livro com o título *Ars magna*, no qual descrevia um método combinatorial com o qual se pretendia gerar todas as «verdades». A ideia de uma *ars magna* é retomada por Cardano em 1545 e por Leibniz em 1666 (que distingue entre a *ars iudicandi*, para decidir, e a *ars inveniendi*, para enumerar) e influencia o pensamento filosófico e matemático até aos nossos dias. A geometria analítica de Fermat e Descartes era, na intenção deste último, encarada como uma tentativa de aplicar à geometria os algoritmos algebrico-aritméticos.

Alguns problemas clássicos, em diferentes áreas da matemática, resistiram, contudo, a todas as tentativas de resolução algoritmica. A impossibilidade de resolução algoritmica de alguns problemas pode ter ocorrido a algumas pessoas após as demonstrações, no séc. XIX, da impossibilidade de algumas construções com régua e compasso, trissecção de um ângulo arbitrário, a quadratura do círculo ou a duplicação do cubo, em geometria, e da impossibilidade de resolver por radicais toda a equação quíntica (teoria de Galois), em álgebra. O próprio conceito de algoritmo, porém, não estava ainda suficientemente elaborado para permitir a demonstração de impossibilidade de resolução algoritmica de outros problemas onde tal tipo de solubilidade era procurada. Três problemas, em particular, mereceram a atenção prolongada dos lógicos e matemáticos desde finais do séc. XIX e princípios do presente, a saber:

(i) O problema da decisão em lógica (*Entscheidungsproblem*);

(ii) O décimo problema de Hilbert;

(iii) O problema das palavras para grupos.

O problema da decisão em lógica tem duas vertentes, uma sintáctica e outra semântica, mas pode assumir a forma geral seguinte, em ambas: dado um conjunto F de fórmulas de certa linguagem $\mathcal{L}$, saber se existe um algoritmo que permita decidir (num número finito de passos), para cada fórmula ϕ de $\mathcal{L}$, se ϕ está ou não em F. O conjunto F pode ser, por exemplo, o conjunto das fórmulas de certa forma sintáctica que são leis lógicas ou o conjunto dos teoremas de certa forma sintáctica de certa teoria (vertente sintáctica), o conjunto das fórmulas válidas de $\mathcal{L}$ ou o conjunto das sentenças de $\mathcal{L}$ verdadeiras em certa estrutura (vertente semântica). Acontece que, para certos conjuntos restritos de fórmulas F, o problema de decisão para F tem solução positiva, isto é, existe um algoritmo que decide da pertença ou não a F. Os primeiros exemplos foram dados por Schröder em 1890. Mas, para outros conjuntos importantes, como o conjunto de todas as fórmulas válidas de uma linguagem de primeira ordem $\mathcal{L}$ ou o conjunto de todas as

sentenças aritméticas verdadeiras em $(\mathbb{N}, ...)$, um tal algoritmo de decisão não fora ainda encontrado.

O décimo problema de Hilbert foi por este formulado numa célebre comunicação ao congresso internacional de matemáticos em Paris, em 1900. Hilbert propôs que se investigasse a existência de um algoritmo para decidir, para uma equação diofantina arbitrária, se ela tem ou não soluções inteiras não triviais. Uma equação diofantina é uma equação da forma

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

onde $f(x_1, ..., x_n)$ é um polinómio nas variáveis x_1, ..., x_n com coeficientes inteiros. As mais célebres equações diofantinas são, talvez, as equações da forma

$$x^n + y^n - z^n = 0 \; (n \geq 2)$$

Para $n = 2$ estas equações são chamadas *equações pitagóricas*, e possuem uma infinidade de soluções inteiras. Fermat (1601-1665) comentou na margem de uma página de um livro de Diofanto que tinha descoberto uma demonstração muito simples de que, para todo o natural $n \geq 3$, aquela equação não tem soluções inteiras não triviais (isto é, não nulas). Para diversos valores particulares de n foi sendo demonstrada a não existência de soluções inteiras não triviais, mas só muito recentemente é que os matemáticos (Andrew Wiles, 1996) conseguiram uma demonstração geral daquela antiga conjectura de Fermat. Dos esforços efectuados nesse sentido resultaram, contudo, grandes progressos em diferentes áreas matemáticas, e uma disciplina inteiramente nova, a chamada teoria algébrica dos números.

É óbvio, portanto, que o algoritmo procurado por Hilbert para decidir da existência de soluções inteiras não triviais das equações diofantinas gerais, a existir, ainda não foi encontrado.

Na verdade, não existe mesmo um tal algoritmo. Na época em que Hilbert formulou o problema, porém, a noção *matemática* (por oposição a *intuitiva*) de algoritmo ainda não estava elaborada de modo a permitir uma demonstração de que não existe nenhum algoritmo para resolver determinada questão ou classe de questões semelhantes. De facto, há uma diferença qualitativa fundamental entre demonstrar que existe um algoritmo — basta *exibi-lo*! — e demonstrar que não existe nenhum. No primeiro caso, a exibição de um algoritmo é consentânea com o reconhecimento de que de um algoritmo efectivamente se trata, e para isto basta a noção intuitiva.[181]. No segundo caso, somente uma demonstração matemática satisfaz, e para isso é imprescindível uma noção também matemática de algoritmo.

Tal noção foi elaborada nos anos trinta por diversos matemáticos, nomeadamente por Alan Turing, em Cambridge. Os algoritmos são, para Turing, os programas de certos computadores ideais (sem limitações físicas de memória) chamados máquinas de Turing. Equivalentemente, alguns autores elaboraram a

---

[181] É caso para recordar o ditado inglês «*the proof of the pudding is in the eating*» («a prova do pudim está em comê-lo»). O termo «*proof*» significa, conforme o contexto, demonstração ou degustação.

noção de função numérica (isto é, com argumentos e valores em $\mathbb{N}$) *computável* (ou *função recursiva*): uma função é computável (ou recursiva) se e somente se existe um algoritmo que computa os seus valores. Uma classe restrita de funções computáveis (as chamadas funções *recursivas primitivas*) fora já utilizada por Gödel, no entanto, nas demonstrações dos seus metateoremas de incompletude (ver final do Cap. IV).

Estabelecidas as bases científicas da teoria da computabilidade, foi então possível obter diversos resultados de indecidibilidade em lógica e em matemática. Por exemplo, A. Church demonstrou em 1936 que o problema de decisão para a lógica de primeira ordem é algoritmicamente insolúvel: não existe nenhum algoritmo para decidir, para cada sentença ϕ, se ϕ é ou não válida (ou, equivalentemente, se ϕ é ou não uma lei lógica). Novikov demonstrou em 1955 a insolubilidade algoritmica do problema das palavras nos grupos, formulado em 1912 por M. Dehn. Trata-se do problema de saber se duas expressões arbitrárias $a_1 \cdots a_n$, $b_1 \cdots b_m$, onde os a_i e os b_j denotam elementos de um grupo $(G, \cdot, e)$, denotam ou não o mesmo elemento do grupo, isto é, se $a_1 \cdots a_n = b_1 \cdots b_m$. Finalmente, em 1970, culminando décadas de esforços continuados (por Julia Robinson, Martin Davis e outros), o jovem lógico russo Y. Matiyasevitch demonstrou a insolubilidade algoritmica do 10º problema de Hilbert.[182]

Para terminar, falta dizer algo sobre a teoria dos conjuntos e a lógica e matemática intuicionistas, que merecem secções distintas.

[182] O livro de M. DAVIS contém uma exposição técnica da teoria da computabilidade e, em apêndice, os resultados mais recentes relativos à insolubilidade algoritmica do décimo problema de Hilbert. O livro de R. PENROSE, de outra índole, contém, na primeira parte (cerca de 150 páginas) uma exposição relativamente informal muito boa das máquinas de Turing e dos resultados de Gödel.

V.4 Sobre a teoria dos conjuntos

A teoria (axiomática) dos conjuntos pode considerar-se uma teoria matemática particular mas, pela sua grande potência e generalidade, tem um papel privilegiado na fundamentação de praticamente toda a matemática pura e aplicada e, portanto, também em todas as ciências dedutivas de base matemática. Em particular, ela é utilizada extensivamente em discussões técnicas de lógica matemática e de filosofia analítica. Alguns autores (por exemplo, A.A. FRAENKEL *et. al*) adoptam mesmo o ponto de vista de que «fundamentos da matemática» é sinónimo de «fundamentos da teoria dos conjuntos». Em partes mais avançadas da teoria estudam-se as consequências de diversos «axiomas fortes do infinito» (isto é, axiomas que postulam a existência de cardinais muito grandes) e questões metateóricas diversas, como as de consistência e independência relativa, utilizando métodos da teoria dos modelos. A discussão nesta secção é de cariz bem mais elementar.

Desde a antiguidade que os matemáticos lidam com colecções infinitas, por exemplo, a colecção dos inteiros positivos, mas somente no século XIX é que foi definitivamente ultrapassada a relutância em considerar tais colecções ou «pluralidades» como objectos singulares — *conjuntos*, para utilizar a terminologia prevalecente. A ideia de uma infinidade «completada» ou «actual» parecia implicar que todos os seus membros estivessem de algum modo concebidos ou «presentes» perante os nossos olhos ou espírito e era, por isso, encarada com grande suspeição desde os tempos de Aristóteles, para quem só era legítimo o infinito «potencial». Os desenvolvimentos e necessidades da matemática durante o séc. XIX impuseram a concepção do infinito «actual», veiculado na *Mengenlehre* (teoria dos conjuntos) criada por Georg Cantor (1845-1918) nos anos setenta. Apesar de alguma hostilidade inicial, a maioria dos matemáticos adoptou decisivamente a nova teoria que logo se revelou um instrumento poderoso e indispensável para as investigações matemáticas.

O sucesso da nova teoria levou os seus cultores, incluindo o próprio Cantor, a supor que *toda* a colecção é conjunto. Esta suposição está implícita na «definição» que Cantor dá da noção de conjunto: «Um conjunto é uma colecção M de objectos m bem definidos e distintos da nossa intuição ou pensamento, concebida num todo». A notação «$m \in M$» exprime que o objecto m é membro ou elemento do conjunto M. A referida suposição é conhecida por *princípio da compreensão* (ou *princípio da abstracção*) e pode ser expressa dizendo que para toda a condição $\phi(x)$, a colecção ou classe $\{x : \phi(x)\}$[183] é conjunto. O outro princípio básico implícito na concepção cantoriana é o *princípio de extensionalidade*, de que conjuntos com os mesmos elementos são iguais, ou seja, de que um conjunto é determinado pelos seus elementos. Enquanto este último princípio é incontestado, o da compreensão revelou-se insustentável por conduzir a paradoxos ou antinomias

[183] Ler «a colecção ou classe de todos os objectos x tais que $\phi(x)$»; o símbolo $\{x : \ldots\}$ é o chamado *operador de abstracção* (na variável muda x).

descobertas posteriormente, chamados *paradoxos lógicos*. O primeiro a ser publicado é o *Paradoxo de Burali-Forti* (1897), mas já era do conhecimento de Cantor dois anos antes. O paradoxo resulta da suposição de que a classe $\mathcal{O}$ de todos os ordinais[184] é conjunto, donde se conclui que $\mathcal{O}$ é ele próprio um ordinal e que $\mathcal{O} < \mathcal{O}$, contrariando uma propriedade básica da ordenação (estrita) dos ordinais, a irreflexividade.

Outros paradoxos foram sendo descobertos (como o *paradoxo de Cantor*, do conjunto de todos os conjuntos). Cantor não ficou execessivamente preocupado. Era claro, por um lado, que os paradoxos em questão tinham a ver com o princípio de compreensão aplicado a classes que eram não apenas infinitas mas extremamente vastas, que ele designou de *absolutamente infinitas*, e que eram extensas em demasia para serem concebidas como um objecto singular. Por outro lado, os paradoxos em questão surgiam apenas em áreas muito avançadas e técnicas da teoria, longe das aplicações e utilizações do dia-a-dia matemático. Tudo estaria bem se o princípio de compreensão fosse restringido a classes de tamanho moderado. Cantor não forneceu, porém, qualquer critério de demarcação. A questão agudizou-se com a descoberta, por Bertrand Russell, em 1901, do paradoxo com o seu nome (ver Nota 114). Este paradoxo, ao contrário dos anteriores, não pressupõe nenhum desenvolvimento técnico da teoria, pois sai directa e imediatamente do princípio de compreensão. Já não era o topo mas a base da teoria que estava precisando de revisão. A descoberta mergulhou a lógica e a teoria dos conjuntos (não facilmente demarcáveis, na altura[185]) numa grande crise.

O ano de 1908 é de significado muito especial nos fundamentos da matemática, pois nele são avançadas três propostas radicais para solução da crise, duas que impõem restrições ao princípio de compreensão e uma terceira que se demarca de tudo o resto e será discutida na secção seguinte.

A proposta de Russell está contida na sua *teoria dos tipos*, tentativamente formulada em 1903, abandonada em 1905 e retomada em força em 1908[186]. Consiste, muito genericamente, em classificar os objectos do universo em *tipos*, de tal modo que um objecto de certo tipo só pode ser membro de um objecto (conjunto) de tipo imediatamente superior, e em rejeitar a formação do objecto (conjunto) $\{x : \phi(x)\}$ quando a condição $\phi(x)$ é *impredicativa*, isto é, respeitante a uma totalidade da qual o referido objecto, se existisse, faria parte. Isto é mais

---

[184] Não é aqui o lugar para desenvolver a teoria dos ordinais. Digamos apenas que os ordinais são certos objectos (conjuntos) que «prolongam» *ad infinitum* a progressão dos números naturais, sendo estes os ordinais finitos. O primeiro ordinal infinito denota-se ω, o segundo é $\omega + 1$, etc. A progressão ordenada dos ordinais é $0 < 1 < 2 < \ldots < \omega < \omega + 1 < \omega < \omega + 2 < \ldots < \omega + \omega < \ldots$. As monografias de HAMILTON e de MACHOVER contêm capítulos sobre os ordinais de índole introdutória muito bem feitos.

[185] A teoria dos conjuntos era conhecida como a «grande lógica».

[186] No artigo "Mathematical Logic as based on the theory of types", em Van HEIJENOORT, pp. 150-182, desenvolvido nos *Principia Mathematica* (3 volumes publicados em 1910, 1912 e 1913), em colaboração com A. N. Whitehead.

fácil de dizer do que implementar num sistema formal. O sistema resultante é uma aberração notacional que teve muitos poucos aderentes.

A segunda solução foi proposta por Ernst Zermelo e consistiu numa axiomatização da teoria dos conjuntos, pondo em prática a ideia anteriormente expressa por Cantor no sentido de *limitar a grandeza* dos conjuntos através de uma restrição judiciosa do princípio de compreensão. A formulação restrita deste princípio dá pelo nome de *axioma de separação* ou, melhor dizendo, de *axioma-esquema de separação*[187]: para qualquer condição «definite» $\phi(x)$ e conjunto A previamente dado, existe o conjunto dos elementos de A com a propriedade $\phi(x)$, que se denota $\{x : x \in A \wedge \phi(x)\}$ ou $\{x \in A : \phi(x)\}$. Este conjunto não é demasiado grande pois é subconjunto de A. Sobre o significado de «definite» ver adiante.

Outros axiomas de Zermelo [além dos axiomas de extensionalidade, dos pares não ordenados e do conjunto vazio (ver exercício 3.21)] procuram compensar a restrição imposta pelos axiomas de separação. É o caso, por exemplo, do *axioma do conjunto das partes*: para todo o conjunto A existe um conjunto cujos elementos são exactamente os conjuntos contidos em A, que se denota $\mathcal{P}(A)$; o *axioma da união*: para todo o conjunto A existe um conjunto cujos elementos são exactamente os membros dos membros de A, que se denota $\bigcup A$; e o *axioma do infinito* (ver *Nota* no final do exercício 3.21). Com base nestes axiomas consegue-se desenvolver uma parte substancial das matemáticas e, ao mesmo tempo, bloquear os paradoxos lógicos conhecidos, admitindo-se que nem toda a classe ou colecção seja conjunto, ao contrário da permissividade cantoriana. A estes axiomas Zermelo juntou o *axioma da escolha*: para todo o conjunto M de conjuntos não vazios e disjuntos dois a dois, existe um conjunto C contendo exactamente um elemento de cada membro de M. Este axioma é necessário para certos resultados da teoria (nomeadamente, o teorema da boa-ordenação, de que em todo o conjunto existe uma boa-ordem, conjecturado por Cantor e demonstrado por Zermelo em 1904) e, como mostrou Zermelo, necessário também em muitas áreas específicas da matemáticas como a Álgebra e a Análise (teoria das funções, topologia, teoria da medida e do integral, etc.).

Aos axiomas de Zermelo vieram posteriormente juntar-se dois outros. A.A. Fraenkel, Theoralf Skolem e Nels Lennes proposeram (independentemente uns dos outros) por volta de 1921-22 o *axioma da substituição*: se $\mathcal{F}$ é uma operação no universo e A um conjunto, então a classe dos valores $\mathcal{F}(x)$ com $x \in A$, designada $\{\mathcal{F}(x) : x \in A\}$, é conjunto. Este axioma é muito forte mas não tem, aparentemente, aplicações fora da teoria «pura» dos conjuntos, sendo todavia necessário para garantir a existência de certos conjuntos de ordinais e para demonstrar, por exemplo, que todo o conjunto bem-ordenado é isomorfo a um ordinal. Do mesmo Fraenkel é o *axioma da regularidade*: para todo o conjunto não vazio X, existe um

---

[187] Diz-se *axioma-esquema* e não simplesmente *axioma* uma vez que estão englobados muitos axiomas particulares todos com a mesma forma, um para cada condição $\phi(x)$ que se considere.

membro Y de X tal que $Y \cap X = \emptyset$. Este é um axioma técnico, estrutural, sem nenhuma aplicação matemática, cuja única finalidade é excluir do universo certos conjuntos «irregulares» (por exemplo, conjuntos X tais que $X \in X$).

Diga-se de passagem que Zermelo concebeu inicialmente uma teoria dos conjuntos com «elementos atómicos» («urelemente») — objectos que não são conjuntos mas podem ser utilizados como elementos de conjuntos. Zermelo teria em mente, por exemplo, considerar os números naturais como objectos atómicos dados, irredutíveis a coisas mais simples, mas investigações posteriores mostraram que até os numeros naturais podiam ser definidos como sendo certos conjuntos especiais (os ordinais finitos) e que tudo o que era possível fazer, do ponto de vista matemático, com objectos atómicos também era possível fazer sem eles. Todavia, em anos recentes tem havido um interesse renovado por teorias com objectos atómicos e com conjuntos irregulares. Em todo o caso, a teoria axiomática com os axiomas acima ficou conhecida por *teoria de conjuntos de Zermelo-Fraenkel* e designada **ZF** [ou **ZFC**, chamando-se assim a atenção para a presença do axioma da escolha (o "C" do Inglês *Choice*)] por Zermelo em 1930. Há nesta designação uma pequena injustiça histórica que explicamos a seguir.

Zermelo não formalizou a sua teoria numa linguagem formal determinada. Este facto dificulta a formulação precisa dos axiomas de separação, na medida em que a noção de «condição arbitrária em x, $\phi(x)$» carece de precisão, daí a sua insistência de que as condições a considerar fossem «definite». Isto quer dizer essencialmente o seguinte: para cada objecto a do universo, é bem determinado o valor lógico da proposição $\phi(a)$. A ideia de Zermelo seria a de excluir, assim, em princípio, condições ambíguas ou que nada têm a ver com as ciências matemáticas, como «x é um político sincero». Em casos concretos não será difícil obter consenso sobre se certa condição dada é ou não «definite», mas podemos afirmar com clarividência que a noção zermeliana de «definite» é ela própria «definite» e livre de toda a ambiguidade? Há por aqui gato escondido com rabo de fora... Por outro lado, enquanto os paradoxos lógicos conhecidos ficam realmente bloqueados, o mesmo não se pode ainda dizer quanto aos chamados *paradoxos linguísticos* ou *semânticos*, de que já se deu um exemplo no exercício 1.9 (*paradoxo de Tarski*). Eis outro exemplo de paradoxo semântico publicado em 1906 por Russell e atribuído por este a um bibliotecário obscuro de nome G.G. Berry, conhecido naturalmente por *paradoxo de Berry*.

Algumas frases da língua portuguesa definem números naturais, por exemplo, «quarenta e oito», «o terceiro número primo», «o menor número primo maior do que vinte e nove mil duzentos e três». Se não impusermos nenhuma limitação no comprimento (número de palavras) das frases, então seremos capazes, pelo menos em princípio, de definir números naturais arbitrariamente grandes e até podemos, se quisermos, enumerar tais frases por ordem alfabética, como numa pauta de exame (infinita). Mas se limitarmos o número máximo de palavras que as frases podem ter (30 palavras no máximo, por exemplo), então, como o número total de palavras da língua portuguesa é finito (digamos, para fixar ideias, no primeiro dia do ano civil em que o leitor está lendo estas linhas), haverá um número finito

máximo de números naturais definíveis por frases da língua portuguesa, por razões meramente combinatoriais. Existirá também, portanto, pelo menos, um número natural que não é definível por frases da língua portuguesa (com quando muito 30 palavras). E, existindo um, existirá o menor deles, pela conhecida *propriedade de mínimo* (todo o conjunto não vazio de números naturais tem elemento mínimo, com respeito à ordem usual). Muito bem, consideremos a frase seguinte, que define um número natural, a que chamamos *número de Berry:*

O menor número natural que não é definível por nenhuma frase da língua portuguesa, sem referências a números anteriormente definidos, com menos de trinta palavras.[188]

Se o leitor contar o número de palavras da frase anterior, que define o número de Berry, verá que é 25. Todavia, este número de Berry, pela sua definição mesma, não deveria poder ser definido numa frase com menos de 30 palavras!

Como sair desta encrenca? Devemos concluir que a expressão «definível por uma frase da língua portuguesa com menos de trinta palavras» não é de significado tão preciso como seria desejável, não será «definite» no sentido zermeliano. Hermann Weyl foi o primeiro a propor, em 1918, uma definição precisa de «definite», mas foi a proposta de Skolem em 1922 que acabou por ser adoptada universalmente, nomeadamente, a de se tomar como linguagem da teoria dos conjuntos uma linguagem de primeira ordem (a linguagem $\mathcal{L}_{\text{tc}}$ definida no exercício 3.21). O conceito de «condição em x» está perfeitamente definido nesta linguagem, e os paradoxos semânticos ficam bloquados[189].

Não podemos terminar esta secção sem mencionar um desenvolvimento recente na teoria axiomática dos conjuntos que julgamos, a todos os títulos, um dos acontecimentos mais importantes na matemática deste século.

Na secção IV.6 falou-se em *modelos não-standard da aritmética* e, em nota de rodapé (Nota 99), em *modelos não-standard da Análise* e *Análise Não-standard* (ANS), segundo a versão de A. Robinson. Devemos agora falar de uma outra versão da ANS tendo por base uma extensão conservativa da teoria axiomática dos conjuntos de Zermelo-Fraenkel, a chamada *Teoria Interna dos Conjuntos* (**IST**), do matemático americano E. Nelson.[190] É precisamente esta teoria a primeira a tirar partido da possível discrepância entre noções intuitivas e noções formais de

---

[188] Um tal referência seria, por exemplo, do tipo «O número definido na frase anterior mais um». A restrição destina-se a evitar situações de recorrência. O paradoxo de Berry é uma versão simplificada de um outro conhecido por *paradoxo de Richard* (1905), ver BETH, FRAENKEL *et al*.

[189] H. WEYL, *The Continuum, A Critical Examination of the Foundation of Analysis*, Dover, 1994. O artigo de Skolem "Some remarks on axiomatized set theory" pode ser consultado em Van HEIJENOORT, pp. 290-301.

[190] "Internal Set Theory: a new approach to Nonstandard Analysis", *Bull. Amer. Math. Soc.* **83** (1977), pp. 1165-1198. A recente colectânea editada pelo casal DIENER contém um capítulo tutorial, diversas aplicações desenvolvidas pela escola francesa de Análise Não-standard e uma importante bibliografia final.

número referida na Nota 88, se bem que o ponto de partida para os axiomas de Nelson seja, como ele próprio observa, a identificação dos *princípios* em uso na prática da ANS segundo a perspectiva robinsoniana.

A versão de Nelson da ANS é, em certos aspectos, radicalmente diferente da de Robinson. Tomando por base **ZFC**, Nelson acrescenta um novo predicado primitivo unário à linguagem $\mathcal{L}_{\text{tc}}$ de **ZFC**, o predicado

$$\mathit{standard}(x),$$

que se lê «x é standard». Este predicado tem como efeito criar uma distinção no universo de todos os conjuntos: uns são standard e outros não. Para lidar com este novo predicado e, bem entendido, assegurar que a distinção é genuína, isto é, que existem de facto objectos (conjuntos) não-standard, Nelson introduz três novos axiomas (melhor dizendo, axiomas-esquemas). Para evitar contradições (se elas não estiverem já presentes em **ZFC** — está provado que **IST** é consistente relativamente a **ZFC**) haverá que ter certas precauções de natureza sintáctica como, por exemplo, não utilizar o novo predicado em axiomas de **ZFC** (nomeadamente, nos axiomas-esquemas de separação e de substituição). Não é aqui o lugar para apresentar os axiomas de Nelson e desenvolver a sua teoria. Mencionemos apenas alguns aspectos que nos parecem mais interessantes, sem entrar em pormenores técnicos.

Como **IST** contém **ZFC**, todos os conjuntos e construções da matemática clássica (na medida em que esta está representada em **ZFC**) permanecem como são. Nomeadamente, $\mathbb{N}$, $\mathbb{R}$ e todos os outros conjuntos com que os matemáticos habitualmente lidam estão presentes com todas as propriedades usuais. Mas há mais coisas neles do que se julgava... Um dos primeiros teoremas de **IST** garante que *em todo o conjunto infinito existem elementos não-standard.* Assim, em particular, existem elementos não-standard em $\mathbb{N}$ e em $\mathbb{R}$. No que respeita a $\mathbb{N}$, prova-se que (i) 0 é standard, e (ii) sempre que n é standard, $n+1$ também é standard, de modo que tais elementos não-standard de $\mathbb{N}$ (que não deixam, por isso, de ser números naturais) são maiores do que todos os elementos standard. São, portanto, genuínos naturais infinitamente grandes (com respeito aos standard). Mas, dirá o leitor, face a (i) e (ii), o princípio de indução não implica que todos os naturais são standard? A resposta é NÃO, pelo simples facto de não ser legítimo aplicar o princípio de indução à condição

$$(*) \qquad n \in \mathbb{N} \wedge \mathit{standard}(n),$$

visto que esta condição não está expressa na linguagem original de **ZFC**. Também em $\mathbb{R}$ há elementos standard e não-standard e, entre estes, encontram-se os infinitamentes grandes positivos e negativos (relativamente aos standard), os seus recíprocos, que são infinitesimais ou infinitamente pequenos genuínos, positivos e negativos (0 é o único infinitesimal standard) e números reais da forma $x+\varepsilon$ com x standard e ε infinitesimal. Isto é chocante, para quem está habituado a encarar os números reais como «vacas sagradas» das matemáticas, mas é apenas mais um

desenvolvimento das matemáticas formais, tão legítimo e natural (mas igualmente difícil de aceitar, de princípio) como foram as noções de número negativo ou de número complexo, de «ponto no infinito» em geometria projectiva, etc. Tudo se passa, na realidade, como se o novo predicado representasse uma lupa de maior poder resolvente relativamente às estruturas clássicas que permite ver nelas *mais coisas* que, afinal de contas, sempre lá estiveram, mas invisíveis ao olhar clássico.

As possibilidades são imensas, e a vasta literatura já existente aí está a comprová-lo. Só não vê quem não quiser ver...

Para além da espectacularidade do desenvolvimento da Análise Não-standard (mais correcto seria dizer, na actualidade, da Matemática Não-standard), chamamos a atenção para o seguinte aspecto de interesse para os fundamentos. Desde a criação da teoria dos conjuntos por Cantor e posterior axiomatização por Zermelo, hoje em dia coisas banais aceites sem revervas por toda a gente (excepto pelos intuicionistas, ver secção seguinte), o predicado *standard*(x) é o primeiro exemplo, no presente século, de um *novo conceito primitivo* a enriquecer (com sucesso) o ideário matemático «clássico» e, a nosso ver, uma das contribuições mais significativas da matemática (saída da lógica matemática) no milénio que está terminando.

V.5 Sobre a lógica e a matemática intuicionistas

No princípio do século XX teve lugar um grande debate na filosofia da matemática centrado na questão da legitimidade das demonstrações não construtivas em matemática. Seria legítimo demonstrar que existe um número ou uma função com certas propriedades sem se ser capaz, nem em princípio, de exibir um ou uma tal? Contribuiu para incentivar o debate a grande crise de fundamentos na viragem do século, provocada em parte pelos paradoxos que povoavam a teoria intuitiva (ou ingénua) dos conjuntos de Cantor (remediados, a um preço, pela axiomática de Zermelo), e noutra parte pelo mal estar provocado pela crescente abstracção dos princípios e métodos em matemática (por exemplo, a utilização irrestrita do Axioma da Escolha). Para enfrentar e tentar resolver os problemas surgiram diversas escolas de pensamento e programas de reconstrução da matemática, as mais importantes das quais são o *logicismo* de Russell (antecipado por Frege), o *formalismo* de Hilbert (a tradição euclidiana na sua forma mais pura) e o *intuicionismo/construtivismo* de Brouwer [antecipado por Kronecker e ao gosto (inconfessado) dos grandes mestres da «Escola de Paris» (Baire, Borel, Lebesgue)]. Como programa, nos termos inicialmente propostos, apenas sobreviveu o último, embora os seus custos tenham parecido e continuem a parecer excessivos para a maioria dos matemáticos.

Brouwer constituiu-se no chefe de fila de um construtivismo extremo, rejeitando muita da matemática que se estava fazendo com o argumento de que ela não fornecia demonstrações de existência apropriadas. Ele achava que uma demonstração de uma disjunção $\phi \vee \psi$ deveria consistir ou numa demonstração de ϕ ou numa demonstração de ψ (*propriedade da disjunção*), e que uma demonstração de $\exists x \phi(x)$ deveria conter a construção de um objecto apropriado

(testemunha) c, juntamente com a prova de $\phi(c)$ (*propriedade de existência*). No cerne de muitas demonstrações não construtivas parece estar a lei do terceiro excluído $\phi \vee \neg\phi$, pressuposto fundamental de uma concepção platonista da «verdade», independente dos meios ao nosso dispor para a alcançar, que Brouwer rejeita. $\exists x \phi(x)$ poderá ser demonstrada (classicamente) mostrando que a sua negação conduz a um absurdo e sem que se tenha a menor ideia de como encontrar uma testemunha c tal que $\phi(c)$; $\phi \vee \psi$ poderá ser demonstrada classicamente, mostrando que se tem $\neg(\neg\phi \wedge \neg\psi)$ e sem que se fique sabendo qual das componentes é demonstrável.

Exemplo. Mostramos que existe um par (a, b) de números irracionais a, b tais que a^b é racional. Seja $c = \sqrt{2}^{\sqrt{2}}$. Se c é racional, tomemos $a = b = \sqrt{2}$; se c não é racional, tome-se $a = c$, $b = \sqrt{2}$:

$$a^b = c^{\sqrt{2}} = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = (\sqrt{2})^2 = 2$$

Em qualquer dos casos, a^b é racional.■

A lei do terceiro excluído foi utilizada na proposição particular «c é racional ou c não é racional», e ficamos sem saber qual dos pares (a, b) tem os números pretendidos.[191]

Mesmo discordando das opções filosóficas de base do intuicionismo, não se pode deixar de reconhecer o contributo positivo que a escola construtivista deu para questões fundamentais da filosofia e fundamentos da matemática e, também, para a motivação da investigação em diversas áreas da lógica e da matemática clássicas, particularmente relevantes hoje em dia, desde a mais abstracta teoria das categorias (a «lógica» dos raciocínios categoricais é intuicionista) à mais aplicada análise construtivista.[192] De facto, os raciocínios e as demostrações construtivistas são, pela sua própria natureza, mais informativos e consubstanciam, em geral, um conteúdo numérico e algoritmíco ou computacional mais rico do que os «clássicos». Sabe-se ou adivinha-se como é importante essa informação suplementar nos tempos actuais de matemática assistida por computador.

Um discípulo de Brouwer, A. Heyting desenvolveu nos anos trinta um sistema de lógica formal que tenta captar as posições filosóficas brouwerianas e a essência do raciocínio construtivista — a lógica intuicionista. Se bem que o projecto de Heyting não seja defensável do ponto de vista intuicionista, ele contribuiu notavelmente para a sua compreensão pelos classicistas e para transformar a lógica intuicionista, sob os aspectos sintáctico-dedutivo e semântico, num objecto de

---

[191] Pode saber-se qual dos pares é o pretendido, mas somente após uma incursão nas profundezas da teoria dos números. Por um teorema de Gelfand, c é, de facto, irracional.

[192] Para uma exposição do moderno construtivismo ver o livro de BISHOP & BRIDGES indicado na bibliografia.

estudo da lógica matemática e suas aplicações extralógicas, como o desenvolvimento de programas computacionais (construtivos) de verificação da correcção de deduções.

Se, do ponto de vista sintáctico-dedutivo, a lógica intuicionista é fácil de descrever, como uma certa sublógica da clássica (ver adiante), do ponto de vista semântico as coisas complicam-se substancialmente, o que torna muito difícil ou mesmo impossível uma comparação simplista entre as lógicas clássica e intuicionista. É que a interpretação das noções lógicas primitivas não é a mesma que no caso clássico. No intuicionismo, já não podemos basear as interpretações da lógica na «ficção» de que o universo matemático é uma totalidade platónica pré-determinada que pode (pelo menos, em princípio) ser observada e cartografada do exterior pela mente inquisitiva do matemático. Pelo contrário, somos nós próprios que temos de fornecer uma heurística ou paradigma interpretativo para nela basearmos a semântica. Ora, no caso intuicionista, são diversas as heurísticas possíveis e, com elas, diversas as semânticas válidas, não equivalentes.

Historicamente a heurística mais antiga para a lógica intuicionista é a *demonstrativa*, proposta inicialmente por Heyting e posteriormente retocada por A. Kolmogorover É conhecida pela sigla BHK (Brouwer-Heyting-Kolmogorov). Na base desta interpretação está a ideia de que uma proposição ϕ é intuicionisticamente verdadeira ou I-verdadeira sse possuímos uma demonstração para ela. Por «demonstração» deve-se entender uma construção que estabelece ϕ, não uma dedução em algum sistema formal. Por exemplo, uma demonstração de

$$3 + 4 = 7$$

consiste nas construções sucessivas de 3, 4 e 7, seguida de uma construção que soma 3 com 4 e terminando com outra construção que compara este resultado com 7.

Para descrever (informalmente) a interpretação BHK vamos supor conhecida alguma maneira (construtiva) para demonstrar sentenças atómicas, por exemplo, sentenças aritméticas como acima. Pretende-se explicar o conceito

$$A \textit{ demonstra } \phi$$

mostrando como as demonstrações de fórmulas ou sentenças compostas dependem das demonstrações das suas componentes. As letras A, B, C, ... (possivelmente com índices) denotam construções. Não especificamos quais as construções admissíveis (fazê-lo seria, até, contrário ao espírito intuicionista, que encara as matemáticas como uma actividade construtiva em permanente expansão com novos métodos e construções). Por outras palavras, o conceito «construção» encara-se como um conceito primitivo. Em todo o caso, teremos de admitir que as construções têm certas propriedades de fecho, por exemplo, que um par ordenado (A, B) de construções é uma construção e que uma construção A se pode aplicar a outra construção B para produzir uma nova construção $A(B)$. Por conveniência técnica admitimos que os conectivos primitivos são $\wedge$, $\vee$, $\rightarrow$, $\perp$ e que $\neg\phi = \phi \rightarrow \perp$. Temos então:

• A demonstra $\phi \wedge \psi \Leftrightarrow A$ é um par ordenado (B, C) tal que B demonstra ϕ e C demonstra ψ;

• A demonstra $\phi \vee \psi \Leftrightarrow A$ é um par ordenado (a, C) tal que a é um número natural, se $a = 0$ então C demonstra ϕ, e se $a \neq 0$ então C demonstra ψ;

• A demonstra $\phi \rightarrow \psi \Leftrightarrow A$ é uma construção que converte toda a demonstração B de ϕ numa demonstração $A(B)$ de ψ;

• nenhuma construção demonstra $\perp$.[193]

Resulta da definição de $\neg$ que uma demonstração de $\neg\phi$ é uma construção A que converte toda a demonstração B de ϕ numa demonstração $A(B)$ de $\perp$.

Para lidar com os quantificadores $\forall$, $\exists$ temos de supor dado um domínio (não vazio) D de objectos referentes das variáveis de quantificação. Por abuso, identificamos cada objecto d em D com a constante $\overline{d}$ que o designa.

• A demonstra $\forall x\, \phi(x) \Leftrightarrow A$ é uma construção tal que para cada $d \in \mathsf{D}$, $A(d)$ demonstra $\phi(d)$;

• A demonstra $\exists x\, \phi(x) \Leftrightarrow A$ é um par ordenado (d, C) tal que $d \in \mathsf{D}$ e C demonstra $\phi(d)$.

Esta interpretação dos primitivos lógicos dá uma ideia intuitiva do que é ou não correcto em lógica intuicionista. Ela incorpora as propriedades da disjunção e de existência gratas a Brouwer (ver acima). Os exemplos seguintes ilustram a sua utilização prática.

Exemplos. **1**) Para quaisquer ϕ e ψ, $\phi \wedge \psi \rightarrow \phi$ é I-verdadeira. Pois se (A, B) demonstra $\phi \wedge \psi$, a construção C tal que $C(A, B) = A$ (primeira projecção) converte a demonstração de $\phi \wedge \psi$ numa demonstração de ϕ, logo C demonstra $\phi \wedge \psi \rightarrow \phi$. Por outras palavras, a regra ($\wedge^+$) é intuicionisticamente válida.

2) Para quaisquer ϕ, ψ e θ, $(\phi \wedge \psi \rightarrow \theta) \rightarrow (\phi \rightarrow (\psi \rightarrow \theta))$ é I-verdadeira. Pois seja C uma demonstração de $\phi \wedge \psi \rightarrow \theta$, quer dizer, C converte uma demonstração (A, B) de $\phi \wedge \psi$ numa demonstração $C(A, B)$ de θ.

Pretende-se encontrar uma demonstração D de $\phi \rightarrow (\psi \rightarrow \theta)$, quer dizer, uma construção que converta uma demonstração A de ϕ numa demonstração $D(A)$ de $\psi \rightarrow \theta$; $D(A)$ há-de ser uma contrução que converta uma demonstração B de ψ numa demonstração $(D(A))(B)$ de θ. Recorde-se que já temos uma demonstração $C(A, B)$ de θ, logo podemos pôr

$$(D(A))(B) = C(A, B);$$

seja E definida por $E(B) = C(A, B)$, de modo que podemos definir D por

[193] No caso de $\neg$ ser primitivo, em vez de $\perp$, estipula-se que nenhuma construção demonstra uma contradição.

$$D(A) = E.$$

É claro, portanto, que ficou descrita uma construção F que converte uma demonstração C de $\phi \wedge \psi \rightarrow \theta$ numa demonstração D de $\phi \rightarrow (\psi \rightarrow \theta)$, quer dizer, $F(C) = D$ e, portanto, a sentença dada é I-verdadeira.

3) Não é de esperar que $\neg\neg\phi \rightarrow \phi$ seja I-verdadeira: para que assim fosse, precisaríamos de uma construção C que convertesse toda a demonstração de $\neg\neg\phi$ numa demonstração de ϕ; ora, uma demonstração A de $\neg\neg\phi$ converteria toda a demonstração B de $\neg\phi$ numa demonstração de $\perp$, logo não pode existir nenhuma demonstração B de $\neg\phi$. Uma tal B converteria toda a demonstração D de ϕ numa demonstração de $\perp$. Quer dizer, portanto, que não pode existir nenhuma construção que converta uma demonstração de ϕ numa demonstração de $\perp$. Saber isto fica muito aquém de obter uma demonstração de ϕ (ver exercício 5.4).

4) $\neg\exists x\, \phi(x) \rightarrow \forall x \neg\phi(x)$ é I-verdadeira. Pois seja A uma construção que converte toda a demonstração de $\exists x \phi(x)$ numa demonstração de $\perp$. Pretende-se obter uma construção B que produza para cada $d \in D$ uma demonstração de $\phi(d) \rightarrow \perp$, isto é, uma construção B que converta uma demonstração de $\phi(d)$ numa demonstração de $\perp$. Se C demonstra $\phi(d)$, então (d, C) demonstra $\exists x \phi(x)$ e $A(d, C)$ demonstra $\perp$. Então B tal que

$$(B(d))(C) = A(d, C)$$

demonstra $\forall x \neg\phi(x)$. Ficou assim descrita uma construção D que converte A em B, o que mostra que $\neg\exists x \phi(x) \rightarrow \forall x \neg\phi(x)$ é I-verdadeira.

O leitor pode tentar por si mais alguns exemplos, mas fica avisado de que alguns pormenores se podem tornar bastante complicados. Existe, de facto, uma maquinaria formal (o *cálculo-λ*, uma versão da chamada lógica combinatória) para facilitar notacionalmente tais pormenores da combinatória das construções, mas a sua exposição sai fora do âmbito deste livro. Por outro lado, existem outras semânticas mais ou menos formalizadas que, inclusive, permitem obter um meta-teorema de completude semântica, mas isso levar-nos-ia muito longe.

Completamos esta secção com a descrição de um sistema dedutivo para a lógica intuicionista e algumas das suas propriedades. Bastará, aliás, uma pequena alteração ao sistema **DN** para obter um sistema de dedução natural para a lógica proposicional intuicionista, $\mathbf{DN}_I$, e a alteração correspondente à parte proposicional de **DNQ** para obter um sistema de dedução natural para a lógica de primeira ordem intuicionista, $\mathbf{DNQ}_I$.

No caso proposicional (para uma linguagem $\mathcal{L}^0$ com primitivos $\wedge$, $\vee$, $\rightarrow$, $\neg$) basta substituir a regra ($\neg\neg^-$) pela regra ($\perp$), e no caso do cálculo de predicados (para uma linguagem elementar $\mathcal{L}$ com primitivos $\wedge$, $\vee$, $\rightarrow$, $\neg$, $\forall$, $\exists$, $=$) é fazer exactamente a mesma troca. As restantes regras dos conectivos e dos quantificadores ficam inalteradas, pois são intuicionisticamente válidas. Note-se que a regra ($\perp$) é intuicionisticamente válida, pela interpretação BHK: como não

podem existir construções A e B que demonstrem ϕ e $\neg\phi$, respectivamente, qualquer construção demonstra ψ. Todavia, como já foi dito várias vezes, é tecnicamente preferível uma formulação do cálculo dedutivo com o primitivo $\perp$ no lugar de $\neg$ e este definido por $\neg\phi = \phi \rightarrow \perp$. Se isto for feito, pode-se simplificar a forma de ($\perp$) em

$$(\perp) \qquad \frac{\perp}{\psi},$$

e a forma de ($\neg^+$) em

$$(\neg^+) \qquad \frac{\begin{array}{c}\phi \quad [\mathrm{H}] \\ \vdots \\ \perp\end{array}}{\neg\phi},$$

só que esta regra fica agora redundante, pois é um caso particular de ($\rightarrow^+$), atendendo à definição de $\neg$. Observe-se, por outro lado, que a regra derivada (RA) vai deixar, em princípio,[194] de se poder derivar no sistema $\mathbf{DN}_I$ (ver Nota 53).

A alteração parece pequena, mas tem um grande alcance. Por um lado, todas as derivações no sistema dedutivo clássico que fazem uso essencial de ($\neg\neg^-$) vão deixar, em geral, de poder efectuar-se na lógica intuicionista. Ficam de fora, por exemplo, algumas leis de conversão e outras, como na lista seguinte, onde, nas três últimas, x não ocorre em ϕ.

$$\begin{gathered}
\neg(\phi \wedge \psi) \rightarrow \neg\phi \vee \neg\psi, \\
(\phi \rightarrow \psi) \rightarrow (\neg\phi \vee \psi), \\
\neg(\phi \rightarrow \psi) \rightarrow (\phi \wedge \neg\psi), \\
(\neg\phi \rightarrow \neg\psi) \rightarrow (\psi \rightarrow \phi), \\
\neg\forall x \phi(x) \rightarrow \exists x \neg\phi(x), \\
(\phi \rightarrow \forall x \psi(x)) \rightarrow \exists x (\phi \rightarrow \psi(x)), \\
\forall x (\phi \vee \psi(x)) \rightarrow (\phi \vee \forall x \psi(x)), \\
(\forall x \psi(x) \rightarrow \phi) \rightarrow \exists x (\psi(x) \rightarrow \phi).
\end{gathered}$$

Por outro lado, o facto de ϕ não ser equivalente a $\neg\neg\phi$ significa, para todos os efeitos, que $\neg\neg$ se comporta como um novo conectivo sem correspondente na lógica clássica. Se é verdade que, do ponto de vista dedutivo, a lógica intuicionista é um subsistema da clássica (mais precisamente, se $\vdash_I \phi$, então $\vdash \phi$, onde $\vdash_I$ é a

[194] Dizemos «em princípio» apenas por precaução de honestidade porque, poderia pensar o leitor, poderia haver *outras* maneiras de derivar esta regra. Na realidade não há. Prová-lo é outra estória. Em geral, para provar que certas regras, leis ou derivações são impossíveis na lógica intuicionista teríamos de desenvolver uma semântica apropriada a questões de independência como, por exemplo, a semântica de Kripke. Uma exposição introdutória desta semântica e de diversas outras questões relativas à lógica intuicionista pode ser consultada na monografia de Van DALEN.

relação de derivabilidade em **DNQ**$_I$ e $\vdash$ é a clássica, em **DNQ**), Gentzen e Gödel mostraram que, interpretando $\vee$ e $\exists$ num sentido fraco, a lógica clássica pode-se «mergulhar» na intuicionista.

A lógica e a matemática intuicionistas são assuntos fascinantes, como são tantos outros assuntos da lógica matemática, mas com pouquíssimos praticantes no nosso País. Este livro é, antes de mais, um convite ao leitor para mergulhar na abundante literatura sobre esses assuntos. Se me acompanhou até aqui, já pode de aqui em diante caminhar pelos seus próprios meios sem os tropeços, dúvidas e hesitações que fazem desitir tanto iniciandos como seniores (noutras áreas).

V.6 Exercícios e Complementos

5.1 Deduza, em **DN**$_I$, as seguintes leis:

(a) $\neg\neg(\phi \vee \neg\phi)$;

(b) $\neg(\phi \wedge \neg\phi)$;

(c) $\neg\neg(\neg\neg\phi \to \phi)$;

(d) $(\phi \to \psi) \to (\neg\psi \to \neg\phi)$ *(contraposição intuicionista)*;

(e) $\neg\phi \leftrightarrow \neg\neg\neg\phi$;

(f) $(\phi \wedge \neg\psi) \to \neg(\phi \to \psi)$;

(g) $(\phi \to \psi) \to (\neg\neg\phi \to \neg\neg\psi)$;

(h) $\neg(\phi \to \psi) \leftrightarrow \neg\neg\phi \wedge \neg\psi$;

(i) $\phi \wedge \neg\psi \to \neg\neg\phi \wedge \neg\psi$;

(j) $\neg\neg(\phi \to \psi) \leftrightarrow (\neg\neg\phi \to \neg\neg\psi)$;

(k) $\neg\neg(\phi \wedge \psi) \leftrightarrow (\neg\neg\phi \wedge \neg\neg\psi)$.

5.2 Deduza, em **DNQ**$_I$, a lei $\neg\neg\forall x\phi(x) \to \forall x\neg\neg\phi(x)$.

5.3 Mostre, utilizando a interpretação BHK, que $\neg\phi \vee \neg\psi \to \neg(\phi \wedge \psi)$ é I-verdadeira, mas a implicação recíproca não.

5.4* Seja $\phi(n)$ uma condição decidível na variável natural n [quer dizer, existe um algoritmo para decidir, para cada $n \in \mathbb{N}$, se $\phi(n)$ é ou não verdadeira em $\mathbb{N}$] tal que nem $\exists n\phi(n)$ nem $\forall n\neg\phi(n)$ foram estabelecidas. Por exemplo, $\phi(n)$ poderia ser a condição «n é o maior número natural tal que n e $n+2$ são ambos primos»

(ver Nota 7). Considere a sucessão de números racionais de termo geral

$$a_n = \begin{cases} \sum_{i=1}^{n} 2^{-i} & \text{se } \forall k < n \neg\phi(k), \\ \sum_{i=1}^{k} 2^{-i} & \text{se } k < n \text{ e } \phi(k) \text{ e } \neg\phi(i) \text{ para todo } i < k \end{cases}.$$

Mostre que:

(a) $\langle a_n \rangle$ é uma sucessão de Cauchy, a qual define, portanto, um número real a;

(b) $\neg\neg$(a é racional), mas não há nenhuma evidência de que a seja racional.

5.5 O exercício seguinte esquematiza uma prova de independência das leis (clássicas) $\phi \vee \neg\phi$ e $\neg\neg\phi \rightarrow \phi$ relativamente à lógica proposicional intuicionista (nos primitivos $\wedge$, $\vee$, $\rightarrow$, $\neg$). Para $n \geq 2$ define-se uma semântica com $n+1$ valores lógicos do seguinte modo. Uma valoração é uma função

$$v : \text{Prop}(P) \rightarrow \{0, 1, ..., n\},$$

que se estende de uma única maneira a uma função

$$\widehat{v} : \text{Form}(\mathcal{L}^0) \rightarrow \{0, 1, ..., n\}$$

tal que, para quaisquer fórmulas ϕ, ψ,

$$\widehat{v}(\phi \wedge \psi) = \max\{\widehat{v}(\phi), \widehat{v}(\psi)\}, \ \widehat{v}(\phi \vee \psi) = \min\{\widehat{v}(\phi), \widehat{v}(\psi)\},$$

$$\widehat{v}(\phi \rightarrow \psi) = \begin{cases} 0 & \text{se } \widehat{v}(\phi) \geq \widehat{v}(\psi) \\ \widehat{v}(\psi) & \text{se } \widehat{v}(\phi) < \widehat{v}(\psi) \end{cases},$$

$$\widehat{v}(\neg\phi) = \begin{cases} 0 & \text{se } \widehat{v}(\phi) = n \\ n & \text{se } \widehat{v}(\phi) < n \end{cases}.$$

Mostre que:

(a) $\widehat{v}(\phi) = 0$ para todo o teorema lógico ϕ de $\mathbf{DN}_I$ [Sugestão: indução completa no comprimento das deduções; o valor 0 é o valor «verdade»];

(b) $\widehat{v}(\phi \wedge \neg\phi)$ e $\widehat{v}(\neg\neg\phi \rightarrow \phi)$ não são necessariamente iguais a 0, se $n \geq 2$.

5.6 Demonstre o seguinte

TEOREMA DE ZERMELO
Não existe nenhum conjunto ao qual pertencem todos os conjuntos.

SOLUÇÕES

Capítulo I

1.1 (a) p: existe petróleo no Algarve; q: os peritos estão certos; r: o Governo mente. Simbolização:

$$\begin{array}{l} \neg p \rightarrow (q \vee r) \\ p \vee \neg q \\ \hline \neg r. \end{array}$$

(c) p: 2 é primo; q: 2 é o menor primo; r: 1 é primo. Simbolização:

$$p \rightarrow q,\ q \rightarrow \neg r,\ \neg r \ \ / \ p.$$

1.2 (a) Tabela de verdade:

p	q	r	$\neg p \rightarrow (q \vee r)$	$p \vee \neg q$	$\neg r$
0	0	0	0	1	1
0	0	1	1	1	0
0	1	0	1	0	1
0	1	1	1	0	0
1	0	0	1	1	1
1	0	1	1	1	0
1	1	0	1	1	1
1	1	1	1	1	0

Não era necessário ter construído a tabela na totalidade, pois para a atribuição de valores lógicos na segunda linha já se constata que a conclusão não é verdadeira, embora as duas premissas sejam verdadeiras. Portanto, o argumento não é válido.

(c) Em vez de construir uma tabela de verdade procedemos no sentido de verificar que se a conclusão for falsa, então, pelo menos, uma das premissas é falsa também. Se isto acontecer, o argumento é válido. Se, porém, no decurso desse procedimento verificarmos que as premissas podem ser todas verdadeiras (mas a conclusão falsa, como suposto), podemos concluir que o argumento é inválido.

Consideremos, pois, uma qualquer atribuição de valores lógicos às letras p, q, r que torne a conclusão p falsa. A primeira premissa vem verdadeira, qualquer que seja o valor lógico de q e, em particular, com q verdadeira e r falsa a segunda e a terceira premissas são verdadeiras. Portanto, o argumento é inválido.

1.3 (a) Todo o múltiplo de 2 é par. Verdadeira.

(b) 3 é divisível por um número par. Falsa.

(c) 0 divide um número ímpar. Falsa (0 não divide nenhum número não nulo).

(d) Nenhum número não par é múltiplo de 2. Verdadeira.

(e) Todo o múltiplo de um número par é par. Verdadeira.

(f) Todo o primo divide um número par. Verdadeira.

(g) Nenhum número ímpar divide todos os primos. Falsa, pois 1 divide todos os primos.

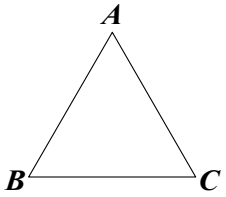
1.4 (a) A) *Domínio:* pessoas; Mx*:* x é modelo; Vx*:* x é vaidoso(a); Bx*:* x é bonito(a).

1) $\forall x(Mx \rightarrow Vx)$; 2) $\exists x(Mx \wedge Vx)$;

3) $\forall x(Mx \rightarrow \neg Vx)$ ou $\neg\exists x(Mx \wedge Vx)$; 4) $\exists x(Mx \wedge \neg Vx)$;

5) $\forall x(Vx \rightarrow Mx)$; 6) $\forall x(Mx \vee Vx)$; 7) $\exists x((Mx \wedge Bx) \wedge Vx)$.

(b) Pontos: A, B, C; linhas: os conjuntos $\{A, B\}$, $\{A, C\}$ e $\{B, C\}$. Esquematicamente:



1.5 (a) $\forall x\, xRx$; (b) $\forall x, y(xRy \rightarrow yRx)$; (c) $\forall x, y, z(xRy \wedge yRz \rightarrow xRz)$;

(d) $\forall x, y\,(xRy \wedge yRx \rightarrow x = y)$; (e) $\forall x, y\,(xRy \vee yRx)$; (f) $\forall x \neg\, xRx$;

(g) $\exists x \neg\, xRx$; (h) $\exists x, y\; xRy$; (i) $\forall x, y\,(x = y \vee xRy \vee yRx)$;

(j) $\exists x, y, z(xRy \wedge yRz \wedge \neg xRz)$; (k) $\exists x, y\,(xRy \wedge \neg yRx)$;

(l) $\forall x \exists y\, xRy$; (m) $\forall x \exists y(y \neq x \wedge xRy)$;

(n) $\forall x, y, z\,(xRy \wedge xRz \rightarrow y = z)$;[195]

(o) $\forall x \exists y\, xRy \wedge$ (n) [abreviadamente, $\forall x \exists^1 y\, xRy$];

(p) $\forall x, y, z\,(xRz \wedge yRz \rightarrow x = y)$; (q) $\forall y \exists x\, xRy$;

(r) (o) $\wedge$ (p) $\wedge$ (q).

---

[195] Se R é funcional e a está no domínio de R, o único b tal que aRb [isto é, $(a, b) \in R$] denota-se $R`a$ ou $R(a)$ e chama-se o *valor de* R *em* a, de modo que, para quaisquer a e b, aRb sse $b = R(a)$.

1.6 (a) Domínio: animais; Lx: x é um leão; Fx: x é feroz; Ax: x bebe água. Simbolização:

$$\forall x(Lx \rightarrow Fx),\ \exists x(Lx \wedge \neg Ax) \ /\ \exists x(Fx \wedge \neg Ax).$$

O argumento é válido: qualquer que seja o domínio (não vazio) considerado e quaisquer que sejam as interpretações nesse domínio de L, F, A, se as premissas forem simultaneamente verdadeiras então a conclusão também é verdadeira: se x_0 é um objecto desse domínio que tem as propriedades L e $\neg A$ (existe pelo menos um tal pela segunda premissa), então x_0 tem a propriedade F, por virtude da primeira premissa; por conseguinte, x_0 tem as propriedades F e $\neg A$, logo existe pelo menos um objecto no domínio com estas propriedades, o que quer dizer que a conclusão é verdadeira.

(c) Inválido: Russell pode não ser lógico.

1.7 (a) (1) $\exists x\,(Mx \wedge \neg Sx)$; (2) $\forall x(Lx \rightarrow Sx)$;

(3) $\forall x(Mx \rightarrow \forall y\,(Lx \rightarrow Fxy))$ ou $\forall x, y\,(Mx \wedge Lx \rightarrow Fxy)$;

(4) $\exists x, y(Lx \wedge Ly \wedge x \neq y \wedge Fxy)$.

(c) (1) $\exists x(Px \wedge \forall y(Dy \rightarrow \neg Rxy))$; (2) $\exists xy(Dx \wedge Dy \wedge Rbx \wedge \neg Rby)$;

(3) $\forall x(Px \rightarrow \exists yz(Dx \wedge Dy \wedge Rxy \wedge \neg Rxz))$;

(4) Quem tem todo o dinheiro tem tudo.

1.8 O culpado não pode ser A nem B nem D.

Capítulo II

2.3 (a) $e[p] = d[p]$ para toda a letra proposicional p. Suponhamos (hipótese de indução) que a propriedade é verdadeira para ϕ, quer dizer $e[\phi] = d[\phi]$; ora $e[\neg\phi] = e[\phi] = e[\phi] = e[\neg\phi]$, o que mostra que a propriedade é verdadeira para $\neg\phi$. Suponhamos (hip. de ind.) que a propriedade é verdadeira para ϕ e para ψ, isto é, que $e[\phi] = d[\phi]$ e $e[\psi] = d[\psi]$; ora

$$e[(\phi \wedge \psi)] = e[\phi] + d[\phi] + 1 = e[\psi] + d[\psi] + 1 = \ d[(\phi \wedge \psi)],$$

o que mostra que a propriedade também é verdadeira para $(\phi \wedge \psi)$. Analogamente para $(\phi \vee \psi)$ e para $(\phi \rightarrow \psi)$.

(b) Sejam v e v' duas valorações que coincidem em todas as letras proposicionais que ocorrem em ϕ, e demonstremos que $\widehat{v}(\phi) = \widehat{v'}(\phi)$, por indução na complexidade de ϕ. Se ϕ é uma letra proposicional, digamos p, então $v(p) = v'(p)$ por hipótese sobre v e v'. Se ϕ é uma negação, digamos $\neg\psi$, e v e v' coincidem nas letras proposicionais que ocorrem em $\neg\psi$, então v e v' coincidem nas letras proposicionais que ocorrem em ψ (exactamente as mesmas que ocorrem em $\neg\psi$), logo $\widehat{v}(\psi) = \widehat{v'}(\psi)$ por hipótese de indução, donde $\widehat{v}(\neg\psi) = \widehat{v'}(\neg\psi)$ em

virtude da tabela de verdade de $\neg$. Se ϕ é uma conjunção, digamos $\psi \wedge \theta$, e v e v' coincidem nas letras proposicionais que ocorrem em $\psi \wedge \theta$, então, em particular, v e v' coincidem nas letras proposicionais que ocorrem em ψ e em θ, logo $\widehat{v}(\psi) = \widehat{v}'(\psi)$ e $\widehat{v}(\theta) = \widehat{v}'(\theta)$ por hipótese de indução, donde $\widehat{v}(\psi \wedge \theta) = \widehat{v}'(\psi \wedge \theta)$ por virtude da tabela de verdade de $\wedge$. Analogamente nos outros casos (ϕ uma disjunção ou uma condicional).

2.5 Derivação de (40) $(\phi \rightarrow \psi) \rightarrow \phi \vdash \phi$:

$\{1\}$	1	$(\phi \rightarrow \psi) \rightarrow \phi$	H
$\{2\}$	2	$\neg\phi$	[H]
$\{1,2\}$	3	$\neg(\phi \rightarrow \psi)$	1, 2 (MT)
$\{2\}$	4	$\phi \rightarrow \psi$	2, (T^+, 38)
$\{1,2\}$	5	$(\phi \rightarrow \psi) \wedge \neg(\phi \rightarrow \psi)$	3, 4 (MT)
$\{1\}$	6	$\neg\neg\phi$	2-5 ($\neg^-$)
$\{1\}$	7	ϕ	6 ($\neg\neg^-$).

2.6 Construa uma tabela de verdade (8 linhas) com colunas para p, q, r, ϕ, ψ, θ onde p: A é inocente, q: B é inocente, r: C é inocente. Para responder a (f) procure uma linha em que os valores lógicos atribuídos a p, q, r são os mesmos que os resultantes para ϕ, ψ, θ, respectivamente.

2.7 (a) ($\Rightarrow$) Suponhamos $\Gamma \cup \{\neg\phi\}$ incompatível, e seja v um modelo qualquer de Γ, com vista a provar que $v(\phi) = 1$; se fosse $v(\phi) = 0$, viria $v(\neg\phi) = 1$, logo v seria modelo de $\Gamma \cup \{\neg\phi\}$, contra a hipótese de $\Gamma \cup \{\neg\phi\}$ ser incompatível; portanto, $v(\phi) = 1$. Como v é arbitrária, podemos concluir que $\Gamma \vDash \phi$.

2.12 (a) Numa dedução de ϕ com hipóteses em Γ, somente pode ocorrer um número *finito* de tais hipóteses (porque uma dedução é uma sequência finita de fórmulas), digamos $\gamma_1, ..., \gamma_k$. Basta pôr, então, $\Gamma_0 = \{\gamma_1, ..., \gamma_k\}$.

(b) Utilize (a).

2.13 Supondo ambos os conjuntos $\Gamma \cup \{\phi\}$, $\Gamma \cup \{\neg\phi\}$ contraditórios, do primeiro deriva-se $\neg\phi$, logo $\Gamma \vdash \neg\phi \rightarrow \phi$, e do segundo deriva-se ϕ, logo $\Gamma \vdash \phi \rightarrow \neg\phi$, e portanto $\Gamma \vdash \phi \leftrightarrow \neg\phi$. V. exercício 2.11 (b).

2.15 (b) Falso. Contra-exemplo: $\Sigma = \{p, p \wedge p\}$, $\Gamma = \{p\}$.

2.17 (a) Suponhamos Γ compatível. Se Γ não fosse consistente, então $\Gamma \vdash \psi \wedge \neg\psi$ para alguma ψ, logo $\Gamma \vDash \psi \wedge \neg\psi$ por ($\mathbf{MV}_G$), o que é absurdo pois, por hipótese, Γ tem, pelo menos, um modelo.

2.18 (a) $\Gamma = \emptyset$, $\phi = p$.

2.19 (c) Se Σ é incompatível, então $\Sigma^* = \mathrm{Form}(\mathcal{L}^0)$ é decidível. No outro caso, seja dada ϕ ao arbítrio. Começando a gerar, um a um, os membros de Σ, digamos $\Sigma = \{\phi_1, \phi_2, ...\}$, testamos «$\phi_1 \vDash \phi$?», «$\phi_1 \vDash \neg\phi$?» durante 1 minuto cada, depois

testamos «$\phi_1, \phi_2 \vDash \phi$?», «$\phi_1, \phi_2 \vDash \neg\phi$?» durante 2 minutos cada, e assim sucessivamente. Mais tarde ou mais cedo, uma das fórmulas ϕ, $\neg\phi$ é consequência de ϕ_1, ϕ_2, ..., ϕ_k para algum k, e nesse preciso momento fica decidido se ϕ pertence ou não a Σ^*.

2.21 (a) 2^{2^n}. (e) Construa tabelas para $\phi \mid \phi$ e $(\phi \mid \phi) \mid (\psi \mid \psi)$, onde $\mid$ é $\wedge$ ou $\vee$. (f) Suponhamos que Π é funcionalmente completo, e seja u a função booleana associada. Se fosse $u(0,0) = 0$, então qualquer fórmula construída só com Π teria o valor 0 sempre que todas as letras proposicionais que nela ocorrem têm o valor 0, logo $\neg$ não seria definível à custa de Π. Portanto, $u(0,0) = 1$. Analogamente, $u(1,1) = 0$. Temos, assim, a tabela parcialmente preenchida

ϕ	ψ	$\phi\Pi\psi$
0	0	1
0	1	
1	0	
1	1	0

Se na segunda e terceira linhas figurarem os valores 0, 0 ou 1, 1, então Π é $\downarrow$ ou $\uparrow$, respectivamente. No caso de os valores serem 0, 1, $\phi\Pi\psi$ seria logicamente equivalente a $\neg\psi$, o que é absurdo pois $\{\neg\}$ não é funcionalmente completo; no caso de os valores serem 1, 0, $\phi\Pi\psi$ seria logicamente equivalente a $\neg\phi$, igualmente absurdo.

2.24 No caso (i) casa-se um rapaz com uma das namoradas e aplica-se a hipótese de indução aos restantes rapazes e raparigas. No caso (ii) casa-se cada rapaz em K com a sua namorada. Mostre, por redução ao absurdo, que quaisquer $l \leq m - k$ dos restantes rapazes têm, pelo menos, l namoradas entre si, de entre as restantes namoradas. (Se L fosse um conjunto de l rapazes com menos de l namoradas entre si, $K \cup L$ seria um conjunto de $k + l$ rapazes com menos de $k + l$ namoradas entre si.)

Capítulo III

3.1 Derivação de (116′) $\forall x\, \phi(x) \dashv\vdash \neg\exists x\, \neg\phi(x)$, onde $\phi(x)$ é uma condição em x. (116) é um caso particular, em que $\phi(x)$ é a fórmula atómica Px. Deduções:

{1}	1	$\forall x\phi(x)$	H
{2}	2	$\exists x\neg\phi(x)$	[H]
{3}	3	$\neg\phi(a_0)$	[H] [a_0 não em $\phi(x)$]
{1}	4	$\phi(a_0)$	1 ($\forall^-$)
{1, 3}	5	$\forall x\phi(x) \wedge \neg\forall x\phi(x)$	3, 4 ($\perp$)
{1, 2}	6	$\forall x\phi(x) \wedge \neg\forall x\phi(x)$	2, 3-5 ($\exists^-$)
{1}	7	$\neg\exists x\neg\phi(x)$	2-6 ($\neg^+$).

Note-se que na linha 3 se teve o cuidado de utilizar um parâmetro que não

ocorresse em $\phi(x)$. Na linha 5, qualquer contradição servia, desde que nela não ocorresse o parâmetro da particularização, a_0.

$\{1\}$	1	$\neg\exists x\neg\phi(x)$	H
$\{2\}$	2	$\neg\phi(a)$	[H] [a não em $\phi(x)$]
$\{2\}$	3	$\exists x\neg\phi(x)$	2 ($\exists^+$)
$\{1, 2\}$	4	$\exists x\neg\phi(x) \wedge \neg\exists x\neg\phi(x)$	1, 3 ($\wedge^+$)
$\{1\}$	5	$\neg\neg\phi(a)$	2-4 ($\neg^+$)
$\{1\}$	6	$\phi(a)$	5 ($\neg\neg^-$)
$\{1\}$	7	$\forall x\phi(x)$	6 ($\forall^+$).

Observe-se que na linha 7 a regra ($\forall^+$) foi aplicada correctamente, pois a não ocorre em nenhuma hipótese de que $\phi(a)$, na linha 6, depende.

3.3 Contra-exemplo para 3.2 (b): (M, P, Q), onde $M = \{1, 2\}$, $P = \{1\}$, $Q = \{2\}$.

3.5 (a) (2) Bx: x é barbeiro; Fxy: x faz a barba a y.

$\forall x(Bx \rightarrow \forall y(\neg Fyy \rightarrow Fxy))$ [ou $\forall xy(Bx \wedge \neg Fyy \rightarrow Fxy)$],
$\forall x(Bx \rightarrow \forall y(Fyy \rightarrow \neg Fxy)) \;/\; \neg\exists x\, Bx$.

3.6 (a) $\neg\exists xPx \vee \exists^1 x\, Px \vee \exists xy\,(Px \wedge Py \wedge \forall z(Pz \rightarrow Px \vee Py))$; melhor ainda: $\forall xyz\,(Px \wedge Py \wedge Pz \rightarrow x = y \vee x = z \vee y = z)$.

(b) $\neg\exists^{\leq 2} xPx$, ou $\exists xyz\,(x \neq y \wedge x \neq z \wedge y \neq z)$.

3.13 (a) (i) $\forall xy\, Pfxy$; (ii) $\forall xyuv\,(fxy = fuv \rightarrow x = u \wedge y = v)$;

(iii) $\exists z\forall xy\, fxy \neq z$.

3.15 (1) $\Rightarrow$ (2): note que, se $\mathbf{T} \vdash \phi$, então ϕ é verdadeira em todos os modelos de **T**, e se $\mathbf{T} \vdash \neg\phi$, então ϕ é falsa em todos os modelos de **T**.

(2) $\Rightarrow$ (3): seja $\mathfrak{M}$ um modelo qualquer de **T**; é claro que se $\phi \in \mathbf{T}$ então ϕ é verdadeira em $\mathfrak{M}$, logo $\phi \in \mathrm{Tr}(\mathfrak{M})$; reciprocamente, se ϕ é verdadeira em $\mathfrak{M}$, então $\phi \in \mathbf{T}$, caso contrário $\mathbf{T} \nvdash \phi$ (pois **T** é uma teoria, quer dizer, é dedutivamente fechado), logo $\mathbf{T} \cup \{\neg\phi\}$ seria consistente e, portanto, compatível; se $\mathfrak{M}'$ fosse um modelo deste conjunto, seria modelo de **T** e de $\neg\phi$, mas $\mathfrak{M} \equiv \mathfrak{M}'$, por (2), o que é absurdo, pois $\mathfrak{M}$ satisfaz ϕ.

(3) $\Rightarrow$ (1): fácil, pois toda a sentença é verdadeira ou é falsa em $\mathfrak{M}$.

3.17 (a) Demonstração informal de T_4: dado a ao arbítrio, seja b tal que $a + b = 0$ (G_3), e seja b' tal que $b + b' = 0$ (novamente por G_3). Mostramos que também $b + a = 0$. Tem-se sucessivamente

$$\begin{aligned} b + a = (b + a) + 0 \quad &= (b + a) + (b + b') = b + ((a + b) + b')) \\ &= b + (0 + b') = (b + 0) + b' = b + b' = 0. \end{aligned}$$

Demonstração informal de T_5: dado a ao arbítrio, mostramos que $0 + a = a$. Seja b tal que $a + b = 0$ e $b + a = 0$ (T_4). Tem-se $0 + a = (a + b) + a = a + (b + a) = a + 0 = a$.

3.21 (a) (i) $\exists x \forall y\ (y \in x)$.

(b) Demonstração informal de T_2 (utilizando as variáveis x, y, z, ... em vez de parâmetros): dados x e y ao arbítrio, a existência de z tal que $\forall u(u \in z \leftrightarrow u = x \vee u = y)$ é garantida por A_2. Falta demonstrar a unicidade. Supondo z_1 e z_2 nas condições de tal z, tem-se que, para todo u, $u \in z_1 \leftrightarrow u = x \vee u = y$, e analogamente para z_2, logo, para todo u, $u \in z_1 \leftrightarrow u \in z_2$, donde $z_1 = z_2$ por extensionalidade.

(h) Verificação de A_2 em $(M, \in)$: supondo x, y em M, tem-se $x \in M_n$, $y \in M_m$ para alguns m, n. Sem perda de generalidade podemos supor que $n \leq m$, de modo que x e y são ambos elementos de M_m. Mas então o conjunto que tem exactamente x e y como elementos, $\{x, y\}$ é subconjunto de M_m, isto é, é elemento de $\mathcal{P}(M_m) = M_{m+1}$, e, por conseguinte, é membro de M.

Capítulo IV

4.5 Para simplificar a notação, supomos que ϕ tem um único parâmetro. Admitamos (IC_1), com vista a demonstrar (IC_2). Suponhamos que

$$\phi(0) \wedge \forall x(\forall z \leq x\, \phi(z) \rightarrow \phi(x')) \rightarrow \forall x \phi(x), \tag{1}$$

com vista a demonstrar $\forall x \phi(x)$. Por virtude de (IC_1), basta demonstrar $\forall x(\forall z < x\ \phi(z) \rightarrow \phi(x))$. Seja a arbitrário (não em ϕ) e suponhamos que

$$\forall z < a\, \phi(z), \tag{2}$$

com vista a demonstrar $\phi(a)$. Ora, $a \geq 0$ (T_{25}). Se $a = 0$, tem-se $\phi(0)$ por (1); se $a > 0$, digamos $a = b' > b$ (T_{22}). Por (1), $\forall z \leq b\, \phi(z) \rightarrow \phi(b')$, logo basta provar $\forall z \leq b\, \phi(z)$. Mas, pelo axioma ($AP_{10}$) tem-se $z \leq b \leftrightarrow z < b'$, portanto basta provar $\forall z < b' \phi(z)$, o que é imediato por (2), visto que $b' = a$.

4.18 (b) Prova de (i): supondo $d = bn - am$, se d não divide b, então d divide a, pois, caso contrário será $a = dq + r$ para certos q, r com $0 < r < d$, donde

$$r = a - dq = a - (bn - am)q = a(\overline{1} + mq) - bnq,$$

logo $\phi(r)$ com $r < d$, contrariando a minimalidade de d.

4.20 Indicações: se, por exemplo, $b = 0$, é $D(a, b) = a$. Supondo a, b ambos não nulos, sem perda de generalidade podemos supor $a \geq b$; se $b \mid a$, é $D(a, b) = b$; se b não divide a, digamos

(1) $$a = bq_1 + r_1,\ 0 < r_1 < b,$$

(pelo teorema da divisão inteira em $\mathbb{N}$), bastando provar que existe $D(b, r_1)$, porque então $D(a, b) = D(b, r_1)$. Repetindo o raciocínio com b e r_1, obtemos

(2) $$b = r_1 q_2 + r_2, \text{ com } 0 < r_2 < r_1,$$

sendo ainda $D(b, r_1) = D(r_1, r_2)$, se este último existir, e assim sucessivamente enquanto obtivermos restos não nulos...

(k) $$r_{k-2} = r_{k-1} q_k + r_k \text{ com } 0 < r_k < r_{k-1},$$

sendo $D(r_{k-2}, r_{k-1}) = D(r_{k-1}, r_k)$, se este último existir. Como os restos são estritamente decrescentes,

$$b > r_1 > r_2 > \cdots > r_{k-1} > r_k,$$

existirá um índice k tal que $r_{k+1} = 0$; caso contrário, haveria uma infinidade de naturais entre 0 e b, tendo-se então

$(k+1)$ $$r_{k-1} = r_k q_{k+1},$$

e portanto $D(r_{k-1}, r_k) = r_k$, donde também $D(a, b) = r_k$.

4.21 Supondo $a \geq b$, se $b \mid a$ é $D(a, b) = b = 1 \cdot b - 0 \cdot a$ da forma (ii); se b não divide a, pela fórmula (1) acima, é $r_1 = a - bq_1 = 1 \cdot a - q_1 \cdot b$ da forma (i), donde, por (2) acima, $r_2 = b - r_1 q_2 = b - (a - bq_1)q_2 = (1 + q_1 q_2)b - q_2 a$ é da forma (ii), etc.

Capítulo IV

5.1 1) (g) Use a contraposição intuicionista (d) [ver (16)] duas vezes.

(h) No sentido $\rightarrow$: use os paradoxos da implicação material; no sentido $\leftarrow$: use a contraposição intuicionista.

(i) Utilize (f) e (h).

(j) No sentido $\rightarrow$:

1	$\neg\neg(\phi \rightarrow \psi)$	H
2	$\neg\neg\phi$	[H]
3	$\neg(\phi \wedge \neg\psi)$	1, T^+ (d)
4	$\neg\psi$	[H]
5	ϕ	[H]
6	$\phi \wedge \neg\psi$	4, 5 ($\wedge^+$)
7	$\perp$	3, 6 ($\perp^+$)
8	$\neg\phi$	5-7 ($\neg^+$)
9	$\perp$	2, 8 ($\perp^+$)
10	$\neg\neg\psi$	4-9 ($\neg^+$)
11	$\neg\neg\phi \rightarrow \neg\neg\psi$	2-10 ($\rightarrow^+$).

No sentido $\leftarrow$:

1	$\neg\neg\phi \rightarrow \neg\neg\psi$	H
2	$\neg(\phi \rightarrow \psi)$	[H]
3	$\neg(\neg\phi \vee \psi)$	2, T^+ (42), (d)
4	$\neg\neg\phi \wedge \neg\psi$	3, T^+ (i), (d)
5	$\neg\neg\phi$	4 ($\wedge^-$)
6	$\neg\neg\psi$	1, 5 (MP)
7	$\neg\psi$	4 ($\wedge^-$)
8	$\perp$	6, 7 ($\perp^+$)
9	$\neg\neg(\phi \rightarrow \psi)$	2-8 ($\neg^+$)
10	$(\neg\neg\phi \rightarrow \neg\neg\psi) \rightarrow \neg(\phi \rightarrow \psi)$	1-9 ($\rightarrow^+$).

(k) No sentido $\rightarrow$: aplicar (g) a $\phi \wedge \psi \rightarrow \phi$ e a $\phi \wedge \psi \rightarrow \psi$ (no lugar de $\phi \rightarrow \psi$).
No sentido $\leftarrow$:

1	$\neg\neg\boldsymbol{\phi} \wedge \neg\neg\boldsymbol{\psi}$	H
2	$\neg(\boldsymbol{\phi} \wedge \boldsymbol{\psi})$	[H]
3	$\boldsymbol{\phi}$	[H]
4	$\boldsymbol{\psi}$	[H]
5	$\boldsymbol{\phi} \wedge \boldsymbol{\psi}$	3, 4 ($\wedge^+$)
6	$\bot$	2, 5 ($\bot^+$)
7	$\neg\boldsymbol{\phi}$	3-6 ($\neg^+$)
8	$\neg\neg\boldsymbol{\phi}$	1 ($\wedge^-$)
9	$\bot$	7, 8 ($\bot^+$)
10	$\neg\boldsymbol{\psi}$	4-9 ($\neg^+$)
11	$\neg\neg\boldsymbol{\psi}$	1 ($\wedge^-$)
12	$\bot$	10, 11 ($\bot^+$)
13	$\neg\neg(\boldsymbol{\phi} \wedge \boldsymbol{\psi})$	2-12 ($\neg^+$)
14	$(\neg\neg\boldsymbol{\phi} \wedge \neg\neg\boldsymbol{\psi}) \rightarrow \neg\neg(\boldsymbol{\phi} \wedge \boldsymbol{\psi})$	1-13 ($\rightarrow^+$).

5.6 Sugestão: supondo, com vista a um absurdo, que existia um tal conjunto A, ter-se-ia $\forall X\,(X \in A)$; defina o conjunto $B = \{X \in A : X \notin X\}$ (existe, por separação) e deduza um absurdo. Tenha em conta que se $\phi \leftrightarrow \psi \wedge \neg\phi$ é verdadeira e ψ é verdadeira, então $\phi \leftrightarrow \neg\phi$ é verdadeira. A situação pode lembrar o paradoxo de Russell (Nota 70), com uma diferença: na dedução desse paradoxo não se fizera nenhuma hipótese com vista a um absurdo.

BIBLIOGRAFIA

A. MONOGRAFIAS[196]

J. ALMEIDA, H. B. RIBEIRO, *Introdução à lógica*, Fac. Ciências Univ. Porto, 1990. [MA]

P. B. ANDREWS, *An Introduction to Mathematical Logic and Type Theory: to Truth Through Proof*, Academic Press, 1986. [IM]

♦J. BARWISE, J. ETCHMENDY, *The Language of First-Order Logic, Including the IBM-compatible Windows version of Tarski's World 4.0*, Third Edition Revised and Expanded, CSLI Lecture Notes, 1992 (existem versões para MacIntosh e NeXT). [I]

♦M. BEN-HARI, *Mathematical Logic for Computer Science,* second edition, Springer-Verlag London, 2001. [IM]

E. W. BETH, *The Foundations of Mathematics*, second revised edition, North-Holland, 1968. [IM, F, H]

I. van den BERG, A. J. F. OLIVEIRA, *Matemática Não-standard, Uma Introdução com Aplicações,* (2006, a publicar).

M. BERGMANN, J. MOOR, J. NELSON, *The Logic Book*, Random House, 1980, suplementado com *Solutions to selected exercices* e *Instructer*'s *Manual.* [I]

♦E. BISHOP, D. S. BRIDGES, *Constructive analysis*, Springer-Verlag, 1985. [MA]

G. S. BOOLOS, J. P. BURGESS, R. C. JEFFREY. *Computability and Logic.* Fouth edition, Cambridge U. P. 2003. [IM]

N. BOURBAKI, *Théorie des ensembles*, Hermann, 1960. [MA]

J. BRIDGE, *Beginning Model Theory*, Clarendon Press, 1977. [IM]

D. S. BRIDGES, *Computability, A Mathematical Sketchbook*, Springer-Verlag, 1994. [IM]

J. R. BROWN, *Philosophy of Mathematics, An Introduction to the World of Proofs and Pictures,* Routledge, 1999. [F]

---

[196] No final de cada referência assinalamos o respectivo nível com uma das letras "I" (Introdutório), "M" (Médio), "A" (Avançado), ou suas combinações. Obras de interesse sobretudo histórico, ou de história da lógica são assinaladas com a letra "H"; obras de especial interesse para a filosofia e os fundamentos são assinaladas com a letra "F"; e obras de interesse ou qualidade excepcional são assinaladas com um ♦ precedendo o nome do autor. A lista é apenas indicativa, e muito longe de exaustiva, mas engloba algumas das melhores obras actualmente em uso por esse mundo fora (onde se estuda lógica matemática). Indicam-se também algumas obras de interesse para a teoria elementar dos números.

R. CORI, D. LASCAR, *Mathematical Logic, A Course with Exercises,* 2 vols., (trad. do original em francês por D.H. Pelletier), Oxford U.P., 2000. [M]

N. C. A. da COSTA, *Introdução aos Fundamentos da Matemática*, Editora Hucitec, 1977. [I, F]; *Ensaio sobre os Fundamentos da Lógica*, Editora Hucitec, Univ. de S. Paulo, 1980. [IM, F]

N. C. A. da COSTA, R. CARRION, *Introdução à Lógica Elementar*, Ed. Univ. Rio Gr. Sul, 1988. [IM]

H. B. CURRY, *Foundations of mathematical logic*, Dover edition, 1977. [M, F]

D. van DALEN, *Logic and Structure*, Third Edition, Springer-Verlag, 1994. [M]

M. DAVIS, *Computability and unsolvability*, Dover edition, 1982. [MA]

♦R. DEDEKIND, *Essays on the Theory of Numbers (Continuity and Irrational Numbers; The Nature and Meaning of Numbers)*, Dover, 1963. [I, F, H]

T. DODD, *PROLOG, A Logical Approach,* Oxford U.P., 1989.

M. DUMMETT, *Elements of intuitionism*, Oxford UP, 1977. [M, F]

H. D. EBBINGHAUS, J. FLUM, W. THOMAS, *Mathematical Logic*, Second Edition, Springer-Verlag, 1994. [M]

H. M. EDGAR, *A First Course in Number Theory*, Wadsworth Publ. Co., 1988. [I]

H. EVES, *Foundations and fundamental concepts of mathematics*, third edition, FWS-KENT Publ. Co., 1990. [IM, F]

♦H. B. ENDERTON, *A Mathematical Introduction to Logic*, Academic Press, 1972, Second edition 2001. [M]

R. L. EPSTEIN, W.A. CARNIELLI, *Computability: Computable Functions, Logic, and the Foundations of Mathematics*, Second edition, Wadsworth & Brooks/Cole, 2000. [IM, F]

Yu. ERSHOV, E. PALIUTIN, *Lógica Matemática*, trad. espanhola por M. A. Andrianova, Ed. Mir, 1990. [MA]

G. FORBES, *Modern Logic, A Text in Elementary Symbolic Logic*, Oxford Univ. Press, 1994. [I]

♦A. A. FRAENKEL, Y. BAR-HILLEL, A. LEVY, D. van DALEN, *Foundations of set theory*, second revised edition, North-Holland, 1973. [MA, F]

J. H. GALLIER, *Logic for Computer Science, Foundations of Automatic Theorem Proving*, John Wiley & Sons, 1987. [MA]

R. GOLDSTEIN, *Incompleteness, The Proof and Paradox of Kurt Gödel,* W. W. Norton, 2005. [I, H]

J.-B. GRIZE, *Lógica Moderna*, Fasc. I, II, III, Liv. Civilização, 1984, 1985. [I]

H. HAMBURGER, D. RICHARDS, *Logic and Language Models for Computer Science,* Prentice Hall, 2002. [I]

A. G. HAMILTON, *Logic for Mathematicians*, Cambridge Univ. Press, 1978. [IM]; *Numbers, Sets and Axioms, The Apparatus of Mathematics*, Cambridge Univ. Press, 1982. [I]

♦W. S. HATCHER, *The Logical Foundations of Mathematics*, Pergamon Press, 1982. [IM, F]

♦S. HEDMAN, *A First Course in Logic,* Oxford Texts in Logic 1, Oxford, 2005. [IM]

H. HERMES , *Introduction to Mathematical Logic*, Springer-Verlag, 1973. [IM]

A. HEYTING, *Intuitionism*, North-Holland, 1956. [M]

D. HILBERT, *Fundamentos da Geometria,* com *Apêndices I-X* do Autor e *Suplementos* de P. Bernays, F. Enriques e H. Poincaré, segunda edição portuguesa traduzida por Maria Pilar Ribeiro (colab. de J. da Silva Paulo), Paulino Lima Fortes e A. J. Franco de Oliveira (colab. de A. Vaz Ferreira), Revisão científica e coordenação por A. J. Franco de Oliveira, Gradiva, 2003.

D. HILBERT, W. ACKERMANN, *Grundzüge der theoretischen Logik.* Springer-Verlag, 1928; trad. inglesa da 2.ª edição alemã (1938), *Principles of Mathematical Logic,* Chelsea, 1950; trad. castelhana da 4.ª edição alemã (1958), *Elementos de lógica teórica.* Tecnos, 1962.

HILBERT, D., BERNAYS, P. *Grundlagen der Mathematik.* 2 vols., Springer-Verlag, 1934-39; trad. franc. da 2.ª edição alemã (1968), *Fondements des Mathématiques*. 2. vols., L'Harmattan, 2001.

♦R. E. HODEL, *An Introduction to Mathematical Logic*, PWS Publ. Comp., 1995. [IM, F].

W. HODGES, *Logic*, Penguin Books, 1977. [I]

♦D. R. HOFSTADTER, *Gödel, Escher, Bach: An Eternal Golden Braid*, Penguin Books, 1979; trad. port. da edição do XX aniversário (1999) coordenada por A. J. F. Oliveira, *Gödel, Escher, Bach: Laços Eternos,* Gradiva, 2000. [F]

P. T. JOHNSTONE, *Notes on Logic and Set Theory*, Cambridge Univ. Press, 1987. [IM]

R. KAYE, *Models of Peano Arithmetic*, Clarendon Press, 1991.[MA]

♦S. C. KLEENE, *Introduction to Metamathematics,* Van Nostrand, 1952 (North-Holland, 1971). [A, F]; *Mathematical Logic*, J. Wiley, 1967. [M, F]

♦W. KNEALE, M. KNEALE, *O Desenvolvimento da Lógica*, Fundação Calouste Gulbenkian, 1972. [IM, H]

G. T. KNEEBONE, *Mathematical Logic and the Foundations of Mathematics*, Van Nostrand, 1963. [IM, F]

S. KÖRNER, *The Philosophy of Mathematics*, Harper & Row, 1962. [F]

G. KREISEL, J.-L. KRIVINE, *Elements of Mathematical Logic*, North-Holland, 1971. [MA, F]

G. C. LEARY, *A Friendly Introduction to Mathematical Logic,* Prentice Hall, 2000. [IM]

E. J. LEMMON, *Beginning Logic*, Nelson, 1965. [I]

W. J. LeVEQUE, *Elementary Theory of Numbers*, Addison-Wesley, 1962. [I]

J. LUKASIEWICZ, *La Syllogistique d'Aristote*, A. Colin, 1972. [H]

M. MACHOVER, *Set Theory, Logic and their limitations*, Cambridge U.P., 1996. [IM]

B. MATES, *Elementary Logic*, second edition., Oxford Univ. Press, 1972. [IM]

♦E. MENDELSON, *Introduction to Mathematical Logic*, third edition, Wadsworth & Brooks, 1987; fourth edition, Chapman & Hall, 1997. [MA, F]

♦A. A. MONTEIRO, J. S. PAULO, *Aritmética Racional*, Livraria Avelar Machado, 1945. [I]

E. NAGEL, J. R. NEWMAN, *Gödel's Proof,* Revised edition, edited and with a new foreword by D. R. Hofstadter, New York U. P., 2002. [I]

♦A. NERODE, R. A. SHORE, *Logic for Applications*, Springer-Verlag, 1993. [IM]

W. H. NEWTON-SMITH, *Logic*, *An Introductory Course*, Routledge & Kegan Paul, 1985. [I]

A. J. F. OLIVEIRA, *Lógica Elementar*, AEFCL, 1980. [I]; *Teoria dos conjuntos, Intuitiva e axiomática (ZFC)*, Escolar Editora, 1982. [IM]; *Lógica e Fundamentos I. Linguagens, Estruturas e teorias elementares*, Textos e Notas do CMAF **31**, 1985. [IM]; *Lógica e Fundamentos II. Computabilidade, Incompletude e Indecidibilidade*, Textos e Notas do CMAF **33**, 1986. [IM, F]; *Infinitesimais: passado, presente e futuro*, Dep. Mat. Univ. Évora, 1987. [IM]; *O Advento da Matemática Não-Standard*, Monografias da Soc. Paranaense de Matemática, nº. **8**, Abril de 1990. [IM]

J.-F. PABION, *Logique Mathématique*, Hermann, 1976. [IM]

♦R. PENROSE, *The emperor's new mind*, Oxford UP, 1989; trad. port. *A mente virtual,* Gradiva, 1997. [MA]

♦W. V. QUINE, *Methods of Logic*, fourth edition, Harvard Univ. Press, 1982. [IM]

A. ROBINSON, *Nonstandard Analysis*, Princeton Landmarks in Mathematics, 1996 (re-edição da segunda edição de 1974 publicada pela North-Holland). [MA]

R. ROGERS, *Mathematical Logic and Formalized Theories*, North-Holland, 1971. [I]

J. E. RUBIN, *Mathematical Logic: Applications and Theory*, Saunders College Publ., 1990. [I]

B. RUSSELL, *Introduction to Mathematical Philosophy*, George Allen & Unwin, 1919; Dover, 1993. [I, H, F]

S. S. SHAPIRO, *Foundations without Foundationalism, A Case for Second-order Logic*, Clarendon Press, 1991; ♦*Thinking about Mathematics,* Oxford U.P., 2000. [M, F]

W. P. van STIGT, *Brouwer*'s *Intuitionism*, North-Holland, 1991. [H,F]

R. R. STOLL, *Set Theory and Logic*, Dover, 1979. [IM]

♦J. R. SHOENFIELD, *Mathematical Logic*, Addison-Wesley, 1967, second printing 1973, reprinted Assoc Symb. Logic 2001. [A, F]

R. SMULLYAN, *What is the name of this book?*, Prentice Hall, 1978. [I]; *To mock a mockingbird*, Knopf, 1985.[I]

P. SUPPES, *Introduction to Logic*, Princeton Univ. Press, 1957. [I]

♦A. TARSKI, *Introduction to Logic and to the Methodology of Deductive Sciences*, Fourth Edition edited by Jan Tarski, Oxford Univ. Press, 1994. [*Introduction à la Logique* (tradução ampliada do original inglês de 1941), Gauthiers-Villars, 1971.] [I]

A. TROELSTRA, D. van DALEN, *Constructivism in Mathematics, An Introduction,* vol. I, North-Holland, 1988. [MA]

R. L. WILDER, *Introduction to the Foundations of Mathematics*, second edition, 1965. [IM, F]

B. COLECTÂNEAS[197]

E. AGAZZI, *Modern Logic—A Survey*, D. Reidel, 1981. [IM]

W. ASPRAY, P. KITCHER, *History and Philosophy of Modern Mathematics*, Univ. Minnesota Press, 1988. [IM, F]

♦J. BARWISE, *Handbook of Mathematical Logic*, North-Holland, 1977. [MA]

♦P. BENACERRAF, H. PUTNAM, *Philosophy of Mathematics*, second edition, Cambridge Univ. Press, 1983. [M, F]

J. BRANQUINHO, D. MURCHO, *Enciclopédia de Termos Lógico-Filosóficos,* Gradiva, 2001.

F. E. BROWDER, *Mathematical problems arising from Hilbert*'s *problems*, 2 vols, Amer. Math. Soc., 1976. [MA, F]

N. CUTLAND, V. NEVES, F. OLIVEIRA e J. SOUSA PINTO, *Developments in nonstandard mathematics*, Pitman Research Notes in Mathematics Series N. 336, Longman, 1995. (Actas do Colóquio Internacional de Matemática Não-standard à memória de A. Robinson, Univ. de Aveiro, Julho de 1994) [MA]

M. DAVIS, *The Undecidable,* Raven Press, 1965; reimp. Dover, 2005. [MA]

---

[197] Indica(m)-se o(s) nome(s) do(s) editor(es) ou organizador(es), excepto nos casos de obras de um único autor.

M. DIENER, F. DIENER, *Nonstandard Analysis in Practice*, Springer-Verlag, 1995. [MA]

T. DRUCKER, *Perspectives on the History of Mathematical Logic*, Birkhäuser, 1991. [H, F]

♦W. B. EWALD, *From Kant to Hilbert, A Source Book in the Foundations of Mathematics,* 2 vols., Oxford Science Publ., 1996.[F, H]

D. GABBAY, F. GUENTHER, *Handbook of philosophical logic*, 3 vols., Reidel, 1983. [M, F]

♦K. GÖDEL, *Collected works* (edited by S. Feferman), vol. I, II, III, Oxford U. P., 1986, 1990, 1995. [A, F]

♦J. van HEIJENOORT, *From Frege to Gödel, A Source Book in Mathematical Logic, 1879-1931*, Harvard Univ. Press, 1967. [H, F]

V. F. HENDRICKS, S. A. PEDERSEN, K. F. JØRGENSEN (editors), *Proof Theory, History and Philosophical Significance,* Kluwer Acad. Publ., 2000. [H, F]

R. I. G. HUGHES, *A Philosophical Companion to First-Order Logic*, Hackett Publ. Comp., 1993. [F, H]

I. LAKATOS, *Problems in the philosophy of mathematics*, North-Holland, 1967. [IM, F]

M. LOURENÇO, *O Teorema de Gödel e a Hipótese do Contínuo*, Fundação Calouste Gulbenkian, 1979. [H, F]

P. MANCOSU, *From Brouwer to Hilbert, The debate on the Foundations of Mathematics in the 1920's,* Oxford U. P., 1998. [F, H]

♦A. TARSKI, *Logic, Semantics, Metamathematics*, second edition (Edited and Introduced by J. CORCORAN), Hackett, third printing, 1997. [MA, F]

T. TYMOCZKO, *New Directions in the Philosophy of Mathemtics,* Revised and expanded edition, Princeton U. P., 1998.

J. SIEKMANN, G. WRIGHTSON, *Automation of Reasoning, 1957-1970,* 2 vols., Springer-Verlag, 1983. [MA, H]

H. WANG, *Logic, computers and sets*, Chelsea, 1970. [IM, F]; *From mathematics to philosophy*, Humanities, 1973. [IM, F].

Alfabeto gótico

𝔄𝔞 𝔅𝔟 ℭ𝔠 𝔇𝔡 𝔈𝔢 𝔉𝔣 𝔊𝔤 ℌ𝔥 ℑ𝔦 𝔍𝔧 𝔎𝔨 𝔏𝔩 𝔐𝔪

𝔑𝔫 𝔒𝔬 𝔓𝔭 𝔔𝔮 ℜ𝔯 𝔖𝔰 𝔗𝔱 𝔘𝔲 𝔙𝔳 𝔚𝔴 𝔛𝔵 𝔜𝔶 ℨ𝔷

Alfabeto grego

$$A\alpha\ B\beta\ \Gamma\gamma\ \Delta\delta\ E\epsilon(\varepsilon)\ Z\zeta\ H\eta\ \Theta\theta(\vartheta)\ I\iota\ K\kappa\ \Lambda\lambda\ M\mu\ N\nu$$
$$\Xi\xi\ Oo\ \Pi\pi(\varpi)\ P\rho(\varrho)\ \Sigma\sigma(\varsigma)\ T\tau\ \Upsilon\upsilon\ \Phi\phi(\varphi)\ X\chi\ \Psi\psi\ \Omega\omega$$

A α	alfa	H η	eta	N ν	niú	T τ	tau
B β	beta	Θ θ	teta	Ξ ξ	csi	Υ υ	úpsilon
Γ γ	gama	I ι	iota	O o	omicron	Φ ϕ, φ	fi
Δ δ	delta	K κ	cá, capa	Π π	pi	X χ	qui
E ϵ, ε	epsilon	$\Lambda\lambda$	lambda	P ρ	ró	Ψ ψ	psi
Z ζ	zeta	M μ	miú	Σ σ	sigma	Ω ω	ómega

BREVE NOTA BIOGRÁFICA DO AUTOR

O autor é licenciado em Ciências Matemáticas pela Faculdade de Ciências da Universidade de Lisboa, e é doutorado em Matemática pela Universidade de Lisboa na especialidade de Álgebra, Lógica e Fundamentos. Lecciona actualmente no Departamento de Matemática da Universidade de Évora. Especializou-se em lógica matemática, em Inglaterra, e a sua tese de doutoramento versa sobre os fundamentos da matemática não-standard e suas aplicações à lógica, mas os seus interesses cobrem igualmente a História e Filosofia da Matemática e a Geometria. Tem diversos livros publicados, como *Teoria dos conjuntos, intuitiva e axiomática (ZFC); Lógica e fundamentos (2 vols.); Infinitesimais: passado, presente e futuro; Geometria; O Advento da matemática não-standard; Geometria Euclidiana; Transformações Geométricas; Cartas de Edmundo Curvelo a Joaquim de Carvalho.* Coordenou as edições portuguesas de *A Mente Virtual,* de Roger Penrose, de *Gödel, Escher, Bach: Laços Eternos,* de Douglas Hofstadter, de *e*: *História de um número*, de Eli Maor, publicados pela Gradiva, e colabora regularmente em revistas e outras actividades de divulgação matemática, nomeadamente, em Encontros da SPM e da APM, Colóquios e Conferências de Matemática em escolas secundárias.

Prefácio à Edição Brasileira

É muito gostoso ver este livrinho editado no Brasil e assim contribuir modestamente para estreitar os laços culturais entre os dois povos de língua portuguesa. Para melhor corresponder ao interesse manifestado pela Editora da Universidade de Brasília, fizémos algumas correções à segunda edição portuguesa (pequenas mas irritantes gralhas introduzidas pela recomposição de partes do texto, principalmente algumas tabelas e deduções). Para mais não houve disponibilidade, mas se o livrinho for bem acolhido certamente que haverá outra oportunidade para melhoramentos mais profundos.

Cotovia, 30 de Junho de 1998

Vejamos alguns exemplos de equivalências lógicas notáveis, e respectivas designações. Para quaisquer fórmulas ϕ, ψ e θ, tem-se:

$\phi \wedge \phi \sim \phi$	$\phi \vee \phi \sim \phi$	*idempotência*
$\phi \wedge \psi \sim \psi \wedge \phi$	$\phi \vee \psi \sim \psi \vee \phi$	*comutatividade*
$(\phi \wedge \psi) \wedge \theta \sim \phi \wedge (\psi \wedge \theta)$	$(\phi \vee \psi) \vee \theta \sim \phi \vee (\psi \vee \theta)$	*associatividade*
$(\phi \wedge \psi) \vee \phi \sim \phi$	$(\phi \vee \psi) \wedge \phi \sim \phi$	*absorção*
$(\phi \wedge \psi) \vee \theta \sim (\phi \wedge \theta) \vee (\psi \wedge \theta)$	$(\phi \vee \psi) \wedge \theta \sim (\phi \vee \theta) \wedge (\psi \vee \theta)$	*distributividade*
$\neg(\phi \wedge \psi) \sim \neg\phi \vee \neg\psi$	$\neg(\phi \vee \psi) \sim \neg\phi \wedge \neg\psi$	*DeMorgan*
$\neg\neg\phi \sim \phi$		*dupla negação*

Além disso:

$\phi \wedge \psi \sim \psi$	$\phi \vee \psi \sim \phi$	se ϕ é válida
$\phi \wedge \psi \sim \phi$	$\phi \vee \psi \sim \psi$	se ϕ é incompatível.