Jair Donadelli

NHI2049-13 Lógica Básica

Uma introdução à lógica clássica de primeira ordem

– Notas de aula –

23 de junho de 2021

CMCC–UFABC

Prefácio

Estas são minhas anotações para a disciplina NHI2049-13 – Lógica básica, oferecida em 2018 e 2019. Essa disciplina é uma introdução à lógica clássica de primeira ordem e aborda: cálculo proposicional (ou sentencial) clássico: noções de linguagem, conectivos, dedução e teorema, semântica de valorações. Cálculo de predicados de primeira ordem clássico: os conceitos de linguagem de primeira ordem, igualdade, teorema da dedução, consequência sintática. Semântica: noções de interpretação, verdade em uma estrutura, modelo.

Esta é uma disciplina de natureza introdutória e que não exige qualquer conhecimento prévio no estudo de lógica, no entanto, requer alguma experiência mínima em alguns temas de matemática como, por exemplo, as noções de função e de conjunto, algumas operações sobre conjuntos além de alguma maturidade matemática. Nela, o estudante tem a possibilidade de experimentar o senso de rigor conceitual e de abstração formal.

O conteúdo expõe alguns aspectos da interrelação entre temas de lógica, matemática e computabilidade.

Santo André, 1º quadrimestre de 2021 *Jair Donadelli*

Sumário

Prelúdio

"A lógica é difícil, e qualquer passo no sentido de tornar o ensino mais parecido com as alegrias ilusórias do fácil é uma mentira que prejudica sobretudo os estudantes com mais dificuldades de aprendizagem, porque o fácil e vazio já eles têm. O professor tem a obrigação profissional de retirar do seu ensino todas as dificuldades pedagógicas desnecessárias, mas só essas. Retirar as outras é como imaginar que se ensina violino mais proficientemente começando por deitar fora as cordas."
Desidério Murcho

O que é lógica?

- *substantivo feminino*
  1. *fil* parte da filosofia que trata das formas do pensamento em geral (dedução, indução, hipótese, inferência etc.) e das operações intelectuais que visam à determinação do que é verdadeiro ou não.
  2. *p.met.* tratado, compêndio de lógica.
  3. p.ext. (*da acp. 1*) maneira rigorosa de raciocinar. *Ex.:* "lógica implacável"
  4. *p.ext.* forma por que costuma raciocinar uma pessoa ou um grupo de pessoas ligadas por um fato de ordem social, psíquica, geográfica etc. *Ex.:* "a lógica do louco"
  5. *p.ext.* maneira por que necessariamente se encadeiam os acontecimentos, as coisas ou os elementos de natureza efetiva. *Ex.:* "a lógica das paixões"
  6. *p.ext.* encadeamento coerente de alguma coisa que obedece a certas convenções ou regras. *Ex.:* "a lógica do discurso musical"
  7. *inf* organização e planejamento das instruções, assertivas etc. em um algoritmo, a fim de viabilizar a implantação de um programa.
- Análise dos métodos de raciocínio. (Folclore)
- Ciência que estuda as leis do raciocínio e as condições de verdade em vários domínios do conhecimento. (Enciclopédia Barsa)
- É a ciência que estuda princípios e métodos de inferência com o objetivo de determinar em que condições certas coisas são consequência (ou não) de outra. (Mortari, C. Introdução à lógica, Ed. da Unesp, 2001.)

De modo geral, entende-se a disciplina chamada *Lógica* como aquela que se ocupa do estudo sistemático das *formas de argumento* válidos, a ideia de que a validade de um argumento é determinada pela sua forma lógica e não pelo seu conteúdo. Um argumento válido é aquele em que existe uma relação específica de suporte lógico entre os pressupostos do argumento e sua conclusão. No entanto, atualmente, a Lógica compreende temas que vão além desse estudo sistemático como, por exemplo, a Teoria dos Modelos, Teoria da Prova, Teoria dos Conjuntos, Teoria da Recursão e da Computabilidade e a Teoria de Tipos.

Um breve histórico

Aristóteles

A lógica como conhecemos hoje tem origem na Grécia antiga com a Teoria do Silogismo de Aristóteles (384–322 a.C.), a qual aparece no livro III, intitulado *Analytica Priora*, da sua obra *Organon*, que é um conjunto de tratados sobre como conduzir uma reflexão. O título do livro significa "instrumento de trabalho" e constitui uma contraposição ao estoicismo para a qual a lógica faz parte da filosofia. O trabalho de Aristóteles foi um dos primeiros sistemas dedutivos já propostos, é um fragmento da lógica de primeira ordem que apresentaremos aqui. Os historiadores da lógica a consideram a mais importante descoberta em toda a história da lógica formal.

Aristóteles foi o primeiro a notar que certos raciocínios são válido em virtude unicamente da sua forma e foi o primeiro a escrever de forma sistemática sobre lógica como ferramenta para disciplinar a argumentação. Assim criou uma ciência inteiramente nova, capaz de estudar e classificar as formas de raciocínio válidos. Além disso, foi ele quem introduziu artifícios como o uso de letras mudas para denotar os termos, bem como termos fundamentais tais como "válido", "não válido", "contraditório", "universal" e "particular".

No silogismo aristotélico

Premissa	*Todo homem é mortal*
Premissa	*Sócrates é homem*
Conclusão	*Sócrates é mortal*

o que interessa é a *forma*

Premissa	*Todo A é B*
Premissa	*C é A*
Conclusão	*C é B*

A verdade das asserções não tem importância para a legitimidade do argumento.

Aristóteles caracteriza a lógica como uma ciência do raciocínio, posteriormente entendida como estabelecedora das formas válidas de raciocínio, a qual repousava sobre três princípios fundamentais: (1) princípio da identidade: todo objeto é idêntico a si mesmo; (2) Princípio da não contradição: uma proposição não pode ser verdadeira e falsa ao mesmo tempo; e (3) Princípio do terceiro excluído: toda proposição é verdadeira ou falsa, não havendo outra possibilidade.

Estóicos

Mais avanços foram feitos pelo filósofo estóico grego Crisipo de Solis, que desenvolveu o básico do que chamamos lógica proposicional. Zenão de Cítio (333–263 a.C.) e Crisipo de Solis (280–208 a.C.) trataram de princípios do cálculo proposicional, incluindo aí um sistema dedutivo. Estudaram a implicação "*se A então B*" e regras de inferência

	Regra 1	Regra 2	Regra 3	Regra 4	Regra 5
Premissa	A	não A	A	A	A
Premissa	$A \to B$	$A \to B$	não A e B	ou A ou B	ou A ou B
Conclusão	B	não A	não B	não B	não B

Durante muitos séculos o estudo da lógica concentrou-se principalmente em diferentes interpretações das obras de Aristóteles e em muito menor grau de Crisipo, cujo trabalho foi esquecido. No entanto, todas as formas de argumento foram descritas em linguagem natural e carecem de maquinaria formal que criasse um cálculo lógico de dedução com o qual seria fácil trabalhar.

Leibniz

Leibniz (1646-1716) foi precursor da metodologia da lógica contemporânea, foi um dos primeiros a perceber a necessidade de formalizar formas de argumento lógico.

Buscava a construção de uma *linguagem simbólica universal*, baseada em um alfabeto do pensamento e a construção de um *cálculo da razão* que reduziria todas as disputas filosóficas a uma questão de mero cálculo, reformulando o raciocínio em tais disputas nesta linguagem.

A maioria das contribuições de Leibniz para a lógica permaneceram não publicadas durante sua vida, tendo ficado desconhecidas até o princípio do século XX. Historicamente, apenas generalidades do programa de Leibniz teriam influenciado os lógicos que o sucederam.

Lógica contemporânea

Na sua forma contemporânea a lógica é vista como um sistema formal dedutivo edificado sobre uma linguagem formal a qual teria a incumbência de eliminar dubiedades interpretativas. Os primeiros passos reais nesta direção foram levados em meados do século XIX pelo matemático inglês George Boole (1815–1864), que desenvolveu um sistema algébrico (a Álgebra Booleana) para discutir a lógica. O trabalho de Boole inaugurou uma revolução na lógica, que avançou ainda mais pelas mãos dos matemáticos e filósofos: Augustus De Morgan (1806–1871), Charles Peirce (1839–1914), Giuseppe Peano (1858–1932), Bertrand Russel

(1872–1970), Alfred Whitehead (1861–1947), David Hilbert (1862–1943), Kurt Gödel (1906–1978).

Século 19

A grande figura do inicio da lógica contemporânea foi Gottlob Frege (1848–1925) que desenvolveu o *Cálculo de Predicados*, uma linguagem simbólica para o *estudo das deduções lógicas* como tentativa de fundamentar a Matemática. Giuseppe Peano (1889), que desconhecia o trabalho de Frege na época, publicou um conjunto de axiomas para a aritmética usando uma variação do sistema lógico de Boole, mas adicionando quantificadores. Em meados do século 19 as falhas nos axiomas de Euclides para a geometria tornaram-se conhecidas. David Hilbert (1899) desenvolveu um conjunto completo de axiomas para a geometria. O sucesso na axiomatização da geometria motivou Hilbert a buscar axiomatizações completas de outras áreas da matemática. Em 1874, Cantor desenvolveu os conceitos fundamentais da Teoria dos Conjuntos infinitos e um dos seus primeiros resultados foi a formalização da noção de *cardinalidade*, com ele provou que os reais e os números naturais têm cardinais diferentes. Em 1897 Cantor publica seus principais trabalhos sobre números ordinais e números cardinais, resultado de três décadas de pesquisa. Para Cantor, um conjunto era, intuitivamente, uma seleção de elementos de um todo satisfazendo uma dada propriedade. Essa aceitação ingênua de qualquer coleção como um conjunto propiciou o aparecimento de paradoxos. Cesare Burali–Forti (1897) foi o primeiro a apresentar um paradoxo: o paradoxo de Burali–Forti mostra que a coleção de todos os números ordinais não pode formar um conjunto. Pouco tempo depois, Bertrand Russell descobriu o paradoxo de Russell em 1901, e Jules Richard (1905) apresentou o paradoxo de Richard.

A teoria dos conjuntos criada por Georg Cantor exibia muitos paradoxos e havia o temor de que a matemática como um todo não estava assentada em um terreno seguro. Esse momento ficou conhecido como “a crise dos fundamentos da matemática” e a saída mais famosa para essa crise foi formulada por David Hilbert. O “programa de Hilbert”, como ficou conhecido, influenciou muitos trabalhos realizados na primeira metade do século 20, inclusive de Kurt Gödel, um dos pensadores mais profundos desse século, e de Alan Turing, o pai da computação.

O programa de Hilbert:

formulado pelo matemático alemão David Hilbert no início do século 20, o programa foi uma proposta para resolver a crise nos fundamentos da matemática, quando se descobriu que as primeiras tentativas de esclarecer os fundamentos da matemática sofriam de paradoxos e inconsistências. Como solução, Hilbert propôs fundamentar todas as teorias existentes em um conjunto finito e completo de axiomas e fornecer uma prova de que esses axiomas eram consistentes. Hilbert propôs que a consistência de sistemas mais complicados, como análises reais, pudesse ser comprovada em termos de sistemas mais simples. Por fim, a consistência de toda a matemática pode ser reduzida à aritmética básica.

A linguagem e a axiomatização da lógica de primeira ordem seguem alguns princípios estabelecidos no programa de Hilbert:

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

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

Século 20

A descoberta de paradoxos na teoria ingênua de conjuntos fez com que alguns pesquisadores se perguntassem se a própria matemática seria inconsistente e procuram provas de consistência. Em 1900, Hilbert colocou uma famosa lista de vinte e três problemas para o próximo século e o trabalho subsequente para resolver esses problemas moldou a direção da lógica matemática. Ernest Zermelo (1908) forneceu o primeiro conjunto de axiomas para a teoria dos conjuntos. Esses axiomas, juntamente com o axioma adicional de substituição proposto por Abraham Fraenkel, são agora denominados axiomas da teoria de Zermelo–Fraenkel (ZF). Em 1910, o primeiro volume de *Principia Mathematica* de Russell e Alfred North Whitehead foi publicado. Este trabalho seminal desenvolveu a teoria das funções e cardinalidade em uma estrutura completamente formal da teoria do tipo, que Russell e Whitehead desenvolveram em um esforço para evitar os paradoxos. *Principia Mathematica* é considerada uma das obras mais influentes do século 20. Em sua tese de doutorado, Kurt Gödel (1929) provou o teorema da completude, que estabelece uma correspondência entre sintaxe e semântica na lógica de primeira ordem. Seus resultados ajudaram a estabelecer a lógica de primeira ordem como a lógica dominante usada pelos matemáticos. Em 1931, Gödel publicou os *teoremas de incompletude de Gödel*, estabelecendo severas limitações em fundações axiomáticas para a matemática, dando um forte golpe ao programa de Hilbert. O teorema de Gödel mostra que uma prova de consistência de um sistema axiomático suficientemente forte e eficaz não pode ser obtida no próprio sistema, se o sistema for consistente, nem em qualquer sistema mais fraco.

Os teoremas da incompletude de Gödel, publicados em 1931, mostraram que o programa de Hilbert era inatingível para áreas-chave da matemática. Em seu primeiro teorema, Gödel mostrou que qualquer sistema consistente com um conjunto computável de axiomas capaz de expressar aritmética nunca pode ser completo: é possível construir uma afirmação que se mostre verdadeira, mas que não pode ser derivada do regras formais do sistema. Em seu segundo teorema, ele mostrou que tal sistema não podia provar sua própria consistência; portanto, certamente não pode ser usado para provar a consistência de algo mais forte com certeza. Isso refutou a suposição de Hilbert de que um sistema finitístico poderia ser usado para provar a consistência de si mesmo e, portanto, qualquer outra coisa.

A década de 1930 testemunhou a chegada de uma nova geração de lógicos ingleses e americanos, incluindo Alonzo Church, Alan Turing, Stephen Kleene, Haskell Curry e Emil Post, que contribuíram grandemente para a definição do conceito de algoritmo e o desenvolvimento da teoria da computabilidade e da teoria da complexidade de algoritmos. No período pós-guerra a lógica matemática também sofre uma revolução devido ao surgimento da informática. Em parte o computador eletrônico foi inspirado pelo modelo de computação descrito por Alan Turing. Na lógica tivemos, por exemplo, a descoberta da correspondência de Curry–Howard, que liga as provas formais à programação de computadores desencadeando um extenso programa de pesquisa.

Os lógicos contemporâneos

1. constroem linguagens simbólicas, rigorosas e livres de ambiguidades e de contexto, adequadas para lidar com a relação de consequência. As linguagens possuem duas componentes relevantes:
   a) a *sintática*: os símbolos da linguagem (chamado *alfabeto*) e as *regras gramaticais* de combinação de símbolos, às quais estes estão sujeitos, para a construção das fórmulas da linguagem;
   b) a *semântica*: define precisamente o significado das fórmulas.
2. constroem um *cálculo*, ou sistema dedutivo, especificando os axiomas dentre as fórmulas e as regras de inferência que independem da semântica (é um aparato sintático).

E assim temos um sistema lógico, ou uma lógica.

A principal característica das fórmulas e deduções (sequências de fórmulas obtidas dos axiomas e regras de inferência) é que eles são objetos finitos. Além disso, cada um dos conjuntos de fórmulas e deduções é recursivo, ou seja, existe um algoritmo que determina se um determinada cadeia de símbolos é uma fórmula correta ou uma dedução correta do sistema.

Sistemas Lógicos

Ao aparato sintático descrito acima dado pelo alfabeto com uma gramática, um conjunto de axiomas e as regras de inferência chamamos de *sistema formal*. Um sistema lógico consiste de um sistema formal munido de uma semântica, em geral dada por uma interpretação da teoria dos modelos, a qual atribui um valor-verdade (por exemplo, *verdadeiro* ou *falso*) para as sentenças da linguagem formal.

As propriedades fundamentais dos sistemas de dedução são:

Correção: afirma que os teoremas são válidos em todos os modelos, significa que os axiomas e as regras de inferência formalizam corretamente o raciocínio nesses modelos.

Consistência: o sistema de dedução admite um modelo ou, o que equivale ao mesmo, se não for possível deduzir toda e qualquer fórmula.

Completude: qualquer proposição válida em todos os modelos é um teorema. Em suma, um sistema está completo se tudo o que for verdadeiro é deduzível.

Exemplos de sistemas lógicos

Lógica proposicional é mais elementar lógica simbólica. A sintaxe é dada a partir de proposições atômicas, parênteses e conectivos lógicos. A Semântica tem como base os princípios do *terceiro excluído* — uma sentença é verdadeira ou falsa — e da *não-contradição* — nenhuma sentença é verdadeira e falsa. É simples e sem força expressiva para formalizar a matemática mas tem muita aplicações (e.g., circuitos digitais).

Lógica de predicados de primeira ordem tem sintaxe da lógica proposicional acrescida de quantificadores e as variáveis, além de símbolos específicos que dependem do assunto que a linguagem aborda. Mais complexa mas ganha muito em expressividade.

Lógica de predicados de segunda ordem possui quantificadores sobre classes de indivíduos, e não apenas sobre indivíduos. Porém, alguns teoremas importantes que valem na lógica de primeira ordem não valem na lógica de segunda ordem. Ademais, a Teoria dos Conjuntos consegue contornar essa limitação da lógica de primeira ordem na formalização da matemática.

Teoria dos tipos de Bertrand Russell, extrapola a ideia da lógica de segunda ordem; quantificamos quantificamos os indivíduos, as classes de indivíduos, as classes de classes de indivíduos, e assim por diante Para fazer isso, classificamos as variáveis por tipos (variáveis de primeiro tipo, variáveis de segundo tipo, e assim por diante).

Lógica modal estende a lógica proposicional acrescendo os operadores "necessariamente" (uma sentença é *necessária* se e somente se ela é não possivelmente falsa) e "possivelmente" (uma proposição é *possível* se e somente se ela é não necessariamente falsa, independente de ser realmente verdadeira ou falsa). Usa a semântica dos mundos possíveis e o valor lógico de uma sentença depende de qual dos "mundos possíveis" ela está sendo analisada.

Lógica descritiva pode ser considerada como um fragmento da lógica de primeira ordem com uma sintaxe mais simples e sem uso de variáveis, tornou-se uma ferramenta útil em ciência da computação.

Lógica paraconsistente permite contradições, nega o princípio da não-contradição tornando possível que uma sentença e sua negação sejam simultaneamente aceitas como verdadeiras. Newton da Costa é um dos precursores. Diversas aplicações em inteligência artificial.

Lógica intuicionista nega o princípio do terceiro excluído, permitindo que uma fórmula e sua negação sejam ambas falsas. É a lógica dos matemáticos construcionistas, nela a dupla negação não se anula e não há provas por absurdo.

Lógica *fuzzy* permite valorar uma fórmula com qualquer valor real no intervalo $[0,1]$ de números reais, possibilitando "verdades parciais", se aproxima de alguns problemas reais, que necessitam lidar com incertezas. Pode ser interpretada do ponto de vista estatístico, onde a valoração das fórmulas representam a probabilidade de um evento ocorrer.

Linguagem

Nesta disciplina abordaremos a lógica proposicional e a lógica de predicados clássicas usando uma abordagem tradicional, identificando uma lógica (de fato, um sistema lógico) a uma linguagem. Para especificar uma lógica introduzimos os seus símbolos primitivos, são dadas regras gramaticais que definem as fórmulas (cadeias finitas de símbolos primitivos),são dadas as regras de inferência que permitem escrever novas fórmulas a partir de fórmulas dadas.

Por que precisamos criar uma linguagem para formalizar as formas de raciocínio?

Para evitar os paradoxos e imprecisões decorrentes do uso da linguagem natural. Isso é importante quando estudamos assuntos mais restritos, com menos complexidade expressiva, porém com maior exigência de rigor.

***54·43.** $\vdash :. \alpha, \beta \in 1 . \supset : \alpha \cap \beta = \Lambda . \equiv . \alpha \cup \beta \in 2$

Dem.

$$\begin{array}{lll}
\vdash . {*}54{\cdot}26 . \supset \vdash : . \alpha = \iota\text{‘}y . \supset : \alpha \cup \beta \in 2 . & \equiv . x \neq y . & \\
[{*}51{\cdot}231] & \equiv . \iota\text{‘}x \cap \iota\text{‘}y = \Lambda . & \\
[{*}13{\cdot}12] & \equiv . \alpha \cap \beta = \Lambda & (1) \\
\vdash . (1) . {*}11{\cdot}11{\cdot}35 . \supset & & \\
\vdash : . (\exists x, y) . \alpha = \iota\text{‘}x . \beta = \iota\text{‘}y . \supset : \alpha \cup \beta \in 2 . & \equiv . \alpha \cap \beta = \Lambda & (2) \\
\vdash . (2) . {*}11{\cdot}54 . {*}51{\cdot}1 . \supset \vdash . \mathit{Prop} & &
\end{array}$$

From this proposition it will follow, when arithmetical addition has been defined, that $1 + 1 = 2$.

Evidentemente, uma linguagem artificial com tais propósitos tem poder expressivo inferior à linguagem natural. Acrescentar expressividade às linguagens lógicas, aproximando-as da linguagem natural, sem que se perca o rigor aumenta-lhes em muito a complexidade.

O objetivo de analisar argumentos impõe implicitamente a utilização de uma linguagem artificial que tenha certas estruturas lógicas.

Paradoxos

Usualmente, um paradoxo é uma declaração que vai contra a intuição comum, as expectativas. Um paradoxo lógico é uma declaração que leva a uma contradição como, por exemplo, o conhecido *paradoxo do mentiroso*

Essa afirmação é falsa.

Se tal afirmação é falsa então concluímos que ela é verdadeira, por outro lado, se tal afirmação é verdadeira então concluímos que ela é falsa. O paradoxo lógico resulta de que a frase contém uma autorreferência.

A autorreferência foi usada por Bertrand Russell na teoria dos conjuntos para concluir que temos que ser muito mais cuidadosos no modo como definimos um conjunto. Também foi usada por Kurt Gödel para provar, em 1931, que qualquer sistema lógico capaz de expressar verdades básicas da aritmética ou é contraditória (existem afirmações falsas que podem ser demonstradas) ou é incompleta (existem afirmações verdadeiras que não podem ser demonstradas). Gödel mostrou que é possível escrever uma expressão aritmética que significa "Eu não posso ser demonstrada".

Paradoxos de Zenão (490–430a.c.)

Zenão de Eleia foi um filósofo pré-socrático conhecidos por desenvolver a argumentação por absurdo. Zenão escreveu vários paradoxos utilizando este recurso lógico. No pensamento dos eleatas, o movimento, tal como as mudanças e as transformações físicas, nada mais eram do que ilusões provocadas pelos nossos sentidos. Para propor que o movimento não existe, Zenão concebeu os seguintes argumentos:

1. O corredor Aquiles nunca alcança a tartaruga, quando postos a correr simultaneamente, com a tartaruga à frente. Pois, cada vez que Aquiles alcança a posição onde a tartaruga estava anteriormente, essa última, por sua vez, já avança um pouco, de modo que nunca será possível alcançá-la.
2. Não há movimento porque o que é movido tem que chegar ao meio antes de chegar ao fim e assim por diante, eternamente.

Paradoxo de Richard

o paradoxo de Richard foi publicado em 1905 no artigo intitulado *Les Principes des mathématiques et le problème des ensembles*. Foi referenciado por Whitehead e Russel no *Principia Mathematica* e por Gödel e Turing em suas famosas obras. Kurt Gödel considerou seu teorema da incompletude como um análogo (sintático) ao paradoxo (semântico) de Richard.

Em sua versão original, diz:

> "Consideremos todas as expressões em português que definem um número real. Por exemplo "a razão entre a circunferência e o seu diâmetro" define o número π. Essas expressões são enumeráveis e podem ser consideradas ordenadas lexicograficamente $e_1, e_2, \dots, e_n, \dots$. A essa enumeração corresponde uma sequência de números reais $r_1, r_2, \dots, r_n, \dots$. Agora definimos o número real r por
>
> > a parte inteira de r é 0, a n-ésima casa decimal de r é 1 se a n-ésima casa decimal de r_n não é 1 e a n-ésima casa decimal de r é 2 se a n-ésima casa decimal de r_n é 1.

> Mas tal expressão da língua portuguesa define um número real r que deve ser um dos números r_n, no entanto, r foi construído de modo a ser diferente de todo r_n."

Existem várias formulações diferentes chamadas de paradoxo de Richard na literatura, algumas apenas vagamente parecidas com a original. Talvez a mais simples seja

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

Porém tal frase define um natural com usando quatorze palavras.

A seguinte variação aparece no livro *Gödel's Proof* de Ernest Nagel e James R. Newman.

> "Considere um idioma, como Português, em que as propriedades aritméticas de números inteiros estão definidos. Por exemplo, "o primeiro número natural" define a propriedade de ser o primeiro número natural; e "não ser divisível por nenhum outro número natural a não ser um ou ele mesmo" define a propriedade de ser um número primo. Embora a lista de todas as definições possíveis seja infinita, cada definição é composta por um número finito de palavras. Uma vez que isso é verdade, podemos ordenar as definições, primeiro por tamanho de palavra e, em seguida, lexicograficamente. Agora, que podemos enumerar cada definição de tal modo que a definição com o menor número de caracteres e por ordem alfabética corresponderá ao número 1, a seguinte definição irá correspondem ao 2, e assim por diante. Uma vez que cada definição está associada com um número inteiro é possível que, ocasionalmente, o número inteiro associado a uma definição satisfaça a esta definição. Por exemplo, se a 43ª definição é "não divisível por qualquer inteiro diferente de 1 e de si mesmo", então temos que 43 satisfaz essa definição. Um número n é dito *Richardiano* se n-ésima definição é uma propriedade que o próprio número n não tem.
> Agora, uma vez que a propriedade de ser Richardiano é em si uma propriedade de números inteiros, a ela é atribuído um número inteiro, r. Finalmente, o paradoxo torna-se evidente: r é Richardiano? Suponhamos que r é Richardiano. Isto só é possível se r não tem a propriedade designada pela r-ésima expressão, isto é, se r não é Richardiano, contrariando a nossa hipótese. No entanto, se supusermos que r não é Richardiano, então ele tem a propriedade designada pela r-ésima expressão, isto é, ele é Richardiano, mais uma contrariando a hipótese."

Paradoxo de Russel

o Paradoxo de Russell é um paradoxo descoberto por Bertrand Russell em 1901 quando tomou conhecimento do trabalho desenvolvido por Frege em *Grundgesetze der Arithmetik* (Fundamentos da Aritmética, nesta obra, Frege tentava reduzir a aritmética à lógica). O paradoxo foi comunicado por uma carta enviada a Frege:

> Seja w o predicado: para ser predicado, não pode ser predicado de si próprio. Pode w ser predicado de si próprio?

Em linguagem de conjuntos

> Seja C o conjunto de todos os conjuntos que não pertencem a si mesmos. C pertence a si mesmo?

$C \in C$ se, e somente se, $C \not\in C$.

Uma versão popular do paradoxo de Russel é o paradoxo do Barbeiro.

> Havia, no vilarejo, um barbeiro que só fazia a barba de todas as pessoas que não faziam a própria barba. Quem faz a barba do barbeiro?

Se fizer a própria barba, não pode fazer a própria barba. Mas se não fizer a própria barba, então tem de fazer a própria barba.

Paradoxo de Burali-Forti

Cesare Burali-Forti publicou em 1897 um artigo em que apontou um paradoxo na teoria de conjuntos de Cantor. Na época, Cantor considerava qualquer coleção que poderia ser manipulada como conjunto. Burali-Forti considerou então a coleção de todos os números ordinais, que, sendo bem ordenada, deveria também ser um número ordinal. Mas, então existiriam ordinais maiores que ele na coleção e, portanto, a coleção inteira seria menor que si mesma!

Metalinguagem

É através da linguagem que exprimimos o que pensamos. Uma lógica é uma linguagem utilizada para descrever deduções com rigor. Em lógica, a metalinguagem é a linguagem usada para descrever algo sobre a própria lógica, pois a lógica em si, como parte da matemática e como qualquer outra parte da matemática, tem resultados e teoremas que dizem a respeito dela. Por exemplo, uma sentença sobre os números naturais, escrito e provado dentro de um sistema lógico, é um teorema da linguagem. O teorema de Gödel, que diz que em certos tipos de sistemas lógicos sempre existe uma sentença que não pode ser provada nem verdadeira nem falsa, é um resultado que fala diretamente da lógica, e por isso é um metateorema.

Mas se a linguagem da matemática é a própria lógica, qual linguagem utilizaremos quando construímos a lógica? A princípio, utilizamos a linguagem natural, mas de forma controlada, para que, após definida a linguagem lógica, possamos transferir o que foi feito para a linguagem lógica.

Quando *mencionamos* um símbolo da linguagem usamos aspas simples para diferenciá-lo do seu *uso*

’Santo André’ é um substantivo próprio

agora, se falamos da cidade, então não usamos aspas

Santo André é vizinha de São Bernardo do Campo.

Se quisermos dizer que a sentença acima é verdadeira, escrevemos

'Santo André é vizinha de São Bernardo do Campo' é uma sentença verdadeira.

A expressão 'quadrado' é o nome da palavra *quadrado* a qual dá nome a forma geométrica. Assim, em quadrado tem quatro lados a palavra 'quadrado' está sendo usada para falar da forma geométrica. Em 'quadrado' tem seis letras não estamos falando mais da forma geométrica, mas da palavra que é o nome dessa forma.

Definição indutiva de conjuntos

Nas definições gramaticais das linguagens dos sistemas lógicos e comum recorrermos às definições indutivas.

Usualmente, e informalmente, conjuntos são definidos de duas maneiras, ou listando seus elementos, ou através de uma propriedade aplicada a elementos de um outro conjunto.

Um conjunto pode também ser definido indutivamente. Supõe-se dado um conjunto E, uma parte não vazio P de E e um conjunto F de operações sobre elementos de E que resulta em elemento de E. O conjunto $D \subseteq E$ é **indutivo** se

1. $P \subseteq D$;
2. D é fechado para as operaçõesde F;
3. nenhum objeto está em D a não ser que possa ser obtido a partir dos elementos de P por um número finito de aplicações de operações de F.

Por exemplo, o conjunto dos números inteiros positivos pares $P = \{2\}$ e F só tem a operação $n \mapsto n+2$.

O conjunto dos inteiros positivos ainda pode ser definido indutivamente tomando E o conjunto dos números primos acrescentado do 1 e F com a única operação $(m,n) \mapsto m \cdot n$.

Uma diferença entre essa duas definições do mesmo conjunto, e que geralmente importa quando se trata de linguagens, é exemplificada a seguir. No primeiro caso, o número 12 é obtido de modo único, a saber, a partir do 1 aplica-se o "soma 1" onze vezes. Já na segunda definição há pelo menos dois modos distintos: $(3,2) \to (6,2)$ e $(2,2) \to (4,3)$.

Se cada elemento de D é gerado a partir dos elementos de P e operações de F de modo único, então dizemos tem **legibilidade única**.

Propriedades de conjuntos definidos indutivamente são, em geral, demonstradas por indução. Por exemplo, seja D o conjunto definido por $P = \{1\}$ e F só tem a operação $n \mapsto n+2$. Podemos reescvever essa definição como: (i) $1 \in D$; (ii) se $n \in D$ então $n+2 \in D$, para qualquer natural n. Lembrando que nenhum objeto está em D a não ser que possa ser obtido a partir de uma das duas regras acima.

Notemos que essa última condição é necessária pois, por exemplo, as outras duas condições são verdadeiras para o conjunto $\mathbb{N}$ de todos os número naturais: é verdade que $1 \in \mathbb{N}$ e é verdade que se $a \in \mathbb{N}$ então $a+2 \in \mathbb{N}$.

Uma aplicação ortodoxa do Princípio da Indução Finita mostra que $2k+1 \in D$ para todo k número natural, logo o conjunto do números ímpares está contido em D. Do exercício 2 abaixo temos que D está contido no conjunto dos número ímpares. Logo *D é o conjunto dos números ímpares.*

Exercícios

1. Aqui, o uso de aspas simples (' ') é uma convenção para distinguir quando de menciona a expressão de quando se fala dela. Identifique abaixo o uso correto ou não dessa convenção
   a) O numeral '3' expressa o resultado da operação 2+1.
   b) '2' é o numeral que dá nome ao número 2.
   c) 2+2 é igual a 3+1 mas '2+2' não é igual a '3+1'.
   d) A expressão 'rosa' permite falar sobre a rosa.
   e) 'Dois' não é o nome de 1+1, mas o nome de 2.
   f) 'Sócrates' é o nome de um filósofo grego.
   g) Sócrates é o nome de um ex-jogador do Corinthians.
   h) O nome da rosa é 'rosa' e tem quatro letras na língua portuguesa.
   i) 'The house is blue' é diferente de 'Das Haus ist blau' e ambas são diferentes de 'La masion est bleu'.
   j) A rosa é vermelha. A expressão 'rosa' permite afirmar sobre a rosa.
   k) A sentença 'A sentença 'A neve é branca' é verdadeira' é uma expressão da metalinguagem.
   l) Haus é a palavra casa na língua alemã e house é a palavra casa na língua inglesa. As duas palavras são diferentes. Na língua francesa, tem-se a palavra maison.
2. Recordemos que um conjunto D é **indutivo** se para certos conjuntos dados E, P e F, temos as regras
   a) $P \subseteq D$;
   b) D é fechado para as operaçõesde F;
   c) nenhum objeto está em D a não ser que possa ser obtido a partir dos elementos de P por um número finito de aplicações de operações de F.

   Prove que D é o menor conjunto que satisfaz as regras (a) e (b), isto é D é dado pela intersecção de todos os subconjuntos de E que satisfazem as regras (a) e (b).

Parte I

Lógica proposicional

Discussão informal

Por ora, queremos uma linguagem simbólica que capture formas de argumentação humana expressa de forma declarativa. Por **argumento válido** entendemos uma sequência de declarações

$$\phi_1,\ \phi_2, \dots, \phi_n, \gamma$$

com $n \geqslant 1$, de modo que sempre que as n declarações iniciais $\phi_1,\ \phi_2, \dots, \phi_n$, chamadas **premissas**, são verdadeiras, a **conclusão** γ é verdadeira. Para tais argumentos adotamos a notação

$$\begin{array}{c} \phi_1 \\ \phi_2 \\ \vdots \\ \phi_n \\ \hline \gamma \end{array}$$

de modo que a ordem das premissas é irrelevante.

Essa descrição de argumento envolve os conceitos *sintático* de 'declaração' e *semântico* de 'verdadeiro' e 'falso'.

As declarações são **proposições** ou **sentenças**, do ponto de vista linguístico, isto é, são frases declarativas de um juízo com verbo no indicativo. Às proposições podemos atribuir um dentre dois dos **valores-verdade**: VERDADEIRO ou FALSO. Em lógica, não é importante saber determinar o valor-verdade de uma proposição, apenas que é possível fazê-lo.

Uma proposição é dita *atômica* se a ela corresponde, individualmente, um desses valores-verdade. Por exemplo, são proposições atômicas da língua portuguesa

1. O time joga bem.
2. O time ganhou o campeonato.
3. O técnico é o culpado.
4. Os torcedores estão felizes.
5. Samuel virá para a festa.
6. Maximiliano vai se divertir.
7. O suborno será pago.
8. As mercadorias são entregues.

Diferente do caso "se as mercadorias são entregues, então o suborno será pago" que admite um valor verdade, mas esse depende dos valores individuais das sentenças 7 e 8.

Do ponto de vista da linguagem natural, na qual sentenças interrogativas ou imperativas são importantes, a restrição para a linguagem formal expressar apenas sentenças declarativas é bastante forte. Observamos que não há a pretensão de traduzir uma linguagem natural para uma linguagem formal (e vice-versa), faremos uso da possibilidade de tradução sob certas limitações pois estamos mais interessado nos enunciados matemáticos como

9. O quadrado de todo número é positivo.
10. 27 é um quadrado perfeito.
11. O conjunto vazio é único.
12. 34 é a soma de quatro quadrados perfeitos.
13. O *quicksort* ordena uma lista de números em tempo quadrático.
14. Se uma sequência numérica é limitada, então ela é convergente.

em que sentenças interrogativas ou imperativas não são importantes. Além disso, queremos regras que permitam construir consistentemente proposições mais complexas a partir de outras

15. Os torcedores estão felizes **e** o técnico foi demitido.
16. Samuel virá para a festa **e** Maximiliano não virá, **ou** Samuel não virá para a festa **e** Maximiliano vai se divertir.
17. **Se** o time joga bem, **então** o time ganha o campeonato.
18. **Se** o time não joga bem, **então** o técnico é o culpado.
19. **Se** o time ganha o campeonato **então** os torcedores estão felizes.
20. O suborno será pago **se, e somente se**, as mercadorias são entregues.
21. **Se** x é um real positivo, **então** x^2 é um real positivo.
22. 27 **não** é um quadrado perfeito.
23. O conjunto vazio **não** é único.
24. Os torcedores **não** estão felizes.

Se denotamos pelas letras α e β proposições da língua portuguesa

não α: expressa a negação da sentença α cujo valor é VERDADEIRO quando, e somente quando, o valor-verdade de α é FALSO;

α e β: expressa a conjunção das sentenças α e β, cujo valor é VERDADEIRO quando, e somente quando, ambas α e β têm valor-verdade VERDADEIRO;

α ou β: expressa a disjunção inclusiva, cujo valor é FALSO quando, e somente quando, ambas α e β têm valor-verdade FALSO;

se α, então β: expressa uma forma condicional, cujo valor é FALSO quando, e somente quando, α é VERDADEIRO e β é FALSO;

α se, e somente se β: representa a bicondicional α se β **e** β se α, é VERDADEIRA quando, e somente quando, α e β têm o mesmo valor-verdade.

Reforçando o que já foi dito acima, o importante não é o valor-verdade que uma proposição possa tomar num determinado contexto interpretativo, mas a possibilidade de que, em princípio, seja possível atribuir sem ambiguidade um valor-verdade. Por exemplo, a sentença $x \cdot y = y \cdot x$ é verdadeira para quaisquer x e y quando se trata de números inteiros e é falsa para quaisquer x e y quando se trata de matrizes. A sentença, “as salas de aula do terceiro andar tem paredes brancas” é verdadeira na UFABC mas pode ser falsa em outro contexto. Isso se faz mais relevante nos argumentos, por exemplo,

$$\frac{\textit{Todo homem é mortal} \qquad \textit{Sócrates é homem}}{\textit{Sócrates é mortal}}$$

é um argumento válido. Se trocarmos 'mortal' por 'ave' o argumento continuaria válido, embora uma das premissas e a conclusão sejam falsas no contexto em que vivemos. Assim como é válido

$$\frac{\begin{array}{c}\textit{Todo carro é Ferrari}\\ \textit{Fusca é carro}\end{array}}{\textit{Fusca é Ferrari}}$$

A corretude dos argumentos não depende de uma particular interpretação das suas proposições, só depende de como se relacionam as interpretações das premissas com a conclusão, em qualquer contexto interpretativo.

1

Linguagem e dedução para a lógica proposicional

1.1 A linguagem formal

O **alfabeto** $\mathscr{A}_0$ é o conjunto dos símbolos que compõem linguagem

$$\mathscr{A}_0 = \{\, p_i \colon i \in \mathbb{N} \} \cup \{ \neg, \vee, \wedge, \rightarrow, \leftrightarrow \} \cup \{ (,) \}$$

classificados em

símbolos proposicionais atômicos:	$p_1\ p_2\ p_3\ \ldots$
conectivos lógicos:	$\neg\ \vee\ \wedge\ \rightarrow\ \leftrightarrow$
símbolos de pontuação:	$(\ )$

Lemos os símbolos $\neg$, $\vee$, $\wedge$, $\rightarrow$ e $\leftrightarrow$ como *negação*, *disjunção*, *conjunção*, *implicação* e *bi-implicação*, respectivamente.

Ressaltamos que esses símbolos são apenas símbolos da linguagem, os conectivos lógicos, por exemplo, não devem ser confundidos com os operadores lógicos que são *interpretações* de tais símbolos. A interpretação faz parte da semântica da linguagem, que será discutida mais adiante.

1.1.1 Fórmulas

As expressões que podemos formar são as cadeias (ou sequências) finitas de símbolos tomados do alfabeto $\mathscr{A}_0$ como, por exemplo, $((p_1 \vee p_7) \wedge p_{100})$, $())p_5$ e $\neg(\neg p_2)\neg$. Claramente, os dois últimos exemplos são expressões que não interessam.

Na metalinguagem que usamos para descrever a lógica proposicional usamos letras gregas

$$\alpha,\ \beta,\ \gamma,\ \delta,\ \epsilon,\ \zeta,\ \eta,\ \theta,\ \iota,\ \kappa,\ \lambda,\ \mu,\ \nu,\ \pi,\ \rho,\ \sigma,\ \tau,\ \upsilon,\ \phi,\ \chi,\ \psi,\ \omega$$

para denotar expressões, são ditas *metavariáveis*, ou *variáveis sintáticas*.

Uma **fórmula bem formada** (FBF) ou simplesmente **fórmula** é qualquer expressão que pode ser formada aplicando-se um número *finito* de vezes as três primeiras regras de:

(F1) os símbolos atômicos são FBF, chamadas **fórmulas atômicas**;
(F2) se α é FBF, então $(\neg\alpha)$ é FBF;
(F3) se α e β são FBFs, então $(\alpha \vee \beta)$ é FBF, $(\alpha \wedge \beta)$ é FBF, $(\alpha \to \beta)$ é FBF e $(\alpha \leftrightarrow \beta)$ é FBF;
(F4) não há outras FBFs além das obtidas pelo uso das regras (F1), (F2) e (F3).

O conjunto $\mathscr{L}_0$ de todas as fórmulas bem formadas é a linguagem da lógica proposicional e é um conjunto definido indutivamente, portanto, pelo exercício 2, página 13, é caracterizado como o *o menor conjunto $\mathscr{L}$ formado pelas cadeias de símbolos da alfabeto que satisfazem as propriedades*:

1. $p_1, p_2, \ldots \in \mathscr{L}$,
2. se $\alpha \in \mathscr{L}$ então $(\neg\alpha) \in \mathscr{L}$,
3. se $\alpha, \beta \in \mathscr{L}$ então $(\alpha \vee \beta), (\alpha \wedge \beta), (\alpha \to \beta), (\alpha \leftrightarrow \beta) \in \mathscr{L}$.

Exemplo 1.1. São exemplos de fórmulas bem formadas:

- p_1, $(\neg p_2)$, $(p_3 \to (p_1 \wedge (\neg p_1)))$;
- Se α, β, γ denotam FBF então $(\alpha \wedge (\beta \wedge \gamma))$ denota uma FBF que é diferente da FBF denotada por $((\alpha \wedge \beta) \wedge \gamma)$.

É importante entender que $(p_1 \to p_2)$, por exemplo, é uma fórmula da linguagem enquanto que $(\alpha \to \beta)$ não é uma fórmula da linguagem, mas uma expressão metalinguística que usamos para nos referir a uma fórmula ou, ainda, a um tipo de FBF, aquelas que são escritas quando trocamos as letras gregas por fórmulas da linguagem como, por exemplo, $(p_1 \to p_1)$, $(p_1 \to p_2)$, $((p_1 \to p_2) \to (p_1 \to p_3))$, $((p_1 \wedge p_2) \to (p_1 \vee p_2))$, etc. Nesse caso, dizemos que $(\alpha \to \beta)$ é um **esquema** de fórmula. Atentemos para o fato de que as letras repetidas num esquema de fórmula representam a mesma cadeia de símbolos da linguagem, então no esquema $(\alpha \to \alpha)$ encaixamos $(p_1 \to p_1)$ e $((p_1 \vee (p_2 \wedge p_3)) \to (p_1 \vee (p_2 \wedge p_3)))$, mas não $(p_1 \to p_2)$.

1.1.2 Indução

As fórmulas são objetos finitos gerados indutivamente e, portanto, podemos demonstrar propriedades das fórmulas usando indução estrutural, isto é, um princípio de indução que trabalha diretamente na estrutura dos objetos gerados. Nesse caso, suponha que uma propriedade de fórmulas (i) vale para toda fórmula atômica, (ii) se vale para uma fórmula, então também vale para sua negação e (iii) se vale para duas fórmulas, então também vale para a fórmula obtida “conectando” as duas. Então essa propriedade vale para toda fórmula.

Vamos formalizar esse princípio no metateorema abaixo onde identificamos um propriedade de fórmulas com um subconjunto $\mathscr{P} \subset \mathscr{L}_0$ composto pelas FBF que têm a propriedade dada.

Metateorema 1.2 (Indução para fórmulas). *Seja $\mathscr{P} \subset \mathscr{L}_0$ uma propriedade de fórmulas de $\mathscr{L}_0$ tal que*

(1) toda fórmula atômica pertence a $\mathscr{P}$*,*
(2) se $\alpha \in \mathscr{P}$*, então* $(\neg\alpha) \in \mathscr{P}$ *e*
(3) se $\alpha \in \mathscr{P}$ *e* $\beta \in \mathscr{P}$*, então* $(\alpha \wedge \beta)$, $(\alpha \vee \beta)$, $(\alpha \rightarrow \beta)$ *e* $(\alpha \leftrightarrow \beta)$ *pertencem a* $\mathscr{P}$*.*

Então $\mathscr{P} = \mathscr{L}_0$*, ou seja, essa propriedade vale para toda fórmula.*

Demonstração. De (1), (2) e (3) do enunciado e da definição de $\mathscr{L}_0$ temos que $\mathscr{L}_0 \subset \mathscr{P}$. Porém $\mathscr{L}_0 \supset \mathscr{P}$, portanto, $\mathscr{P} = \mathscr{L}_0$. ■

Exemplo 1.3. Vamos demonstrar usando a indução que *toda fbf tem uma quantidade par de parênteses.* Cada fórmula atômica tem 0 parênteses. Para todo α que tem um número par, digamos $2n$, de parênteses, $(\neg\alpha)$ tem $2n+2 = 2(n+1)$ parênteses, portanto par. Suponha que α e β tenham, respectivamente, $2n$ e $2m$ parênteses, então $(\alpha \wedge \beta)$ tem $2n+2m+2 = 2(n+m+1)$ parênteses (os casos $(\alpha \vee \beta)$, $(\alpha \rightarrow \beta)$ e $(\alpha \leftrightarrow \beta)$ são idênticos). Usando a indução para fórmulas, concluímos que toda FBF tem um quantidade par de parênteses.

O exemplo a seguir ilustra uma **definição recursiva** para fórmulas baseada no princípio indutivo. Pela indução para fórmulas, se definimos uma função para as fórmulas atômicas e se tal função fica definida para $(\neg\alpha)$, $(\alpha \wedge \beta)$, $(\alpha \vee \beta)$, $(\alpha \rightarrow \beta)$ e $(\alpha \leftrightarrow \beta)$ sempre que está definida para α e para β, então a função fica definida em $\mathscr{L}_0$.

Exemplo 1.4 (Grau de complexidade). As vezes é conveniente medir a complexidade de uma FBF pelo seu *grau* dado pela função $\mathrm{grau}\colon \mathscr{L}_0 \rightarrow \mathbb{N}$ dada por

1. $\mathrm{grau}(\alpha) = 0$ se α é fórmula atômica;
2. $\mathrm{grau}(\neg\alpha) = \mathrm{grau}(\alpha)+1$; e
3. $\mathrm{grau}(\alpha \wedge \beta) = \max\{\mathrm{grau}(\alpha), \mathrm{grau}(\beta)\}+1$;
4. $\mathrm{grau}(\alpha \vee \beta) = \max\{\mathrm{grau}(\alpha), \mathrm{grau}(\beta)\}+1$;
5. $\mathrm{grau}(\alpha \rightarrow \beta) = \max\{\mathrm{grau}(\alpha), \mathrm{grau}(\beta)\}+1$;
6. $\mathrm{grau}(\alpha \leftrightarrow \beta) = \max\{\mathrm{grau}(\alpha), \mathrm{grau}(\beta)\}+1$.

Pelo metateorema 1.2 o grau de complexidade está definido para toda fórmula de $\mathscr{L}_0$.

1.1.3 Leitura única

O leitor atento pode perguntar se as definições dos símbolos e a regra de formação das fórmulas garantem que a as fórmulas de $\mathscr{L}_0$ não são ambíguas no sentido de que uma dada fórmula não pode ser lida de mais de uma maneira de acordo com as regras estabelecidas. De fato, pode se demonstrar (mas *não* faremos aqui) que uma fórmula de $\mathscr{L}_0$ deve satisfazer exatamente uma dentre as condições (F1), (F2) e (F3) que regem a formação de fórmulas.

A demonstração do seguinte resultado é um exercício, ele decorre da seguinte propriedade de fórmulas bem formadas: em toda FBF há um e apenas um conectivo lógico que satisfaz a condição “à esquerda dele, o número de abre-parênteses é exatamente um a mais que o número de fecha-parênteses”.

Metateorema 1.5 (Teorema da unicidade da representação). *Para toda* FBF α, *uma, e apenas uma, das afirmações abaixo é verdadeira:*

- α *é uma fórmula atômica;*
- *existe uma única* FBF β *tal que* α *é a fórmula* $(\neg\beta)$*;*
- *existem únicas* FBF*s* β *e* γ *tais que* α *é a fórmula* $(\beta \wedge \gamma)$*;*
- *existem únicas* FBF*s* β *e* γ *tais que* α *é a fórmula* $(\beta \vee \gamma)$*;*
- *existem únicas* FBF*s* β *e* γ *tais que* α *é a fórmula* $(\beta \rightarrow \gamma)$*;*
- *existem únicas* FBF*s* β *e* γ *tais que* α *é a fórmula* $(\beta \leftrightarrow \gamma)$.

A demonstração dessa afirmação é o resultado dos exercícios 11 a 14 abaixo, na página 29. Uma propriedade importante dessas fórmulas foi enunciada acima:

> Em toda fórmula α há apenas um conectivo lógico $\square \in \{\neg, \wedge, \vee, \rightarrow, \leftrightarrow\}$ que satisfaz a condição *à esquerda dele, o número de abre-parênteses é exatamente um a mais que o número de fecha-parênteses.* (§)

A partir daí podemos descrever a formação de uma fórmula α através de uma árvore binária: começando por α (nó **raiz**), em cada nó temos uma fórmula β da forma $(\gamma\square\delta)$ em que γ e δ são fórmulas e γ pode ser, eventualmente, uma "fórmula vazia" (no caso do conectivo $\neg$). As fórmulas γ e δ são os nós filhos de β. Esse processo termina quando γ e/ou δ são símbolos atômicos (nós **folha**). Essa árvore é chamada de **árvore de formação** da fórmula.

Exemplo 1.6. A primeira etapa da leitura da fórmula $((p_1 \wedge p_2) \wedge ((\neg p_3) \vee (p_4 \vee p_5)))$ usando (§) nos dá a conjunção de $(p_1 \wedge p_2)$ com $((\neg p_3) \vee (p_4 \vee p_5))$

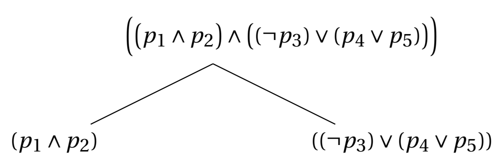

Figura 1.1. Primeira etapa da leitura de $((p_1 \wedge p_2) \wedge ((\neg p_3) \vee (p_4 \vee p_5)))$.

A disjunção do lado esquerdo é lida, usando (§), como

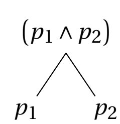

Figura 1.2. Leitura de $p_1 \wedge p_2$.

Agora chegamos na conjunção $(\neg p_3) \vee (p_4 \vee p_5)$ que, por (§), é lida como a disjunção de $\neg p_3$ com $p_4 \vee p_5$. A leitura de $p_4 \vee p_5$ é análoga à conjunção da figura 1.2. A fórmula $\neg p_3$ é, simplesmente, a negação de p. Assim temos

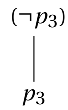

Figura 1.3. A leitura da fórmula $\neg p_3$.

A descrição completa da formação da fórmula $((p_1 \wedge p_2) \wedge ((\neg p_3) \vee (p_4 \vee p_5)))$ é representada pelo diagrama da figura 1.4, a árvore de formação da fórmula.

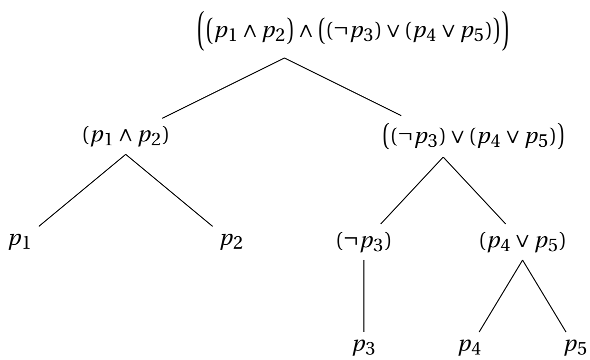

Figura 1.4. A árvore de formação da fórmula $((p_1 \wedge p_2) \wedge ((\neg p_3) \vee (p_4 \vee p_5)))$.

Todas as fórmulas presentes na árvore de formação da fórmula α são as subfórmulas de α. Esse é um conceito definido recursivamente a seguir.

Subfórmulas

As fórmulas intermediárias que aparecem no processo de construção de uma fórmula através das regras (F1)–(F3) são chamadas de **subfórmulas próprias**. Tais subfórmulas próprias juntamente com a fórmula em si definem o conjunto das subfórmulas da fórmula dada.

Exemplo 1.7. p_1, p_2, $(\neg p_1)$ e $(p_2 \wedge (\neg p_1))$ são subfórmulas próprias de $(p_1 \vee (p_2 \wedge (\neg p_1)))$.

Formalmente, a definição do conjunto das subfórmulas de uma fórmula é recursiva. As subfórmulas de α definem o conjunto

1. $\mathrm{Sf}(\alpha) = \{\alpha\}$ para toda FBF atômica p;
2. $\mathrm{Sf}(\neg\alpha) = \mathrm{Sf}(\alpha) \cup \{(\neg\alpha)\}$;
3. $\mathrm{Sf}(\alpha \wedge \beta) = \mathrm{Sf}(\alpha) \cup \mathrm{Sf}(\beta) \cup \{(\alpha \wedge \beta)\}$;
4. $\mathrm{Sf}(\alpha \vee \beta) = \mathrm{Sf}(\alpha) \cup \mathrm{Sf}(\beta) \cup \{(\alpha \vee \beta)\}$.

5. $\mathrm{Sf}(\alpha \to \beta) = \mathrm{Sf}(\alpha) \cup \mathrm{Sf}(\beta) \cup \{(\alpha \to \beta)\}$.
6. $\mathrm{Sf}(\alpha \leftrightarrow \beta) = \mathrm{Sf}(\alpha) \cup \mathrm{Sf}(\beta) \cup \{(\alpha \leftrightarrow \beta)\}$.

As subfórmulas próprias de α são os elementos de $\mathrm{Sf}(\alpha) \setminus \{\alpha\}$.

1.2 Simplificações

Vamos assumir algumas convenções de notação para facilitar nossa escrita e o estudo da lógica de proposições. Todas estas simplificações são convenções metalinguísticas, são regras informais e nos momentos que exigem resultados mais rigorosos nós não devemos considerar essas simplificações.

1.2.1 Abreviaturas

Representamos os símbolos atômicos por algumas das letras do final do alfabeto da Língua Portuguesa, por exemplo p, q, r, s, t, u, v. Quando precisamos de muitos símbolos atômicos usamos os símbolos formais $p_1, p_2, \dots$. Fórmulas bem formadas são denotadas por letras gregas minúsculas $\alpha, \beta, \gamma, \delta, \dots$ e conjuntos de fórmulas por letras gregas maiúsculas $\Gamma, \Delta, \Lambda, \Upsilon, \dots$.

Representamos os conectivos $\vee$, $\wedge$, $\to$ e $\leftrightarrow$ genericamente pelo símbolo $\square$, no caso de múltiplas ocorrências de conectivos nós usaremos índices $\square_1$, $\square_2$ e assim por diante. Com isso $\alpha \square \beta$ indica uma fórmula composta por α, β e algum dos conectivos e qual deles, especificamente, não importa no momento em que se usa o símbolo $\square$. Tomamos o cuidado de que duas ocorrências numa mesma frase significa o mesmo conectivo (indexado ou não). Por exemplo na sentença

'$\alpha \square \eta$ deve ser lido como $(\alpha \square \eta)$'

devemos entender como, por exemplo,

$\alpha \to \eta$ deve ser lido como $(\alpha \to \eta)$

e não entender algo como, por exemplo,

$\alpha \to \eta$ deve ser lido como $(\alpha \wedge \eta)$

Em

'$(\alpha \square_1 (\eta \square_2 \beta)) \square_1 \alpha)$ tem o mesmo valor lógico que $(\alpha \square_2 \eta)$'

a primeira e segunda ocorrências de $\square_1$ devem ser do mesmo conectivo, assim como a primeira e segunda ocorrências de $\square_2$; agora, os símbolos $\square_1$ e $\square_2$ podem, ou não, denotarem o mesmo conectivo.

1.2.2 Omissão de parênteses

Para simplificar notação e facilitar a leitura omitimos a escrita de parênteses de acordo com as seguintes regras, para evitar ambiguidade.

1. Omitimos os parênteses mais externos: $\neg\alpha$ deve ser lido como $(\neg\alpha)$ e $\alpha\Box\eta$ deve ser lido como $(\alpha\Box\eta)$.
2. Adotamos a seguinte ordem de precedência para os conectivos: $\neg, \wedge, \vee, \rightarrow, \leftrightarrow$. Assim, por exemplo, $p \vee q \wedge r$ deve ser lido como $(q \vee (q \wedge r))$; $\neg p \vee r$ deve ser lido como $((\neg p) \vee r)$; $\neg p \vee r \rightarrow q \wedge s$ deve ser lido como $(((\neg p) \vee r) \rightarrow (q \wedge s))$.
3. As repetições de um mesmo conectivo são aninhadas pela direita: $p \rightarrow q \rightarrow r \rightarrow s$ deve ser lido como $(p \rightarrow (q \rightarrow (r \rightarrow s)))$.

Por exemplo,

- $\neg\alpha \vee \beta$ lê-se $((\neg\alpha) \vee \beta)$,
- $\neg\neg\neg\alpha \wedge \beta$ lê-se $((\neg(\neg(\neg\alpha))) \wedge \beta)$,
- $\neg(\neg\neg\alpha \wedge \beta)$ lê-se $(\neg((\neg(\neg\alpha)) \wedge \beta))$,
- $\alpha \vee \beta \rightarrow \gamma$ lê-se $((\alpha \vee \beta) \rightarrow \gamma)$,
- $\delta \rightarrow \alpha \vee (\beta \rightarrow \gamma)$ lê-se $(\delta \rightarrow (\alpha \vee (\beta \rightarrow \gamma)))$,
- $\alpha \vee \beta \wedge \gamma \vee \delta \wedge \xi \vee \phi \wedge \rho$ deve ser lido como $(\alpha \vee ((\beta \wedge \gamma) \vee ((\delta \wedge \xi) \vee (\phi \wedge \rho))))$.

1.3 Exercícios

1. Queremos com uma linguagem simbólica capturar formas de dedução ou argumentação, em alguns casos há situações descritas em linguagem natural que queremos simbolizar na linguagem formal. Por exemplo, denominando as sentenças atômicas conforme abaixo

   - p : O time joga bem
   - q : O time ganha o campeonato.
   - r : O técnico é o culpado.
   - s : Os torcedores estão felizes.

   escrevemos as sentenças compostas
   - $p \rightarrow q$: Se o time joga bem, então ganha o campeonato.
   - $(\neg p) \rightarrow r$: Se o time não joga bem, então o técnico é o culpado.
   - $q \vee \neg s$: O time ganha o campeonato ou os torcedores não ficam felizes.

   Escreva as seguintes frases como fórmulas bem formadas da linguagem da lógica proposicional usando símbolos proposicionais para as frases atômicas. Para fazer alguns dos itens será necessário pesquisar como os termos “necessário”, “suficiente”, “necessário e suficiente”, “somente se” são traduzidos para os conectivos lógicos.
   a) Se há motivação para o estudo, então o estudante estuda muito ou não aprende a matéria.
   b) Se o estudante estuda muito, então, se não há motivação para o estudo, o estudante não aprende a matéria.

c) Não há motivação para o estudo se, e somente se, o estudante estuda muito e não aprende a matéria.
d) Se o Sr. Jones está feliz, Sra. Jones não está feliz, e se o Sr. Jones não é feliz, Sra. Jones não é feliz.
e) Ou Sam virá para a festa e Max não vai, ou Sam não vai vêm para a festa e Max vai se divertir.
f) Uma condição suficiente para x ser estranho é que x seja primo.
g) Uma condição necessária para uma sequência de números reais convergir é ser limitada.
h) A condição necessária e suficiente para o homem ser feliz é ter vinho e música.
i) Schrek vai ao cinema somente se estiver passando uma comédia.
j) O suborno será pago se e somente se as mercadorias são entregues.
k) Karpov vai ganhar o torneio de xadrez, a menos que Kasparov vença hoje.

2. Adicione parênteses nas seguintes expressões de modo que fiquem fórmulas bem formadas (sem usar as regras de omissão de parênteses). Quando houver mais de uma possibilidade, faça pelo menos duas delas.

a) $\neg p_1 \to p_2$
b) $p_1 \land \neg p_2 \land p_3 \land \neg p_4$
c) $p_1 \to p_2 \to p_3 \to p_1 \land p_2 \land p_4$
d) $\neg\alpha \lor \alpha$
e) $\neg(\neg\neg\neg\alpha \land \beta)$
f) $\alpha \to \alpha \lor (\beta \to \gamma)$

3. Para as fórmulas bem formadas encontradas no exercício anterior, determine todas as subfórmulas. (As subfórmulas dependem do modo que os parênteses foram colocados?)
4. Leia com atenção a descrição das regras para a omissão de parênteses e refaça o exercício 2 tendo em mente que os parênteses das fórmulas são omitidos de acordo com as regras.
5. (***Comprimento*** *de uma fórmula*) Use a indução para fórmulas e defina a seguinte função $\ell\colon \mathscr{L}_0 \to \mathbb{N}$: $\ell(\alpha)$ é o comprimento da fórmula α e expressa o número de símbolos da fórmula que não são de pontuação. Por exemplo $\ell((\neg p_1)) = \{2\}$, $\ell((p_1 \lor p_2)) = 3$, $\ell((p_1 \land (p_1 \to p_2) \lor (\neg p_2))) = 8$.
6. Use a indução para fórmulas e defina recursivamente, para toda fórmula α da linguagem, a função átomos(α) que descreve o conjunto dos símbolos proposicionais que ocorrem em α. Por exemplo átomos$(p_1) = \{p_1\}$, átomos$((p_1 \lor p_2)) = \{p_1, p_2\}$, átomos$((p_1 \land (p_1 \to p_2) \lor (\neg p_2))) = \{p_1, p_2\}$.
7. Demonstre que para toda fórmula α vale que grau(α) é no máximo o número de conectivos lógicos que aparecem em α. Demonstre também que grau$(\beta) <$ grau(α) para toda subfórmula própria β da fórmula α.
8. Seja $\mathscr{P}$ uma propriedade de fórmulas. Considere, para todo inteiro $n \geqslant 0$, a sentença $S(n)$ dada por “toda as fórmulas de $\mathscr{L}_0$ escritas com n conectivos lógicos têm a propriedade $\mathscr{P}$”. Use $S(n)$ e o princípio de indução matemática para demonstrar o metateorema de indução para fórmulas.
9. A altura de uma árvore de formação é o maior número de arestas que se dá a partir da raiz até uma das folhas. Por exemplo, na árvore da figura 1.4 a altura

é 3. Dê uma definição recursiva para a função $\text{alt}(\alpha)$ que é a altura da árvore de formação de α.

10. Prove usando indução que $\text{alt}(\alpha) < \ell(\alpha)$ (a função ℓ é definida no exercício 5).
11. Prove usando indução para fórmulas que o número de abre-parênteses em uma fórmula é sempre igual ao número de fecha-parênteses.
12. Prove usando indução para fórmulas que dada qualquer ocorrência de um conectivo numa fórmula dada, o número de abre-parênteses que se localizam à esquerda desse conectivo é estritamente maior que o número de fecha-parênteses que estão à sua esqueda.
13. Prove usando indução para fórmulas que em uma fórmula do tipo $(\neg\alpha)$ ou do tipo $(\alpha\square\beta)$, com α e β fórmulas, à esquerda de $\neg$ e à esquerda de $\square$ o número de abre-parênteses é exatamente um a mais que o número de fecha-parênteses.
14. Prove usando indução para fórmulas que em toda fórmula α ocorre apenas um conectivo lógico que satisfaz a condição "à esquerda dele, o número de abre-parênteses é exatamente um a mais que o número de fecha-parênteses".
15. Prove a partir dos exercícios 11 a 14 o metateorema da leitura única, enunciado na página 24.

1.4 Dedução

São conhecidos alguns sistemas dedutivos para a lógica proposicional como os Sistemas axiomáticos à Hilbert, a Dedução Natural, os Tableaux semânticos e o Cálculo de sequentes de Gentzen, por exemplo. Eles são equivalentes no sentido de deduzirem as mesmas sentenças da lógica proposicional. Cada um deles foi proposto com um propósito, por exemplo, modelar o modo como deduzimos usando raciocínio lógico ou mecanizar mais o processo.

Apresentaremos um sistema axiomático do tipo *Sistema de Hilbert* para a lógica proposicional. Os sistemas à Hilbert foram concebidos no final do século 19, são axiomatizações do lógica. Ele contém um conjunto (finito) de axiomas e algumas (muitas vezes uma única) regras de inferências; provas são construídos como uma sequência de fórmulas, cada um dos quais é ou um axioma (ou uma fórmula que tenha sido anteriormente provada) ou uma derivação de uma fórmula de fórmulas anteriores na sequência usando a regra de inferência. As deduções nesse tipo de sistema são mais difíceis porém facilita-se o estudo das propriedades (metateoremas) do sistema dedutivo, que é o nosso principal objetivo.

Neste texto distinguimos 'prova' de 'demonstração', usamos a primeira para deduções formais e a segunda para o raciocínio que torna evidente o caráter verídico de um proposição a respeito da lógica (um metateorema).

1.4.1 Axiomas

No que segue, chamaremos de axioma uma expressão como as seguintes

$$\alpha \to (\beta \to \alpha) \tag{1.1}$$

$$\alpha \to \alpha \tag{1.2}$$

o que, a rigor, não são fórmulas como já dissemos na seção 1.1.1. São **esquemas** de fórmulas pois usam variáveis da metalinguagem. Os axiomas são obtidos quando substituímos tais variáveis por fórmulas nas quais figuram apenas símbolos do alfabeto, sendo que todas as ocorrências da mesma variável correspondem a mesma fórmula da linguagem.

Exemplo 1.8. A FBF $((p_1 \vee \neg p_2) \leftrightarrow p_3) \to (\neg(p_2 \wedge \neg p_3) \to ((p_1 \vee \neg p_2) \leftrightarrow p_3))$ é uma das fórmulas do esquema (1.1), isto é, é um dos axiomas

$$\underbrace{((p_1 \vee \neg p_2) \leftrightarrow p_3)}_{\alpha} \to (\underbrace{\neg(p_2 \wedge \neg p_3)}_{\beta} \to \underbrace{((p_1 \vee \neg p_2) \leftrightarrow p_3)}_{\alpha})$$

e $((p_1 \vee \neg p_2) \leftrightarrow p_3) \to ((p_1 \vee \neg p_2) \leftrightarrow p_3)$ é uma fórmula do esquema (1.2)

$$\underbrace{((p_1 \vee \neg p_2) \leftrightarrow p_3)}_{\alpha} \to \underbrace{((p_1 \vee \neg p_2) \leftrightarrow p_3)}_{\alpha}$$

O conjunto de (esquemas de) axiomas que adotaremos para o sistema dedutivo é o seguinte, conhecido como sistema de Kleene e denotando, neste texto por K. Lembrando ainda que usamos as convenções para omissão de parênteses.

(A1) $\alpha \to (\beta \to \alpha)$
(A2) $(\alpha \to (\beta \to \xi)) \to ((\alpha \to \beta) \to (\alpha \to \xi))$
(A3) $(\alpha \to \beta) \to ((\alpha \to \neg\beta) \to \neg\alpha)$
(A4) $\alpha \to (\beta \to (\alpha \wedge \beta))$
(A5) $\alpha \wedge \beta \to \alpha$
(A6) $\alpha \wedge \beta \to \beta$
(A7) $\alpha \to \alpha \vee \beta$
(A8) $\beta \to \alpha \vee \beta$
(A9) $(\alpha \to \gamma) \to ((\beta \to \gamma) \to (\alpha \vee \beta \to \gamma))$
(A10) $\neg\neg\alpha \to \alpha$

1.4.2 Regra de inferência

O sistema formal de Kleene tem apenas uma regra de inferência, *Modus Ponens* que abreviamos (MP):

(MP) $\dfrac{\alpha,\ \alpha \to \beta}{\beta}$

e deve ser entendida como: a partir da fórmula α e da fórmula $\alpha \to \beta$ podemos deduzir (provar, inferir ou escrever) a fórmula β. Na prática dedutiva, explicada a seguir, isso significa que se numa prova ocorre a fórmula α e ocorre a fórmula $\alpha \to \beta$, então podemos escrever a fórmula β.

Modus ponens é uma abreviação de *modus ponendo ponens*, frase em latim para "o modo que afirma afirmando".

1.4.3 Prova

Sejam $\alpha \in \mathscr{L}_0$ e $\Gamma \subset \mathscr{L}_0$. Uma **prova** de α a partir de Γ é uma sequência finita de fórmulas de $\mathscr{L}_0$

$$\varphi_1, \varphi_2, \ldots, \varphi_n$$

tal que $\varphi_n = \alpha$ e, para todo $i < n$, φ_i é

1. ou um axioma
2. ou uma fórmula de Γ
3. ou uma fórmula obtida a partir de $\varphi_1, \varphi_2, \ldots, \varphi_{i-1}$ (todo ou uma parte) por regra de inferência.

Nesse caso dizemos que Γ prova α, ou α é **deduzível** a partir de Γ e usamos a notação

$$\Gamma \vdash \alpha.$$

As vezes, também dizemos que α é **consequência sintática** de Γ. Chamamos as fórmulas do conjunto Γ de **premissas** ou **hipóteses iniciais**.

Se α é consequência sintática apenas dos axiomas, isto é $\Gamma = \varnothing$, escrevemos

$$\vdash \alpha$$

e nesse caso dizemos que α é um **teorema lógico**. Em particular, se α é um axioma, então também é um teorema lógico.

Se Γ é finito, digamos que $\Gamma = \{\varphi_1, \varphi_2, \ldots, \varphi_m\}$, escrevemos

$$\{\varphi_1, \varphi_2, \ldots, \varphi_m\} \vdash \alpha.$$

Adotamos as seguintes simplificações nas notações que acabamos de definir:

- Ao invés de $\{\alpha\} \vdash \beta$ escrevemos $\alpha \vdash \beta$.
- Ao invés de $\{\alpha_1, \ldots, \alpha_n\} \vdash \beta$ escrevemos $\alpha_1, \ldots, \alpha_n \vdash \beta$.
- Ao invés de $\Gamma \cup \{\alpha\} \vdash \beta$ escrevemos $\Gamma, \alpha \vdash \beta$.

1.4.4 Propriedades básicas de $\vdash$

A dedução tem as seguintes quatro propriedades básicas.

Autodedução $\Gamma \vdash \alpha$ para todo $\alpha \in \Gamma$.

Para qualquer $\alpha \in \mathscr{L}_0$ vale que

$$\alpha \vdash \alpha$$

ou seja, toda fórmula pode ser deduzida dela mesma. A sequência que tem apenas a fórmula α é uma prova de acordo com a definição dada acima. Autodedução é uma consequência dessa observação simples.

Monotonicidade Se $\Gamma \vdash \alpha$ então $\Gamma \cup \Sigma \vdash \alpha$, isto é, se uma fórmula é dedutível de um conjunto de premissas, então se acrescentamos mais premissas à dedução, ela continuará sendo dedutível desse novo conjunto.

Compacidade $\Gamma \vdash \alpha$ se, e só se, existe $\Delta \subseteq \Gamma$ finito tal que $\Delta \vdash \alpha$.
Basta observar que se $\Gamma \vdash \alpha$ então tomamos Δ como as fórmulas de Γ que ocorrem na prova, que é finita; a recíproca dessa proposição segue da monotonicidade.

Regra do corte Se $\Gamma \vdash \alpha$ para todo $\alpha \in \Delta$ e $\Delta \vdash \beta$ então $\Gamma \vdash \beta$.
Se P é uma prova de $\Delta \vdash \beta$, tome $\{\alpha_1, \dots, \alpha_k\} \subset \Delta$ (finito, garantido pela compacidade) tal que $\{\alpha_1, \dots, \alpha_k\} \vdash \beta$. Agora, para cada $i = 1, 2, \dots, k$, sejam P_i as provas de $\Gamma \vdash \alpha_i$. Então, a sequência de fórmulas $P_1, P_2, \dots, P_k, P$ é uma prova de $\Gamma \vdash \beta$.

A regra do corte garante que, uma vez que tenhamos deduzido uma coleção de fórmulas Δ a partir de Γ, podemos usar as fórmulas de Δ para novas inferências. Devemos ter em mente o seguinte, Γ pode representar os axiomas de uma teoria e Δ uma coleção de teoremas obtidos por dedução a partir dos axiomas. Podemos assim ter novos teoremas deduzindo-os dos teoremas já obtidos antes.

1.4.5 Exemplos de prova

Usualmente, escrevemos uma prova para $\Gamma \vdash \varphi_n$ da seguinte forma

Prova.

1.	φ_1	`(justificativa)`
2.	φ_2	`(justificativa)`
	$\vdots$	
n-1.	φ_{n-1}	`(justificativa)`
n.	φ_n	`(justificativa)`

As linhas são numeradas para referência, a sequência $\varphi_1, \varphi_2, \dots, \varphi_n$ é a prova, a última fórmula é a que esta sendo provada (φ_n nesse caso) e "`(justificativa)`"diz se a fórmula daquela linha é uma premissa de Γ, um axioma do sistema ou um fórmula inferida via regra de inferência.

Teorema 1.9. $\vdash \alpha \to \alpha$

Prova.

1.	$\alpha \to ((\alpha \to \alpha) \to \alpha))$	(A1)
2.	$(\alpha \to ((\alpha \to \alpha) \to \alpha)) \to ((\alpha \to (\alpha \to \alpha)) \to (\alpha \to \alpha))$	(A2)
3.	$\alpha \to (\alpha \to \alpha))$	(A1)
4.	$(\alpha \to (\alpha \to \alpha)) \to (\alpha \to \alpha)$	(MP 2,1)
5.	$\alpha \to \alpha$	(MP 3,4)

Teorema 1.10. $\alpha \to \beta, \beta \to \gamma \vdash \alpha \to \gamma$

Prova.

1.	$\alpha \to \beta$	(hipótese)
2.	$\beta \to \gamma$	(hipótese)
3.	$(\beta \to \gamma) \to (\alpha \to (\beta \to \gamma))$	(A1)
4.	$(\alpha \to (\beta \to \gamma)$	(MP 2,3)
5.	$(\alpha \to (\beta \to \gamma)) \to ((\alpha \to \beta) \to (\alpha \to \gamma))$	(A2)
6.	$(\alpha \to \beta) \to (\alpha \to \gamma)$	(MP 4,5)
7.	$\alpha \to \gamma$	(MP 1,6)

Teorema 1.11. $\theta \to (\phi \to \xi) \vdash \phi \to (\theta \to \xi)$

Prova.

1.	$\theta \to (\phi \to \xi)$	(hipótese)
2.	$\big(\theta \to (\phi \to \xi)\big) \to \big((\theta \to \phi) \to (\theta \to \xi)\big)$	(A2)
3.	$\phi \to (\theta \to \phi)$	(A1)
4.	$(\theta \to \phi) \to (\theta \to \xi)$	(MP 1,2)
5.	$\big((\theta \to \phi) \to (\theta \to \xi)\big) \to \big(\phi \to \big((\theta \to \phi) \to (\theta \to \xi)\big)\big)$	(A1)
6.	$\phi \to \big((\theta \to \phi) \to (\theta \to \xi)\big)$	(MP 4,5)
7.	$\big(\phi \to \big((\theta \to \phi) \to (\theta \to \xi)\big)\big) \to$	
	$\big(\big(\phi \to (\theta \to \phi)\big) \to \big(\phi \to (\theta \to \xi)\big)\big)$	(A2)
8.	$\big(\phi \to (\theta \to \phi)\big) \to \big(\phi \to (\theta \to \xi)\big)$	(MP 6,7)
9.	$\phi \to (\theta \to \xi)$	(MP 3,8)

Notemos que as linhas 1–7 da prova do teorema 1.10 são análogas às linhas 3–9 na prova do teorema 1.11. De fato, na linha 3 deste último nós temos $\phi \to (\theta \to \phi)$ e na 4 temos $(\theta \to \phi) \to (\theta \to \xi)$; o que precisamos agora é concluir afórmula da linha 9 que $\phi \to (\theta \to \xi)$, que é essencialmente o que o teorema 1.10 faz dadas as hipóteses $\phi \to (\theta \to \phi)$ e $(\theta \to \phi) \to (\theta \to \xi)$.

Convidamos o leitor a trocar no teorema 1.10 toda ocorrência de α por ϕ, de β por $\theta \to \phi$ e de γ por $\theta \to \xi$ e observar que se obtém o resultado esperado.

Para evitar esse trabalho extra de escrever uma dedução que já foi feita p permitimos que se justifique os passos de uma prova com teoremas já provados. Para dar um exemplo, a prova acima do teorema 1.11 é reescrita abaixo.

1.	$\theta \to (\phi \to \xi)$	(hipótese)
2.	$\big(\theta \to (\phi \to \xi)\big) \to \big((\theta \to \phi) \to (\theta \to \xi)\big)$	(A2)
3.	$\phi \to (\theta \to \phi)$	(A1)
4.	$(\theta \to \phi) \to (\theta \to \xi)$	(MP 1,2)
5.	$\phi \to (\theta \to \xi)$	(Teo. 1.10 3,4)

O próximo resultado também permite a mesma simplificação. Nas linhas 8–14 da prova a seguir também fazem o mesmo serviço do teorema 1.10. Pode-se verificar isso trocando na prova do teorema 1.10 toda ocorrência de α por $\neg\alpha \to \neg\neg\alpha$, de β por $\neg\neg\alpha$ e de γ por α.

Teorema 1.12. $\neg\alpha \to \neg\neg\alpha \vdash \alpha$

Prova.

1.	$\neg\alpha \to \neg\neg\alpha$	(hipótese)
2.	$\neg\alpha \to ((\neg\alpha \to \neg\alpha) \to \neg\alpha)$	(A1)
3.	$(\neg\alpha \to ((\neg\alpha \to \neg\alpha) \to \neg\alpha)) \to$ $((\neg\alpha \to (\neg\alpha \to \neg\alpha)) \to (\neg\alpha \to \neg\alpha))$	(A2)
4.	$\neg\alpha \to (\neg\alpha \to \neg\alpha)$	(A1)
5.	$(\neg\alpha \to (\neg\alpha \to \neg\alpha)) \to (\neg\alpha \to \neg\alpha)$	(MP 2,3)
6.	$\neg\alpha \to \neg\alpha$	(MP 4,5)
7.	$(\neg\alpha \to \neg\alpha) \to ((\neg\alpha \to \neg\neg\alpha) \to \neg\neg\alpha)$	(A3)
8.	$(\neg\alpha \to \neg\neg\alpha) \to \neg\neg\alpha$	(MP 6,7)
9.	$\neg\neg\alpha \to \alpha$	(A10)
10.	$((\neg\neg\alpha) \to \alpha) \to ((\neg\alpha \to \neg\neg\alpha) \to ((\neg\neg\alpha) \to \alpha))$	(A1)
11.	$((\neg\alpha \to \neg\neg\alpha) \to ((\neg\neg\alpha) \to \alpha)$	(MP 9,10)
12.	$((\neg\alpha \to \neg\neg\alpha) \to ((\neg\neg\alpha) \to \alpha)) \to$ $(((\neg\alpha \to \neg\neg\alpha) \to (\neg\neg\alpha)) \to ((\neg\alpha \to \neg\neg\alpha) \to \alpha))$	(A2)
13.	$((\neg\alpha \to \neg\neg\alpha) \to (\neg\neg\alpha)) \to ((\neg\alpha \to \neg\neg\alpha) \to \alpha)$	(MP 11,12)
14.	$(\neg\alpha \to \neg\neg\alpha) \to \alpha$	(MP 8,13)
15.	α	(MP 1,14)

As linhas 1–7 da prova do teorema 1.10 são análogas às linhas 8–14 na prova do teorema 1.12. A prova reescrita fica assim:

Prova do teorema 1.12.

1.	$\neg\alpha \to \neg\neg\alpha$	(hipótese)
2.	$\neg\alpha \to ((\neg\alpha \to \neg\alpha) \to \neg\alpha)$	(A1)
3.	$(\neg\alpha \to ((\neg\alpha \to \neg\alpha) \to \neg\alpha)) \to$ $((\neg\alpha \to (\neg\alpha \to \neg\alpha)) \to (\neg\alpha \to \neg\alpha))$	(A2)
4.	$\neg\alpha \to (\neg\alpha \to \neg\alpha)$	(A1)
5.	$(\neg\alpha \to (\neg\alpha \to \neg\alpha)) \to (\neg\alpha \to \neg\alpha)$	(MP 2,3)
6.	$\neg\alpha \to \neg\alpha$	(MP 4,5)
7.	$(\neg\alpha \to \neg\alpha) \to ((\neg\alpha \to \neg\neg\alpha) \to \neg\neg\alpha)$	(A3)
8.	$(\neg\alpha \to \neg\neg\alpha) \to \neg\neg\alpha$	(MP 6,7)
9.	$\neg\neg\alpha \to \alpha$	(A10)
10.	$(\neg\alpha \to \neg\neg\alpha) \to \alpha$	(pelo Teo. 1.10 em 8,9)
11.	α	(MP 1,14)

Teorema 1.13. $\vdash \alpha \to \neg\neg\alpha$

Prova.

1.	$\neg\neg\neg\alpha \to \neg\alpha$	(A10)
2.	$(\neg\neg\neg\alpha \to \alpha) \to \big((\neg\neg\neg\alpha \to \neg\alpha) \to \neg\neg\neg\neg\alpha\big)$	(A3)
3.	$(\neg\neg\neg\alpha \to \neg\alpha) \to \big((\neg\neg\neg\alpha \to \alpha) \to \neg\neg\neg\neg\alpha\big)$	(Teo. 1.11 em 2)
4.	$(\neg\neg\neg\alpha \to \alpha) \to \neg\neg\neg\neg\alpha$	(MP 1,3)
5.	$\neg\neg\neg\neg\alpha \to \neg\neg\alpha$	(A10)
6.	$(\neg\neg\neg\alpha \to \alpha) \to \neg\neg\alpha$	(Teo. 1.10 em 4,5)
7.	$\alpha \to (\neg\neg\neg\alpha \to \alpha)$	(A1)
8.	$\alpha \to \neg\neg\alpha$	(Teo. 1.10 em 7,6)

Teorema 1.14 (Lei de Duns Scotus). $\neg\alpha \land \alpha \vdash \beta$

Prova.

1.	$\alpha \land \neg\alpha$	(hipótese)
2.	$(\alpha \land \neg\alpha) \to \alpha$	(A5)
3.	α	(MP 1,2)
4.	$(\alpha \land \neg\alpha) \to \neg\alpha$	(A6)
5.	$\neg\alpha$	(MP 1,4)
6.	$\alpha \to (\neg\beta \to \alpha)$	(A1)
7.	$\neg\alpha \to (\neg\beta \to \neg\alpha)$	(A1)
8.	$\neg\beta \to \alpha$	(MP 1,3)
9.	$\neg\beta \to \neg\alpha$	(MP 2,4)
10.	$(\neg\beta \to \alpha) \to \big((\neg\beta \to \neg\alpha) \to \neg\neg\beta\big)$	(A3)
11.	$(\neg\beta \to \neg\alpha) \to \neg\neg\beta$	(MP 5,7)
12.	$\neg\neg\beta$	(MP 6,8)
13.	$\neg\neg\beta \to \beta$	(A10)
14.	β	(MP 9,10)

Desse resultado temos que se, por algum motivo tenhamos duas fórmulas contraditórias, α e $\neg\alpha$, provamos que pode-se derivar qualquer fórmula β a partir dessas hipóteses. Dizia-se "*ex falso seguitur quodlibet*" (de uma falsidade tudo se segue). A "falsidade" aqui refere-se a fórmula $\alpha \land \neg\alpha$ que pode ser inferida a partir de α e de $\neg\alpha$:

1.	α	(hipótese)
2.	$\neg\alpha$	(hipótese)
3.	$\alpha \to (\neg\alpha \to (\alpha \land \neg\alpha))$	(A4)
4.	$\neg\alpha \to (\alpha \land \neg\alpha)$	(MP 1,3)
5.	$\alpha \land \neg\alpha$	(MP 2,4)

Exercício 1.15. *Dê provas para*

1. $\vdash (\neg\alpha \to \alpha) \to \alpha$.
2. $\vdash (\neg\beta \to \neg\alpha) \to (\alpha \to \beta)$.

1.4.6 Regras de inferência derivadas

Ao invés de mantermos as referências a teoremas, quando esses são muito úteis como o teorema 1.10 acima, preferimos escrevê-los como novas regras de inferência do sistema, as quais chamamos regras **regras de inferência derivadas**. Mantenhamos em mente que, do ponto de vista formal, apenas (MP) é regra de inferência do sistema K, as regras derivadas são mais uma conveniência prática.

As regras correspondentes aos teoremas 1.10 e 1.11 são escritas esquematicamente como

(SH) $\dfrac{\alpha \to \beta, \beta \to \gamma}{\alpha \to \gamma}$ (TH) $\dfrac{\theta \to (\phi \to \xi)}{\phi \to (\theta \to \xi)}$

chamadas, respectivamente, de *silogismo hipotético* e de *troca de hipóteses*. Outra regra derivada bastante útil é a *contrapositiva*

(CP1) $\dfrac{\alpha \to \beta}{\neg\beta \to \neg\alpha}$

que tem a seguinte prova.

1.	$\alpha \to \beta$	(hipótese)
2.	$\beta \to \neg\neg\beta$	(Teo. 1.13)
3.	$\alpha \to \neg\neg\beta$	(SH 1,2)
4.	$\neg\neg\alpha \to \alpha$	(A10)
5.	$\neg\neg\alpha \to \neg\neg\beta$	(SH 3,4)
6.	$(\neg\neg\alpha \to \neg\neg\beta) \to ((\neg\neg\alpha \to \neg\neg\neg\beta) \to \neg\neg\neg\alpha)$	(A3)
7.	$(\neg\neg\alpha \to \neg\neg\neg\beta) \to \neg\neg\neg\alpha$	(MP 5,6)
8.	$\neg\neg\neg\beta \to (\neg\neg\alpha \to \neg\neg\neg\beta)$	(A1)
9.	$\neg\neg\neg\beta \to \neg\neg\neg\alpha$	(SH 8,7)
10.	$\neg\beta \to \neg\neg\neg\beta$	(Teo. 1.13)
11.	$\neg\beta \to \neg\neg\neg\alpha$	(SH 10,9)
12.	$\neg\neg\neg\alpha \to \neg\alpha$	(A10)
13.	$\neg\beta \to \neg\alpha$	(SH 11,12)

As regras derivadas são escritas, genericamente, como

$$\frac{\alpha_1, \ldots, \alpha_k}{\beta}$$

e entende-se: se $\alpha_1, \ldots, \alpha_k$ são teoremas do sistema formal, então β é teorema do sistema formal.

Como exemplo de aplicação dessa, considere

$$p_1 \to p_2, p_2 \to p_3, \neg p_1 \to p_4, \neg p_3 \vdash p_4$$

cuja prova é

1.	$p_1 \to p_2$	(hipótese)
2.	$p_2 \to p_3$	(hipótese)
3.	$\neg p_1 \to p_4$	(hipótese)
4.	$\neg p_3$	(hipótese)
5.	$p_1 \to p_3$	(SH 1,2)
6.	$\neg p_3 \to \neg p_1$	(CP1 em 4)
7.	$\neg p_1$	(MP 4,6)
8.	p_4	(MP 3,7)

A seguintes regras são regras de inferência derivadas notáveis, dentre outras que veremos mais adiante: (RA) *redução ao absurdo*, (IC) *introdução da conjunção*, (EC) *exclusão da conjunção*, (ID) *introdução da disjunção*, (MT) *modus tolens*, (DM) *leis de De Morgan*, (Assoc) *associatividade* da disjunção, (DN) *Dupla negação*

(RA) $\dfrac{\alpha \to \beta, \alpha \to \neg\beta}{\neg\alpha}$ (ID2) $\dfrac{\beta}{\alpha \vee \beta}$ (Assoc) $\dfrac{\alpha \vee (\beta \vee \gamma)}{(\alpha \vee \beta) \vee \gamma}$

(IC) $\dfrac{\alpha, \beta}{\alpha \wedge \beta}$ (MT) $\dfrac{\alpha \to \beta, \neg\beta}{\neg\alpha}$ (CP2) $\dfrac{\neg\beta \to \neg\alpha}{\alpha \to \beta}$

(EC1) $\dfrac{\alpha \wedge \beta}{\alpha}$ (SD) $\dfrac{\alpha \vee \beta, \neg\alpha}{\beta}$ (DN1) $\dfrac{\alpha}{\neg\neg\alpha}$

(EC2) $\dfrac{\alpha \wedge \beta}{\beta}$ (DM∨) $\dfrac{\neg(\alpha \vee \beta)}{\neg\alpha \wedge \neg\beta}$ (DN2) $\dfrac{\neg\neg\alpha}{\alpha}$

(ID1) $\dfrac{\alpha}{\alpha \vee \beta}$ (DM∧) $\dfrac{\neg(\alpha \wedge \beta)}{\neg\alpha \vee \neg\beta}$ (C) $\dfrac{\neg\alpha \to \alpha}{\alpha}$.

1.5 O Teorema da Dedução

O seguinte resultado nos dá uma propriedade importante da dedução na lógica proposicional.

Metateorema 1.16 (Teorema da Dedução). *Sejam α, β fórmulas e Γ conjunto de fórmulas.*

$$\Gamma, \alpha \vdash \beta \text{ se, e somente se, } \Gamma \vdash \alpha \to \beta.$$

Demonstração do Teorema da Dedução

Vamos demonstrar que se $\Gamma, \alpha \vdash \beta$ então $\Gamma \vdash \alpha \to \beta$. Suponha que $\Gamma, \alpha \vdash \beta$ e seja

$$\theta_1, \theta_2, \dots, \theta_{n-1}, \beta$$

uma prova de β a partir de $\Gamma \cup \{\alpha\}$. Vamos demonstrar por indução em i que $\Gamma \vdash \alpha \to \theta_i$ para todo $1 \leq i \leq n$ em que θ_n é a fórmula β.

Lembremos que o uso de teoremas ou de regras de inferência derivadas numa prova é apenas uma abreviação, para efeitos de formalismo uma prova contém fórmulas que são axiomas ou hipóteses ou inferências por *Modus Ponens*.

Base: a fórmula θ_1 ou é um axioma ou uma fórmula de Γ. Se é axioma ou hipótese (de $\Gamma \cup \{\alpha\}$) então

1.	θ_1	(axioma ou hipótese)
2.	$\theta_1 \to (\alpha \to \theta_1)$	(A1)
3.	$\alpha \to \theta_1$	(MP 1,2)

Em ambos os casos vale que $\Gamma \vdash \alpha \to \theta_1$. Para a *hipótese indutiva*, assumamos que $\Gamma \vdash \alpha \to \theta_j$ para todo $j = 1, 2, \dots, i-1$.

Para o *passo indutivo* vamos demonstrar que a hipótese indutiva implica $\Gamma \vdash \alpha \to \theta_i$.

A fórmula θ_i ou é uma axioma ou fórmula de $\Gamma \cup \{\alpha\}$, ou é resultado do uso de *modus ponens*, digamos que (MP j,k) com $j, k < i$. Nos dois primeiros casos

$\Gamma \vdash \alpha \to \theta_i$, a prova é similar ao caso feito na base da indução. Resta verificar o caso θ_i é resultado de (MP j,k) com $j, k < i$.

Se θ_i é resultado de (MP j,k) com $j, k < i$ então na linha j temos θ_j e na linha k temos $\theta_j \to \theta_i$. Pela hipótese indutiva $\Gamma \vdash \alpha \to \theta_j$ e $\Gamma \vdash \alpha \to (\theta_j \to \theta_i)$, assim, com hipóteses Γ

1.	$\alpha \to \theta_j$	(teorema de Γ)
2.	$\alpha \to (\theta_j \to \theta_i)$	(teorema de Γ)
3.	$(\alpha \to (\theta_j \to \theta_i)) \to ((\alpha \to \theta_j) \to (\alpha \to \theta_i))$	(A2)
4.	$(\alpha \to \theta_j) \to (\alpha \to \theta_i)$	(MP 2,3)
5.	$\alpha \to \theta_i$	(MP 1,4)

ou seja, $\Gamma \vdash \alpha \to \theta_i$ o que completa o passo indutivo. Pelo princípio da indução matemática $\Gamma \vdash \alpha \to \theta_i$, para todo i, portanto $\Gamma \vdash \alpha \to \beta$.

Agora, vamos demonstrar que se $\Gamma \vdash \alpha \to \beta$ então $\Gamma, \alpha \vdash \beta$. Suponha que $\Gamma \vdash \alpha \to \beta$. Então

$$\Gamma, \alpha \vdash \alpha \to \beta$$

pela monotonicidade de $\vdash$. Pela autodedução de $\vdash$ temos $\Gamma, \alpha \vdash \alpha$, portanto pelo destacamento temos $\Gamma, \alpha \vdash \beta$. ■

Algumas consequências simples do Teorema da Dedução são:

- $\neg\beta \to \neg\alpha \vdash (\alpha \to \beta)$ a partir do exercício 1.15, item 2,
- $\neg\neg\alpha \vdash \alpha$ a partir do axioma (A10),
- $\alpha \vdash \neg\neg\alpha$ do teorema 1.13.

Esses três resultados prova as regras derivadas (CP2), (DN1) e (DN2) enunciadas na página 36.

1.6 Exercícios

16. Escreva uma demonstração para autodedução, a monotonicidade e regra do corte de $\vdash$.
17. Seja $\theta_1, \theta_2, \ldots, \theta_n$ uma prova. A sequência $\theta_1, \theta_2, \ldots, \theta_\ell$ para todo ℓ com $1 \le \ell \le n$ é uma prova?
18. Prove os seguintes teoremas lógicos para quaisquer fórmulas α e β.
    a) $\vdash (\beta \vee \alpha) \to (\alpha \vee \beta)$.
    b) $\vdash (\beta \to \neg\alpha) \to (\alpha \to \neg\beta)$.
    c) $\vdash (\neg\beta \to \alpha) \to (\neg\alpha \to \beta)$.
    d) $\vdash \alpha \to (\neg\beta \to \neg(\alpha \to \beta))$.
    e) $\vdash (\alpha \to \beta) \to ((\neg\alpha \to \beta) \to \beta)$.
    f) $\vdash \neg\delta \to (\neg\beta \to \neg(\delta \vee \beta))$.
    g) $\vdash \neg\alpha \vee \alpha$
    h) $\vdash \alpha \to (\beta \to (\alpha \wedge \beta))$
    i) $\vdash \alpha \wedge \beta \to \alpha$
    j) $\vdash \alpha \wedge \beta \to \beta$

k) $\vdash \alpha \to \alpha \vee \beta$
l) $\vdash \beta \to \alpha \vee \beta$
m) $\vdash (\alpha \to \gamma) \to ((\beta \to \gamma) \to (\alpha \vee \beta \to \gamma))$
n) $\vdash \neg\alpha \to (\alpha \to \beta)$

19. Prove cada uma das regras de inferência derivadas da página 36.
20. Dê uma demonstração para o seguinte resultado que vale para a dedução:

$$\text{Se } \Gamma \cup \{\neg\alpha\} \vdash \beta \text{ e } \Gamma \cup \{\neg\alpha\} \vdash \neg\beta \text{ então } \Gamma \vdash \alpha.$$

21. Use o resultado dado no exercício anterior para verificar que a partir das premissas $\{\neg\alpha \to (\beta \wedge \gamma), (\gamma \vee \delta) \to \varepsilon, \varepsilon \to \neg\beta\}$ a fórmula α é dedutível.
22. Dê uma demonstração para o seguinte resultado que vale para a dedução: $\Gamma \cup \{\alpha\} \vdash \beta$ e $\Gamma \cup \{\neg\alpha\} \vdash \beta$ então $\Gamma \vdash \beta$.
23. Sejam $\Gamma_1 \subset \Gamma_2 \subset \cdots \subset \Gamma_n \subset \cdots$ subconjuntos de fórmulas de $\mathscr{L}_0$ e tome $\Sigma = \bigcup_{i \geq 1} \Gamma_i$. Demonstre que se $\Sigma \vdash \alpha$ então $\Gamma_n \vdash \alpha$ para algum n.
24. Chamamos de K o sistema dedutivo que desenvolvemos no texto para a lógica proposicional. Há vários outros sistemas dedutivos axiomáticos, cada um com um conjunto de axiomas, a regra *modus Ponens* e, eventualmente, com a linguagem construída sobre outros conectivos básicos como, por exemplo, somente com o $\neg$ e o $\vee$. O sistema formal PM é o que aparece no *Principia Mathematica* de Russel e Whitehead tem os axiomas

(PM1) $(\alpha \vee \alpha) \to \alpha$.
(PM2) $\alpha \to (\alpha \vee \beta)$.
(PM3) $(\alpha \to \beta) \to ((\gamma \vee \alpha) \to (\gamma \vee \beta))$.
(PM4) $(\alpha \vee \beta) \to (\beta \vee \alpha)$.

a) Prove que todo axioma de PM é um teorema lógico de K. Conclua que todo teorema lógico de PM é um teorema lógico de K.
b) Prove que todo axioma de K é um teorema lógico de PM. Conclua que todo teorema lógico de K é um teorema lógico de PM.

25. O sistema formal L tem a regra *modus ponens* como a única regra de inferência e os axiomas

(L1) $\alpha \to (\beta \to \alpha)$.
(L2) $(\alpha \to (\beta \to \gamma)) \to ((\alpha \to \beta) \to (\alpha \to \gamma))$.
(L3) $\neg\alpha \to (\alpha \to \beta)$.
(L4) $(\neg\alpha \to \alpha) \to \alpha$.

Em L há dois conectivos primitivos, $\neg$ e $\to$, edefinem-se os seguintes conectivos lógicos

a) $\alpha \wedge \beta$ é abreviação de $\neg(\alpha \to \neg\beta)$
b) $\alpha \vee \beta$ é abreviação de $\neg\alpha \to \beta$
c) $\alpha \leftrightarrow \beta$ é abreviação de $(\alpha \to \beta) \wedge (\beta \to \alpha)$ que, por sua vez, usa uma abreviação.

Demonstre que L e K têm os mesmos teoremas.

26. O sistema formal H tem a regra *modus ponens* como a única regra de inferência e tem os axiomas

(H1) $\alpha \to (\beta \to \alpha)$.

(H2) $(\alpha \to (\beta \to \xi)) \to ((\alpha \to \beta) \to (\alpha \to \xi))$.
(H3) $(\neg\alpha \to \neg\beta) \to ((\neg\alpha \to \beta) \to \alpha)$.

a) Deduza nesse sistema:

i. $\vdash \alpha \to \alpha$.
ii. $\neg\alpha \vdash (\neg\beta \to \alpha) \to \beta$.
iii. $\vdash \neg\alpha \to ((\neg\beta \to \alpha) \to \beta)$.
iv. $\vdash \alpha \to \neg\neg\alpha$.
v. $\alpha, \neg\neg\alpha \vdash \beta$.
vi. $\vdash \neg\alpha \to (\alpha \to \beta)$.
vii. $\neg\beta \to \neg\alpha \vdash \alpha \to \beta$.
viii. $\alpha \to \beta \vdash \neg\beta \to \neg\alpha$.
ix. $\vdash (\alpha \to \beta) \to ((\alpha \to \neg\beta) \to \neg\alpha)$.

b) Demonstre que H e K têm os mesmos teoremas.

2

Semântica e metateoria da lógica proposicional

2.1 Interpretação e Valoração

Uma interpretação para os símbolos de uma linguagem formal atribui significado a tais símbolos, é uma função que associa aos símbolos qualquer fórmula da linguagem um elemento em uma estrutura abstrata que permite definir a validade das fórmulas. A semântica formal é o estudo da interpretações de uma linguagem formal.

No caso da lógica proposicional uma interpretação padrão é uma função que associa a cada símbolo proposicional um dentre dois **valores-verdade**

$$v\colon \{p_1, p_2, \dots\} \to \{0,1\}$$

o 0 representa o 'falso' e 1 o 'verdadeiro', que são nomes sem qualquer significado lógico específico.

Chamamos de **valoração** de $\mathscr{L}_0$ uma função $w : \mathscr{L}_0 \to \{0,1\}$ que atribui valor-verdade para as todas fórmulas bem formadas da linguagem e que satisfaz as seguintes condições[1]

- $w(\neg\alpha) = 1 - w(\alpha)$.
- $w(\alpha \wedge \beta) = \min\big(w(\alpha), w(\beta)\big)$.
- $w(\alpha \vee \beta) = \max\big(w(\alpha), w(\beta)\big)$.
- $w(\alpha \to \beta) = \max\big(1 - w(\alpha), w(\beta)\big)$
- $w(\alpha \leftrightarrow \beta) = \min\Big(\max\big(1 - w(\alpha), w(\beta)\big), \max\big(w(\alpha), 1 - w(\beta)\big)\Big)$.

Observemos que $w(\alpha \leftrightarrow \beta) = \min\big(w(\alpha \to \beta), w(\beta \to \alpha)\big)$ e que $w(\alpha \to \beta) = \max\big(w(\neg\alpha), w(\beta)\big)$; além disso

1. $w(\neg\alpha) = 1$ se, e só se, $w(\alpha) = 0$,
2. $w(\alpha \wedge \beta) = 1$ se, e só se, $w(\alpha) = 1$ e $w(\beta) = 1$,
3. $w(\alpha \vee \beta) = 1$ se, e só se, $w(\alpha) = 0$ ou $w(\beta) = 0$,

[1] $\max(a,b)$ é o maior dos dois números a e b, claramente, $\max(a,b) = \max(b,a)$. Idem para min, que é o menor.

4. $w(\alpha \to \beta) = 0$ se, e só se, $w(\alpha) = 1$ e $w(\beta) = 0$ e,
5. $w(\alpha \leftrightarrow \beta) = 1$ se, e só se, $w(\alpha) = w(\beta)$.

Isso parece sugerir que só precisaríamos definir a valoração para a negação, a disjunção e a cojunção. De fato, é mais que isso e voltaremos a esse assunto na seção 2.2.4.

Exercício 2.1. *Verifique que* $w(\alpha \leftrightarrow \beta) = 1 - |w(\alpha) - w(\beta)|$.

Exemplo 2.2. Seja w uma valoração tal que $w(p_1) = w(p_3) = 0$ e $w(p_2) = 1$. Então,

$$\begin{aligned}
w((p_1 \vee p_2) \to p_3) &= \max\big(1 - w(p_1 \vee p_2), w(p_3)\big) \\
&= \max\big(1 - \max(w(p_1), w(p_2)), w(p_3)\big) \\
&= \max\big(1 - \max(w(p_1), w(p_2)), w(p_3)\big) \\
&= \max(1 - \max(0, 1), 0) \\
&= \max(0, 0) = 0.
\end{aligned}$$

Exercício 2.3. *Tome uma valoração w tal que $w(p_4) = w(p_2) = 1$ e $w(p_1) = w(p_3) =$* 0. *Determine $w(\alpha)$ quando α é dada por*

1. $\neg p_2 \to \neg p_3$.	*3.* $\neg(\neg p_4 \to p_1)$.	*5.* $\neg(p_4 \wedge \neg p_1)$.
2. $\neg p_2 \to p_3$.	*4.* $\neg p_4 \vee p_1$.	*6.* $p_4 \to p_1$.

Exercício 2.4. *Verifique que $\alpha \to \beta$ e $\neg\alpha \vee \beta$ têm sempre o mesmo valor lógico em qualquer valoração. Qual é a fórmula escrita somente com $\wedge$, $\vee$ e $\neg$ que sempre tem o mesmo valor lógico de $\alpha \leftrightarrow \beta$ em qualquer valoração?*

O primeiro resultado da semântica da lógica proposicional que demonstraremos diz que o valor-verdade de uma fórmula depende somente dos valores de suas subfórmulas *atômicas*, como mostra o seguinte resultado.

Metateorema 2.5. *Sejam u e w duas valorações de $\mathscr{L}_0$. Se $\alpha \in \mathscr{L}_0$ é uma fórmula tal que $u(p) = w(p)$ para toda fórmula atômica $p \in \mathrm{Sf}(\alpha)$, então $u(\alpha) = w(\alpha)$.*

Demonstração. A demonstração é por indução na estrutura das fórmulas. Sejam u e w duas valorações de $\mathscr{L}_0$. Seja $\alpha \in \mathscr{L}_0$ uma fórmula tal que $u(p) = w(p)$ para toda subfórmula atômica $p \in \mathrm{Sf}(\alpha)$.

Se α é fórmula atômica então é imediato que $u(\alpha) = w(\alpha)$. Assuma que α não é fórmula atômica e que o resultado vale para as subfórmulas próprias de α.

Se α é $\neg\beta$. Pela hipótese indutiva $u(\beta) = w(\beta)$, logo $1 - u(\beta) = 1 - w(\beta)$, portanto $u(\alpha) = w(\alpha)$.

Se α é $\beta \vee \gamma$. Pela hipótese indutiva $u(\beta) = w(\beta)$ e $u(\gamma) = w(\gamma)$, então $\max(u(\beta), u(\gamma)) = \max(w(\beta), w(\gamma))$, portanto $u(\alpha) = w(\alpha)$.

Se α é $\beta \wedge \gamma$. Pela hipótese indutiva $u(\beta) = w(\beta)$ e $u(\gamma) = w(\gamma)$, então $\min(u(\beta), u(\gamma)) = \min(w(\beta), w(\gamma))$, portanto $u(\alpha) = w(\alpha)$.

Se α é $\beta \to \gamma$ e $u(\beta) = w(\beta)$ e $u(\gamma) = w(\gamma)$ então $1 - w(\beta) = 1 - u(\beta)$, portanto, $w(\beta \to \gamma) = \max(1 - w(\beta), w(\gamma)) = \max(1 - u(\beta), u(\gamma)) = u(\beta \to \gamma)$. Logo $w(\alpha) = u(\alpha)$.

Se α é $\beta \leftrightarrow \gamma$ e $u(\beta) = w(\beta)$ e $u(\gamma) = w(\gamma)$, então pelo exercício 2.1 $w(\beta \leftrightarrow \gamma) = 1 - |w(\beta) - w(\gamma)| = 1 - |u(\beta) - u(\gamma)| = u(\beta \leftrightarrow \gamma)$. Logo $w(\alpha) = u(\alpha)$.

Pelo princípio de indução para fórmulas, para toda FBF α tal que u e w coincidem nas subfórmulas atômicas vale que $u(\alpha) = w(\alpha)$. ■

Uma valoração v **estende** uma interpretação w se elas coincidem nas fórmulas atômicas, isto é, para todo símbolo proposicional atômico p (que é fórmula) vale que $v(p) = w(p)$. Notemos que v é uma função definida sobre fórmula e que w é uma função definida sobre os símbolos atômicos. O próximo resultado demonstra que para cada v há uma única w que estende v, portanto, para definir uma valoração basta ter uma interpretação.

Corolário 2.6 (Extensão única de uma interpretação). *Dada uma interpretação $v : \{p_1, p_2, \dots\} \to \{0,1\}$, existe uma única valoração $w : \mathscr{L}_0 \to \{0,1\}$ tal que $w(p) = v(p)$ para toda fórmula atômica p.*

Demonstração. Sejam u e w duas valorações que estendem v. Suponha que

$$\{\alpha \in \mathscr{L}_0 : w(\alpha) \neq u(\alpha)\} \neq \varnothing.$$

Tome α nesse conjunto cujo grau seja mínimo. O grau é positivo pois α não é atômica.

Se α é atômica então $w(\alpha) = v(\alpha) = u(\alpha)$, por definição, portanto α ou é $\neg\beta$ ou é $\beta \square \gamma$.

Se α é $\neg\beta$ então temos $\mathrm{grau}(\beta) < \mathrm{grau}(\alpha)$ (exerc. 7, pág. 28), portanto $w(\beta) = u(\beta)$ donde deduzimos que $w(\alpha) = 1 - w(\beta) = 1 - u(\beta) = u(\alpha)$.

Se α é $\beta \square \gamma$ então temos $\mathrm{grau}(\beta), \mathrm{grau}(\gamma) < \mathrm{grau}(\alpha)$ portanto $w(\beta) = u(\beta)$ e $w(\gamma) = u(\gamma)$. Assim, qualquer que seja $\square \in \{\wedge, \vee, \to, \leftrightarrow\}$ teremos $w(\alpha) = u(\alpha)$. ■

A única valoração que estende a interpretação v é denotada $\hat{v}$.

Dizemos que a valoração $w : \mathscr{L}_0 \to \{0,1\}$ **satisfaz** α ou, ainda, α é **satisfazível** ou **verdadeira** para w se, e somente se, $w(\alpha) = 1$ e escrevemos

$$w \vDash \alpha.$$

2.1.1 Interpretação de uma fórmula

Usando o Metateorema 2.5 podemos estabelecer que o valor de uma fórmula fica determinada de foma não ambígua por uma atribuição de valor-verdade 0 ou 1 para cada uma das suas fórmulas atômicas.

Por exemplo, uma interpretação da fórmula $p \to (q \vee s)$ é dada por uma atribuição de valor-verdade 0 ou 1 para p, q e s, por exemplo[2]

$$p \rightsquigarrow 0,\ q \rightsquigarrow 1,\ s \rightsquigarrow 0$$

e, nesse caso, respeitando as condições de uma valoração, temos que a fórmula $p \to (q \vee s)$ assume o valor-verdade 1.

2.1.2 Tautologia e contradição

Dizemos que uma fórmula é uma **tautologia** se o valor-verdade da fórmula é sempre 1, ou seja, $v \vDash \alpha$ para toda valoração v e nesse caso simplesmente escrevemos

$$\vDash \alpha.$$

Temos, por exemplo, que $p_1 \to (p_2 \to p_1)$, $\neg(p_1 \wedge \neg p_1)$ e $(\neg p_1 \vee p_2) \leftrightarrow (p_1 \to p_2)$ são tautologias. Duas das tautologias notáveis são (os esquemas)

1. a lei da não-contradição: $\neg(\alpha \wedge (\neg\alpha))$ e
2. a lei do terceiro excluído: $\alpha \vee (\neg\alpha)$.

Vamos verificar a *não-contradição*. Seja v uma interpretação qualquer e temos

$$\begin{aligned} \hat{v}(\neg(\alpha \wedge \neg\alpha)) &= 1 - \hat{v}(\alpha \wedge \neg\alpha) \\ &= 1 - \min(\hat{v}(\alpha), \hat{v}(\neg\alpha)) \\ &= 1 - \min(\hat{v}(\alpha), 1 - \hat{v}(\alpha)) = 1 - 0 = 1. \end{aligned}$$

Mais **tautologias notáveis** são dadas abaixo:

3. comutatividade: $(\alpha \vee \beta) \leftrightarrow (\beta \vee \alpha)$ e $(\alpha \wedge \beta) \leftrightarrow (\beta \wedge \alpha)$;
4. associatividade: $((\alpha \vee \beta) \vee \gamma) \leftrightarrow (\alpha \vee (\beta \vee \gamma))$ e $((\alpha \wedge \beta) \wedge \gamma) \leftrightarrow (\alpha \wedge (\beta \wedge \gamma))$;
5. distributividade: $(\alpha \wedge (\beta \vee \gamma)) \leftrightarrow ((\alpha \wedge \beta) \vee (\alpha \wedge \gamma))$ e $(\alpha \vee (\beta \wedge \gamma)) \leftrightarrow ((\alpha \vee \beta) \wedge (\alpha \vee \gamma))$;
6. absorção: $\alpha \vee (\alpha \wedge \beta) \leftrightarrow \alpha$ e $\alpha \wedge (\alpha \vee \beta) \leftrightarrow \alpha$;
7. idempotência: $(\alpha \vee \alpha) \leftrightarrow \alpha$ e $(\alpha \wedge \alpha) \leftrightarrow \alpha$;
8. involução ou dupla negação: $\alpha \leftrightarrow \neg(\neg\alpha)$;
9. leis de De Morgan: $\neg(\alpha \vee \beta) \leftrightarrow ((\neg\alpha) \wedge (\neg\beta))$ e $\neg(\alpha \wedge \beta) \leftrightarrow ((\neg\alpha) \vee (\neg\beta))$.

Vamos ver um exemplo verificando diretamente a *dupla negação*. Seja v uma interpretação qualquer e temos $\hat{v}(\neg\neg\alpha) = 1 - \hat{v}(\neg\alpha) = 1 - (1 - \hat{v}(\alpha)) = \hat{v}(\alpha)$, portanto

$$\begin{aligned} \hat{v}(\alpha \leftrightarrow \neg\neg\alpha) &= \max(\min(\hat{u}(\alpha), \hat{u}(\neg\neg\alpha)), \min(1 - \hat{u}(\alpha), 1 - \hat{u}(\neg\neg\alpha))) \\ &= \max(\hat{u}(\alpha), 1 - \hat{u}(\alpha)) \\ &= 1 \end{aligned}$$

Do exercício 2.4 temos as tautologias

[2] $p \rightsquigarrow 0$ significa que a p é atribuído o valor-verdade 0.

10. implicação: $(\alpha \to \beta) \leftrightarrow (\neg\alpha \vee \beta)$,
11. bi-implicação: $(\alpha \leftrightarrow \beta) \leftrightarrow \big((\alpha \to \beta) \wedge (\beta \to \alpha)\big)$.

Uma bi-implicação tautológica bastante útil é

12. negação da implicação: $\neg(\alpha \to \beta) \leftrightarrow (\alpha \wedge (\neg\beta))$.

De fato é tautologia pois para qualquer valoração w temos que $w(\neg(\alpha \to \beta)) = w(\neg(\neg\alpha \vee \beta))$ pela tautologia da bi-implicação acima e $w(\neg(\neg\alpha \vee \beta)) = w(\neg\neg\alpha \wedge \neg\beta) = w(\alpha \wedge \neg\beta)$ pela lei de De Morgan e dupla negação. Portanto, para qualquer que seja a valoração w sempre vale que $w(\neg(\alpha \to \beta)) = w(\alpha \wedge \neg\beta)$ de modo que a bi-implicação da *negação da implicação* é uma tautologia.

Exercício 2.7 (Contrapositiva). *A seguinte tautologia, por sua utilidade, também faz parte da lista das notáveis e é chamada de contrapositiva*

$$\big(\alpha \to \beta\big) \leftrightarrow \big((\neg\beta) \to (\neg\alpha)\big).$$

Verifique que a fórmula acima é uma tautologia.

Dizemos que uma fórmula é uma **contradição** se seu valor verdade for 0 em qualquer interpretação. Certamente, as fórmulas $\neg(p_1 \vee \neg p_1)$ e $\neg(p_2 \to p_2)$ são contradições. Também, a negação de uma tautologia é uma contradição.

Metateorema 2.8. *α é uma tautologia se, e só se, $\neg\alpha$ é uma contradição.*

Demonstração. Exercício. ■

Se para $\alpha \in \mathscr{L}_0$ há valoração u tal que $u(\alpha) = 0$ e há valoração v tal que $v(\alpha) = 1$ então chamamos α de **contingência**.

Implicações tautológicas

As implicações tautológicas, ou tautologias do esquema $\alpha \to \beta$, são importantes nos sistemas lógicos, elas validam os mecanismos sintáticos de dedução. Algumas das implicações tautológicas notáveis da lógica proposicional são

13. lei da adição: $\alpha \to (\alpha \vee \beta)$,
14. lei da simplificação: $(\alpha \wedge \beta) \to \alpha$,
15. *modus ponens*: $(\alpha \wedge (\alpha \to \beta)) \to \beta$,
16. *modus tollens*: $((\neg\beta) \wedge (\alpha \to \beta)) \to \neg\alpha$,
17. silogismo disjuntivo: $((\alpha \vee \beta) \wedge \neg\alpha) \to \beta$,
18. silogismo hipotético: $((\alpha \to \beta) \wedge (\beta \to \gamma)) \to (\alpha \to \gamma)$,
19. redução ao absurdo: $((\alpha \wedge (\neg\beta)) \to (\gamma \wedge (\neg\gamma))) \to (\alpha \to \beta)$.
20. redução ao absurdo: $((\alpha \to \beta) \wedge (\alpha \to \neg\beta)) \to \neg\alpha$.

Exercício 2.9. *Verifique o valor-verdade das fórmulas listadas acima.*

2.1.3 Abreviações

Note que na fórmula

$$((\alpha \wedge (\neg\beta)) \rightarrow (\gamma \wedge (\neg\gamma))) \rightarrow (\alpha \rightarrow \beta)$$

o papel da subfórmula $\gamma \wedge (\neg\gamma)$ é simplesmente "expressar uma falsidade", ou seja, uma contradição. Usaremos o símbolo $\perp$ para expressar uma contradição qualquer, ou seja, esse símbolo representa uma fórmula cuja valoração é 0 em qualquer interpretação e o usamos sempre que a fórmula propriamente dita for irrelevante para a situação em discurso.

A rigor, dizemos que $\perp$ abrevia a fórmula $p_1 \wedge (\neg p_1)$. Ademais $\top$ abrevia $\neg\perp$. A fórmula acima fica reescrita como $((\alpha \wedge (\neg\beta)) \rightarrow \perp)) \rightarrow (\alpha \rightarrow \beta)$.

Exercício 2.10. *Verifique que são tautologias:*

21. *complemento:* $(\alpha \wedge (\neg\alpha)) \leftrightarrow \perp$ *e* $(\alpha \vee (\neg\alpha)) \leftrightarrow \top$*;*
22. *elemento neutro:* $(\alpha \vee \perp) \leftrightarrow \alpha$ *e* $(\alpha \wedge \top) \leftrightarrow \alpha$.

2.2 Consequência lógica

Começamos essa seção com um exemplo. Consideremos as seguintes sentenças atômicas

p: O time joga bem
q: O time ganha o campeonato.
r: O técnico é o culpado.
s: Os torcedores estão felizes.

com as quais formamos as seguintes sentenças compostas

$p \rightarrow q$: Se $\underbrace{\text{o time joga bem}}_{p}$, então $\underbrace{\text{o time ganha o campeonato}}_{q}$.

$\neg p \rightarrow r$: Se $\underbrace{\text{o time não joga bem}}_{\neg p}$, então $\underbrace{\text{o técnico é o culpado}}_{r}$.

$q \rightarrow s$: Se $\underbrace{\text{o time ganha o campeonato}}_{q}$ então $\underbrace{\text{os torcedores estão felizes}}_{s}$.

$\neg s$: Os torcedores não estão felizes.

Dessas premissas, podemos deduzir r: "O técnico é culpado"

$$\{p \rightarrow q, \neg p \rightarrow r, q \rightarrow s, \neg s\} \vdash r$$

Prova.

1.	$p \to q$	(premissa)
2.	$q \to s$	(premissa)
3.	$p \to s$	(SH 1,2)
4.	$\neg s$	(premissa)
5.	$\neg p$	(MT 3,4)
6.	$\neg p \to r$	(premissa)
7.	r	(MP 6,7)

Em uma abordagem semântica olhamos para todas as interpretações dos símbolos atômicos e fixamos aqueles que satisfazem as premissas concomitantemente. Como são 4 símbolos atômicos, a quantidade de interpretações possíveis é $2^4 = 16$. Dessas 16 apenas 1 interpretação satisfaz as premissas

p	q	r	s	$p \to q$	$\neg p \to r$	$q \to s$	$\neg s$
0	0	1	0	1	1	1	1

Se supomos que são verdadeiras as premissas

> Se o time joga bem então o time ganha o campeonato.
> Se o time não joga bem então o técnico é o culpado.
> Se o time ganha o campeonato então os torcedores estão felizes.
> Os torcedores não estão felizes.

então uma **conclusão lógica** é que "o técnico é culpado". Isso porque todas as interpretações que fazem as premissas verdadeiras tornam "o técnico é culpado" uma sentença verdadeira, escrevemos

$$\{p \to q, \neg p \to r, q \to s, \neg s\} \vDash r.$$

Assim, o análogo semântico para a dedução sintática representada pelo símbolo $\vdash$ é a dedução semântica, que chamamos de argumento válido, representada pelo símbolo $\vDash$.

Mudando as premissas, assumindo que são verdadeiras

> Se o time joga bem então o time ganha o campeonato.
> Se o time ganha o campeonato então os torcedores estão felizes.
> Os torcedores não estão felizes.

as interpretações que as satisfazem são

p	q	s	$p \to q$	$q \to s$	$\neg s$
0	0	0	1	1	1
0	1	0	1	1	1

donde **concluímos logicamente** $\neg p$, ou seja, o time não joga bem. Note que não podemos concluir nem que "o time ganhou o campeonato" (q) é verdadeira, nem que o "time não ganhou o campeonato" ($\neg q$) é verdadeira, pois as duas situações são possíveis. Porém, também podemos concluir $\neg s$.

Por outro lado, se agora supomos verdadeiras as premissas

Se o time joga bem então o time ganha o campeonato.
Se o time não joga bem então o técnico é o culpado.
Se o time ganha o campeonato então os torcedores estão felizes.

então não podemos concluir nenhuma das sentenças atômicas, nem suas negações, pois nas interpretações que tornam as premissas verdadeiras não há um *único* valor lógico para sentenças atômicas

p	q	r	s	$p \to q$	$\neg p \to r$	$q \to s$
0	0	1	0	1	1	1
0	0	1	1	1	1	1
0	1	1	1	1	1	1
1	1	0	1	1	1	1
1	1	1	1	1	1	1

2.2.1 Consequência lógica

Usamos letras gregas maiúsculas Γ, Λ, Σ, Ψ, Δ, Ω, Θ, Π, Φ para denotar **conjunto de fórmulas** tomadas de $\mathscr{L}_0$. Uma valoração w **satisfaz o conjunto** Γ se satisfaz cada fórmula do conjunto, isto é, $w(\alpha) = 1$ para todo $\alpha \in \Gamma$ e, se esse é o caso, dizemos que Γ é **satisfazível**, que w **satisfaz** ou é um **modelo** para Γ e denotamos tal fato por

$$w \vDash \Gamma.$$

Uma fórmula α é **consequência lógica** (ou **consequência semântica**) das fórmulas de Γ, fato denotado por

$$\Gamma \vDash \alpha$$

se, e só se, toda valoração w que satisfaz Γ também satisfaz α.

Usamos a notação

$$\Gamma \vDash \bot$$

para expressar que Γ *não é satisfazível.*

Exemplo 2.11. $\{(p \vee q) \to r\} \vDash p \to r$. De fato, seja v uma interpretação qualquer, então de $1 - \max(v(p), v(q)) \leq 1 - v(p)$ temos

$$\hat{v}((p \vee q) \to r) = \max\big(1 - \max(v(p), v(q)), v(r)\big) \leq \max\big(1 - v(p), v(r)\big) = \hat{v}(p \to r)$$

de modo que se $\hat{v}((p \vee q) \to r) = 1$ então $\hat{v}(p \to r) = 1$.

Exemplo 2.12. Temos que $\{(p \wedge q) \to r\} \nvDash p \to r$ pois se $v(p) = 1$ e $v(q) = v(r) = 0$ então $\hat{v}((p \wedge q) \to r) = 1$ mas $\hat{v}(p \to r) = 0$.

Simplificações de notação

- Ao invés de $\{\alpha\} \vDash \beta$ escrevemos $\alpha \vDash \beta$.
- Ao invés de $\{\alpha_1, \ldots, \alpha_n\} \vDash \beta$ escrevemos $\alpha_1, \ldots, \alpha_n \vDash \beta$.
- Ao invés de $\Gamma \cup \{\alpha\} \vDash \beta$ escrevemos $\Gamma, \alpha \vDash \beta$.

2.2.2 Propriedades básicas de $\vDash$

Metateorema 2.13. *A consequência semântica tem as seguintes propriedades.*

1. $\alpha \vDash \beta$ *se, e só se,* $\vDash \alpha \to \beta$.
2. $\Gamma, \alpha \vDash \beta$ *se, e só se,* $\Gamma \vDash \alpha \to \beta$.
3. $\{\alpha_1, \alpha_2 \dots, \alpha_n\} \vDash \beta$ *se, e só se,* $\vDash (\alpha_1 \wedge \alpha_2 \wedge \cdots \wedge \alpha_n) \to \beta$.

Demonstração. Para a demonstração de (1) suponhamos $\alpha \vDash \beta$. Seja w uma interpretação.

Se $\hat{w}(\alpha) = 0$ então $\hat{w}(\alpha \to \beta) = 1$ por definição. Se $\hat{w}(\alpha) = 1$ então $\hat{w}(\beta) = 1$, pois assumimos $\alpha \vDash \beta$, portanto, $\hat{w}(\alpha \to \beta) = 1$. Logo a implicação $\alpha \to \beta$ é uma tautologia, isto é, $\vDash \alpha \to \beta$.

Agora, assumamos $\vDash \alpha \to \beta$ e seja w uma interpretação. Se $\hat{w}$ satisfaz α então $\hat{w}(\beta) = 1$, pois $\alpha \to \beta$ é tautologia, portanto $\alpha \vDash \beta$.

A prova de (2) é análoga a prova de (1) e é deixada como exercício.

Para a demonstração de (3) suponha que $\{\alpha_1, \alpha_2 \dots, \alpha_n\} \vDash \beta$ e seja w uma interpretação. Se $\hat{w}(\alpha_1 \wedge \alpha_2 \wedge \cdots \wedge \alpha_n) = 0$ então $\hat{w}((\alpha_1 \wedge \alpha_2 \wedge \cdots \wedge \alpha_n) \to \beta) = 1$ por definição. Se $\hat{w}(\alpha_1 \wedge \alpha_2 \wedge \cdots \wedge \alpha_n) = 1$ então $\hat{w}(\beta) = 1$ por hipótese, portanto, $\hat{w}((\alpha_1 \wedge \alpha_2 \wedge \cdots \wedge \alpha_n) \to \beta) = 1$. Logo $(\alpha_1 \wedge \alpha_2 \wedge \cdots \wedge \alpha_n) \to \beta$ é tautologia.

Por outro lado, se $(\alpha_1 \wedge \alpha_2 \wedge \cdots \wedge \alpha_n) \to \beta$ é tautologia e w é uma interpretação tal que $\hat{w}(\alpha_1 \wedge \alpha_2 \wedge \cdots \wedge \alpha_n) = 1$, então, $\hat{w}(\beta) = 1$. ■

Exercício 2.14. *Sejam* $\alpha_1, \dots, \alpha_n$ *e* β *fórmulas. Mostre um algoritmo que decide se* β *é consequência lógica de* $\{\alpha_1, \dots, \alpha_n\}$.

Em particular, a partir da propriedade (2) do metateorema 2.13 e das tautologias notáveis (página 44) temos, por exemplo,

Modus Ponens	$\alpha, (\alpha \to \beta) \vDash \beta$
Modus Tollens	$(\neg\beta), \alpha \to \beta \vDash \neg\alpha$
Silogismo disjuntivo	$\alpha \vee \beta, \neg\alpha \vDash \beta$
Silogismo hipotético	$\alpha \to \beta, \beta \to \gamma \vDash \alpha \to \gamma$

Ademais, podemos novas deduzir tautologias de consequências lógicas

(i) de $\alpha, \beta \vDash \alpha \wedge \beta$ temos $\vDash \alpha \to (\beta \to (\alpha \wedge \beta))$,
(ii) de $\alpha \vee \beta, \alpha \to \gamma, \beta \to \gamma \vDash \gamma$ temos $\vDash (\alpha \to \gamma) \to ((\beta \to \gamma) \to (\alpha \vee \beta \to \gamma))$ usando (2) e temos $\vDash ((\alpha \to \gamma) \wedge (\beta \to \gamma)) \to (\alpha \vee \beta \to \gamma)$ usando (2) e, em seguida, usando (3) do metateorema 2.13,

e vice versa, deduzir consequências lógicas de tautologias, com por exemplo

(iii) de $\vDash (\alpha \wedge (\alpha \to \beta)) \to \beta$ temos $\alpha, (\alpha \to \beta) \vDash \beta$,
(iv) de $\vDash ((\alpha \to \gamma) \wedge (\beta \to \gamma)) \to (\alpha \vee \beta \to \gamma)$ temos $(\alpha \to \gamma), (\beta \to \gamma) \vDash (\alpha \vee \beta \to \gamma)$.

Exercício 2.15. *Verifique se vale a afirmação: Se* $\Gamma \vDash \alpha$*, então* $\Gamma, \beta \vDash \alpha$.

2.2.3 Equivalência lógica

Dizemos que as fórmulas α e β são **logicamente (ou semanticamente) equivalentes** se

$$\hat{v}(\alpha) = \hat{v}(\beta), \text{ para toda interpretação } v$$

e denotamos esse fato por $\alpha \equiv \beta$.

Notemos que se toda valoração que satisfaz α também satisfaz β e toda valoração que satisfaz β também satisfaz α então α é verdadeira se, e somente se, β é verdadeira. Assim,

$$\alpha \equiv \beta \text{ se, e somente se, } \alpha \vDash \beta \text{ e } \beta \vDash \alpha.$$

Também decorre dessa definição que $\alpha \equiv \beta$ é equivalente a dizer que $\alpha \leftrightarrow \beta$ é uma tautologia, isto é,

$$\alpha \equiv \beta \text{ se, e somente se, } \vDash \alpha \leftrightarrow \beta.$$

Todas as bi-implicações tautológicas notáveis da página 44 e seguintes são equivalências semânticas como, por exemplo,

comutatividade	$(\alpha \vee \beta) \equiv (\beta \vee \alpha)$
associatividade	$((\alpha \vee \beta) \vee \gamma) \equiv (\alpha \vee (\beta \vee \gamma))$
distributividade	$(\alpha \wedge (\beta \vee \gamma)) \equiv ((\alpha \wedge \beta) \vee (\alpha \wedge \gamma))$
absorção	$\alpha \vee (\alpha \wedge \beta) \equiv \alpha$
idempotência	$(\alpha \vee \alpha) \equiv \alpha$
dupla negação	$\alpha \equiv \neg\neg\alpha$
De Morgan	$\neg(\alpha \vee \beta) \equiv ((\neg\alpha) \wedge (\neg\beta))$
implicação	$\gamma \rightarrow \delta \equiv (\neg\gamma) \vee \delta$
bi-implicação	$\gamma \leftrightarrow \delta \equiv (\gamma \rightarrow \delta) \wedge (\delta \rightarrow \gamma)$
contrapositiva	$(\alpha \rightarrow \beta) \equiv ((\neg\beta) \rightarrow (\neg\alpha))$
negação da implicação	$\neg(\alpha \rightarrow \beta) \equiv (\alpha \wedge (\neg\beta))$.

só para citar algumas (e parcialmente, são duas as leis de De Morgan, por exemplo).

Equivalência lógica é uma relação de equivalência pois, para quaisquer fórmulas α, β, γ valem as propriedades

– reflexiva: $\alpha \equiv \alpha$
– simétrica: se $\alpha \equiv \beta$ então $\beta \equiv \alpha$
– transitiva: se $\alpha \equiv \beta$ e $\beta \equiv \gamma$, então $\alpha \equiv \gamma$.

Exemplo 2.16. A sequência de equivalências abaixo estabelece, por transitividade, que a fórmula $\neg(p \vee (\neg p \wedge q))$ é semanticamente equivalente a $\neg(p \vee q)$

$\neg(p \vee (\neg p \wedge q))$	$\equiv$	$\neg p \wedge \neg(\neg p \wedge q))$	por De Morgan
	$\equiv$	$\neg p \wedge (\neg\neg p \vee \neg q)$	por De Morgan
	$\equiv$	$\neg p \wedge (p \vee \neg q)$	por dupla negação
	$\equiv$	$(\neg p \wedge p) \vee (\neg p \wedge \neg q)$	por distributiva
	$\equiv$	$\perp \vee (\neg p \wedge \neg q)$	pela abreviação
	$\equiv$	$(\neg p \wedge \neg q)$	pela conjunção
	$\equiv$	$\neg(p \vee q)$	por De Morgan

2.2.4 Conjunto adequado de conectivos

Sejam α, β e γ fórmulas de $\mathscr{L}_0$ tais que α e β são semanticamente equivalentes e $\alpha \in \mathrm{Sf}(\gamma)$, i.e., γ é uma fórmula na qual α ocorre como subfórmula. Então, trocando uma ou mais das ocorrências de α por β em γ o resultado é uma fórmula δ de $\mathscr{L}_0$ semanticamente equivalente a γ.

Por exemplo, em $((p_1 \to p_2) \wedge ((\neg p_3) \vee (p_1 \to p_2)))$ trocamos as ocorrências de $p_1 \to p_2$ por $(\neg p_1) \vee p_2$ e obtemos $(((\neg p_1) \vee p_2) \wedge ((\neg p_3) \vee ((\neg p_1) \vee p_2)))$. Evidentemente

$$((p_1 \to p_2) \wedge ((\neg p_3) \vee (p_1 \to p_2))) \equiv (((\neg p_1) \vee p_2) \wedge ((\neg p_3) \vee ((\neg p_1) \vee p_2))).$$

Nesse sentido, por causa das equivalências lógicas da implicação, a saber $\gamma \to \delta \equiv (\neg\gamma) \vee \delta$ e da bi-implicação, $\gamma \leftrightarrow \delta \equiv (\gamma \to \delta) \wedge (\delta \to \gamma)$ em que essa última, por sua vez, pode ser escrita como $\gamma \leftrightarrow \delta \equiv (\neg\gamma \vee \delta) \wedge (\neg\delta \vee \gamma)$, é possível demonstrar o seguinte resultado que diz que toda a fórmula de $\mathscr{L}_0$ admite uma equivalente em que ocorrem apenas os conectivos $\neg, \wedge, \vee$.

Metateorema 2.17. *Para qualquer formula α de $\mathscr{L}_0$ existe uma fórmula $\alpha' \equiv \alpha$ tal que*

1. *α e α' têm os mesmos símbolos atômicos*
2. *em α' não ocorrem os conectivos $\to$ e $\leftrightarrow$.*

Demonstração. A prova é por indução. Se α é fórmula atômica então o enunciado fica automaticamente satisfeito pelo próprio α. Se α é $\neg\beta$, por hipótese existe $\beta' \equiv \beta$ que satisfaz o enunciado, portanto, $\neg\beta'$ é equivalente a α, tem os mesmos átomos, e não não ocorrem $\to$ e $\leftrightarrow$. Se α é $\beta\vee\delta$ ou se α é $\beta\wedge\delta$ o mesmo argumento vale.

Se α é $\beta \to \delta$. Por hipótese, existem $\beta' \equiv \beta$ e $\delta' \equiv \delta$ tal que $\beta' \to \delta' \equiv \beta \to \delta$ e $\beta' \to \delta'$ tem os mesmos átomos de $\beta \to \delta$. Então $\alpha \equiv (\neg\beta') \vee \delta'$ e essa última tem os mesmos átomos de α e não tem ocorrência de $\to$ e $\leftrightarrow$.

Se α é $\beta \leftrightarrow \delta$ então consideramos β' e δ' como no parágrafo anterior e temos que $\beta \leftrightarrow \delta \equiv (\neg\beta' \vee \delta') \wedge (\neg\delta' \vee \beta')$ e essa última fórmula tem os mesmos átomos de α e não tem ocorrência de $\to$ e $\leftrightarrow$.

Assim, pelo princípio de indução para fórmulas o enunciado do metateorema vale para toda fórmula $\alpha \in \mathscr{L}_0$. ■

Um conjunto de conectivos lógicos é **adequado** se para toda fórmula proposicional existe uma fórmula equivalente escrita somente com os conectivos do conjunto dado. O metateorema acima afirma que $\{\neg, \wedge, \vee\}$ é um conjunto adequado de conectivos.

Usando as leis de De Morgan e a dupla negação nós obtemos, como corolário desse metateorema, que $\{\neg, \wedge\}$ e $\{\neg, \vee\}$ são outros dois conjuntos adequados de conectivos pois, por exemplo, $\alpha \wedge \beta \equiv \neg(\neg\alpha) \vee (\neg\beta))$.

Exercício 2.18. *Demonstre que*

1. $\{\neg, \to\}$ *é um conjunto adequado de conectivos;*
2. $\{\neg, \leftrightarrow\}$ *não é um conjunto adequado de conectivos.*

Na formulação do sistema K nós optamos por usar todos os conectivos como primitivos. No entanto, a escolha poderia ser qualquer outro conjunto adequado de conectivos. Isso nos conduziria a outro sistema formal, equivalente ao sistema K no sentido de que teriam os mesmos teoremas.

2.3 Argumentos

Um **argumento** é uma sequência de fórmulas $\alpha_1, \alpha_2, \ldots, \alpha_n \therefore \beta$ e ele é **semanticamente válido** se, e só se,

$$\alpha_1, \alpha_2, \ldots, \alpha_n \vDash \beta$$

caso contrário é inválido. Em outras palavras, um argumento é válido se não pode ser o caso das premissas serem verdadeiras e a conclusão ser falsa.

São exemplos imediatos de argumentos válidos as regras *Modus Ponens*, *Modus Tollens*, *Silogismo disjuntivo* e o*Silogismo hipotético*. O argumento $\neg(p \wedge q), \neg p \vDash q$ é inválido pois se $v(p) = v(q) = 0$ então $\hat{v}(\neg(p \wedge q)) = \hat{v}(\neg q) = 1$ enquanto que $\hat{v}(q) = 0$.

Veremos mais adiante que a validade semântica é equivalente a sintática no caso do cálculo proposicional. Ademais, a validade depende da lógica subjacente e existem argumentos que válidos em um sistema lógico mas inválidos em outro. Um exemplo é a redução ao absurdo, válido na lógica clássica mas não na lógica intuicionista.

2.3.1 Exemplos em linguagem natural

Abaixo damos alguns exemplos de formalização de sentenças da linguagem natural.

Exemplo 2.19. Sócrates diz: "*Se eu sou culpado, eu devo ser punido. Eu sou culpado. Logo eu devo ser punido.*" Esse argumento é **logicamente correto** pois se o formalizamos com

p : "eu sou culpado"
q : "eu devo ser punido"

então $(p \to q) \wedge q \vDash q$ (Modus Ponens).

Exemplo 2.20. Sócrates diz: "*Se eu sou culpado, eu devo ser punido. Eu não sou culpado. Logo eu não devo ser punido.*"

Esse argumento é **não é logicamente correto** pois $(p \to q) \wedge \neg q \nvDash \neg q$, basta tomar v com $v(p) = 0$ e $v(q) = 1$.

Exemplo 2.21. Bob encontra dois *pendrives* A e B. Ele sabe que cada um deles contém, exclusivamente, ou um tesouro ou uma armadilha fatal. No *pendrive* A está escrito: "Pelo menos um desses dois *pendrive* contém criptomoedas." No *pendrive* B está escrito: "No *pendrive* A há uma armadilha fatal." Bob sabe que ambas as inscrições são verdadeiras, ou ambas são falsas. É possível Bob escolher um *pendrive* com a certeza de que ele vai encontrar as criptomoedas? Se este for o caso, qual *pendrive* ele deve abrir?

Seja a : "o *pendrive* A contém criptomoedas" e b : "o *pendrive* B contém criptomoedas", donde $\neg a$: "o *pendrive* A contém a armadilha" e $\neg b$: "o *pendrive* B contém a armadilha".

A inscrição no *pendrive* A é $a \vee b$ e no *pendrive* B é $\neg a$.

Ademais, temos a seguinte informação $\hat{v}(a \vee b \leftrightarrow \neg a) = 1$. Se a for verdadeiro, $\neg a$ é falso, portanto $a \vee b$ deve ser falso, o que é impossível. Logo a é falso. Se a é falso, $\neg a$ é verdadeiro, portanto $a \vee b$ deve ser verdadeiro e como a é falso, então b deve ser verdadeiro.

Assim, a interpretação buscada é $v(a) = 0$ e $v(b) = 1$, ou seja, Bob deve abrir o *pendrive* B.

Exemplo 2.22. Três caixas são apresentadas. Uma contém ouro, as outras duas estão vazias. Cada caixa tem estampada nela uma pista sobre o seu conteúdo; as pistas são: CAIXA 1: "O ouro não está aqui". CAIXA 2: "O ouro não está aqui". CAIXA 3: "O ouro está na caixa 2". Apenas uma mensagem é verdadeira, as outras são falsas. Qual caixa tem o ouro?

Seja p_i o átomo proposicional que representa "a caixa i tem ouro" para cada $i = 1, 2, 3$. "Uma caixa tem ouro e as outras estão vazias" é formalizado por

$$(p_1 \wedge \neg p_2 \wedge \neg p_3) \vee (\neg p_1 \wedge p_2 \wedge \neg p_3) \vee (\neg p_1 \wedge \neg p_2 \wedge p_3) \tag{2.1}$$

e "uma pista é verdadeira as outras duas são falsas" por

$$(\neg p_1 \wedge \neg\neg p_2 \wedge \neg p_2) \vee (\neg\neg p_1 \wedge \neg p_2 \wedge \neg p_2) \vee (\neg\neg p_1 \wedge \neg\neg p_2 \wedge p_2) \tag{2.2}$$

que é logicamente equivalente a

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

Agora, se p_1 é verdadeiro então 2.1 é equivalente a $(\neg p_2 \wedge \neg p_3)$, portanto, ambas variáveis proposicionais devem ser falsas.

Assim, deduzimos que a única interpretação que satisfaz (2.1) e (2.2) é $v(p_1) = 1$ e $v(p_2) = v(p_3) = 0$.

2.4 Álgebras booleanas

Uma álgebra booleana é uma estrutura algébrica $(A, \mathbf{0}, \mathbf{1}, \sqcup, \sqcap, \sim)$, em que A é um conjunto que aqui consideramos com pelo menos dois elementos, $\sqcup, \sqcap$ são operações binárias sobre A (isto é, funções $A \times A \to A$), $\sim$ uma operação unária sobre A (isto é, função $A \to A$) e $\mathbf{0}, \mathbf{1} \in A$ constantes. Essa estrutura deve satisfazer os seguintes axiomas: para quaisquer $x, y, z \in A$

1. comutatividade: $x \sqcup y = y \sqcup x$ e $x \sqcap y = y \sqcap x$;
2. associatividade: $x \sqcup (y \sqcup z) = (x \sqcup y) \sqcup z$ e $x \sqcap (y \sqcap z) = (x \sqcap y) \sqcap z$;
3. distributividade: $x \sqcap (y \sqcup z) = (x \sqcap y) \sqcup (x \sqcap z)$ e $x \sqcup (y \sqcap z) = (x \sqcup y) \sqcap (x \sqcup z)$;
4. complemento: $x \sqcap (\sim x) = \mathbf{0}$ e $x \sqcup (\sim x) = \mathbf{1}$;
5. absorção: $x \sqcup (x \sqcap y) = x$ e $x \sqcap (x \sqcup y) = x$.

Decorrem das propriedades enumeradas acima as seguintes propriedades que também valem para qualquer álgebra booleana

6. idempotência: $x \sqcup x = x$ e $x \sqcap x = x$;
7. elemento neutro: $x \sqcup \mathbf{0} = x$ e $x \sqcap \mathbf{1} = x$;
8. involução: $\sim\sim x = x$;
9. leis de De Morgan: $\sim (x \sqcup y) = (\sim x) \sqcap (\sim y)$ e $\sim (x \sqcap y) = (\sim x) \sqcup (\sim y)$.

São exemplos de álgebra booleana

- $\mathscr{B} = \left(\{0,1\}, 0, 1, \max, \min, \overline{}\right)$. Aqui $\max, \min$ têm seus significados habituais no domínio $\{0,1\}$ e $\overline{x} = 1 - x$.
- $\mathscr{P} = \left(\wp(X), \varnothing, X, \cup, \cap, ^{\complement}\right)$. Aqui X é um conjunto não vazio, $\cup$ e $\cap$ têm seus significados habituais para conjuntos e $^{\complement}(A) = A^{\complement}$ é o complemento do A com respeito a X.

Exercício 2.23. *Verifique que $\mathscr{B}$ e $\mathscr{P}$ são álgebras booleanas, isto é, satisfazem as propriedades 1–5. Também, reescreva as propriedades 6–9 para cada uma dessas álgebras booleanas.*

Exercício 2.24. *Deduza os enunciados dos itens 6–9 daqueles enunciados nos itens 1–5.*

2.4.1 Algebrização da lógica proposicional

A lógica proposicional pode ser tratada algebricamente. Os conectivos lógicos são interpretados como operadores da álgebra booleana $\mathscr{B}$. O $\wedge$ é interpretado como o operador min, o $\vee$ como max e o $\neg$ como o $\overline{}$. A implicação e a bi-implicação são interpretados em função do min e max.

Vimos que a equivalência lógica, denotada por $\equiv$, é uma relação de equivalência sobre $\mathscr{L}_0$. Com isso podemos tomar as classes de equivalência das fórmulas

$$[\alpha]_\equiv = \{\beta \in \mathscr{L}_0 \colon \beta \equiv \alpha\}$$

e o conjunto dessas classes é o *conjunto quociente* $\mathscr{L}_0/\equiv$. Nessas classes definimos as operações

- $\overline{[\alpha]_\equiv}$ é a classe de $\neg\alpha$, isto é, $[\neg\alpha]_\equiv$
- $[\alpha]_\equiv \sqcup [\beta]_\equiv$ é a classe de $\alpha \vee \beta$, isto é, $[\alpha \vee \beta]_\equiv$
- $[\alpha]_\equiv \sqcap [\beta]_\equiv$ é a classe de $\alpha \wedge \beta$, isto é, $[\alpha \wedge \beta]_\equiv$
- $\mathbf{1}$ é a classe de $\alpha \vee \neg\alpha$, isto é, $[\alpha \vee \neg\alpha]_\equiv$
- $\mathbf{0}$ é a classe de $\alpha \wedge \neg\alpha$, isto é, $[\alpha \wedge \neg\alpha]_\equiv$

e assim a estrutura $(\mathscr{L}_0/\equiv, \mathbf{0}, \mathbf{1}, \sqcup, \sqcap, -)$ é uma álgebra booleana, chamada **álgebra de Lindenbaum**.

A partir daí, podemos estudar a lógica de pelo menos dois pontos de vista equivalentes: a partir de uma linguagem, dando a gramática, os axiomas, as regras de inferência e definindo dedução (o método preferido dos filósofos, principalmente a partir de Russell) e pelo método algébrico (como preferem muitos matemáticos).

2.5 Exercícios

1. Verifique se cada uma das fórmulas abaixo é tautologia, contradição ou contingência

   a) $p \rightarrow (\neg(p \vee q))$
   b) $p \rightarrow (\neg(p \leftrightarrow q))$
   c) $(r \rightarrow q) \rightarrow ((p \leftrightarrow q) \rightarrow (p \rightarrow q))$
   d) $((p \rightarrow q) \wedge (q \wedge r)) \rightarrow (p \rightarrow r)$
   e) $(p \vee (q \wedge r)) \leftrightarrow ((\neg q \vee \neg r) \rightarrow p)$
   f) $p \vee (q \wedge (p \vee (\neg q \wedge r)))$
   g) $((p \rightarrow q) \wedge (q \wedge r)) \leftrightarrow (p \rightarrow r)$

2. Demonstre que as fórmulas abaixo são tautologias, use ou uma cadeia de equivalências como no exemplo 2.16 ou calcule diretamente da definição o valor-verdade para uma interpretação arbitrária como no exemplo da dupla-negação na página 44.

   a) $\neg(\neg p) \leftrightarrow p$
   b) $\neg(p \wedge q) \leftrightarrow (\neg p \vee \neg q)$
   c) $\neg(p \vee q) \leftrightarrow (\neg p \wedge \neg q)$
   d) $\neg(p \rightarrow q) \leftrightarrow (p \wedge \neg q)$
   e) $\neg(p \leftrightarrow q) \leftrightarrow (p \wedge \neg q) \vee (\neg p \wedge q)$

3. Para cada fórmula a seguir, escreva uma fórmula que seja logicamente equivalente à negação da fórmula mas que só ocorra símbolos atômicos negados (o exercício anterior pode ser útil).

   a) $(p \wedge q) \rightarrow r$
   b) $p \rightarrow (p \wedge q)$
   c) $p \leftrightarrow (q \vee r)$
   d) $p \vee (q \wedge (r \vee s))$
   e) $p \rightarrow (q \rightarrow r)$
   f) $\neg p \rightarrow (q \vee r)$
   g) $(p \vee q) \rightarrow (r \wedge s)$
   h) $p \vee (q \rightarrow r)$
   i) $(p \rightarrow q) \rightarrow (r \rightarrow s)$

4. Escreva a negação das seguintes sentenças da língua portuguesa.
   a) Se a canoa não virar então eu chego lá.
   b) Se eu fizer faculdade, eu vou cursar Matemática ou Física.
   c) Se chover ou fizer frio, eu vou ficar em casa ou vou para o cinema.
   d) Se eu estudar física, eu não vou estudar história, a menos que eu também estude português.
   e) Eu não ouço Beethoven quando leio Kafka, a menos que esteja chovendo e eu esteja deprimido.
5. Se $\big((\phi \rightarrow \tau) \wedge (\phi \rightarrow \neg\tau)\big)$ é uma tautologia então o que pode ser dito a respeito do valor-verdade de ϕ?
6. Determine se é verdadeiro ou falso (e justifique):

a) $\neg(p \to q) \equiv (\neg q) \wedge p$
b) $(p \to q) \equiv ((p \wedge \neg q) \to (s \wedge \neg s))$
c) $(p \to q) \equiv ((p \wedge \neg q) \to \neg p)$
d) $(p \to q) \equiv ((p \wedge \neg q) \to q)$

7. Verifique a equivalência

$$\alpha_1 \to \alpha_2 \to \cdots \to \alpha_n \equiv \alpha_1 \wedge \alpha_2 \wedge \cdots \wedge \alpha_{n-1} \to \alpha_n$$

para todo natural $n \geq 1$.

8. O conectivo lógico $\mathtt{c}$ é **definível** a partir dos conectivos $\mathtt{c}_1, \mathtt{c}_2, \cdots, \mathtt{c}_k$ se a fórmula $p \mathbin{\mathtt{c}} q$ é semanticamente equivalente a uma fórmula escrita com os conectivos $\mathtt{c}_1, \mathtt{c}_2, \cdots, \mathtt{c}_k$ e só envolve os átomos proposicionais p e q. Por exemplo, os conectivos $\vee$, $\to$ e $\leftrightarrow$ são definíveis a partir de $\neg$ e $\wedge$ pois

a) $p \vee q \equiv \neg(\neg p \wedge \neg q)$
b) $p \to q \equiv \neg(p \wedge \neg q)$
c) $p \leftrightarrow q \equiv \neg(p \wedge \neg q) \wedge \neg(q \wedge \neg p)$

a) Mostre que os conectivos $\vee$, $\wedge$ e $\leftrightarrow$ são definíveis a partir de $\neg$ e $\to$.
b) Mostre que os conectivos $\vee$, $\to$ e $\leftrightarrow$ são definíveis a partir de $\neg$ e $\wedge$.
c) Mostre que os conectivos $\wedge$, $\to$ e $\leftrightarrow$ são definíveis a partir de $\neg$ e $\vee$.

9. Mostre que se tratarmos a "falsidade" $\perp$ como um conectivo (0-ário), então $\vee, \wedge, \neg$ são definíveis a partir de $\perp$ e $\to$.

10. O `nand`, denotado por $\otimes$, é um conectivo lógico que satisfaz $w(p \otimes q) = 1 - \min(w(p), w(q))$ em qualquer valoração w, ou seja, tem a seguinte interpretação:

$w(p)$	$w(q)$	$w(p \otimes q)$
0	0	1
0	1	1
1	0	1
1	1	0

Mostre que todos os outros conectivos $(\wedge, \vee, \neg, \to, \leftrightarrow)$ são definíveis a partir do `nand`.

11. Repita o exercício anterior para o `nor`, denotado por $\oplus$, dado por $w(p \oplus q) = 1 - \max(w(p), w(q))$.

12. Sejam w uma interpretação para $\mathscr{L}_0$ e $\{\gamma_1, \gamma_2, \ldots, \gamma_n\}$ um subconjunto de fórmulas de $\mathscr{L}_0$.
a) Se $w \vDash \{\gamma_1, \gamma_2, \ldots, \gamma_n\}$ então $w \vDash \gamma_1 \wedge \gamma_2 \wedge \cdots \wedge \gamma_n$?
b) Se $w \vDash \gamma_1 \wedge \gamma_2 \wedge \cdots \wedge \gamma_n$ então $w \vDash \{\gamma_1, \gamma_2, \ldots, \gamma_n\}$?

13. Verifique as consequências e não-consequências semânticas abaixo.

a) $\alpha, \alpha \to \neg\beta \vDash \neg\beta$
b) $\alpha, \beta \to \alpha \nvDash \neg\beta$
c) $\alpha, \beta \to \alpha \nvDash \beta$
d) $\alpha, \beta \vDash \alpha \wedge \beta$
e) $\alpha_1, \alpha_2, \ldots, \alpha_n \vDash \alpha_1 \wedge \alpha_2 \wedge \cdots \wedge \alpha_n$
f) $\alpha \to \beta \vDash \neg\alpha \vee \beta$
g) $\neg\alpha \vee \beta \vDash \alpha \to \beta$
h) $\alpha \to \beta, \beta \to \gamma \vDash \alpha \to \gamma$?

14. Prove que a equivalência lógica é uma relação de equivalência em $\mathscr{L}_0$.
15. Determine se é verdadeiro ou falso (e justifique):

a) $\vDash (p \wedge (\neg p)) \to p$
b) $p \wedge q \vDash p$
c) $\{p \vee q, \neg p\} \vDash q$
d) $p \vDash p \vee q$
e) $\{p \to q,\ q \to r\} \vDash p \to r$
f) $\{p \to q,\ \neg q\}) \vDash \neg p$
g) $\{p \to q,\ p \to r\} \vDash p \to (q \wedge r)$

16. Dê um exemplo de fórmulas ϕ_1 e ϕ_2 tais que $\phi_1 \vDash \phi_2$ mas que $\phi_2 \nvDash \phi_1$.
17. Responda com justificativa:
   a) Se $\Gamma \vDash \phi$ e $\Gamma \vDash \tau$ então $\Gamma \vDash \phi \vee \tau$?
   b) Se $\Gamma \vDash \phi \vee \tau$ então $\Gamma \vDash \phi$ e $\Gamma \vDash \tau$?
   c) Se $\Gamma \vDash \phi$ e $\Gamma \vDash \tau$ então $\Gamma \vDash \phi \wedge \tau$?
   d) Se $\Gamma \vDash \phi \wedge \tau$ então $\Gamma \vDash \phi$ e $\Gamma \vDash \tau$?
   e) Se $\Gamma \vDash \phi \to \tau$ e $\Gamma \vDash \phi$ então $\Gamma \vDash \tau$?
   f) Se $\Gamma \vDash \phi \to \tau$ então $\Gamma \vDash (\gamma \to \phi) \to (\gamma \to \tau)$?
18. Use o item (2) do metateorema 2.13 para justificar a tautologia $p \to q \to p$. Faça o mesmo para $(p \to q \to r) \to (p \to q) \to (p \to r)$ e para $(p \to q) \to (q \to r) \to (p \to r)$ (atenção com a regra de omissão de parênteses).
19. Dado um conjunto Γ de fórmulas sobre n símbolos atômicos, demontre que se $|\Gamma| > 2^{2^n}$ então existem $\alpha, \beta \in \Gamma$ tais que $\vDash \alpha \leftrightarrow \beta$.
20. Quais argumentos abaixo são logicamente corretos? Justifique formalizando-os.
   a) Se eu sou culpado, eu devo ser punido. Eu devo ser punido. Logo eu sou culpado.
   b) Se Carlos ganhou a competição, então Mario ficou em segundo lugar ou Sérgio ficou em terceiro lugar. Sérgio não ficou em terceiro lugar. Logo, se Mario não chegou em segundo lugar, então Carlos não ganhou a competição.
   c) Se Carlo ganhou a competição, então Mario ficou em segundo lugar ou Sérgio ficou em terceiro lugar. Mario não ficou em segundo lugar. Logo, se Carlos ganhou a competição então Sérgio não ficou em terceiro lugar.
21. Formule os quebra-cabeças abaixo em linguagem da Lógica Proposicional e encontre uma solução.

   (A) Suponha que sabemos que: (1) Se Paulo é magro, então Carlo não é loiro ou Roberta não é alta. (2) Se Roberta é alta, então Sandra é adorável. (3) Se Sandra adorável e Carlo é loiro, então Paulo é magro. (4) Carlo é loiro. Podemos deduzir que Roberta não é alta?

   (B) Você está andando em um labirinto e de repente se depara com três caminhos possíveis: o caminho à sua esquerda é por uma via pavimentada com ouro, o caminho em frente é pavimentado com mármore, o caminho à direita é por uma via feita de pequenas pedras. Cada caminho é protegido por um guardião. Você conversa com os guardiões e isso é o que eles dizem:

- O guardião da via de ouro: "Esta via irá levá-lo direto para o centro. Além disso, se as pedras levá-lo para o centro, em seguida, também o mármore leva-o para o centro."
- O guardião da via de mármore: "Nem a via de ouro nem a de pedras leva-o para o centro."
- O guardião da rua de pedra: "Siga a via de ouro e você vai chegar ao centro, siga a de mármore e você estará perdido."

Dado que você sabe que todos os guardiões são mentirosos, é possível escolher um caminho com a certeza de que ele vai levar você para o centro do labirinto? Se esse é o caso, o caminho que você escolher?

(C) Huguinho, Zezinho e Luizinho se encontram presos em um calabouço escuro e frio (como eles chegaram lá é outra história). Depois de uma rápida pesquisa os meninos encontram três portas, a primeira vermelha, a segunda azul, e a terceira verde. Atrás de uma das portas há um caminho para a liberdade. Atrás das outras duas portas, no entanto, há um maldoso dragão que cospe fogo. Abrindo uma porta do dragão a morte é certa. Em cada porta há uma inscrição:

- Na porta vermelha: "A liberdade está atrás desta porta."
- Na porta azul: "A liberdade não está atrás desta porta."
- Na porta verde: "A liberdade não está atrás da porta azul."

Os meninos sabem que pelo menos uma das três inscrições é verdadeira e pelo menos uma é falsa, qual porta levaria os meninos para a liberdade.

22. (Enderton) Você está em uma terra habitada por pessoas que sempre dizem a verdade ou sempre falam falsidades. Você chega numa bifurcação na estrada e você precisa saber qual das dois caminhos leva à capital. Há um nativo nas proximidades, mas ele tem tempo apenas para responder a uma pergunta sim-ou-não. O que você pergunta para ele a fim de saber por qual estrada seguir?
23. Há três suspeitos de assassinato: Adams, Brown e Clark. Adams diz: "Eu não fiz isso. A vítima era um velho conhecido de Brown. Mas Clark odiava." Brown afirma que "eu não fiz isso. Eu não conhecia o cara. Além disso, eu estava fora da cidade tudo a semana." Clark diz: "Eu não fiz isso. Eu vi ambos Adams e Brown no cidade com a vítima naquele dia; um deles deve ter feito isso." Suponha que os dois homens inocentes estão falando a verdade, mas que o homem culpado pode não estar falando a verdade.
    Escreva os fatos como sentenças na Lógica Proposicional e resolva o crime.
24. Brown, Jones e Smith são suspeitos de um crime. Eles testemunham do seguinte modo:
    - Brown: "Jones é culpado e Smith é inocente".
    - Jones: "Se Brown é culpado então também é Smith".
    - Smith: "Eu sou inocente, mas pelo menos um dos outros é culpado".

    Sejam B, J e S as declarações "Brown é culpado", "Jones é culpado" e ""Smith é culpado", respectivamente.
    a) Expresse o testemunho de cada suspeito como uma fórmula proposicional.

b) Responda as seguintes perguntas:
   i. Existe uma valoração que satisfaz, concomitantemente, os três testemunhos?
   ii. O testemunho de um dos suspeitos segue (é consequência lógica) da de outro. Qual a partir do qual?
   iii. Supondo que todo mundo é inocente, quem cometeu perjúrio?
   iv. Supondo que todos os testemunhos são verdadeiros, quem é inocente e quem é culpado?
   v. Supondo que o inocente disse a verdade e os culpados disseram mentiras, quem é inocente e quem é culpado?

25. Determine quem é culpado de *doping*. Das 5 primeira declarações, 4 são verdadeiras e uma é falsa. A última declaração é verdadeira. Os suspeitos são: Silvia Danekova, Michael O'Reilly, Kleber Ramos, Adrian Zielinski, Chen Xinyi.
   a) Silvia disse: "Michael ou Kleber tomaram drogas, mas não os dois."
   b) Michael disse: "Adrian ou Silvia tomaram drogas, mas não os dois."
   c) Kleber disse: "Xinyi ou Michael tomaram drogas, mas não os dois."
   d) Adrian disse: "Kleber ou Xinyi tomaram drogas, mas não os dois."
   e) Xinyi disse: "Kleber ou Adrian tomaram drogas, mas não os dois."
   f) Tom disse: "se Adrian tomou drogas, então Kleber tomou drogas."

2.6 Correção

Um sistema dedutivo é dito **correto**, ou **válido**, se qualquer teorema nesse sistema dedutivo é válido em todas as interpretações da teoria semântica da linguagem sobre a qual esse sistema se baseia. No nosso caso o metateorema da correção afirma que qualquer teorema obtido no sistema dedutivo axiomático de Kleene, o qual denotamos por K, é uma tautologia da lógica proposicional.

Metateorema 2.25 (Teorema da correção). *O sistema formal* K *é correto, ou seja, se* $\vdash \alpha$ *então* $\vDash \alpha$.

Em um sistema dedutivo axiomático como o que estudamos a prova de correção se resume a verificar a validade dos axiomas e que as regras de inferência preservam a validade das fórmulas.

Já vimos que $\vDash (\alpha \wedge (\alpha \to \beta)) \to \beta$ e do Metateorema 2.13, página 49, temos $\alpha, \alpha \to \beta \vDash \beta$, ou seja, toda valoração que satisfaz α e $\alpha \to \beta$ deve satisfazer β, ou ainda, a regra de inferência *modus ponens* infere uma sentença verdadeira a partir de premissas verdadeiras. Além disso, o leitor pode verificar facilmente, que os axiomas do sistema K são tautologias. Assim, para demonstrar o teorema da correção vamos assumir as seguintes hipóteses, que

1. os axiomas (A1) – (A10) são tautologias;
2. se $\vDash \alpha$ e $\vDash \alpha \to \beta$ então $\vDash \beta$.

Disso é intuitivamente claro que se $\vdash \alpha$ então cada fórmula na prova de α é uma tautologia.

Demonstração do teorema da correção. A prova é por indução (matemática) no número de fórmulas na prova. Suponha $\vdash \alpha$ e seja $\theta_1, \theta_2, \ldots, \theta_{n-1}, \alpha$ uma prova de α com n fórmulas.

Para $i = 1$, temos que $\vDash \theta_1$ pois a única possibilidade que a definição de prova deixa é que tal fórmula seja um axioma que sabemos ser tatuologia.

Agora, fixe i inteiro, $i > 1$ e $i \leqslant n$, e assumamos que $\vDash \theta_1, \vDash \theta_2, \ldots, \vDash \theta_{i-1}$. Para a notação ser consistente tomamos $\theta_n = \alpha$.

Se θ_i é um axioma então $\vDash \theta_i$, senão θ_i é resultado de uma inferência (MP j,k) com $j, k < i$. Pela hipótese indutiva $\vDash \theta_j$ e $\vDash \theta_k$ edo uso de MP sabemos que θ_k é da forma $\theta_j \to \theta_i$. Logo temos $\vDash \theta_j$ e $\vDash \theta_j \to \theta_i$, portanto, vale que $\vDash \theta_i$.

Pelo princípio da indução matemática $\vDash \theta_j$ para todo j, em particular, $\vDash \alpha$. ■

Não é difícil adaptar a demonstração acima para acrescentar o caso em que as fórmulas da prova também possam ser tomadas de um conjunto de premissas Γ. Um sistema dedutivo é **fortemente correto**, ou correto no sentido forte, se qualquer sentença α da linguagem sobre a qual o sistema dedutivo é baseado e que é *deduzível* a partir de um conjunto Γ de sentenças da linguagem é também uma consequência lógica desse conjunto. Em símbolos: para quaisquer Γ e α como acima, se $\Gamma \vdash \alpha$, então $\Gamma \vDash \alpha$. Com tal demostração, temos a **correção forte** do sistema K.

Metateorema 2.26 (Teorema da correção forte). *O sistema formal* K *é fortemente correto, ou seja, se* $\Gamma \vdash \alpha$ *então* $\Gamma \vDash \alpha$.

Exercício 2.27. *Demonstre o metateorema da correção forte.*

Notemos que a correção nos dá um método para demonstrar *não* dedutibilidade pois se $\nvDash \alpha$ então $\nvdash \alpha$.

2.7 Consistência

Dizemos que um sistema dedutivo é **consistente**, ou **não contraditório**, se não for possível provar uma fórmula da sua linguagem e a negação dessa fórmula. Caso contrário, o sistema é dito **inconsistente** ou **contraditório**.

Claramente, o sistema K é consistente pois, se para alguma fórmula β da linguagem temos $\vdash \beta$ e $\vdash \neg\beta$ e então, $\vDash \beta$ e $\vDash \neg\beta$, o que é um absurdo pelo metateorema 2.8, na página 45.

Metateorema 2.28 (Teorema da consistência). *O sistema formal* K *é consistente.*

De um modo geral, dizemos que um conjunto de fórmulas Γ da linguagem $\mathscr{L}_0$ é **inconsistente** se é possível derivar uma contração, $\Gamma \vdash \bot$. Lembramos que $\bot$ abrevia o esquema $\alpha \wedge \neg\alpha$. Equivalentemente, Γ é inconsistente se para alguma fórmula α da linguagem temos $\Gamma \vdash \alpha$ e $\Gamma \vdash \neg\alpha$. Por exemplo, para qualquer fórmula α o conjunto $\{\alpha, \neg\alpha\}$ é, trivialmente, inconsistente.

Dizemos que Γ é **consistente** se não for inconsistente.

Exercício 2.29. *O conjunto* $\{\neg p_1 \wedge p_2 \to p_0, p_1 \to (\neg p_1 \to p_2), p_0 \leftrightarrow \neg p_2\}$ *é consistente?*

O seguinte resultado nos ajuda a resolver o exercício acima.

Lema 2.30 (Propriedades de conjuntos inconsistentes). *Se um conjunto de fórmulas* Γ *é inconsistente, então*

1. Γ *não é satisfazível;*
2. $\Gamma \vdash \alpha$ *para toda fórmula* α.

Demonstração. Seja Γ um conjunto inconsistente de fórmulas de $\mathscr{L}_0$ e β uma fórmula da linguagem tal que $\Gamma \vdash \beta$ e $\Gamma \vdash \neg\beta$.

Para demonstrar o item 1 basta observarmos que, pelo exercício 2.27 acima, o metateorema da correção forte, $\Gamma \vDash \beta$ e $\Gamma \vDash \neg\beta$, portanto não deve haver uma valoração que satisfaça Γ pois tal valoração faria α e $\neg\alpha$ verdadeira.

Para demonstrar o item 2 observamos que $\{\beta, \neg\beta\} \vdash \alpha$ para qualquer α pelo teorema 1.14 (lei de Duns Scotus). Pela regra do corte (página 32) de $\vdash$ concluímos que $\Gamma \vdash \alpha$ para qualquer fórmula α. ■

Lema 2.31. *Se* $\Gamma \nvdash \alpha$*, então* $\Gamma \cup \{\neg\alpha\}$ *é consistente.*

Demonstração. Seja $\Gamma \subset \mathscr{L}_0$ tal que $\Gamma \nvdash \alpha$. Nesse caso, pelo lema anterior (item 2), Γ consistente. Suponhamos que $\Gamma \cup \{\neg\alpha\}$ não seja consistente. Existe $\beta \in \mathscr{L}_0$ tal que $\Gamma \cup \{\neg\alpha\} \vdash \beta$ e $\Gamma \cup \{\neg\alpha\} \vdash \neg\beta$ e, pelo teorema da dedução (página 32), temos $\Gamma \vdash \neg\alpha \to \beta$ e $\Gamma \vdash \neg\alpha \to \neg\beta$.

Obtemos a partir do axioma (A3) aplicando o teorema da dedução, duas vezes, que

$$\neg\alpha \to \beta, \neg\alpha \to \neg\beta \vdash \neg\neg\alpha$$

e usando o axioma (A10) $\neg\neg\alpha \vdash \alpha$ logo concluímos com ajuda da regra do corte

$$\neg\alpha \to \beta, \neg\alpha \to \neg\beta \vdash \alpha.$$

Resumindo, temos $\Gamma \vdash \neg\alpha \to \beta$, $\Gamma \vdash \neg\alpha \to \neg\beta$ e $\{\neg\alpha \to \beta, \neg\alpha \to \neg\beta\} \vdash \alpha$ e da regra do corte concluímos $\Gamma \vdash \alpha$, um absurdo. Portanto, $\Gamma \cup \{\neg\alpha\}$ é consistente. ■

2.7.1 Consistência maximal de um conjunto de fórmulas

Um conjunto de fórmulas Γ é **consistente maximal** se

1. é consistente
2. $\Gamma \cup \{\beta\}$ é inconsistente para todo $\beta \not\in \Gamma$.

Ou seja, o conjunto Γ de fórmulas de $\mathscr{L}_0$ é consistente maximal se não pode ser aumentado com fórmulas da linguagem sem perder a consistência. Qualquer conjunto consistente de fórmulas ou é maximal ou pode ser "aumentado" até formar um, é o que diz o próximo metateorema.

Lema 2.32. *Se Γ é consistente então existe $\Delta \supseteq \Gamma$ consistente maximal.*

Demonstração. Seja $\theta_1, \theta_2, \ldots$ uma enumeração qualquer das fórmulas da linguagem $\mathscr{L}_0$. Definimos, indutivamente, a sequência de conjuntos de fórmulas pondo $L_0 = \Gamma$ e

$$L_{i+1} = \begin{cases} L_i \cup \{\theta_i\} & \text{se } L_i \cup \{\theta_i\} \text{ consistente} \\ L_i & \text{caso contrário,} \end{cases}$$

Agora, definimos $\Delta = \bigcup_{i \geq 0} L_i$. Pela construção temos que cada L_i é consistente. O conjunto Δ é consistente pois, caso contrário, $\Delta \vdash \beta \wedge \neg\beta$, para algum β. Mas, se esse é o caso então $L_i \vdash \beta \wedge \neg\beta$, para algum i (justifique), o que é uma contradição.

Ainda, Δ é maximalmente consistente. Seja $\alpha \in \mathscr{L}_0$ tal que $\alpha \not\in \Delta$. Existe um j tal que $\alpha = \theta_j$ e se $\alpha \not\in L_{j+1}$ é porque $L_j \cup \{\alpha\}$ é inconsistente, portanto $\Delta \cup \{\alpha\}$ é inconsistente. ■

Convém chamar a atenção para dois pontos importantes na demonstração acima cujas justificativas não daremos, mas não são tão óbvios quanto possa parecer (também não tão difícil quanto pode se sugerir): a existência da enumeração $\theta_1, \theta_2, \ldots$ e a existência de i tal que $L_i \vdash \beta \wedge \neg\beta$ (essa, de fato, é a mais fácil de justificar).

O próximo resultado estabelece uma "equivalência" entre dedutibilidade e pertinência com respeito a conjuntos consistentes maximais.

Lema 2.33. *Se Δ é consistente maximal então*

$$\Delta \vdash \alpha \text{ se, e só se, } \alpha \in \Delta$$

Demonstração. Fixamos um $\Delta \subset \mathscr{L}_0$ consistente maximal. Se $\alpha \in \Delta$ então $\Delta \vdash \alpha$, pela autodedução.

Agora, supomos que $\Delta \vdash \alpha$. Se $\alpha \not\in \Delta$ então, da maximalidade, temos que $\Delta \cup \{\alpha\}$ é inconsistente, isto é, $\Delta \cup \{\alpha\} \vdash \beta \wedge \neg\beta$ para alguma fórmula β. Pelo Teorema da Dedução $\Delta \vdash \alpha \to \beta \wedge \neg\beta$ e, como $\Delta \vdash \alpha$, obtemos $\Delta \vdash \beta \wedge \neg\beta$ contrariando o fato de Δ ser consistente. ∎

Vamos refinar o resultado desse lema a partir da leitura única, metateorema 1.5, página 24, escrevendo a condição de pertinência $\delta \in \Delta$ em função da única representação de δ.

Corolário 2.34. *Se Δ é consistente maximal então*

1. *$\neg\alpha \in \Delta$ se, e só se, $\alpha \not\in \Delta$;*
2. *$\alpha \wedge \beta \in \Delta$ se, e só se, $\alpha \in \Delta$ e $\beta \in \Delta$;*
3. *$\alpha \vee \beta \in \Delta$ se, e só se, $\alpha \in \Delta$ ou $\beta \in \Delta$;*
4. *$\alpha \to \beta \in \Delta$ se, e só se, $\neg\alpha \in \Delta$ ou $\beta \in \Delta$;*
5. *$\alpha \leftrightarrow \beta \in \Delta$ se, e só se, $\neg\alpha \in \Delta$ ou $\beta \in \Delta$ e $\neg\beta \in \Delta$ ou $\alpha \in \Delta$.*

Demonstração. O item 1 segue de

$$\begin{aligned} \neg\alpha \in \Delta &\text{ se e só se } \Delta \vdash \neg\alpha \text{ (pelo Lema acima)}\\ \Delta \vdash \neg\alpha &\text{ se e só se } \Delta \nvdash \alpha \text{ (pelo Lema 2.31 e consistência)}\\ \Delta \nvdash \alpha &\text{ se só se } \alpha \not\in \Delta \text{ (pelo Lema acima).} \end{aligned}$$

Detalhando a segunda linha, temos que se $\Delta \vdash \neg\alpha$ então $\Delta \nvdash \alpha$, caso contrário teríamos inconsistência. Por outro lado, $\Delta \nvdash \alpha$ implica que $\Delta \cup \{\neg\alpha\}$ é consistente, portanto $\neg\alpha \in \Delta$ de modo que $\Delta \vdash \neg\alpha$.

Para demonstrar o item 4 supomos que $\Delta \vdash \alpha \to \beta$. Do teorema da dedução $\Delta \vdash \alpha \to \beta$ se, e só se, $\Delta \cup \{\alpha\} \vdash \beta$.

Se $\alpha \in \Delta$ então $\Delta \cup \{\alpha\} \vdash \beta$ implica que $\beta \in \Delta$ (pelo Lema). Se $\alpha \not\in \Delta$, então $\neg\alpha \in \Delta$ (pelo item 1). Assim, $\beta \in \Delta$ ou $\neg\alpha \in \Delta$.

Agora, vamos supor que $\neg\alpha \in \Delta$ ou $\beta \in \Delta$. Se $\neg\alpha \in \Delta$, então $\Delta \cup \{\alpha\} \vdash \beta$ pela inconsistência das premissas, senão $\beta \in \Delta$, de modo que $\Delta \vdash \beta$ (pelo Lema).

Os outros itens são deixados como exercício. ∎

Lema 2.35. *Qualquer conjunto de fórmulas $\Delta \subset \mathscr{L}_0$ que satisfaz os cinco itens do corolário acima é satisfazível.*

Demonstração. Seja Δ um conjunto de fórmulas como no enunciado. Definimos uma interpretação $v \colon \{p_1, p_2, \dots\} \to \{0,1\}$ tomando

$$v(p) = 1 \text{ se, e somente se } p \in \Delta.$$

Pelo corolário 2.6, página 43, existe uma única valoração $\hat{v}$ que estende v para todas as fórmulas de $\mathscr{L}_0$. Vamos provar usando a indução para fórmulas da lógica proposicional que vale a seguinte propriedade

$$\alpha \in \Delta \textit{ se, e só se, } \hat{v}(\alpha) = 1.$$

Se α é uma fórmula atômica da linguagem então temos $\alpha \in \Delta$ se, e só se, $\hat{v}(\alpha) = 1$ pela definição da interpretação v e da extensão $\hat{v}$, portanto a propriedade acima vale para fórmulas atômicas.

Se α é uma fórmula lida como $\neg\beta$ e, por hipótese indutiva, vale: $\beta \in \Delta$ se, e só se, $\hat{v}(\beta) = 1$. Então, usando a propriedade estabelecida no item 1 do corolário anterior e a hipótese da indução

$$\begin{gathered}\neg\beta \in \Delta \text{ se, e só se, } \beta \notin \Delta\\ \beta \notin \Delta \text{ se, e só se, } \hat{v}(\beta) = 0\\ \hat{v}(\beta) = 0 \text{ se, e só se, } \hat{v}(\neg\beta) = 1\end{gathered}$$

portanto, $\alpha \in \Delta$ se, e só se, $\hat{v}(\alpha) = 1$.

Se α é lida $\beta \to \gamma$ e, por hipótese, valem: $\beta \in \Delta$ se, e só se, $\hat{v}(\beta) = 1$ e $\gamma \in \Delta$ se, e só se, $\hat{v}(\gamma) = 1$. Usando a propriedade estabelecida no item 4 4 do corolário anterior, a hipótese indutiva e a definição de valoração

$$\begin{gathered}\beta \to \gamma \in \Delta \text{ se, e só se, } \neg\beta \in \Delta \text{ ou } \gamma \in \Delta\\ \neg\beta \in \Delta \text{ ou } \gamma \in \Delta \text{ se, e só se, } \hat{v}(\neg\beta) = 1 \text{ ou } \hat{v}(\gamma) = 1\\ \hat{v}(\neg\beta) = 1 \text{ ou } \hat{v}(\gamma) = 1 \text{ se, e só se, } \hat{v}(\neg\beta \vee \gamma) = 1\\ \hat{v}(\neg\beta \vee \gamma) = 1 \text{ se, e só se, } \hat{v}(\beta \to \gamma) = 1.\end{gathered}$$

Portanto $\alpha \in \Delta$ se, e só se, $\hat{v}(\alpha) = 1$ quando α é lida como $\beta \to \gamma$.

Os outros casos, $\wedge$, $\vee$ e $\leftrightarrow$, são deixados como exercício. Pelo Princípio de Indução para Fórmulas concluímos que para toda fórmula bem formada α vale $\alpha \in \Delta$ se, e só se, α é satisfazível. ■

Pelo lema 2.30, página 61, se Γ é satisfazível então Γ é consistente. A recíproca dessa afirmação

$$\text{se } \Gamma \text{ é consistente então } \Gamma \text{ é satisfazível}$$

também vale.

Metateorema 2.36. *Para todo* Γ*, temos* Γ *consistente se, e só se,* Γ *é satisfazível.*

Demonstração. Se Γ é consistente,então podemos tomar $\Delta \supseteq \Gamma$ consistente maximal. Pelo corolario 2.34 Δ satisfaz as hipótese do lema 2.35, portanto Δ é satisfazível.

Como $\Gamma \subseteq \Delta$, temos que Γ é satisfazível. ■

2.8 Completude

Um sistema formal é dito **completo** com respeito a uma propriedade de fórmulas se toda fórmula tendo a propriedade pode ser deduzida nesse sistema, caso contrário, o sistema é dito **incompleto**. Em particular, um sistema formal é **semanticamente completo** se toda tautologia é um teorema lógico.

Um sistema formal é **fortemente completo**, ou completo no sentido forte, se para todo conjunto de premissas Γ, qualquer consequência lógica de Γ é um teorema de Γ.

Metateorema 2.37 (Teorema da Completude). *O sistema formal* K *é completo no sentido forte.*

Demonstração. Sejam Γ um conjunto qualquer de fórmulas de $\mathscr{L}_0$ e $\alpha \in \mathscr{L}_0$ uma fórmula qualquer.

Suponhamos que $\Gamma \vDash \alpha$ mas $\Gamma \nvdash \alpha$. Se $\Gamma \nvdash \alpha$ então $\Gamma \cup \{\neg\alpha\}$ é consistente, pelo lema 2.31. Se é consistente então é satisfazível, pelo metateorema 2.36, mas tal sentença é uma contradição pois toda valoração que satisfaz Γ também satisfaz α. ■

2.9 Decidibilidade

Um conjunto de fórmulas $\Sigma \subset \mathscr{L}_0$ é **decidível** se existe um algoritmo que recebe uma fórmula $\alpha \in \mathscr{L}_0$ e responde corretamente "$\alpha \in \Sigma$?".

Um tipo de pergunta que nos interessa em Lógica é: dados fórmulas lógicas $\alpha_1, \alpha_2, \dots, \alpha_n, \beta$ e uma relação de dedução $\vdash$ decidir

$$\alpha_1, \alpha_2, \dots, \alpha_n \vdash \beta?$$

Um conjunto que não é decidível é dito **indecidível**. Por exemplo, é possível mostrar que a cardinalidade do conjunto dos algoritmos de decisão é enumerável[3], entretanto, a cardinalidade do conjunto das partes de $\mathscr{L}_0$ não é enumerável[4] de modo que há subconjuntos não decidíveis, portanto, demonstra-se que alguns subconjuntos de $\mathscr{L}_0$ não são decidíveis.

Antes de seguir adiante, precisamos dizer o que entendemos por algoritmo. Um **algoritmo** define sem ambiguidade uma sequência finita de passos para resolver um problema computacional. Um *problema computacional*, por sua vez, é caracterizado por um conjunto de *instâncias* (ou entradas), um conjunto de *respostas* e uma *relação* que associa instâncias a respostas. Por exemplo, o problema "Multiplicar dois inteiros positivos" tem como instâncias pares (n, m) de inteiros positivos e como respostas inteiros positivos. A relação que se quer computar é

[3] Isso quer dizer que existe função bijetiva do conjunto dos algoritmos de decisão para o conjunto dos números naturais.

[4] Isso quer dizer que não existe uma função injetiva do conjunto das partes de $\mathscr{L}_0$ para o conjunto dos números naturais.

definida pelos pares $((n,m),z)$ de instâncias e respostas tais que $n \cdot m = z$. Notemos que entre instâncias e respostas temos uma relação e não uma função pois é possível que uma instância esteja associada a mais de uma resposta. Por exemplo, se as instâncias são fórmulas da lógica proposicional e as respostas são valorações das variáveis com verdadeiro ou falso e que tornam a fórmula verdadeira, então a instância $p_1 \vee p_2$ tem três respostas possíveis.

A noção de algoritmo é dada formalmente por uma Máquina de Turing, que não definiremos aqui. Os algoritmos são, geralmente, descritos no que costumamos chamar de *pseudocódigo*, uma mistura de algumas palavras-chave em português com sentenças construídas como em uma linguagem de programação estruturada como a linguagem C. Todo programa em linguagem C tem uma Máquina de Turing equivalente e vice-versa, logo tudo que um decide ou outro também decide.

De certo modo, um algoritmo é uma solução para um problema computacional. Alguns problemas não têm solução, problemas computacionalmente indecidíveis bem conhecidos são, por exemplo,

- o *Entscheidungsproblem* proposto por David Hilbert e Wilhelm Ackermann em 1928: o problema de decidir se uma fórmula da lógica de primeira ordem é logicamente válida ou não em todo modelo. Foi para tratar esse problema que Alan Turing concebeu as Máquinas de Turing. A completude da lógica de primeira ordem foi estabelecida por Gödel em 1928 de modo que o problema pode ser posto como: decidir se uma fórmula da lógica de primeira ordem é deduzível naquela lógica;
- o décimo problema de Hilbert: decidir se uma equação polinomial com coeficientes inteiros e um número finito de incógnitas tem uma solução com todas as incógnitas assumindo valores inteiros. Não existe um algoritmo para tal problema como foi demonstrado por Martin Davis, Yuri Matiyasevich, Hilary Putnam e Julia Robinson;
- o problema da parada: é o problema de decidir se um dado programa e uma entrada arbitrária para esse programa terminará a execução ou executará para sempre. Alan Turing provou em 1936 que um algoritmo para o problema de parada não pode existir.

Assumimos daqui em diante que o alfabeto $\mathscr{A}_0$ que definimos para a Lógica Proposicional é decidível.

Exercício 2.38. *Mostre um algoritmo que recebe uma cadeia α de caracteres do alfabeto $\mathscr{A}_0$ e decide se α é uma fórmula bem formada da lógica proposicional.*

Exercício 2.39. *Justifique a sentença: se Σ é um conjunto finito de fórmulas de $\mathscr{L}_0$, então Σ é decidível.*

Os conjuntos indecidíveis são infinitos. Um conjunto Σ é chamado de **recursivamente enumerável** se existe um algoritmo que enumera os membros de Σ, isso significa que sua saída é simplesmente uma lista de todos os membros de Σ: $\sigma_1, \sigma_2, \sigma_3, \ldots$.

Se Σ for infinito esse algoritmo será executado para sempre, porém, se se quer decidir "$\alpha \in \Sigma$?" então sempre que a resposta for *sim* o algoritmo encontra α em tempo finito. Denotemos por A um algoritmo que enumera as fórmulas de Σ. Para decidir "$\alpha \in \Sigma$?" escrevemos um algoritmo B que com entrada α:

1. executa o algoritmo A para imprimir $\sigma_1, \sigma_2, \dots$ e para cada i
   1.a. se $\sigma_i = \alpha$ termina a execução de A e responde *sim*.

Se $\alpha \in \Sigma$ o algoritmo B termina e responde *sim*; se $\alpha \notin \Sigma$ o algoritmo B não termina.

Agora, suponha que exista um algoritmo C que com qualquer fórmula α responde *sim* se, e somente se, $\alpha \in \Sigma$. Podemos um algoritmo D que usa C para construir uma enumeração $\sigma_1, \sigma_2, \dots$ de Σ. Como fórmula α o algoritmo D:

1. cria uma lista L vazia;
2. enumera todas as fórmulas $\alpha_1, \alpha_2, \dots$;
3. para cada $k = 1, 2, \dots$
   3.a. para cada $j = 1, 2, \dots, i$ tal que $\alpha_j \notin L$
      3.a.1. executa C por $10k$ passos para decidir "$\alpha_j \in \Sigma$?";
      3.a.2. se respondeu sim para α_j então acrescente-a em L e imprima.

Desse modo, concluímos que Σ é recursivamente enumerável.

Do exposto acima, no exercício e no parágrafo que o precede, podemos concluir a seguinte equivalência à definição de recursivamente enumerável.

Lema 2.40. *Um conjunto de fórmulas $\Sigma \subset \mathscr{L}_0$ é recursivamente enumerável se, e somente se, existe um algoritmo que para cada fórmula α responde* sim *se e só se $\alpha \in \Sigma$.*

Notemos que no caso $\alpha \notin \Sigma$ para um conjunto recursivamente enumerável o algoritmo que o lema acima afirma existir poderá responder *não* ou executar indefinidamente, sem nunca terminar.

Agora, estabelecemos duas propriedades importantes sobre conjuntos recursivamente enumeráveis quaisquer.

Metateorema 2.41 (Teorema de Post). *$\Sigma \subset \mathscr{L}_0$ é decidível se e somente se ele e seu complemento são recursivamente enumeráveis.*

Demonstração. Se $\Sigma \subset \mathscr{L}_0$ é decidível então existe um algoritmo A que com fórmula α responde *sim* se $\alpha \in \Sigma$ e responde *não* se $\alpha \notin \Sigma$. Pelo lema 2.40 o conjunto Σ é recursivamente enumerável. Para o complemento, escrevemos um algoritmo B que com entrada α:

1. executa o algoritmo A com entrada α;
2. se A respondeu sim, então responda *não*;
3. se A respondeu não, então responda *sim*.

Esse algoritmo B demonstra que o complemento do conjunto Σ, denotado por $\overline{\Sigma}$, é decidível, portanto, recursivamente enumerável, como demonstrado no parágrafo anterior.

Suponhamos agora que tanto Σ quanto $\overline{\Sigma}$ sejam recursivamente enumeráveis e sejam A e B os algoritmos que o lema 2.40 afirma existirem para Σ e $\overline{\Sigma}$ respectivamente. Escrevemos um algoritmo C que com uma fórmula α:

1. Executa, sequencialmente, um passo de A com fórmula α;
2. Executa, sequencialmente, um passo de B com fórmula α;
3. Se A respondeu sim, responda *sim* ou se B respondeu sim, responda *não*; senão volte para 1.

Assim, se $\alpha \in \Sigma$ então esse fato é eventualmente reconhecido pelo algoritmo A e C responderá *sim*. Senão, $\alpha \notin \Sigma$, ou seja $\alpha \in \overline{\Sigma}$, e esse fato é eventualmente reconhecido pelo algoritmo B e C responderá *não*. Portanto, C decide pertinência em Σ. ∎

Metateorema 2.42 (Teorema da enumerabilidade). *Se $\Sigma \subset \mathscr{L}_0$ é recursivamente enumerável então o conjunto das consequências (sintáticas) $\{\alpha \in \mathscr{L}_0 : \Sigma \vdash \alpha\}$ é recursivamente enumerável.*

Um esboço da demonstração é como segue. Dado α decidimos se $\Sigma \vdash \alpha$ avaliando $\Sigma \vDash \alpha$. Para avaliar $\Sigma \vDash \alpha$ usamos a enumerabilidade $\sigma_1, \sigma_2, \dots$ de Σ da seguinte forma, avaliamos "$\sigma_1 \vDash \alpha$?", "$\sigma_1, \sigma_2 \vDash \alpha$?", "$\sigma_1, \sigma_2, \sigma_3 \vDash \alpha$?", e assim por diante. Se $\Sigma \vDash \alpha$ então vai existir n natural tal que $\sigma_1, \sigma_2, \dots, \sigma_n \vDash \alpha$, nesse momento respondemos *sim*. Essa última afirmação segue da equivalência entre $\vdash$ e $\vDash$ e da observação que, como jã vimos, se $\Gamma \vdash \alpha$ então $\Sigma \vDash \alpha$ para algum Σ finito, pois prova é finita assim baseada num número finito de premissas.

2.9.1 Tabela-verdade e a decidibilidade de K

O programa de Hilbert visava estabelecer a consistência, a completude e a decidibilidade da lógica clássica de primeira ordem, o que se mostrou impossível com os resultados de Gödel de 1931. Por decidibilidade de um sistema formal entendemos um algoritmo que em um número finito de passos decide se uma dada fórmula é ou não um teorema desse sistema. O problema de decisão é o de encontrar um tal algoritmo ou provar que ele não existe. No sistema K as tabelas-verdade fornecem um algoritmo de decisão para a Lógica Proposicional.

Vimos na seção 2.1.1 que o valor lógico de uma fórmula $\alpha \in \mathscr{L}_0$ numa valoração qualquer depende exclusivamente do valor lógico de seus símbolos atômicos e podemos concluir que, para analisarmos todos os possíveis valores-verdade que a fórmula α pode assumir, basta analisarmos todas as interpretações em um conjunto finito de fórmulas atômicas. Isso garante a existência de um algoritmo que, dado uma fórmula $\alpha \in \mathscr{L}_0$, descobre o valor-verdade de α em cada interpretação possível

(1) O primeiro passo para valorar uma fórmula é destrinchá-la nas subfórmulas.

(2) Em seguida, montamos uma tabela com uma coluna para cada subfórmula, colocando as mais elementares à esquerda, e as mais complexas à direita, partindo das fórmulas atômicas até a fórmula toda.
(3) Nessa tabela, escrevemos uma linha para cada possível interpretação (valoração das fórmulas atômicas) e usamos as regras de valoração para completar a tabela.

Cada linha da tabela representa uma interpretação na qual cada variável proposicional toma o valor correspondente a ela na tabela. Essa tabela é conhecida como **tabela-verdade** da fórmula α.

Por exemplo, para avaliar a fórmula $p \vee \neg p$

p	$\neg p$	$p \vee \neg p$
0	1	1
1	0	1

atesta que $p \vee \neg p$ é uma tautologia.

Exemplo 2.43. Tabelas-verdade para (1) $\neg(p \wedge \neg p)$, (2) $\neg(p \to (q \to p))$ e (3) $\neg p \vee q$.

1.

p	$\neg p$	$p \wedge \neg p$	$\neg(p \wedge \neg p)$
0	1	0	1
1	0	0	1

2.

p	q	$q \to p$	$p \to (q \to p)$	$\neg(p \to (q \to p))$
0	0	1	1	0
0	1	0	1	0
1	0	1	1	0
1	1	1	1	0

3.

p	q	$\neg p$	$\neg p \vee q$
0	0	1	1
0	1	1	1
1	0	0	0
1	1	0	1

Assim, na Lógica Proposicional, para determinar se $\vdash \alpha$ basta construir a tabela-verdade de α e verificar se a fórmula é uma tautologia. Mais que isso, se a fórmula for uma contingência então podemos descobrir a partir da tabela-verdade quais interpretações satisfazem a fórmula.

Metateorema 2.44. *Existe um algoritmo que, dado uma fórmula $\alpha \in \mathscr{L}_0$, decide se α é satisfazível.*

Metateorema 2.45 (Teorema da Decidibilidade). *O sistema formal* K *é decidível.*

Demonstração. O algoritmo recebe uma fórmula e verifica se é tautologia usando tabela-verdade; se for então é teorema e se não for tautologia, então não é teorema. ■

Embora seja possível descobrir a partir da tabela-verdade quais interpretações satisfazem uma fórmula essa tarefa pode não ser viável por requisitar muita computação. Dentro da Teoria da Computação, a Teoria da Complexidade Computacional aborda o problema da dificuldade de se encontrar um algoritmo "rápido" para problemas computacionais e nela o problema de determinar a satisfazibilidade de uma fórmula da Lógica Proposicional num número viável de passos em função do tamanho da fórmula é um problema reconhecidamente difícil e central na teoria. Esse problema é conhecido na Teoria da Computação como o problema da *satisfazibilidade* de uma fórmula booleana e é chamado SAT.

Exemplo 2.46. Tabela-verdade para $\big(p_1 \wedge p_2\big) \rightarrow \big((\neg p_3) \vee (p_4 \leftrightarrow p_5)\big)$

p_1	p_2	p_3	p_4	p_5	$p_1 \wedge p_2$	$\neg p_3$	$p_4 \leftrightarrow p_5$	$(\neg p_3) \vee (p_4 \leftrightarrow p_5)$	$(p_1 \wedge p_2) \rightarrow ((\neg p_3) \vee (p_4 \leftrightarrow p_5))$
0	0	0	0	0	0	1	1	1	1
0	0	0	0	1	0	1	0	1	1
0	0	0	1	0	0	1	0	1	1
0	0	0	1	1	0	1	1	1	1
0	0	1	0	0	0	1	1	1	1
0	0	1	0	1	0	1	0	1	1
0	0	1	1	0	0	1	0	1	1
0	0	1	1	1	0	1	1	1	1
0	1	0	0	0	0	0	1	1	1
0	1	0	0	1	0	0	0	0	1
0	1	0	1	0	0	0	0	0	1
0	1	0	1	1	0	0	1	1	1
0	1	1	0	0	0	0	1	1	1
0	1	1	0	1	0	0	0	0	1
0	1	1	1	0	0	0	0	0	1
0	1	1	1	1	0	0	1	1	1
1	0	0	0	0	0	1	1	1	1
1	0	0	0	1	0	1	0	1	1
1	0	0	1	0	0	1	0	1	1
1	0	0	1	1	0	1	1	1	1
1	0	1	0	0	0	0	1	1	1
1	0	1	0	1	0	0	0	0	1
1	0	1	1	0	0	0	0	0	1
1	0	1	1	1	0	0	1	1	1
1	1	0	0	0	1	1	1	1	1
1	1	0	0	1	1	1	0	1	1
1	1	0	1	0	1	1	0	1	1
1	1	0	1	1	1	1	1	1	1
1	1	1	0	0	1	0	1	1	1
1	1	1	0	1	1	0	0	0	0
1	1	1	1	0	1	0	0	0	0
1	1	1	1	1	1	0	1	1	1

Vimos que o valor lógico de uma fórmula de $\mathscr{L}_0$ depende exclusivamente do valor de seus átomos e isso garante um procedimento efetivo que, dado uma fórmula $\alpha \in \mathscr{L}_0$, descobre o valor-verdade de α em toda interpretação possível.

Na prática, a viabilidade desse método depende da quantidade de subfórmulas atômicas da fórmula pois o tamanho da tabela cresce exponencialmente nesse parâmetro. Uma fórmula sobre n átomos tem uma tabela com 2^n linhas. Uma fórmula com 10 átomos resulta numa tabela com 1.024 linhas, certamente muito trabalhoso para um humano mas facilmente resolvido por um computador. Entretanto, deve ficar claro que mesmo para um computador há um limite. Se há 30 átomos, a tabela irá conter mais de um bilhão de combinações de valores.

Embora existam outras técnicas além da tabela-verdade e atalhos como, por exemplo, se se atribui o valor 0 para p pode-se atribuir o valor 0 para $p \wedge q$ independentemente do valor atribuído ao q, o que reduz o número de cálculos a serem realizados, em tese, esses atalhos podem não ajudar, eles não mudam fundamentalmente a dificuldade do problema.

Estamos na seguinte situação: dada uma fórmula α da lógica proposicional, queremos determinar se α é satisfazível, i.e., há interpretação para os símbolos proposicionais de α que a torna verdadeira. Determinar via força-bruta se alguma interpretação satisfaz a fórmula toma tempo exponencial no número de átomos e não se sabe se é possível tomar algum atalho que seja efetivo para toda fórmula e que diminua consideravelmente a quantidade computação necessária para tomar a decisão correta.

Ademais, dada uma valoração podemos verificar rapidamente o valor-verdade da fórmula α. Isso é uma característica da família de problemas computacionais classificados pela Teoria da Computação como problemas NP. O problema SAT desempenha um papel fundamental nessa disciplina uma vez que podemos mostrar que a descoberta de um algoritmo eficiente para este problema implica em algoritmos eficientes para todos os problemas computacionais da classe NP. O SAT não é o único com essa característica, de fato há muitos deles, e são chamados de problema computacional NP-completo.

2.10 Compacidade

Vimos no metateorema 2.13, item (3), que se Γ é finito então $\Gamma \models \alpha$ é equivalente a decidir uma tautologia. No caso infinito veremos que se $\Gamma \models \alpha$ então existe $\Delta \subseteq \Gamma$ finito tal que $\Delta \models \alpha$. Esse resultado é equivalente ao teorema de compacidade da Lógica Proposicional.

Metateorema 2.47 (Teorema da compacidade, versão I). *Um conjunto de fórmulas é satisfazível se, e somente se, todo subconjunto finito é satisfazível.*

A parte relevante nessa equivalência é a condicional: *um conjunto de fórmulas é satisfazível sempre que todo subconjunto finito é satisfazível* pois a recíproca é imediata, isto é, se um conjunto é satisfazível então, imediatamente, seus subconjuntos finitos são satisfazíveis. Esse fato é equivalente ao que reportamos acima, ou seja, os seguintes resultados são equivalentes.

Metateorema 2.48 (Teorema da compacidade, versão I'). *Um conjunto de fórmulas é satisfazível sempre que todo subconjunto finito é satisfazível.*

Metateorema 2.49 (Teorema da compacidade, versão II). *Se* $\Gamma \models \alpha$ *então existe* $\Delta \subseteq \Gamma$ *finito tal que* $\Delta \models \alpha$.

Vamos chamar Γ de *finitamente satisfazível* quando *todo* subconjunto finito é satisfazível.

Exercício 2.50. *Se* Γ *é um subconjunto de fórmulas finitamente satisfazível e* α *uma fórmula, então* $\Gamma \cup \{\alpha\}$ *ou* $\Gamma \cup \{\neg\alpha\}$ *é finitamente satisfazível.*

Solução:. Assumamos Γ finitamente satisfazível. Podemos supor que $\alpha \notin \Gamma$ e $\neg\alpha \notin \Gamma$. Suponhamos que ambos $\Gamma \cup \{\alpha\}$ e $\Gamma \cup \{\neg\alpha\}$ não são finitamente satisfazíveis. Então existem $\Delta_0, \Delta_1 \subset \Gamma$ finitos tais que $\Delta_0 \cup \{\alpha\}$ e $\Delta_1 \cup \{\neg\alpha\}$ não são satisfazíveis.

$\Delta_0 \cup \Delta_1$ é subconjunto finito de Γ logo existe uma interpretação v tal que $v \vDash \Delta_0 \cup \Delta_1$. Se $\hat{v}(\alpha) = 1$ então $\Delta_0 \cup \{\alpha\}$ é satisfazível e temos uma contradição. Senão $\hat{v}(\neg\alpha) = 1$, logo $\Delta_1 \cup \{\neg\alpha\}$ é satisfazível e temos uma contradição novamente. ■

Demonstração do metateorema 2.48. Suponha que Γ seja um conjunto finitamente satisfazível. Fixemos $\theta_1, \theta_2, \ldots$ uma enumeração das fórmulas de $\mathscr{L}_0$.

Construimos um conjunto de fórmulas Δ finitamente satisfazível e que contém Γ pondo $L_0 = \Gamma$ e

$$L_{i+1} = \begin{cases} L_i \cup \{\theta_{i+1}\} & \text{se esse conjunto é finitamente satisfazível,} \\ L_i \cup \{\neg\theta_{i+1}\} & \text{caso contrário.} \end{cases}$$

Dessa forma cada L_n é finitamente satisfazível. Tomemos $\Delta = \bigcup_{i \geq 0} L_i$. Pela construção temos $\Gamma \subseteq \Delta$ e para toda fórmula α temos $\alpha \in \Delta$ ou $\neg\alpha \in \Delta$. Além disso, Δ é finitamente satisfazível pois todo subconjunto finito de Δ é um subconjunto finito de L_n para algum $n \geq 0$.

Agora, vamos verificar que Δ satisfaz os cinco itens do corolário 2.34 e que, portanto, de acordo com lema 2.35 é satisfazível. Para quaisquer fórmulas α e β

(i) $\alpha \in \Delta$ ou $\neg\alpha \in \Delta$, mas não ambas. Caso contrário teríamos $\{\alpha, \neg\alpha\} \subset \Delta$ satisfazível pela satisfazibilidade finita.
(ii) $\alpha \vee \beta \in \Delta$ se, e só se, $\alpha \in \Delta$ ou $\beta \in \Delta$. Se $\alpha \vee \beta \in \Delta$ e $\alpha, \beta \notin \Delta$, teríamos $\neg\alpha, \neg\beta \in \Delta$ e $\{\alpha \vee \beta, \neg\alpha, \neg\beta\} \subset \Delta$ satisfazível por ser finito, uma contradição. Portanto $\alpha \in \Delta$ ou $\beta \in \Delta$. Por outro lado, se $\alpha \in \Delta$ ou $\beta \in \Delta$ e $\alpha \vee \beta \notin \Delta$ teríamos $\{\alpha, \neg(\alpha \vee \beta)\} \subset \Delta$ satisfazível ou $\{\beta, \neg(\alpha \vee \beta)\} \subset \Delta$ satisfazível, ambas são contradições.
(iii) $\alpha \wedge \beta \in \Delta$ se, e só se, $\alpha \in \Delta$ e $\beta \in \Delta$. Se $\alpha \wedge \beta \in \Delta$ e $\alpha \notin \Delta$, então $\{\alpha \wedge \beta, \neg\alpha\} \subset \Delta$ é satisfazível, uma contradição. Analogamente, se $\alpha \wedge \beta \in \Delta$ e $\beta \notin \Delta$, derivamos uma contradição. Portanto $\alpha, \beta \in \Delta$. Por outro lado, se $\alpha, \beta \in \Delta$ e $\alpha \wedge \beta \notin \Delta$ então $\{\alpha, \beta, \neg(\alpha \wedge \beta)\} \subset \Delta$ portanto é satisfazível, uma contradição.
(iv) $\alpha \to \beta \in \Delta$ se, e só se, $\neg\alpha \in \Delta$ ou $\beta \in \Delta$. Se $\alpha \to \beta \in \Delta$ e $\neg\alpha, \beta \notin \Delta$, teríamos $\alpha, \neg\beta \in \Delta$ e $\{\alpha \to \beta, \alpha, \neg\beta\} \subset \Delta$ satisfazível, uma contradição. Portanto $\neg\alpha \in \Delta$ ou $\beta \in \Delta$. Por outro lado, se $\neg\alpha \in \Delta$ ou $\beta \in \Delta$ e $\alpha \to \beta \notin \Delta$ teríamos $\{\neg\alpha, \neg(\alpha \to \beta)\} \subset \Delta$ satisfazível ou $\{\beta, \neg(\alpha \to \beta)\} \subset \Delta$ satisfazível, ambas são contradições.
(v) Que $\alpha \leftrightarrow \beta \in \Delta$ se, e só se, $\{\alpha, \beta\} \subset \Delta$ ou $\{\neg\alpha, \neg\beta\} \subset \Delta$ é um exercício.

Pelo lema 2.35 Δ é satisfazível, logo Γ é satisfazível. ■

Para provar que a versão II segue da versão I dos enunciados do metateorema da compacidade dados acima, usamos a seguinte afirmação deixada como exercício para o leitor.

Exercício 2.51. $\Gamma \vDash \alpha$ *se, e somente se,* $\Gamma \cup \{\neg\alpha\} \vDash \bot$.

Solução:. Assuma $\Gamma \vDash \alpha$. Se $v \vDash \Gamma \cup \{\neg\alpha\}$ então $v \vDash \Gamma$ e $v \vDash \neg\alpha$. De $v \vDash \Gamma$ e $\Gamma \vDash \alpha$ temos $v \vDash \alpha$. Portanto $v \vDash \alpha$ e $v \vDash \neg\alpha$, um absurdo. Agora, assuma que $\Gamma \cup \{\neg\alpha\} \vDash \bot$. Pelo metateorema 2.13 obtemos $\Gamma \vDash \neg\alpha \to \bot$. De $\neg\alpha \to \bot \equiv \alpha \vee \bot$ e $\alpha \vee \bot \equiv \alpha$ segue que $\Gamma \vDash \alpha$. ■

Demonstração da equivalência das versões I' *e* II. Começamos com a demonstração da versão II usando a versão I'. Suponha que $\Gamma \vDash \alpha$ mas que para todo $\Delta \subset \Gamma$ finito vale que $\Delta \nvDash \alpha$, então $\Delta \cup \{\alpha\}$ não é satisfazível, portanto, $\Delta \cup \{\neg\alpha\}$ é satisfazível. Logo $\Gamma \cup \{\neg\alpha\}$ é finitamente satisfazível e por compacidade, versão I', $\Gamma \cup \{\neg\alpha\}$ é satisfazível, uma contradição pois pelo exercício acima de $\Gamma \vDash \alpha$ temos $\Gamma \cup \{\neg\alpha\} \vDash \bot$.

Agora, se Γ não é satisfazível então, pela versão II, existe $\Delta \subseteq \Gamma$ finito e não satisfazível, portanto Γ não é finitamente satisfazível. ■

2.10.1 Aplicação em Teoria dos Grafos — coloração

Um grafo é um par de conjuntos (V, E) tal que todo elemento de E é um conjunto formado por exatamente dois elementos distintos de V. Os elementos de V são chamados de vértice e os elementos de E são chamados de aresta. Um subgrafo desse grafo é uma grafo (X, F) tal que $X \subseteq V$ e $F \subseteq F$. Um grafo é finito se o conjunto de vértices é finito.

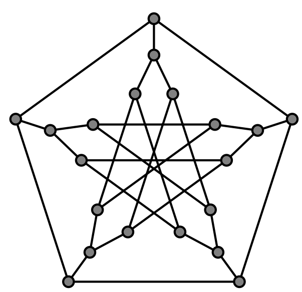

Figura 2.1. Representação gráfica de um grafo finito

Dados k cores, denominadas $c_1, c_2, \dots, c_k$, um grafo G é dito k-**colorível** se os vértices de G podem ser pintados com as k cores sem que quaisquer dois vértices que formam uma aresta tenham a mesma cor.

Seja (V, E) um grafo com vértices $v_1, v_2, v_3, \dots$ (o conjunto V é enumerável). O seguinte é um resultado da Teoria dos Grafos: *(V, E) é k-colorível se e somente se todo subgrafo finito é k-colorível.*

Se (V, E) é k-colorível então um subgrafo finito (X, F) é k-colorível, basta mater as cores de dadas V no conjunto $X \subset V$.

Para a recíproca usamos o Metateorema de Compacidade. Sem perda de generalidade, assumimos que $V = \mathbb{N}$. Consideremos a proposição p_{i,c_j} que é interpretada como "o vértice i tem a cor c_j" e o conjunto Γ das fórmulas

1. $p_{i,c_1} \vee p_{i,c_2} \vee \cdots \vee p_{i,c_k}$ para cada vértice $i \in \mathbb{N}$ (interpretada como "o vértice i tem alguma cor");
2. $\neg(p_{i,c_j} \wedge p_{i,c_\ell})$ para todos $1 \leqslant j < \ell \leqslant k$ e $i \in \mathbb{N}$ (interpretada como "o vértice i tem no máximo uma cor");
3. $\neg(p_{i,c_\ell} \wedge p_{j,c_\ell})$ para todo $1 \leqslant \ell \leqslant k$ e toda aresta $\{i,j\}$ do grafo (interpretado como "os vértices adjacentes i e j não têm a mesma cor").

Suponhamos que v seja uma valoração que satisfaz Γ, definimos uma k-coloração atribuindo ao vértice i a cor c_j se e só se p_{i,c_j} tem valor 1. Pelos itens 1 e 2, cada vértice i há uma única cor para a qual $v(p_{i,c_j}) = 1$ tem valor 1. Pelo item 3,se i e ℓ são vértices adjacentes então a cor de i é diferente da cor de ℓ. Assim as fórmulas de fato modelam o problema em Lógica Proposicional.

Agora, se $\Delta \subset \Gamma$ é finito, então tomamos $X \subset V$ como conjunto de todos os vértices mencionados nas fórmulas de Δ e F o conjunto de todas as arestas de E que incidem nos vértices de X. O grafo finito (X,F) é k-colorível, por hipótese, assim a valoração v que faz $p_{i,j}$ igual a 1, para todo $i \in X$, se e só se a cor de i é c_j satisfaz Δ, portanto, Γ é satisfazível por compacidade e assim o grafo é k-colorível.

O conjunto Γ é satisfazível se, e só se, o grafo $(\mathbb{N},E)$ é k-colorível. Por hipótese, todo subgrafo finito de $(\mathbb{N},E)$ admite uma k-coloração. Segue-se que todos os subconjuntos finitos de Γ são satisfazíveis. Pelo teorema da compacidade Γ é satisfazível e, portanto, $(\mathbb{N},E)$ é k-colorível.

Outra aplicação em Teoria dos Grafos — emparelhamento

Considere agora um grafo bipartido $(P \cup M, E)$ com as classes de vértices P e M disjuntas.

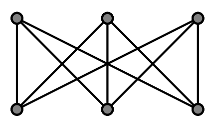

Figura 2.2. Representação gráfica de um grafo bipartido

Esse grafo modela o *problema do casamento*, um conjunto de professores P e um conjunto de disciplinas M e cada aresta associa um professor a uma disciplina que poderia ser coordenada por ele. O problema é associar cada professor a uma disciplina. O caso finito tem uma caracterização: é possível casar todos os professores se, e só se, para cada subconjunto $S \subset P$ o conjunto de disciplinas associadas a eles $P \subset M$ satisfaz $|P| \geqslant |M|$; e o famoso Teorema de Hall e essa desigualdade é a **condição de Hall**.

Suponha, agora, que $P = \{h_1, h_2, \dots\}$, $M = \{m_1, m_2, \dots\}$ e $m_{i_1}, m_{i_2}, \dots m_{i_{n_i}}$ a relação das matérias de $h_i \in P$ (i.e., cada professor tem um número finito de disciplinas). Vamos supor que vale a condição de Hall, i.e., qualquer grupo de k professores tem pelo menos k disciplinas, para todo inteiro positivo k. Vamos mostrar que é possível formar pares de professor com disciplina coordenada.

Consideremos as proposições $p_{i,j}$ para $i, j \geqslant 1$, cuja intenção é modelar a sentença "o professor h_i casa com a disciplina m_j". Seja Γ o conjunto das fórmulas

1. $p_{i,i_1} \vee p_{i,i_2} \vee \cdots \vee p_{i,i_{n_i}}$ para cada professor h_i (interpretada como "o professor h_i casa com alguma disciplina");
2. $\neg(p_{i,i_j} \wedge p_{i,i_k})$ para todo i e todos $j, k \in \{1, \ldots, n_i\}$ com $j \neq k$ (interpretada como "o professor h_i coordena só uma disciplina");
3. $\neg(p_{i,\ell} \wedge p_{j,\ell})$ para todo $\ell \in \mathbb{N}$ e para todo $i, j \in \mathbb{N}$ com $i \neq j$ e $\{i, \ell\}$ e $\{j, \ell\}$ arestas (interpretado como "a disciplina m_j tem um único coordenador").

Pelo teorema de Hall Γ é finitamente satisfazível, portanto, Γ é satisfazível. Se $v \vDash \Gamma$ temos que as arestas

$$\{h_i, m_{i_k}\} \text{ se, e só se, } v(p_{i,i_k}) = 1$$

é uma solução para o problema do casamento.

2.11 Exercícios

26. Verifique quais dos seguintes conjuntos são consistentes
    a) $\{\neg p_1 \wedge p_2 \to p_0, p_1 \to (\neg p_1 \to p_2), p_0 \leftrightarrow \neg p_2\}$.
    b) $\{p_0 \to p_1, p_1 \to p_2, p_2 \to p_3, p_3 \to \neg p_0\}$.
    c) $\{p_0 \to p_1, p_0 \wedge p_2 \to p_1 \wedge p_3, p_0 \wedge p_2 \wedge p_4 \to p_1 \wedge p_3 \wedge p_5, \ldots\}$.
27. Demonstre que são equivalentes as seguintes afirmações
    a) $\{\varphi_1, \ldots, \varphi_n\}$ é consistente
    b) $\nvdash \neg(\varphi_1 \wedge \cdots \wedge \varphi_n)$
    c) $\nvdash \varphi_1 \wedge \cdots \wedge \varphi_{n-1} \to \varphi_n$
28. Dê um exemplo de um conjunto Γ de fórmulas e uma fórmula φ tais que $\Gamma \nvdash \varphi$ e $\Gamma \nvdash \neg\varphi$.
29. Seja $\Gamma = \{p_1, \neg p_2 \vee p_3\}$. Demonstre que não há uma prova de p_3 a partir de Γ.
30. Demonstre que se $\Gamma \cup \{\neg\alpha\}$ é um conjunto de fórmulas satisfazível então a fórmula α não pode ser provada a partir de Γ.
31. Demonstre que $\Gamma \cup \{\neg\alpha\}$ é um conjunto de fórmulas satisfazível se e somente se $\Gamma \nvDash \alpha$.
32. Demonstre usando somente noções semânticas $\Gamma \cup \{\neg\alpha\}$ é um conjunto de fórmulas satisfazível se e somente se $\Gamma \nvDash \alpha$.
33. Demonstre que $\Gamma \nvdash \alpha$ se, e só se, existe uma valoração que satisfaz Γ mas não satisfaz α.
34. Demonstre que se Γ é consistente então ou $\Gamma \cup \{\phi\}$ ou $\Gamma \cup \{\neg\phi\}$ é consistente para qualquer fórmula ϕ.
35. Demonstre que o conjunto de fórmulas Γ é maximalmente consistente se, e só se, existe uma *única* valoração que satisfaz Γ.
36. Demonstre que se Γ é um conjunto de fórmulas consistente maximal então
    a) para todo $\alpha \in \mathscr{L}_0$, vale $\Gamma \vdash \neg\alpha$ se, e só se, $\Gamma \nvdash \alpha$.
    b) para todos $\beta, \gamma \in \mathscr{L}_0$, vale $\beta \to \gamma \in \Gamma$ se, e só se, se $\beta \in \Gamma$ então $\gamma \in \Gamma$

37. Demonstre que Γ é um conjunto de fórmulas consistente se, e somente se, existe pelo menos uma fórmula que não pode ser provada a partir de Γ.
38. Demonstre que $\Gamma \vdash \alpha$ se, e só se, $\Gamma \cup \{\neg\alpha\}$ é inconsistente.
39. Seja w uma valoração de $\mathscr{L}_0$. Demonstre que o conjunto de fórmulas $\{\phi \in \mathscr{L}_0 : w(\phi) = 1\}$ é consistente maximal.
40. Tome $\Gamma = \{p_2, p_3, p_4, \dots\}$ e demonstre que não há uma prova de p_1 a partir de Γ, nem de $\neg p_1$ a partir de Γ.
41. Um sistema formal é **sintaticamente completo** se para cada fórmula φ da linguagem do sistema, temos $\vdash \varphi$ ou $\vdash \neg\varphi$ (essa é uma propriedade mais forte do que completude semântica) O sistema formal K é sintaticamente completo?
42. Dizemos que o conjunto de fórmulas Γ é **sintaticamente completo** se para toda fórmula α vale que $\Gamma \vdash \alpha$ ou que $\Gamma \vdash \neg\alpha$. Demonstre que se Γ é sintaticamente completo e w é uma valoração de $\mathscr{L}_0$ que satisfaz Γ então, para toda fórmula α, vale $w \vDash \alpha$ se, e só se, $\Gamma \vdash \alpha$.
43. Demonstre que se Γ é um conjunto consistente de fórmulas de $\mathscr{L}_0$ então existe um conjunto $\Delta \subset \mathscr{L}_0$ tal que $\Delta \supseteq \Gamma$ consistente e é sintaticamente completo.
44. Demonstre que o conjunto de fórmulas $\{\sigma \in \mathscr{L}_0 : \Gamma \vdash \sigma\}$ é consistente maximal se, e só se, Γ é sintaticamente completo.
45. Dizemos que a fórmula $\varphi \in \mathscr{L}_0$ é **independente** do conjunto $\Gamma \subset \mathscr{L}_0$ se $\Gamma \nvdash \varphi$ e $\Gamma \nvdash \neg\varphi$. Mostre que $p_1 \to p_2$ é independente de $\{p_1 \leftrightarrow p_0 \wedge \neg p_2, p_2 \to p_0\}$.
46. (**Extensão de ordens parciais**) Uma relação binária $\preceq$ sobre um conjunto $A \neq \varnothing$ é uma **ordem parcial** em A se valem as propriedades *reflexiva, antissimétrica, transitiva*. Uma ordem parcial em que quaisquer $x, y \in A$ vale $x \preceq y$ ou $y \preceq x$ é chamada de **ordem total**. Em A, a ordem total $\leqslant$ **estende** a ordem parcial $\preceq$ caso
$$x < y \text{ sempre que } x \prec y.$$
    a) Seja A um conjunto finito e não vazio. Verifique que $(\wp(A), \subseteq)$, o conjunto das partes de A com a relação de inclusão, é uma ordem parcial. Defina uma ordem total que estenda essa ordem parcial.
    b) Seja $(A, \preceq)$ um conjunto parcialmente ordenado com A finito e não vazio. Demonstre que existe uma ordem total que estende essa ordem parcial.
    c) Seja $(A, \preceq)$ um conjunto parcialmente ordenado com A infinito e enumerável. Demonstre usando o metateorema da compacidade que existe uma ordem total sobre A que estende $\preceq$.
47. Demonstre que se Γ é inconsistente então existe $\Delta \subset \Gamma$ finito e inconsistente.
48. Demonstre que se todo subconjunto finito de Γ é consistente, então Γ é consistente.
49. Mostre que se Δ e Σ são conjuntos de fórmulas recursivamente enumeráveis então também são $\Sigma \cup \Delta$ e $\Sigma \cap \Delta$.
50. Mostre que se Δ e Σ são conjuntos de fórmulas decidíveis então também são $\Sigma \cup \Delta$, $\Sigma \cap \Delta$ e $\Sigma \setminus \Delta = \{\alpha \in \Sigma : \alpha \notin \Delta\}$.
51. (**Lema de Kalmár**) Seja α uma fórmula de $\mathscr{L}_0$ cujas subfórmulas atômicas são $p_1, \dots, p_n$. Seja v uma interpretação. Defina para todo $i \in \{1, 2, \dots, n\}$

$$q_i = \begin{cases} p_i & \text{se } v(p_i) = 1 \\ \neg p_i & \text{se } v(p_i) = 0 \end{cases}$$

e tome $\Gamma = \{q_1, q_2, \ldots, q_n\}$. Demonstre que

a) se $\hat{v}(\alpha) = 1$ então $\Gamma \vdash \alpha$.

b) se $\hat{v}(\alpha) = 0$ então $\Gamma \vdash \neg\alpha$.

(Sugestão: indução em α.)

52. Nesse exercício provaremos a completude usando o Lema de Kalmár (assegure-se de não ter usado completude no exercício anterior).

a) Se α é uma tautologia e $p_1, \ldots, p_n$ as subfórmulas atômicas de α então

$$\{q_1, \ldots, q_{n-1}\} \vdash \alpha. \tag{2.3}$$

(Dica: v uma interpretação e w uma interpretação que coincide com v em todas as variáveis exceto p_n.
Verifique $\{q_1, \ldots, q_{n-1}, p_n\} \vdash \alpha$ e $\{q_1, \ldots, q_{n-1}, \neg p_n\} \vdash \alpha$. Use o Teorema da dedução para concluir (2.3).)

b) Se α é uma tautologia e $p_1, \ldots, p_n$ as subfórmulas atômicas de α então $\{q_1, \ldots, q_{n-2}\} \vdash \alpha$.

c) Se α é uma tautologia então $\vdash \alpha$.

Parte II

Lógica de predicados

Discussão informal

A lógica de predicados de primeira ordem é uma extensão da logica proposicional para uma linguagem mais rica, portanto de maior poder de expressão. Argumentos como

Premissa	*O quadrado de qualquer inteiro é positivo*
Premissa	*9 é um quadrado*
Conclusão	*9 é positivo*

não são validados pela lógica proposicional. Na lógica de primeira ordem usamos variáveis, quantificadores e predicados para capturar elementos mais finos da estrutura gramatical.

A lógica de primeira ordem é o padrão para a formalização axiomática da matemática. A Aritmética de Peano e a Teoria de Conjuntos de Zermelo–Fraenkel, por exemplo, são axiomatizações da Teoria dos Números e da Teoria de Conjuntos.

O que queremos formalizar com a Lógica de predicados? Sentenças como

- Todo aluno é mais novo que algum professor.
- Todo número primo maior ou igual a dois é ímpar.
- Todo anel de divisão finito é um corpo.

podem ser simbolizadas no cálculo proposicional mas o dito não captura toda estrutura da sentença. Os alvos do discurso (sujeito e objeto gramaticais) têm qualidades e mantêm relações. O que procuramos? Uma linguagem mais rica que leva em conta a estrutura interna das sentenças

sujeito – predicado – objeto

na qual sujeito e objetos de quem se fala são elementos de um **universo do discurso** e são representados por **constantes** ou por objetos genéricos e não especificados (pronomes) que são representados por **variáveis**; os **predicados** e as **relações** são explicitados. Além disso, o "**para todo**" e o "**existe**" são incorporados como primitivas da linguagem.

Exemplo 2.52. Num universo (de discurso) *far, far away ....*

Constantes:	a para 'Armando', d para 'Daniel' e j para 'Manoel'.
Predicados:	P para 'é professor' e A para 'é aluno'.
Relações:	J para 'lecionam juntos' e N para 'é mais novo'.

$P(a)$ simboliza a sentença 'Armando é professor'. $\neg A(j)$ simboliza a sentença 'Manoel não é aluno'. $J(a,d)$ simboliza a sentença 'Armando e Daniel lecionam juntos'. $M(d,a)$ simboliza a sentença 'Daniel é mais novo que Armando'. Obervemos que, considerando o significado natural das sentenças, $J(a,d)$ e $J(d,a)$ têm o mesmo significado, mas $M(a,d)$ e $M(d,a)$ *não* têm o mesmo significado.

Usamos as *variáveis* $x, y, z\dots$ para representar membros genéricos do universo. $P(x)$ simboliza 'x é professor' e $M(x,y)$ simboliza 'x é mais novo que y'. Nem $P(x)$ nem $M(x,y)$ têm valor lógico, não são sentenças no sentido da lógica proposicional que vimos na Parte 1 destas notas. São chamadas de *sentenças abertas*.

As sentenças abertas tornam-se sentenças lógicas quando substituímos as variáveis por elementos do universo ou se *quantificamos*. O *quantificador* $\forall$ é lido "para todo" e o *quantificador* $\exists$ é lido "existe". $\forall x\, P(x)$ simboliza a sentença todo x é professor' a qual pode ser atribuída valor lógico: significa que todo elemento do universo do discurso é professor. $\exists x\, P(x)$ simboliza a sentença 'algum x é professor' a qual pode ser atribuída valor lógico: significa que pelo menos um elemento do universo do discurso é professor.

Notemos que, por exemplo

1. $\forall x\, M(x, y)$ é uma sentença aberta
2. $\exists y \forall x\, M(x, y)$ e $\forall x \exists y\, M(x, y)$ têm significados diferentes.

A sentença 'Todo aluno é mais novo que algum professor' pode ser simbolizada por

$$\forall x \exists y (A(x) \wedge P(y) \rightarrow M(x, y))$$

A sentença 'Há um professor tal que todo aluno aprende algo com ele', considerando as relações $B(x, y, z)$ para 'y aprende z com x' e $H(x)$ para 'x é um assunto', pode ser simbolizada por

$$\exists x \Big(P(x) \wedge \forall y \big(A(y) \rightarrow \exists z\, (H(z) \wedge B(x, y, z)) \big) \Big)$$

Em matemática, muitas vezes tratamos de estruturas que consistem em um conjunto com operações e relações entre seus elementos. Por exemplo, na Teoria Elementar de Números o conjunto de elementos em discussão é o conjunto de números inteiros $\mathbb{Z} = \{0, \pm 1, \pm 2, \dots\}$ Pode-se precisar de símbolos para alguns números, para variáveis, para funções (como $\cdot$ e $+$) e para as relações (como $=$, $<$, e $|$). A sentença "Para todo x, se x é um inteiro maior que ou igual a zero e todo inteiro é divisível por x, então x é igual a um" considerando que

- 0 e 1 são constantes;
- $>(x, y)$ simboliza a relação "x é maior que y";
- $=(x, y)$ simboliza a relação "x é igual a y" e
- $|\,(x, y)$ simboliza a relação "x divide y",

é simbolizada como

$$\forall x \Big(\big(>(x, 0) \vee =(x, 0) \big) \wedge \forall y\, (|\,(x, y)) \rightarrow =(x, 1) \Big)$$

ou , usando as simplificações já adotadas e $\geqslant$ para '> ou =', escrevemos

$$\forall x \Big((x \geqslant 0 \wedge \forall y\, x|y) \rightarrow x = 1 \Big).$$

A expressão

$$\forall x \exists y \Big(0 < y \wedge \forall z \big((z|y \wedge 0 < z) \rightarrow (z = 1 \vee z = y) \big) \Big)$$

pode ser interpretada, nesse contexto, que "existem inifinitos números primos", ou seja, que para todo inteiro x existe um inteiro positivo y cujos únicos divisores são o 1 e o próprio y.

3

Cálculo de predicados

3.1 Linguagens formais de primeira ordem

Diferente da lógica de proposições não temos uma única linguagem na lógica predicados. Uma *linguagem lógica de primeira ordem* é um conjunto de fórmulas escritas a partir de um alfabeto que considera símbolos comuns a todas as linguagens e os símbolos que são específicos de cada linguagem, ditos *não lógicos* ou *extra lógicos*.

Em vista do que vimos no estudo da lógica de proposições, reduziremos o número de conectivos usados, isso fará com que as definições e demonstrações provas sejam mais curtas.

A seguir descrevemos uma linguagem lógica *genérica* de primeira ordem denotada por $\mathscr{L}_1$. O alfabeto genérico é

$$\mathscr{A}_1 = \{x_i \colon i \in \mathbb{N}\} \cup \left\{\neg, \rightarrow, (,) \forall, \doteq\right\} \cup \{c_i \colon i \in \mathbb{N}\} \cup \bigcup_{n\geqslant 1} \left\{R_i^n \colon i \in \mathbb{N}\right\} \cup \bigcup_{n\geqslant 1} \left\{F_i^n \colon i \in \mathbb{N}\right\}$$

dos símbolos permitidos para as expressões na linguagem genérica incluem

símbolos lógicos	variáveis:	$x_1 \ x_2 \ \dots$
	conectivos lógicos:	$\neg \ \rightarrow$
	quantificador:	$\forall$
	pontuação:	$(\ )$
símbolo relacional de igualdade	$\doteq$	
símbolos não-lógicos	Constantes:	$c_1 \ c_2 \ \dots$
	Para cada $n \geqslant 1$:	
	relacionais n-ários:	$R_1^n \ R_2^n \ \dots$
	funcionais n-ários:	$F_1^n \ F_2^n \ \dots$

As constantes, os símbolos relacionais e funcionais são **específicos de cada linguagem** de primeira ordem e um ou mais deles pode ser vazio. Os símbolos lógicos são compartilhados por toda linguagem de primeira ordem. *O símbolo de igualdade é um símbolo relacional binário especial.* Há autores que tratam a igualdade como um símbolo lógico e outros que tratam como não-lógico de modo a distinguir-se as linguagens de primeira ordem com igualdade e sem igualdade. Aqui não faremos essa distinção, não o chamaremos de lógico mas consideraremos que *toda linguagem de primeira ordem tem o símbolo de igualdade.* As constantes e os simbolos relacionais e funcionais são os *símbolos não-lógicos* e são específicos de cada linguagem, as quais, geralmente, dependem do uso pretendido.

Exemplo 3.1 (linguagem da Teoria dos Grafos). A linguagem da teoria dos grafos não tem constantes, não tem símbolos funcionais e tem apenas um símbolo relacional binário R_1^2 que abreviamos por A, simplesmente.

Exemplo 3.2 (linguagem da Teoria Aritmética de Números). A linguagem da aritmética tem uma constante, o 0, tem um símbolo funcional unário F_1^1, que abreviamos por S, tem dois símbolos funcionais binários F_1^2 e F_2^2, que abreviamos por $+$ e $\cdot$ respectivamente, e um relacional binário R_1^2 que abreviamos por $<$.

Exemplo 3.3 (linguagem da Teoria dos Conjuntos). A linguagem da teoria dos conjuntos não tem constantes, não tem símbolos funcionais e tem apenas um símbolo relacional binário R_1^2 que abreviamos por $\in$.

Exemplo 3.4 (linguagem da Igualdade). A linguagem da igualdade não tem constantes, não tem símbolos funcionais e não tem símbolos relacionais.

Intuitivamente, as constantes são interpretadas como elementos específicos do universo de discurso da linguagem; os símbolos da função n-ária são interpretados como funções específicas que mapeiam n-úplas de elementos do universo de discurso à elementos do universo; os símbolos de relação n-ária destinam-se a designar relações entre n elementos. O símbolo quantificador destina-se a representar “para todos” em referência à todos os elementos do universo e é usado com variáveis.

3.1.1 Termos

São as sequências de símbolos do alfabeto obtidas a partir das regras abaixo.

(T1) Variáveis e constantes são termos.
(T2) Para qualquer natural n, e qualquer símbolo funcional F_i^n, se $t_1, t_2, \dots, t_n$ são termos então $F_i^n t_1 t_2 \dots t_n$ é termo.
(T3) Não há outros termos além dos obtidos pela aplicação de um número finito de vezes das regras acima.

Exemplo 3.5. São termos: c_1, x_{101}, $F_2^1 x_1$, $F_2^2 x_1 c_8$, $F_1^4 c_1 c_2 x_1 x_2$. Note que $F_2^2 x_1$ não é termo (por quê?). A cadeia de símbolos $F_1^1 F_1^2 x_1 x_2$ é um termo? $F_1^1 F_1^2 F_1^1 x_1 x_2$ é um termo?

Metateorema 3.6 (Teorema da unicidade de representação dos termos). *Se t é um termo de uma linguagem de primeira ordem, então uma, e apenas uma, das asserções abaixo é verdadeira:*

- *t é uma variável;*
- *t é uma constante;*
- *há um único n para o qual t é $F^n t_1 t_2 \dots t_n$ para únicos termos $t_1, \dots, t_n$ e único símbolo funcional n-ário F^n.*

Metateorema 3.7 (Princípio de indução para termos). *Seja Γ um conjunto de termos de uma linguagem de primeira ordem. Se*

1. *as variáveis e as constantes pertencem a Γ;*
2. *se $t_1, t_2, \dots t_n$ pertencem a Γ então $F t_1 t_2 \dots t_n$ pertence a Γ para qualquer que seja o símbolo funcional n-ário F.*

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

3.1.2 Fórmulas

Fórmulas bem formadas (FBF) são as sequências de símbolos do alfabeto obtidas a partir das regras abaixo.

(F1) Se t e s são termos, então $(\doteq ts)$ é uma fórmula. Também, para qualquer natural n, e qualquer símbolo relacional R_i^n, se $t_1, \dots, t_n$ são termos então $R_i^n t_1 t_2 \dots t_n$ é uma fórmula. Toda fórmula obtida por aplicação exclusiva dessa regra é dita **fórmula atômica**.

(F2) Se α e β são fórmulas, então $(\neg\alpha)$ e $(\alpha \to \beta)$ são fórmulas.

(F3) Se α é fórmula e x é uma variável, então $(\forall x\, \alpha)$ é fórmula.

(F4) Não há outras fórmulas além daquelas obtidas pela aplicação um número finito de vezes as regras acima.

A linguagem genérica obtida dos símbolos do alfabeto genérico $\mathscr{A}_1$ é denotada por $\mathscr{L}_1$.

Exemplo 3.8. $\Big(\big(R_1^1 x_1 \to R_2^3 x_4 x_2 c_1\big) \to \big(\forall x_1 ((\forall x_2\, R_2^3 c_4 x_2 c_1) \to (\neg(\doteq F_1^1 x_1 F_1^1 c_1)))\big)\Big)$.

Metateorema 3.9 (Teorema da unicidade de representação das fórmulas). *Seja α uma fórmula de uma linguagem de primeira ordem. Então α satisfaz uma, e apenas uma, das condições abaixo*

- *α é uma fórmula atômica da forma $R t_1 t_2 \dots t_n$, onde R é um símbolo relacional n-ário e $t_1, \dots, t_n$ são termos, para únicos n, R e t_i's;*

- *α é uma fórmula atômica da forma $(\doteq s\,t)$ para únicos s e t termos;*
- *α é da forma $(\neg\beta)$, para uma única fórmula β;*
- *α é da forma $(\beta \to \gamma)$ para únicos β e γ fórmulas;*
- *α é da forma $(\forall x \beta)$, para uma única fórmula β e uma única variável x.*

Metateorema 3.10 (Princípio de indução para as fórmulas). *Seja Γ um conjunto de fórmulas de uma linguagem de primeira ordem. Se*

1. *as fórmulas atômicas pertencem a Γ;*
2. *se α pertence a Γ então $(\neg\alpha)$ pertence a Γ;*
3. *se α e β pertencem a Γ então $(\alpha \to \beta)$ pertence a Γ;*
4. *se α pertence a Γ e x é uma variável, então $(\forall x\, \alpha)$ pertence a Γ.*

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

3.1.3 Simplificações, abreviaturas e omissão de parênteses

Vamos assumir algumas convenções de notação para facilitar nossa vida. No uso dos símbolos admitimos algumas simplificações na escrita, como já fizemos na lógica proposicional.

- Fórmulas: usamos as metavariáveis $\alpha, \beta, \gamma, \ldots$ possivelmente com índices.
- Termos: usamos as metavariáveis s, t, u, v possivelmente com índices.
- Variáveis: usamos as metavariáveis x, w, y, z possivelmente com índices.
- Constantes: usamos as metavariáveis a, b, c, d, e, f possivelmente com índices.
- Símbolos relacionais: ao invés de R_i^n escrevemos R e também usamos outros símbolos como $P, Q, R, S, <, \prec$. Ainda, escrevemos

  $$R(t_1, t_2, \ldots, t_n) \text{ ao invés de } R^n t_1 t_2 \ldots t_n.$$

  Para as relações R binárias escrevemos

  $$(a\, R\, b) \text{ ao invés de } R(a, b)$$

  como em $(a < b)$, em particular, escrevemos

  $$(t \doteq s) \text{ ao invés de } \doteq(t, s)$$

  como é usual.
- Símbolos funcionais: ao invés de F_i^n escrevemos F e também usamos outros símbolos como $F, G, H, +, \cdot$. Ainda, ao invés de $F^n t_1 t_2 \ldots t_n$ escrevemos $F(t_1, t_2, \ldots, t_n)$. Para as operações binárias F escrevemos $(a\, F\, b)$ ao invés de $F(a, b)$, como em $(a + b)$.

Abreviaturas

Para resultados teóricos (metamatemáticos) é vantajoso possuirmos o mínimo possível de símbolos, entretanto, para expressarmos de maneira clara e sucinta quanto mais símbolos, melhor. Tratando alguns símbolos como abreviaturas de outros nós ganhamos dos dois lados.

símbolo	*lê-se*	*uso*
$\wedge$	*conjunção*	$(\alpha \wedge \beta)$ abrevia $(\neg(\alpha \to (\neg \beta)))$
$\vee$	*disjunção*	$(\alpha \vee \beta)$ abrevia $((\neg \alpha) \to \beta)$
$\leftrightarrow$	*biimplica*	$(\alpha \leftrightarrow \beta)$ abrevia $((\alpha \to \beta) \wedge (\beta \to \alpha))$
$\exists$	*existe*	$(\exists x \alpha)$ abrevia $(\neg(\forall x(\neg \alpha)))$
$\nexists$	*não existe*	$(\nexists x \alpha)$ abrevia $(\neg(\exists x \alpha))$
$\neq$	*diferente*	$(s \neq t)$ abrevia $(\neg(s \doteq t))$
$\perp$	*falsum*	abrevia $(\alpha \wedge (\neg \alpha))$
$\top$	*verum*	abrevia $(\neg \perp)$

Exercício 3.11. *Escreva* $(\alpha \leftrightarrow \beta)$ *e* $(\nexists x \alpha)$ *usando apenas conectivos e quantificadores do alfabeto* $\mathscr{A}_1$.

Representamos os conectivos lógicos binários $\vee$, $\wedge$, $\to$ e $\leftrightarrow$ genericamente, pelo símbolo $\square$, no caso de múltiplas ocorrências de conectivos distintos usaremos índices $\square_1$, $\square_2$ e assim por diante. Com isso $\alpha \square \beta$ indica uma fórmula composta por α, β e algum dos conectivos e qual deles, especificamente, não importa no momento em que se usa o símbolo $\square$ com o cuidado de que duas ocorrências numa mesma frase significa o mesmo conectivo; por exemplo em "$\alpha \square \eta$ deve ser lido como $(\alpha \square \eta)$" *não* deve ser entendido como, por exemplo, "$\alpha \to \eta$ deve ser lido como $(\alpha \wedge \eta)$" mas sim como "$\alpha \to \eta$ deve ser lido como $(\alpha \to \eta)$" (e, respectivamente, o mesmo para $\square$ sendo $\wedge, \vee, \leftrightarrow$).

Ademais, representamos os quantificadores $\forall$ e $\exists$ genericamente por $\textcircled{Q}$ possivelmente com índices.

Omissão de parênteses

- Omitimos os parênteses externos de uma fórmula, recolocando quando a usamos para compor outras fórmulas. Por exemplo, escrevemos $\alpha \to \beta$ no lugar de $(\alpha \to \beta)$, mas recolocamos os parênteses quando escrevemos, por exemplo, $\forall x(\alpha \to \beta)$.
- $\forall$ tem precedência sobre $\neg$ que tem precedência sobre $\to$; considerando as abreviações ordem de precedência é $\forall, \exists, \neg, \wedge, \vee, \to, e \leftrightarrow$.
- Em sequências de conectivos omitimos o uso sucessivo de parênteses. Isto é, escrevemos $\alpha \wedge \beta \wedge \gamma$ no lugar de $\alpha \wedge (\beta \wedge \gamma)$ e $\alpha \to \beta \to \gamma$ é lido como $\alpha \to (\beta \to \gamma)$. O mesmo valendo para os outros conectivos.
- Quando não houver riscos de más interpretações, omitimos os parênteses externos em subfórmulas do tipo $\forall x \alpha$, $\exists x \alpha$ e $\neg \alpha$. Por exemplo, escrevemos $\neg \forall x \exists y \alpha$, em vez de $\neg(\forall x(\exists y \alpha))$.

Exemplo 3.12. De volta ao exemplo 3.8

$$\Big(\big(R_1^1 x_1 \to R_2^3 x_4 x_2 c_1\big) \to \big(\forall x_1 ((\forall x_2\, R_2^3 c_4 x_2 c_1) \to (\neg(\doteq F_1^1 x_1 F_1^1 c_1)))\big)\Big)$$

que simplificando fica escrito como

$$(R(x) \to S(z,y,c)) \to \forall x \forall y \big(S(a,y,c) \to (F(x) \neq F(c))\big).$$

3.1.4 Linguagem de primeira ordem para a Aritmética

Vejamos um exemplo de linguagem de primeira ordem para a Aritmética que consiste do estudo dos números naturais e suas propriedades. Denotaremos essa linguagem por $\mathscr{L}_N$ cujo alfabeto contém, além dos símbolos lógicos, os não-lógicos

- a constante 0,
- o símbolo funcional unário S e os símbolos funcionais binários $+$ e $\cdot$, e
- o símbolo relacional binário $<$.

São exemplos de termos dessa linguagem $+\cdot 0 x_1 x_2$, $SSSS0$, $+x_1 S0$, $\doteq \cdot x_1 + S0SS0 \cdot x_1 SSS0$. Usando as convenções de simplificação reescrevemo-os $(0 \cdot x) + y$, $S(S(S(S(0))))$, $x + S(0)$, $x \cdot (S(0) + S(S(0))) \doteq x \cdot S(S(S(0)))$. São fórmulas da linguagem:

1. $< \cdot S0S0 + S0S0$ ou, simplesmente, $S(0) \cdot S(0) < S(0) + S(0)$.
2. $(\forall x_1 \doteq +0 x_1 x_1)$ ou, simplesmente, $\forall x (x + 0 \doteq x)$.
3. $\Big(\forall x_1 \big(\forall x_2 (\doteq +S0 x_1 + x_2 S0 \to \doteq x_1 x_2)\big)\Big)$ ou $\forall x \forall y (x + S(0) \doteq y + S(0) \to x \doteq y)$.
4. Já simplificado $\forall x \forall y \exists z \big(y \doteq x + z \to (x < y \vee x \doteq y)\big)$.

A intenção é interpretar a constante 0 como o número *zero*, S como a *função sucessor* e $+, \cdot, <$ interpretados como, respectivamente, a adição, a multiplicação é o menor que em $\mathbb{N}$. Os termos $0, S0, SS0, SSS0, SSSS0, \ldots$ intencionam descrever os números naturais zero, um , dois, três, quatro, etc. Com essa interpretação, que ainda é somente uma intenção, podemos dar alguns exemplos intuitivos de expressões da aritmética nessa linguagem.

Exemplo 3.13. 'Não existe raiz de 2' é expresso por $\nexists x (x \cdot x \doteq S(S(0)))$ que reescrita usando somente símbolos do alfabeto fica $(\neg(\neg(\forall x_1 (\neg(\doteq \cdot x_1 x_1 SS0)))))$. Também podemos expressar a mesma ideia usando $(\forall x_1 (\neg(\doteq \cdot x_1 x_1 SS0)))$.

Exercício 3.14. *Expresse em $\mathscr{L}_N$ a sentença 'existem infinitos números primos'.*

Outros exemplos informais em linguagens de primeira ordem

Na linguagem da igualdade pura, $\mathscr{L}_=$, que não tem símbolos não-lógicos, conseguimos expressar certas ideias, por exemplo, 'existe um único sujeito' por $\exists x \forall y (y \doteq x)$, ou 'existem somente dois sujeitos' por $\exists x \exists y ((x \neq y) \wedge \forall z (z \doteq x \vee z \doteq y))$.

Na linguagem para Teoria dos Conjuntos $\mathscr{L}_C$, que só tem o símbolo relacional binário $\in$, a intenção das variáveis é representar conjuntos e $x \in y$ diz que o conjunto x é elemento do conjunto y. A Teoria de Conjuntos de Zermelo–Fraenkel é escrita nessa linguagem. A existência do conjunto vazio é expressa por $\exists x \forall y \neg(y \in x)$.

A existência do conjunto definido no paradoxo de Russel (página 11) é expresso por

$$\exists x \forall y (y \in x \leftrightarrow \neg(y \in y)). \tag{3.1}$$

Exercício 3.15. *Escreva uma fórmula que simboliza a sentença 'existe um único conjunto vazio' em $\mathscr{L}_C$.*

3.2 Variáveis livres, ligadas e substituição de variáveis

Dizemos que uma variável x ocorre **livre** em uma fórmula α se

1. α é atômica e x ocorre em α;
2. α é da forma $(\neg\beta)$ e x ocorre livre em β;
3. α é da forma $(\beta \square \gamma)$ e x ocorre livre em β ou γ;
4. α é da forma $Q\, y\psi$ e x é diferente de y e x ocorre livre em ψ.

Uma ocorrência de x em α que não é livre é dita **ligada**. O item 4 acima é a chave para classificarmos a ocorrência de uma variável como livre ou ligada: a ocorrência de uma variável x é ligada se ela está no escopo de uma ocorrência de um quantificador. O escopo de um quantificador numa fórmula α é a subfórmula β na qual o quantificador se aplica (quando a regra de formação de fórmula quantificada foi aplicada, isto é, em $(\forall x\, \beta)$ o escopo de x é β).

Cada ocorrência de uma variável x é livre ou ligada, mas não ambas. Entretanto, a mesma variável pode ocorrer livre e ligada na mesma fórmula. Por exemplo,

1. Em $\forall x_7 (x_5 \doteq x_7)$ a ocorrência de x_5 é livre e a ocorrência de x_7 é ligada.
2. Em $\forall x_0 ((x_0 \doteq F(x_6)) \to (\neg \forall x_6\, R(x_6)))$ a primeira ocorrência de x_6 é livre e a última ocorrência é ligada.
3. Em $\forall z (\forall x (P(x) \to R(z))) \to (Q(y) \to P(x))$ a variável x é livre e ligada, y é livre e z é ligada.

Uma fórmula α sem ocorrência de variáveis livre é dita **sentença**.

O conjunto das variáveis livres

Antes de irmos adiante, definimos recursivamente o conjunto VL das variáveis livres de uma fórmula:

1. se t é termo então

$$VL(t) = \begin{cases} \varnothing, & \text{se } t \text{ é } c \\ \{x\}, & \text{se } t \text{ é } x \\ VL(t_1) \cup \cdots \cup VL(t_n), & \text{se } t \text{ é } F(t_1, \ldots, t_n) \end{cases}$$

2. se α é fórmula então

$$VL(\alpha) = \begin{cases} VL(t_1) \cup VL(t_2), & \text{se } \alpha \text{ é } t_1 \doteq t_2 \\ VL(t_1) \cup \cdots \cup VL(t_n), & \text{se } \alpha \text{ é } R(t_1, \ldots, t_n) \\ VL(\beta), & \text{se } \alpha \text{ é } \neg\beta \\ VL(\beta) \cup VL(\gamma), & \text{se } \alpha \text{ é } \beta\Box\gamma \\ VL(\beta) \setminus \{x\}, & \text{se } \alpha \text{ é } Q x \beta \end{cases}$$

Pelos metateoremas de indução o conjunto VL está definido para todos os termos e todas as formulas da linguagem $\mathscr{L}_1$.

3.2.1 Substituição de variáveis

Se t e s são termos e x é uma variável, definimos $[t]^s_x$ o termo obtido substituindo *toda* ocorrência da variável x pelo termo s. Formalmente, definimos a **substituição em termos** recursivamente:

- $[x]^s_x$ é o termo s e $[y]^s_x$ é o termo y;
- se c é uma constante, $[c]^s_x$ é o termo c;
- se t é da forma $F(t_1, \ldots, t_n)$, então $[t]^s_x$ é o termo $F([t_1]^s_x, \ldots, [t_n]^s_x)$.

Se α é uma fórmula, x é uma variável e t é um termo, definimos $[\alpha]^t_x$ a fórmula obtida substituindo todas as ocorrências *livres* da variável x pelo termo t.

Formalmente, definimos a **substituição em fórmulas** recursivamente

- se α é $(s \doteq t)$ então $[\alpha]^t_x$ é $([s]^t_x \doteq [t]^t_x)$;
- Se α é $R(t_1, t_2, \ldots, t_n)$ então $[\alpha]^t_x$ é $R([t_1]^t_x, [t_2]^t_x, \ldots, [t_n]^t_x)$;
- Se α é $\neg\beta$ então $[\alpha]^t_x$ é $\neg[\beta]^t_x$;
- Se α é $\gamma\Box\beta$ então $[\alpha]^t_x$ é $[\gamma]^t_x\Box[\beta]^t_x$;
- Se α é $Q x \beta$ então $[\alpha]^t_x$ é α; senão, sempre que $y \neq x$, se α é $Q y \beta$ então $[\alpha]^t_x$ é $Q y [\beta]^t_x$.

Por exemplo

1. $[(x \doteq y)]^x_y$ é $(x \doteq x)$.
2. $[(x \doteq y)]^y_x$ é $(y \doteq y)$.
3. $[\forall x (x \doteq y)]^y_x$ é $\forall x (x \doteq y)$.
4. $[\forall x (x \doteq y)]^x_y$ é $\forall x (x \doteq x)$.
5. $[(\forall x P(x)) \to P(x)]^\tau_x$ é $\forall x P(x) \to P(\tau)$.
6. $[\forall x (\neg\forall y (x \doteq y)) \to (\neg\forall y (x \doteq y))]^y_x$ é $\forall x (\neg\forall y (x \doteq y)) \to (\neg\forall y (y \doteq y))$.
7. $[\forall x (P(x, y) \to (\neg Q(y) \vee \exists y P(x, y)))]^{F(y,z)}_y$ é $\forall x (P(x, F(y, z)) \to (\neg Q(F(y, z)) \vee \exists y P(x, y)))$.

Exemplo 3.16. Considere em $\mathscr{L}_N$ a fórmula $\exists x(y \doteq S(S(0)) \cdot x)$. Se substituímos y pelo termo $S(S(S(0)))$ temos $\exists x (S(S(S(0))) \doteq S(S(0)) \cdot x)$. Se substituímos por x então temos $\exists x(x \doteq S(S(0)) \cdot x)$

Substituição admissível

A substituição da variável x pelo termo t na fórmula φ é **admissível** se nenhuma ocorrência livre de x em φ estiver no escopo de um quantificador que *liga* qualquer variável que aparece em t. Isto é, para cada variável y que aparece em t, nenhum lugar onde x ocorre livre em φ está no escopo de '$\exists y$' ou '$\forall y$'.

Por exemplo, o termo x não é admissível para a variável y na fórmula $\forall x P(x,y)$; o termo $F(x,y)$ não é admissível para a variável x em $\forall y P(x,y)$; o termo z é admissível para y em $P(y,z) \to \forall y Q(y,z)$.

Formalmente, o termo t é **admissível** para a variável x na fórmula α se

1. α é atômica;
2. α é $\neg\beta$ e t é admissível para t em β;
3. α é $\beta \Box \gamma$ e t é admissível para x em α e em β;
4. α é $Q y \beta$ e se $x \in VL(\beta)$ então $y \notin VL(t)$ e t é admissível para x em β.

Exercício 3.17. *Prove usando indução em fórmulas que t é admissível para x em α se, e só se, as variáveis de t na fórmula $[\alpha]_x^t$ não são ligadas por um quantificador.*

Se $x \notin VL(\alpha)$, então $[\alpha]_x^t$ é admissível para qualquer termo t e, nesse caso, as fórmulas α e $[\alpha]_x^t$ são idênticas. Uma variável x sempre é admissível para ela mesmo em qualquer fórmula e $[\varphi]_x^x$ é a fórmula φ. A variável y não é uma substituição admissível para x na fórmula $\forall y\,(x \doteq y)$ porque se substituímos x por y a nova ocorrência de y seria ligada. Isso fará diferença no valor verdade de uma sentença, enquanto que $\forall y\,(y \doteq y)$ será uma tautologia em qualquer interpretação, a fórmula $\forall y\,(x \doteq y)$ tem valor verdade que dependerá da interpretação.

Exercício 3.18. *É x uma substituição admissível para z em φ se φ é $z \doteq x \to \forall z\,(z \doteq x)$? Em caso afirmativo, o que é $[\varphi]_z^x$?*

3.2.2 Generalização

Se α é uma fórmula então uma **generalização** de α é a fórmula

$$\forall x_1 \forall x_2 \cdots \forall x_n\, \alpha$$

para quaisquer coleção de variáveis $x_1, x_2, \ldots, x_n$, independente delas ocorrerem ou não em α.

Exemplo 3.19. São generalizações de $x \doteq y$ as fórmulas: $\forall x\,(x \doteq y)$, $\forall y\,(x \doteq y)$, $\forall y \forall x\,(x \doteq y)$, $\forall z \forall y \forall x\,(x \doteq y)$, $\forall w \forall z \forall y \forall x\,(x \doteq y)$.

3.3 Sistema dedutivo axiomático

Como na lógica proposicional, são conhecidos alguns sistemas dedutivos para o cálculo de predicados que são equivalentes no sentido de deduzirem os mesmos teoremas. Apresentaremos um do tipo **Sistema de Hilbert** para a linguagem $\mathscr{L}_1$ da lógica de primeira ordem. Tal sistema é axiomático, consiste numa lista finita de **axiomas** e outra de **regras de inferência** que podem ser usados para derivar os teoremas do sistema.

Também como na lógica proposicional chamaremos de axioma e teorema, por exemplo, $\alpha \to (\beta \to \alpha)$ e $\forall x\,(\alpha \to \beta) \to (\alpha \to \forall x\,\beta)$ o que, de fato, são **esquemas de axiomas e de teoremas** pois usam variáveis da metalinguagem. Os axiomas são obtidos quando substituímos tais variáveis por fórmulas nas quais figuram apenas símbolos do alfabeto de modo que toda ocorrência da mesma (meta)variável é substituída pela mesma fórmula.

Exemplo 3.20. Uma linguagem para a Teoria dos Grupos tem uma constante, denotada por e, e uma função binária, denotada por $\circ$. Essa teoria é a coleção dos teoremas que podem ser provados a partir dos seguintes axiomas não-lógicos

(G1) $\forall x\,((x \circ e \doteq x) \land (e \circ x \doteq x))$;
(G2) $\forall x \exists y\,(x \circ y \doteq e)$;
(G3) $\forall x \forall y \forall z\,(x \circ (y \circ z) \doteq (x \circ y) \circ z)$.

3.3.1 Axiomas

Um sistema dedutivo para uma linguagem de primeira ordem tem duas classes de axiomas, os *lógicos* comuns a todas as linguagens e os *não-lógicos*. Um axioma lógico é uma sentença ou uma fórmula universalmente válida (ou seja, é verdadeira em qualquer possível universo, não importa como os termos da fórmula são interpretados). Normalmente, toma-se como axiomas lógicos algum conjunto mínimo de fórmulas suficiente para derivar todas as fórmulas universalmente válidas. No exemplo 3.49 apresentamos três axiomas não lógicos da Teoria dos Grupos. Os esquemas de **axiomas lógicos** são

(A1) $\alpha \to (\beta \to \alpha)$
(A2) $(\alpha \to (\beta \to \xi)) \to ((\alpha \to \beta) \to (\alpha \to \xi))$
(A3) $(\alpha \to \beta) \to ((\alpha \to \neg\beta) \to \neg\alpha)$
(A4) $\alpha \to (\beta \to (\alpha \land \beta))$
(A5) $\alpha \land \beta \to \alpha$
(A6) $\alpha \land \beta \to \beta$
(A7) $\alpha \to \alpha \lor \beta$
(A8) $\beta \to \alpha \lor \beta$
(A9) $(\alpha \to \gamma) \to ((\beta \to \gamma) \to (\alpha \lor \beta \to \gamma))$
(A10) $\neg\neg\alpha \to \alpha$
(A11) $(\forall x\,(\alpha \to \beta)) \to (\forall x\,\alpha \to \forall x\,\beta)$.
(A12) $(\forall x\,\alpha) \to [\alpha]_x^t$ sempre que t é admissível para x em α.
(A13) $\alpha \to \forall x\,\alpha$ sempre que $x \not\in VL(\alpha)$.
(A14) $t \doteq t$
(A15) $t_1 \doteq t_2 \to t_2 \doteq t_1$
(A16) $(t_1 \doteq t_2 \land t_2 \doteq t_3) \to t_1 \doteq t_3$

(A17) $(t_1 \doteq t_1' \wedge \cdots \wedge t_n \doteq t_n') \to \big(R(t_1,\ldots,t_n) \to R(t_1',\ldots,t_n')\big)$
(A18) $(t_1 \doteq t_1' \wedge \cdots \wedge t_n \doteq t_n') \to \big(F(t_1,\ldots,t_n) \doteq F(t_1',\ldots,t_n')\big)$
(A19) as generalizações dos esquemas de fórmulas acima.

em que α,β,γ,ξ são fórmulas, x é variável, t e $t_1,t_2,t_3,\ldots,t_n$ são termos, R é símbolo relacional (podendo ser o $\doteq$)e F símbolo funcional.

Exemplo 3.21. Caso não houvesse restrição sobre a substituição de variável nos axiomas do $\forall$ seria possível o axioma $\forall x \exists y\,(x \neq y) \to \exists y\,(y \neq y)$, por exemplo, que intuitivamente deveria ser falso. Numa interpretação onde o universo tem mais de um elemento, a fórmula $\forall x \exists y\,(x \neq y)$ é válida e usando o esquema (A12) incondicionalmente teríamos o axioma $\forall x \exists y\,(x \neq y) \to [\exists y\,(x \neq y)]^x_y$, ou seja, teríamos o axioma $\forall x \exists y\,(x \neq y) \to \exists y\,(y \neq y)$ que, intuitivamente, deveria ser falso.

Exemplo 3.22. A fórmula

$$\neg\forall y \neg P(y) \to \big(P(x) \to \neg\forall y \neg P(y)\big)$$

é uma instância do esquema (A1), portanto é um axioma. A fórmula

$$(R(x,y) \to (\exists y\,(y \doteq 0) \vee R(x,y))$$

é uma instância de $\beta \to (\alpha \vee \beta)$, portanto é um axioma do esquema (A8). A fórmula

$$\forall x\big(\neg\forall y\,(x \doteq y)\big) \to \big(\neg\forall y\,(z \doteq y)\big)$$

é um axioma do esquema (A12). Também é a fórmula

$$\forall x\big(A(x) \to \forall y\,A(y)\big) \to \big(A(y) \to \forall y\,A(y)\big)$$

porém a fórmula

$$\forall x\big(\forall y\,B(x,y)\big) \to \forall y\,B(y,y)$$

não é um axioma desse esquema porque viola a condição de admissibilidade.

Exemplo 3.23. Na linguagem aritmética, por exemplo, temos o axioma lógico

$$(x < y) \to (\exists y\,(y \doteq 0) \vee (x < y))$$

do esquema $\beta \to (\alpha \vee \beta)$.

Exercício 3.24. *A fórmula* $(x \doteq y) \to ((x + x \doteq 0) \to (x + y \doteq 0))$ *é um axioma?*

3.3.2 Regras de inferência

Há uma única regra de inferência (de fato esquema) do sistema

(MP) $\dfrac{\alpha,\ \alpha \to \beta}{\beta}$

3.3.3 Dedução

Sejam α uma fórmula da linguagem de primeira ordem $\mathscr{L}_1$ e $\Gamma \subset \mathscr{L}_1$ um conjunto de *hipóteses* ou *premissas*. Uma **prova** de α a partir de Γ é uma sequência finita de fórmulas

$$\langle \varphi_1, \varphi_2, \ldots, \varphi_n \rangle$$

tal que $\varphi_n = \alpha$ e, para $i < n$, φ_i é

1. ou um axioma lógico
2. ou uma fórmula de Γ
3. ou uma fórmula obtida de $\varphi_1, \varphi_2, \ldots, \varphi_{i-1}$ por regra de inferência.

$\Gamma \vdash \alpha$ e lê-se "α é um **teorema de** Γ". No caso Γ vazio escrevemos $\vdash \alpha$ e, nesse caso, α é um **teorema lógico**.

Simplificações de notação:

usamos as mesmas simplificações adotadas na lógica proposicional, ao invés de $\{\alpha\} \vdash \beta$ escrevemos $\alpha \vdash \beta$; ao invés de $\{\alpha_1, \ldots, \alpha_n\} \vdash \beta$ escrevemos $\alpha_1, \ldots, \alpha_n \vdash \beta$; ao invés de $\Gamma \cup \{\alpha\} \vdash \beta$ escrevemos $\Gamma, \alpha \vdash \beta$.

Propriedades de $\vdash$

As seguintes propriedades valem exatamente como na lógica de proposições. Como os esquemas de axiomas (A1)–(A10) e a única regra de inferência são os mesmos da lógica proposicional (agora para fórmulas da lógica de predicados) e definição de dedução é a mesma, temos que o $\vdash$ na lógica de predicados tem as mesmas propriedades de $\vdash$ do sistema dedutivo para a lógica de proposições.

Metateorema 3.25. *Se* Γ *é um conjunto de fórmulas de* $\mathscr{L}_1$

Autodedução $\Gamma \vdash \alpha$ *para todo* $\alpha \in \Gamma$.
Monotonicidade *Se* $\Gamma \vdash \alpha$ *então* $\Gamma \cup \Sigma \vdash \alpha$.
Regra do corte *Se* $\Gamma \vdash \alpha_i$ *para* $i = 1, 2, \ldots, k$ *e* $\{\alpha_1, \ldots, \alpha_k\} \vdash \beta$ *então* $\Gamma \vdash \beta$.
Compacidade $\Gamma \vdash \alpha$ *se, e só se, existe* $\Delta \subseteq \Gamma$ *finito tal que* $\Delta \vdash \alpha$.
Teorema da Dedução $\alpha \vdash \beta$ *se, e somente se,* $\vdash \alpha \to \beta$ *ou, genericamente,*

$$\Gamma, \alpha \vdash \beta \text{ se, e somente se, } \Gamma \vdash \alpha \to \beta.$$

O teoremas lógicos proposicionais valem com a mesma dedução na lógica de predicados.

Teorema 3.26. $\vdash \alpha \to \alpha$

Prova. Deduz-se como no teorema 1.9.

1.	$\alpha \to ((\alpha \to \alpha) \to \alpha))$	(por A1)
2.	$(\alpha \to ((\alpha \to \alpha) \to \alpha)) \to ((\alpha \to (\alpha \to \alpha)) \to (\alpha \to \alpha))$	(por A2)
3.	$\alpha \to (\alpha \to \alpha))$	(por A1)
4.	$(\alpha \to (\alpha \to \alpha)) \to (\alpha \to \alpha)$	(MP 2,1)
5	$\alpha \to \alpha$	(MP 3,4)

∎

Teorema 3.27 (Redução ao absurdo (RA)). $\alpha \to \beta, \alpha \to \neg\beta \vdash \neg\alpha$

Demonstração. Segue do Teorema da Dedução em (A3). ■

Teorema 3.28 (Introdução da conjunção (IC)). $\alpha, \beta \vdash \alpha \wedge \beta$

Demonstração. Segue do Teorema da Dedução em (A4). ■

Teorema 3.29 (Eliminação da conjunção (EC1)). $\alpha \wedge \beta \vdash \alpha$

Demonstração. Segue do Teorema da Dedução em (A5). ■

Teorema 3.30 (Eliminação da conjunção (EC2)). $\alpha \wedge \beta \vdash \beta$

Demonstração. Segue do Teorema da Dedução em (A6). ■

Teorema 3.31 (Introdução da disjunção (ID1)). $\alpha \vdash \alpha \vee \beta$

Demonstração. Segue do Teorema da Dedução em (A7). ■

Teorema 3.32 (Introdução da disjunção (ID2)). $\beta \vdash \alpha \vee \beta$

Demonstração. Segue do Teorema da Dedução em (A8). ■

Teorema 3.33 (Duns Scotus (DS)). $\alpha, \neg\alpha \vdash \beta$

Prova. Dá-se como na dedução do teorema 1.14.

1.	α	(hip.)
2.	$\neg\alpha$	(hip.)
3.	$\alpha \to (\neg\beta \to \alpha)$	(A1)
4.	$\neg\alpha \to (\neg\beta \to \neg\alpha)$	(A1)
5.	$\neg\beta \to \alpha$	(MP 1,3)
6.	$\neg\beta \to \neg\alpha$	(MP 2,4)
7.	$(\neg\beta \to \alpha) \to \big((\neg\beta \to \neg\alpha) \to \neg\neg\beta\big)$	(A3)
8.	$(\neg\beta \to \neg\alpha) \to \neg\neg\beta$	(MP 5,7)
9.	$\neg\neg\beta$	(MP 6,8)
10.	$\neg\neg\beta \to \beta$	(A10)
11.	β	(MP 9,10)

■

Teorema 3.34 (Modus Tollens (MT)). $\alpha \to \beta, \neg\beta \vdash \neg\alpha$

Prova.

1.	$\alpha \to \beta$	(hip.)
2.	$\neg\beta$	(hip.)
3.	$(\alpha \to \beta) \to ((\alpha \to \neg\beta) \to \neg\alpha)$	(A3)
4.	$\neg\beta \to (\alpha \to \neg\beta)$	(A1)
5.	$\alpha \to \neg\beta$	(MP 2,4)
6.	$(\alpha \to \neg\beta) \to \neg\alpha$	(MP 1,3)
7.	$\neg\alpha$	(MP 5,6)

■

Teorema 3.35 (Contra-positiva (CP1)). $\alpha \to \beta \vdash \neg\beta \to \neg\alpha$

Demonstração. Segue de Modus Tollens por aplicação do Teorema da Dedução. ■

Teorema 3.36 (Silogismo hipotético (SH)). $\alpha \to \beta, \beta \to \gamma \vdash \alpha \to \gamma$

Prova. Dá-se como a dedução do teorema 1.10. ■

Teorema 3.37 (Silogismo disjuntivo (SD)). $\alpha \vee \beta, \neg\alpha \vdash \beta$

Prova.

1.	$\alpha \vee \beta$	(hip.)
2.	$\neg\alpha \to \beta$	(def. de $\vee$)
3.	$\neg\alpha$	(hip.)
4.	β	(por MP 2,3)

■

Teorema 3.38 (Troca condicional (TC)). $\theta \to (\phi \to \xi) \vdash \phi \to (\theta \to \xi)$

Prova. Segue a dedução do teorema 1.11. ■

Teorema 3.39 (Dupla negação (DN1)). $\neg\neg\alpha \vdash \alpha$.

Prova. Segue de (A10) e o teorema da Dedução. ■

Teorema 3.40 (Dupla negação (DN2)). $\vdash \alpha \to \neg\neg\alpha$

Prova. Deduz-se como no teorema 1.13. ■

Teorema 3.41 (Contra-positiva (CP2)). $\neg\beta \to \neg\alpha \vdash \alpha \to \beta$

Prova.

1.	$\neg\beta \to \neg\alpha$	(hip.)
2.	$(\neg\beta \to \neg\alpha) \to (\neg\neg\alpha \to \neg\neg\beta)$	(CP1)
3.	$\neg\neg\alpha \to \neg\neg\beta$	(MP 1,2)
4.	$\alpha \to \neg\neg\alpha$	(DN2)
5.	$\neg\neg\beta \to \beta$	(DN1)
6.	$\alpha \to \neg\neg\beta$	(SH 4,3)
7.	$\alpha \to \beta$	(SH 6,5)

■

Regras de inferências derivadas

Os sistemas dedutivos do estilo de Hilbert têm poucas regras de dedução. Aaas regras de inferência adicionais advindas dos teoremas lógicos não acrescentam nenhum poder dedutivo ao sistema, no sentido de que uma dedução usando as novas regras de dedução pode ser convertida em uma dedução usando apenas a dedução com a regra original.

Uma regra de inferência derivada é uma regra de inferência que não é dada a nós como parte do sistema dedutivo, mas que constitui uma abreviatura usando um teorema previamente provado. Em particular, suponha que tenhamos $\Gamma \vdash \alpha$ com $\Gamma = \{\gamma_1, \dots, \gamma_k\}$ um conjunto finito de teoremas. Então sempre que deduzimos, digamos numa prova de $\Sigma \vdash \beta$, os teoremas de Γ, podemos usar $\Gamma \vdash \alpha$ para deduzir α. Assim, acrescentamos a regra

$$\frac{\gamma_1, \dots, \gamma_k}{\alpha}$$

à nossa lista de regras de inferência. O teoremas acima nos dão várias regras derivadas, todas já conhecidas do cálculo porposicional e que agora valem para fórmulas da lógica de predicados. Vejamos algumas regras de inferência derivadas dos "novos" axiomas.

Teorema 3.42 (Instanciação universal (IU)). $\forall x \alpha \vdash [\alpha]^t_x$, *para todo termo t admissível para x.*

Demonstração. Segue do Teorema da Dedução em (A12). ∎

Teorema 3.43 (Generalização universal (G)). $\alpha \vdash \forall x \alpha$, *se $x \notin VL(\alpha)$.*

Demonstração. Segue do Teorema da Dedução em (A13). ∎

Teorema 3.44 (Generalização existencial (GE)). $[\alpha]^t_x \vdash \exists x \alpha$, *se t é admissível para x.*

Prova. Provaremos $\vdash [\alpha]^t_x \to \exists x \alpha$, se t é admissível para x; o teorema segue do teorema da Dedução. Seja t uma substituição admissível para x em α.

1.	$\forall x \neg\alpha \to \neg[\alpha]^t_x$	(A12)
2.	$(\forall x \neg\alpha \to \neg[\alpha]^t_x) \to (\neg\neg[\alpha]^t_x \to \neg\forall x \neg\alpha)$	(CP1)
3.	$\neg\neg[\alpha]^t_x \to \neg\forall x \neg\alpha$	(MP 1,2)
4.	$[\alpha]^t_x \to \neg\neg[\alpha]^t_x$	(DN2)
5.	$[\alpha]^t_x \to \neg\forall x \neg\alpha$	(SH 3,4)
6.	$[\alpha]^t_x \to \exists x \alpha$	(def. de $\exists$)

∎

Teorema 3.45. $\vdash \forall x \alpha \to \exists x \alpha$

Prova. Fixado t admissível para x em α

1.	$\forall x \alpha \to [\alpha]^t_x$	(A12)
2.	$[\alpha]^t_x \to \exists x \alpha$	(GE)
3.	$\forall x \alpha \to \exists x \alpha$	(SH 1,2)

∎

Com a notação usual temos as seguintes regras derivadas dos teoremas acima.

(RA) $\dfrac{\alpha \to \beta, \alpha \to \neg\beta}{\neg\alpha}$

(IC) $\dfrac{\alpha, \beta}{\alpha \wedge \beta}$

(EC1) $\dfrac{\alpha \wedge \beta}{\alpha}$

(EC2) $\dfrac{\alpha \wedge \beta}{\beta}$

(ID1) $\dfrac{\alpha}{\alpha \vee \beta}$

(ID2) $\dfrac{\beta}{\alpha \vee \beta}$

(DS) $\dfrac{\alpha, \neg\alpha}{\beta}$

(MT) $\dfrac{\alpha \to \beta, \neg\beta}{\neg\alpha}$

(SH) $\dfrac{\alpha \to \beta, \beta \to \gamma}{\alpha \to \gamma}$

(TC) $\dfrac{\theta \to (\phi \to \xi)}{\phi \to (\theta \to \xi)}$

(CP1) $\dfrac{\alpha \to \beta}{\neg\beta \to \neg\alpha}$

(CP2) $\dfrac{\neg\beta \to \neg\alpha}{\alpha \to \beta}$

(DN1) $\dfrac{\neg\neg\alpha}{\alpha}$

(DN2) $\dfrac{\alpha}{\neg\neg\alpha}$

(G) $\dfrac{\alpha}{\forall x\,\alpha}$, se $x \notin VL(\alpha)$.

(IU) $\dfrac{\forall x\,\alpha}{[\alpha]_x^t}$, se t admissível para x.

(GE) $\dfrac{[\alpha]_x^t}{\exists\alpha}$, se t admissível para x.

$(\forall/\exists)$ $\dfrac{\forall x\,\alpha}{\exists x\,\alpha}$

Metateorema 3.46 (Teorema da Generalização). *Seja* Γ *tal que a variável* x *não ocorre livre em nenhuma fórmula de* Γ. *Se* $\Gamma \vdash \alpha$ *então* $\Gamma \vdash \forall x\,\alpha$.

Demonstração. Suponha que $\Gamma \vdash \alpha$ e seja $\langle\theta_1, \ldots, \theta_n\rangle$ uma prova. Demonstraremos por indução em i que $\Gamma \vdash \forall x\theta_i$.

Se θ_1 é axioma lógico então $\forall x\theta_1$ é axioma lógico, portanto $\Gamma \vdash \forall x\theta_1$.

Se $\theta_1 \in \Gamma$ então $x \notin VL(\theta_1)$ e podemos usar o esquema (A13) como em

1. θ_1 (hip.)
2. $\theta_1 \to \forall x\theta_1$ (A13)
3. $\forall x\theta_1$ (MP 1,2)

Portanto, $\theta_1 \vdash \forall x\theta_1$ e por monotonicidade $\Gamma \vdash \forall x\theta_1$.

Assuma, como hipótese da indução, que $\Gamma \vdash \forall x\theta_i$ para $i = 1, 2, \ldots, m-1$. Vamos provar $\Gamma \vdash \forall x\theta_m$. Se θ_m é axioma lógico ou está em Γ então $\Gamma \vdash \forall x\theta_m$ (a demonstração é análoga ao caso $i = 1$). Senão, existem $j, k < m$ tais que θ_m é *modus ponens* de θ_j (na linha j) e $\theta_j \to \theta_m$ (na linha k). Por hipótese de indução temos

$$\Gamma \vdash \forall x\theta_j \quad \text{e} \quad \Gamma \vdash \forall x(\theta_j \to \theta_m) \tag{3.2}$$

agora

1.	$\forall x \theta_j$	(teorema)
2.	$\forall x (\theta_j \to \theta_m)$	(teorema)
3.	$\forall x (\theta_j \to \theta_m) \to (\forall x \theta_j \to \forall x \theta_m)$	(A11)
4.	$\forall x \theta_j \to \forall x \theta_m$	(MP 2,3)
5.	$\forall x \theta_m$	(MP 1,4)

portanto $\forall x \theta_j, \forall x (\theta_j \to \theta_m) \vdash \forall x \theta_m$ e da regra do corte com (3.2) concluímos $\Gamma \vdash \forall x \theta_m$.

Portanto $\Gamma \vdash \forall x \theta_i$ para todo i, $1 \le i \le n$, em particular, $\Gamma \vdash \forall x \alpha$. ■

Nos próximos exemplos x não ocorre livre na fórmula α.

$$\alpha \to \forall x \beta \vdash \forall x(\alpha \to \beta).$$

Prova.

1.	$\alpha \to \forall x \beta$	(hip.)
2.	$\forall x \beta \to \beta$	(A13)
3.	$\alpha \to \beta$	(SH 1,2)
4.	$\forall x(\alpha \to \beta)$	(TG)

$$\forall x(\alpha \to \beta) \vdash (\alpha \to \forall x \beta).$$

Prova.

1.	$\forall x(\alpha \to \beta)$	(hip.)
2.	$\forall x(\alpha \to \beta) \to (\forall x\alpha \to \forall x\beta)$	(A11)
3.	$\forall x\alpha \to \forall x\beta$	(MP 1,2)
4.	$\alpha \to \forall x\alpha$ pois $x \notin VL(\alpha)$	(A13)
5.	$\alpha \to \forall x\beta$	(SH 3,4)

■

Portanto, se x não ocorre livre em α

$$\vdash (\alpha \to \forall x \beta) \leftrightarrow \forall x(\alpha \to \beta).$$

Prova.

1.	$\forall x(\alpha \to \beta) \to (\alpha \to \forall x \beta)$	(teo.)
2.	$(\alpha \to \forall x \beta) \leftrightarrow \forall x(\alpha \to \beta)$	(teo.)
3.	$\forall x(\alpha \to \beta) \to (\alpha \to \forall x \beta) \land (\alpha \to \forall x \beta) \leftrightarrow \forall x(\alpha \to \beta)$	(IC 1,2)
4.	$\forall x(\alpha \to \beta) \leftrightarrow (\alpha \to \forall x \beta)$	(def. $\leftrightarrow$)

■

Metateorema 3.47 (Teorema da Generalização em constantes). *Sejam c uma constante e Γ um conjunto de fórmulas em uma linguagem de primeira ordem tais que c não ocorre numa fórmula φ e $\Gamma \vdash \varphi$. Então há uma variável x que não ocorre em φ tal que $\Gamma \vdash \forall x [\varphi]_x^c$. Além disso, há uma dedução $\Gamma \vdash \forall x [\varphi]_x^c$ em que c não ocorre.*

Demonstração. Exercício. Dica: seja $\langle \theta_1, \ldots, \theta_n \rangle$ uma prova de $\Gamma \vdash \varphi$. Demonstre que $\langle [\theta_1]_x^c, \ldots, [\theta_n]_x^c \rangle$ é uma prova de $\Gamma \vdash [\varphi]_x^c$ e considere $\Sigma \subset \Gamma$ o conjunto (finito) de fórmulas que ocorrem nessa prova. Se x não ocorre em Σ, pode-se usar o teorema de generalização. ■

Corolário 3.48 (regra (IE)). *Assuma que a constante c não ocorre em φ, ψ e que $[\varphi]_x^c \vdash \psi$. Então $\exists x \varphi \vdash \psi$ e existe uma prova dessa dedução na qual c não ocorre.*

Demonstração. Exercício. Dica: prove que se $\vdash [\varphi]_x^c$ e c não ocorre em φ, então $\vdash \forall x \varphi$ e c não ocorre nessa dedução. Use a contrapositiva em $[\varphi]_x^c \vdash \psi$. ■

Note que (IE) não afirma $\exists x \varphi \vdash [\varphi]_x^c$ que pode não ser válido.

Há axiomas redundantes

Observamos aqui que os axiomas que estabelecemos para o sistema dedutivo não é o menor conjunto possível, dentre eles há várias redundâncias. Por exemplo, com respeito a igualdade, podemos provar a propriedade simétrica (A14) usando os outros axiomas

$$\vdash (x \doteq y) \to (y \doteq x)$$

Prova.

1.	$x \doteq y$	(hipótese)
2.	$(x \doteq y \land x \doteq x) \to (x \doteq x \to y \doteq x)$	(A17)
3.	$(x \doteq y \land x \doteq x) \to (x \doteq x)$	(A6)
4.	$((x \doteq y \land x \doteq x) \to (x \doteq x \to y \doteq x)) \to (((x \doteq y \land x \doteq x) \to$	
4.	$(x \doteq x)) \to ((x \doteq y \land x \doteq x) \to y \doteq x))$	(A2)
5.	$((x \doteq y \land x \doteq x) \to (x \doteq x)) \to ((x \doteq y \land x \doteq x) \to y \doteq x)$	(MP 3,4)
6.	$(x \doteq y \land x \doteq x) \to y \doteq x)$	(MP 4,5)
7.	$x \doteq x$	(A13)
8.	$x \doteq x \to (x \doteq y \to (x \doteq y \land x \doteq x))$	(A4)
9.	$x \doteq y \to (x \doteq y \land x \doteq x)$	(MP 7,8)
10.	$x \doteq y \land x \doteq x$	(MP 1,9)
11.	$y \doteq x$	(MP 1,10)

Existem várias axiomatizações da lógica de predicados, uma vez que, para qualquer lógica, há liberdade na escolha de axiomas e regras de inferência que caracterizam essa lógica. Descrevemos aqui um sistema axiomático à Hilbert. Poderíamos ter restringido os 10 primeiros axiomas aos 3 seguintes

1. $\phi \to \big(\psi \to \phi\big)$
2. $\big(\phi \to \big(\psi \to \xi\big)\big) \to \big(\big(\phi \to \psi\big) \to \big(\phi \to \xi\big)\big)$
3. $\big(\neg\phi \to \neg\psi\big) \to \big(\psi \to \phi\big)$

Esses axiomas descrevem a lógica proposicional clássica. Para manipular quantificadores universais basta

4. $\forall x \phi \to [\phi]_x^t$ onde t é admissível para x em ϕ

dos três esquemas de axioma lógico que usamos (aqui em outra ordem)

- $\forall x \phi \to [\phi]_x^t$ onde t é admissível para x em ϕ
- $\forall x \big(\phi \to \psi\big) \to \big(\forall x \phi \to \forall x \psi\big)$
- $\phi \to \forall x \phi$ onde x não é uma variável livre de ϕ.

os dois últimos são redundante se adotarmos a regra de generalização (G) como regra de inferência primitiva.

Dos esquemas de axioma para a igualdade, basta

5. $x \doteq x$ para cada variável x
6. $\left(x \doteq y\right) \rightarrow \left([\phi]_z^x \rightarrow [\phi]_z^y\right)$

3.3.4 Axiomas não lógicos e teorias de primeira ordem

Uma **teoria formal de primeira ordem**, ou simplesmente uma **teoria elementar**, é uma teoria que tem subjacente uma lógica de primeira ordem. Uma teoria consiste de um conjunto Γ de *sentenças* de uma linguagem de primeira ordem $\mathscr{L}$ **dedutivamente fechado**, isto é, tal que todo teorema de Γ pertence a Γ.

Se os teoremas de Γ podem ser deduzidos a partir de um subconjunto Σ de sentenças, então chamamos Σ de um **sistema de axiomas** para a teoria. Obviamente, Γ é um sistema de axiomas mas, geralmente, estamos interessados num sistema om descrição mais simples que a teoria. Em particular, todo teorema lógico é teorema das teorias elementares, portanto, quando tratamos de uma linguagem de primeira ordem podemos considerar os axiomas que descrevem apenas as propriedades dos símbolos não lógicos. Tais sentenças de Σ são os **axiomas não lógicos** da teoria

$$\mathrm{T}(\Sigma) = \{\sigma \colon \sigma \in \mathscr{L} \text{ e } \Sigma \vdash \sigma\}.$$

Exemplo 3.49. A linguagem $\mathscr{L}_G$ para a Teoria dos Grupos tem os símbolos não lógicos: uma constante, denotada por e, e uma função binária, denotada por $\circ$. A teoria elementar dos grupos é dada pela linguagem $\mathscr{L}_G$ e os axiomas não lógicos

(G1) $\forall x\,((x \circ e \doteq x) \wedge (e \circ x \doteq x))$;
(G2) $\forall x \exists y\,(x \circ y \doteq e)$;
(G3) $\forall x \forall y \forall z\,(x \circ (y \circ z) \doteq (x \circ y) \circ z)$.

Exemplo 3.50. A linguagem $\mathscr{L}_{\mathscr{G}}$ para a Teoria dos Grafos tem um único símbolo não lógicos, a saber um símbolo relacional binário $\sim$ chamado de *adjacência*. A teoria elementar dos grafos é definida a partir da linguagem $\mathscr{L}_{\mathscr{G}}$ e os axiomas não lógicos

(Gr1) $\forall x\,(x \nsim x)$;
(Gr2) $\forall x, \forall y\,(x \sim y \rightarrow y \sim x)$.

Axiomas não lógicos da Teoria dos Conjuntos

Axioma da existência

Existe um conjunto que não tem elementos

$$\exists y \forall x (x \not\in y).$$

Esse conjunto é único e denotado por $\varnothing$.

Axioma da extensionalidade

Quaisquer dois conjuntos com os mesmos elementos são iguais

$$\forall y \forall z((\forall x(x \in y \leftrightarrow x \in z)) \to y = z).$$

Axioma do par

Dados conjuntos y e z, existe um conjunto w tal que se $x \in w$ então $x = y$ ou $x = z$

$$\forall y \forall z \exists w \forall x(x \in w \leftrightarrow x = y \vee x = z).$$

Axioma da união

Para qualquer conjunto z existe um conjunto $\bigcup z$ tal que $y \in \bigcup z$ se, e só se, $y \in w$ para algum $w \in z$

$$\forall z \exists w \forall x(x \in w \leftrightarrow \exists y(x \in y \wedge y \in z)).$$

Axioma das partes

Para qualquer conjunto y, existe o conjunto z tal que $x \in z$ se, e só se, $x \subseteq y$.

$$\forall y \exists z \forall x(x \in z \leftrightarrow \forall z(x \in x \to z \in y)).$$

Axioma da especificação

De um conjunto y e um predicado P, formamos o conjunto $\{x \in y \colon P(y)\}$

$$\forall y \exists z \forall x(x \in z \leftrightarrow x \in y \wedge P(z)).$$

Esse axioma também é chamado de compreensão, separação ou seleção. De fato, especificação não é um axioma, mas um esquema de axiomas, um para cada predicado que pode ser escrito na linguagem formal da teoria dos conjuntos.

Axioma do infinito

Existe um conjunto indutivo[1], que tem $\varnothing$ como elemento e, se x é elemento, também é $x \cup \{x\}$

$$\exists z(\varnothing \in z \wedge \forall x(x \in z \to x \cup \{x\} \in z))$$

Sem esse axioma, só obtemos conjuntos finitos.

Axioma da fundação

Cada conjunto não vazio x tem um elemento y com $x \cap y = \varnothing$.

$$\forall x(x \neq \varnothing \to \exists y(y \in x \wedge x \cap y = \varnothing)).$$

Também chamado de axioma da regularidade, esse axioma evita construções "estranhas" como $x = \{x\}$ e permite indução em conjuntos bem-ordenados.

[1] Isto dá uma codificação de $\mathbb{N}$, $\varnothing$ representa 0 e $x \cup \{x\}$ representa $x + 1$. Efetivamente, define cada número natural como o conjunto de todos números menores, e.g., $0 = \varnothing$, $1 = \{0\}$, $2 = \{0, 1\}$, $3 = \{0, 1, 2\} = \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}$.

Axioma da substituição

Para todo conjunto x e para todo predicado $R(s,t)$ com a propriedade $\forall s \exists! t R(s,t)$, existe o conjunto z tal que $y \in z$ se, e só se, existe $w \in x$ para o qual $R(w,y)$. Esse também é um esquema de axiomas e é usado em partes mais sofisticadas da teoria dos conjuntos.

Axioma da escolha

Para todo conjunto x de conjuntos não vazios e dois-a-dois disjuntos existe um conjunto z que tem exatamente um elemento em comum com cada conjunto de x.

O conjunto z "escolhe" um elemento de cada y em x. Esse axioma tem um enunciado equivalente que usa uma *função escolha*: *Para qualquer conjunto x formado de conjuntos não-vazios, existe uma função f que atribui para cada $y \in x$ uma imagem $f(y) \in y$.*

O último axioma é controverso para alguns matemáticos e quando usado é explicitamente mencionado. Embora seu enunciado pareça coerente há alguns enunciados equivalentes, ou decorrentes dele, que não são intuitivos como, por exemplo, o paradoxo de Banach–Tarski. Também segue desse axioma a afirmação de que os números reais podem ser ordenado de modo que qualquer subconjunto não vazio contenha um menor elemento.

Por fim, como já dissemos, note-se a forma diferente com que se escreve um conjunto por especificação, com respeito a teoria intuitiva. Agora não temos mais o paradoxo de Russell pois se

$$S = \{x \in A \colon x \not\in x\}$$

então $S \in S$ se e só se $S \in A$ e $S \not\in S$ o que não é contraditório, a conclusão é que $S \not\in A$. Como subproduto temos o fato já mencionado de que em teoria dos conjuntos *não há conjunto universo.*

Teorema $\neg\exists y \forall x (x \in y)$.

De fato, se existisse então tomaríamos-o por A no argumento acima o que daria uma contradição pois $S \not\in A$.

3.3.5 Axiomas não lógicos da Aritmética

À linguagem $\mathscr{L}_N$ acrescentamos, além dos axiomas lógicos, os seguintes axiomas não lógicos da teoria elementar de números

(PA0) $\forall x\,(Sx \neq 0)$
(PA1) $\forall x \forall y (Sx \doteq Sy \to x \doteq y)$
(PA2) $\forall x\,(x + 0 \doteq x)$
(PA3) $\forall x \forall y\,(x + Sy \doteq S(x+y))$
(PA4) $\forall x\,(x \cdot 0 \doteq 0)$
(PA5) $\forall x \forall y\,(x \cdot Sy \doteq (x \cdot y) + x)$

(PA6) Se $\varphi \in \mathscr{L}_N$ com $x \in VL(\varphi)$, então

$$\left([\varphi]_x^0 \wedge \forall x \left(\varphi \to [\varphi]_x^{Sx}\right)\right) \to \forall x \varphi$$

Notemos que (PA0)–(PA5) são axiomas, i.e. fórmulas da linguagem, enquanto que (PA6) é um esquema de axioma, é o esquema de axioma da indução. Além desses, os axiomas de ordem

(OA0) $\forall x \neg(x < 0)$
(OA1) $\forall x \forall y (x < Sy \leftrightarrow x < y \vee x \doteq y)$
(OA2) $\forall x \forall y (x < y \vee x \doteq y \vee y < x)$.

Exercício 3.51. *Abaixo vamos usar o seguinte teorema lógico*

$$\beta, \alpha \to \gamma, \alpha \vdash \beta \wedge \gamma$$

Solução. $\langle \alpha, \beta, \alpha \to \gamma, \gamma, \beta \wedge \gamma \rangle$. ■

Agora, denotamos por PA o conjunto de fórmulas

$$\mathsf{PA} = \{\mathrm{PA0}, \mathrm{PA1}, \mathrm{PA2}, \mathrm{PA3}, \mathrm{PA4}, \mathrm{PA5}, \mathrm{PA6}, \mathrm{OA0}, \mathrm{OA1}, \mathrm{OA2}\}$$

e vamos provar usando o esquema de indução que

$$\mathrm{PA} \vdash \forall y (0 + y \doteq y). \tag{3.3}$$

cuja prova será feita por indução em y via

$$\left([0 + y \doteq y]_y^0 \wedge \forall y \left(0 + y \doteq y \to [0 + y \doteq y]_y^{Sy}\right)\right) \to \forall y (0 + y \doteq y)$$

A *base* da indução para (3.3.5) consiste em provar $[0+y \doteq y]_y^0$, ou seja, $0+0 \doteq 0$.

1.	$\forall x(x + 0 = 0)$	(PA2)
2.	$\forall x(x + 0 = 0) \to 0 + 0 = 0$	(A1I)
3.	$0 + 0 = 0$	(MP 1,2)

O *passo indutivo* para (3.3.5) consiste em provar $\forall y \left(0 + y \doteq y \to [0 + y \doteq y]_y^{Sy}\right)$, ou seja, vamos derivar a fórmula $\forall y (0 + y \doteq y \to 0 + Sy \doteq Sy)$

1.	$\forall x \forall y(x + Sy \doteq S(x + y))$	(PA3)
2.	$\forall x \forall y(x + Sy \doteq S(x + y)) \to \forall y(0 + Sy \doteq S(0 + y))$	(A1I)
3.	$\forall y(0 + Sy \doteq S(0 + y))$	(MP 1,2)
4.	$\forall y(0 + Sy \doteq S(0 + y)) \to 0 + Sy \doteq S(0 + y)$	(A1I)
5.	$0 + Sy \doteq S(0 + y)$	(MP 4,5)
6.	$0 + y \doteq y \to S(0 + y) \doteq Sy$	(A18)
7.	$0 + y \doteq y \to (0 + Sy \doteq S(0 + y) \wedge S(0 + y) \doteq Sy)$	(exerc. 3.51 5,6)
8.	$(0 + Sy \doteq S(0 + y) \wedge S(0 + y) \doteq Sy) \to (0 + Sy \doteq Sy)$	(A16)
9.	$0 + y \doteq y \to 0 + Sy \doteq Sy$	(SH 7,8)
10.	$\forall y (0 + y \doteq y \to 0 + Sy \doteq Sy)$	(TG 9)

Feito isso, a conclusão de (3.3.5) se dá da seguinte forma.

1.	$0+0 \doteq 0$	(base)
2.	$\forall y\,(0+y \doteq y \to 0+Sy \doteq Sy)$	(passo)
3.	$(0+0 \doteq 0) \wedge \forall y\,(0+y \doteq y \to 0+Sy \doteq Sy)$	(IC 1,2)
4.	$\big((0+0 \doteq 0) \wedge \forall y\,(0+y \doteq y \to 0+Sy \doteq Sy)\big) \to \forall y\,(x+y \doteq y+x)$	(PA6)
5.	$\forall y\,(0+y \doteq y)$	(MP 3,4)

Exercício 3.52. *Escreva uma prova formal para*

$$\mathsf{PA} \vdash \forall y\,(0+y \doteq y+0).$$

Note que provamos $\forall y\,(0+y \doteq 0)$ *e que* $\forall y\,(y+0 \doteq 0)$ *é axioma.*

O exercício acima é a base da indução para provar que a soma é comutativa

$$\mathsf{PA} \vdash \forall x \forall y\,(x+y \doteq y+x).$$

Se provarmos que $\forall x\,\big((\forall y\,(x+y \doteq y+x)) \to [\forall y\,(x+y \doteq y+x)]^{Sx}_{x}\big)$ é consequência sintática de PA então

1.	$\forall y\,(0+y \doteq y+0)$	(base)
2.	$\forall x\,\big((\forall y\,(x+y \doteq y+x)) \to (\forall y\,(Sx+y \doteq y+Sx)\big)$	(passo)
3.	$\forall y\,(0+y \doteq y+0) \wedge \forall x\big((\forall y\,(x+y \doteq y+x)) \to (\forall y\,(Sx+y \doteq y+Sx)\big)$	(IC 1,2)
4.	$\big(\forall y\,(0+y \doteq y+0) \wedge \forall x\big((\forall y\,(x+y \doteq y+x)) \to (\forall y\,(Sx+y \doteq y+Sx))\big)\big) \to \forall x(\forall y\,(x+y \doteq y+x))$	(PA6)
5.	$\forall x(\forall y\,(x+y \doteq y+x))$	(MP 3,4)

Exercício 3.53. $\mathsf{PA} \vdash \forall x\,\big((\forall y\,(x+y \doteq y+x)) \to (\forall y\,(Sx+y \doteq y+Sx)\big)$

3.4 Exercícios

1. Seja A uma relação binária interpretada como "ama", i.e., $A(x,y)$ simboliza a sentença x ama y. Simbolize as seguintes sentenças
   a) Todo mundo ama alguém.
   b) Todo mundo é amado alguém.
   c) Alguém ama todo mundo.
   d) Há alguém que é amado por todo mundo.
   e) Todo mundo ama todo mundo.
   f) Alguém ama alguém.
   g) Se algém é amado por todos então alguém ama a si mesmo.
2. Simbolize as seguintes sentenças (abertas ou não) na linguagem da Aritmética.
   a) Todo número par maior do que dois pode ser escrito como soma de dois números primos.
   b) x possui exatamente três divisores.

c) Todo número positivo admite raiz quadrada.
d) z é o máximo divisor comum de x e y.
e) Existem infinitos números primos.

3. Defina uma linguagem de primeira ordem $\mathscr{F}$ que trata das relações familiares e escreva em símbolos as sentenças abaixo.
   a) Ana é irmã de José.
   b) Maria é irmã de Ana.
   c) Pedro é pai de Ana.
   d) Pedro é pai de Maria e de José.
   e) Ana é irmã de José e Maria é irmã de Ana, então Maria é irmã de José.
   f) Tarso é irmão de Pedro e tio de Ana.
   g) Tarso é irmão de Pedro então é tio de José.
   h) Tarso é tio de Maria.
   i) Tarso é tio de Maria e de Ana, que são irmãs de José, logo Tarso é tio de José.
   j) Ele é primo de Maria.
   k) Maria possui uma avó que tem quatro filhos(as).
4. Identifique as ocorrências livres e não-livres de variáveis nas fórmulas abaixo.
   a) $(\exists x((1+y) \doteq x)) \wedge \forall y(y < x)$.
   b) $(\exists x(x \cdot x \doteq 2)) \rightarrow (x+1 \doteq 0)$.
   c) $\forall x \exists y(z < 1)$.
   d) $(\exists x((1+y) \doteq x)) \wedge (\forall y(y < x))$.
   e) $(x < y+1) \rightarrow \forall x \exists y(x \neq y)$.
   f) $\forall x(x > (1+1) \rightarrow y < (x+x))$.
   g) $(\forall y \exists z(x+y \doteq z)) \rightarrow (x \doteq 0)$.
   h) $\forall x(((x < 6) \wedge (0 < x)) \rightarrow \exists y(x \cdot y \doteq z))$.
   i) $\forall x((x \doteq 0) \vee (0 < x)) \wedge \exists y(y \cdot (1+1) \doteq x)$.
   j) $\forall y \forall z((y \cdot z \doteq x) \rightarrow ((y \neg z) \wedge ((y \doteq 1) \vee (z \doteq 1))))$.
5. (**Subfórmulas**) Defina indutivamente o conceito de subfórmula para as fórmulas da linguagem genérica de primeira ordem.
6. Determine todas as subfórmulas atômicas das fórmulas do exercício 4.
7. Exiba as subfórmulas de cada uma das fórmulas que você encontrou no exercício 2.
8. Dê uma definição precisa de *escopo* de um quantificador.
9. Use indução para definir o grau de complexidade de uma fórmula (veja o exemplo 1.4 da lógica proposicional). Por exemplo grau$(s \doteq t) = 0$, grau$(R^2(x,y)) = 0$, grau$(\neg(s \doteq t)) = 1$, grau$(\forall x\, R^2(x,y)) = 1$, grau$(\forall y \forall x\, R^2(x,y)) = 2$.
10. Restabeleça os parênteses de acordo com as regras de omissão de parênteses.
    a) $\forall x_1 R_1^1 x_1 \wedge \neg R_1^1 x_2$.
    b) $\forall x_2 R_1^1 x_2 \leftrightarrow R_1^1 x_2$.
    c) $\forall x_2 \exists x_1 R_1^2 x_1, x_2$.
    d) $\forall x_1 \forall x_3 \forall x_4 R_1^1 x_1 \rightarrow R_1^1 x_2 \wedge \neg R_1^1 x_1$
    e) $\exists x_1 \forall x_2 \exists x_3 R_1^1 x_1 \vee \exists x_2 \neg \forall x_3 R_1^2 x_3, x_2$.
    f) $\forall x_2 \neg R_1^1 x_1 \rightarrow R_1^3 x_1, x_1, x_2 \vee \forall x_1 R_1^1 x_1$.
    g) $\neg \forall x_1 R_1^1 x_1 \rightarrow \exists x_2 R_1^1 x_2 \rightarrow R_1^2 x_1, x_2 \wedge R_1^1 x_2$.

11. Use indução para mostrar que x é admissível para x em φ, para qualquer variável x e qualquer fórmula φ, e $[\varphi]^x_x$ é a fórmula φ.
12. Sejam t é um termo e α uma sentença. O termo t é uma substituição admissível em α para qualquer variável x? Qual é o resultado da substituição?
13. O algoritmo da divisão diz que para quaisquer naturais a, b, com $b \neq 0$, existem naturais q e r únicos tais que $a = bq + r$ e $\leqslant 0 < r < b$. Expresse o teorema da divisão na linguagem da aritmética.
14. Defina indutivamente o conjunto $LV(\cdot)$ das variáveis ligadas de uma fórmula.
15. Use o princípio de indução para termos para definir *comprimento* de um termo como o número de símbolos do alfabeto que ocorrem no termo, exceto os de pontuação.
16. Para cada uma das fórmulas abaixo determine se é um axioma lógico.
    a) $\forall x \forall z\,(x \doteq y \to (x \doteq c \to x \doteq y))$
    b) $x \doteq y \to (y \doteq z \to z \doteq x)$
    c) $\forall z\,(x \doteq y \to (x \doteq c \to y \doteq c))$
    d) $\forall w \exists x\,(P(w,x) \to P(w,w)) \to \exists x\,(P(x,x) \to P(x,x))$
    e) $\forall x (\forall x\,(c \doteq f(x,c) \to \forall x \forall x\,(c \doteq f(x,c))))$
    f) $(\exists x\, P(x) \to \exists y\, \forall z R(z, f(y))) \to ((\exists x P(x) \to \forall y \neg \forall z\, R(z, f(y))) \to \forall x\, \neg P(x))$
    g) $\forall x \exists y\,(\neg(y \doteq x)) \to \exists y\,(\neg(y \doteq 0))$
    h) $\forall x \exists y\,(\neg(x \doteq y))$
    i) $\forall x \exists y (y < x) \to \exists y (y < y)$
    j) $\forall x\,((0 < x) \to (0 < x + x)) \to ((0 < x) \to \forall x (0 < x + x))$
    k) $\forall x \forall y\,((x + 1 \doteq 0) \to ((y \doteq 1) \to (x + 1 \doteq 0)))$
17. Escreva uma prova para
    a) $\vdash (\forall x_1 (R^1_1(x_1) \vee R^1_2(x_1))) \to (R^1_2(x_1) \vee R^1_1(x_1))$.
    b) $\vdash R^1_1(c_1) \to (R^1_1(c_2) \to (R^1_1(c_1) \wedge r^1_1(c_2)))$.
    c) $\vdash \forall x_1 (\forall x_2 (R^1_1(x_1) \to (R^1_1(x_2) \to R^1_1(x_1))))$.
    d) $\{Q(x), \forall y\,(Q(y) \to \forall z\, P(z))\} \vdash \forall x\, P(x)$
    e) $\vdash (\alpha \to \exists x\, \beta) \leftrightarrow \exists x\,(\alpha \to \beta)$ se x não ocorre livre em α
    f) $\vdash (\forall x\, \beta \to \alpha) \leftrightarrow \exists x\,(\beta \to \alpha)$ se x não ocorre livre em α
    g) $\vdash P(y) \leftrightarrow \forall x\,(x \doteq y \to P(x))$
18. Demonstre as propriedades de $\vdash$.
19. Escreva uma prova para $\mathsf{PA} \vdash S0 + SS0 \doteq SSS0$ e para $PA \vdash 0 < S0$.
20. Escreva uma prova para $\mathsf{PA} \vdash \forall x (0 \cdot x \doteq 0)$.
21. Escreva uma prova para $\mathsf{PA} \vdash \forall x (x \doteq 0 \vee \exists y (x \doteq Sy))$.

4

Semântica para a lógica de predicados

Para interpretar as fórmulas de uma linguagem de primeira ordem, precisamos estabelecer um universo de discurso, também chamado de domínio; os símbolos funcionais n-ários correspondem à operações n-árias nesse domínio; os símbolos relacionais n-ários serão interpretados como relações n-árias sobre o domínio e as constantes são elementos do domínio.

Exemplo 4.1. Intuitivamente, para

$$\forall x_1\, R_1^2(x_1, x_1)$$

se o domínio é $\mathbb{N}$ e R_1^2 representa a relação de divisibilidade então a fórmula é verdadeira, nos diz que "todo número natural é divisível por ele mesmo". Se o domínio é $\mathbb{Z}$ e R_1^2 representa a relação *menor que* então a fórmula é falsa, não é verdade que "todo número inteiro é menor que ele mesmo".

Para

$$\exists x_1\, (R_1^2(x_2, x_1) \wedge R_1^2(x_1, x_3))$$

no domínio $\mathbb{Z}$ e R_1^2 a relação *menor que*, também devemos interpretar as variáveis livres x_2, x_3. Se interpretamos x_2 como 5 e x_3 como 8 obtemos a sentença verdadeira "existe um inteiro n tal que $5 < n$ e $n < 8$". Se interpretamos x_2 como 5 e x_3 como 6 obtemos a sentença falsa "existe um inteiro n tal que $5 < n$ e $n < 6$".

Intuitivamente, para a linguagem da teoria dos grupos, exemplo 3.49, com domínio $\mathbb{Z}$ e interpretando a constante e como o $0 \in \mathbb{Z}$ e interpretando a operação $\circ$ como a soma de inteiros temos, intuitivamente, que os axiomas G1, G2 e G3 são verdadeiros. Por outro lado, com domínio $\mathbb{N}$ e interpretando a constante e como o $1 \in \mathbb{Z}$ e interpretando a operação $\circ$ como a soma de números naturais o axioma G3 é falso.

Uma interpretação é dada por uma estrutura matemática e uma atribuição nos elementos do universo para cada variáveis.

4.1 Estrutura e atribuição

Uma **estrutura** $\mathfrak{M}$

$$\mathfrak{M} = (M, c_1, c_2, \dots, c_\ell, R_1, \dots, R_m, F_1, \dots, F_n)$$

é tal que M é um conjunto não vazio, $c_1, c_2, \dots, c_\ell$ são alguns (possivelmente nenhum) elementos tomados de M, $R_1, \dots, R_m$ são relações (possivelmente nenhuma) sobre M e $F_1, \dots, F_m$ operações sobre M (possivelmente nenhuma). O conjunto M é denominado **domínio** ou **universo** de $\mathfrak{M}$. São estruturas

- $\mathscr{B} = (\{0,1\}, 0, 1, \max, \min, \overline{})$. Aqui max, min têm seus significados habituais no domínio $\{0,1\}$, $\overline{(x)} = 1 - x$ e não há relações ou constantes.
- $\mathscr{P} = (\wp(X), \varnothing, X, \cup, \cap, ^{\complement})$. Aqui X é um conjunto não vazio, $\cup$ e $\cap$ têm seus significados habituais para conjuntos e $^{\complement}(A) = A^{\complement}$ é o complemento do A com respeito a X.
- $(\mathbb{N}, 0, 1, <, +, \cdot)$ é uma estrutura cujo universo é o conjunto $\mathbb{N}$ dos números naturais e $0, 1, <, +, \cdot$ têm os seus significados usuais.
- $(\mathbb{R}, 0, 1, +, \cdot)$ é uma estrutura cujo universo é o conjunto $\mathbb{R}$ dos números reais e as operações são a soma e produto usuais.
- $(\mathbb{N}, <)$ é uma estrutura cujo universo é o conjunto $\mathbb{N}$ dos números naturais e $<$ é a relação binária "menor que " usual.
- (V, E) com V não vazio e $E \subset V \times V$ uma relação binária é uma estrutura para grafos.

Se $\mathfrak{M}$ não contém funções ou constantes, então $\mathfrak{M}$ também é chamada de *estrutura relacional*, como em $(\mathbb{N}, <)$ e (V, E). Se $\mathfrak{M}$ não tem relações é chamado de *estrutura algébrica*, como é o caso dos outros exemplos.

Estrutura para uma linguagem

Uma estrutura para uma linguagem de primeira ordem $\mathscr{L}$ é uma estrutura que dá significado aos símbolos não lógicos da linguagem, é formada por um conjunto não-vazio (chamado de domínio ou universo), uma operação n-ária para cada símbolo funcional n-ário da linguagem, uma relação n-ária para cada símbolo relacional n-ário e um elemento do domínio para cada constante da linguagem. Uma $\mathscr{L}$**-estrutura**

$$\mathfrak{M} = \left(M, c_1^{\mathfrak{M}}, \dots, c_\ell^{\mathfrak{M}}, R_1^{\mathfrak{M}}, \dots, R_m^{\mathfrak{M}}, F_1^{\mathfrak{M}}, \dots, F_n^{\mathfrak{M}}\right)$$

consiste, portanto, de

1. um conjunto não vazio M chamado de domínio ou universo da linguagem;
2. cada constante c da linguagem corresponde a um elemento $c^{\mathfrak{M}}$ de E;
3. cada símbolo relacional n-ário R da linguagem corresponde a uma relação n-ária $R^{\mathfrak{M}}$ em M (isto é, $R^{\mathfrak{M}} \subseteq M^n$);
4. cada símbolo funcional n-ário F corresponde a uma função $F^{\mathfrak{M}}$ de M^n em M (isto é, $F^{\mathfrak{M}} : M^n \to M$).

Exemplo 4.2. A *linguagem da Teoria das Ordens* $\mathscr{L}_O$ com símbolo relacional binário < como o único símbolo não lógico admite as $\mathscr{L}_O$-estruturas

1. $(\mathbb{N}, <^{\mathfrak{M}})$ com $<^{\mathfrak{M}} = \{(a,b) \in \mathbb{N}\times\mathbb{N} : a+n=b$ para algum natural $n \neq 0\}$, a relação "menor que" usual sobre $\mathbb{N}$.
2. $(\mathbb{Z}, \leq^{\mathfrak{M}})$ com $\leq^{\mathfrak{M}} = \{(a,b) \in \mathbb{N}\times\mathbb{N} : a+n=b$ para algum natural $n\}$.
3. $(\mathbb{N}, \mathbb{N}\times\mathbb{N})$.
4. $(\wp(\mathbb{R}), \subset^{\mathfrak{M}})$ com $\subset^{\mathfrak{M}}$ a inclusão usual de conjuntos.

Exemplo 4.3. A linguagem $\mathscr{L}_N$ da aritmética, a qual tem os símbolos extralógicos 0, S, $<$, $+$, $\cdot$, admite as seguintes estruturas

1. [5] Definimos $\mathfrak{U} = (U, 0^{\mathfrak{U}}, S^{\mathfrak{U}}, <^{\mathfrak{U}}, +^{\mathfrak{U}}, \cdot^{\mathfrak{U}})$ onde
   - $U = \{1,2,3\}$, $0^{\mathfrak{U}} = 1$ e $S^{\mathfrak{U}} = \{(1,1),(2,2),(3,3)\}$;
   - A relação binária é dada por $<^{\mathfrak{U}} = \{(1,1),(1,2),(1,3),(2,2),(2,3),(3,3)\}$;
   - as operações são dadas pelas seguintes tabelas (na linha i coluna j lê-se $i +^{\mathfrak{U}} j$

$+^{\mathfrak{U}}$	1	2	3
1	1	2	3
2	2	3	1
3	3	1	2

$\cdot^{\mathfrak{U}}$	1	2	3
1	1	1	1
2	1	2	3
3	1	3	2

2. A interpretação usual $\mathfrak{N} = (\mathbb{N}, 0^{\mathfrak{N}}, <^{\mathfrak{N}}, S^{\mathfrak{N}}, +^{\mathfrak{N}}, \cdot^{\mathfrak{N}})$ onde $0^{\mathfrak{N}}$ é o número $0 \in \mathbb{N}$; a função $S^{\mathfrak{U}} : \mathbb{N} \to \mathbb{N} \setminus \{0\}$ é dada por $S^{\mathfrak{U}}(n) = n+1$, a relação binária $<^{\mathfrak{N}}$ e as operações $+^{\mathfrak{N}}, \cdot^{\mathfrak{N}}$ são o "menor que", a soma e o produto usuais de números naturais.
3. Tomamos para algum conjunto X não vazio a estrutura $\mathfrak{C} = (\wp(X), 0^{\mathfrak{C}}, <^{\mathfrak{C}}, S^{\mathfrak{C}}, +^{\mathfrak{C}}, \cdot^{\mathfrak{C}})$ onde $0^{\mathfrak{C}}$ é o conjunto vazio; a função $S^{\mathfrak{C}}$ é dada por $S^{\mathfrak{C}}(A) = A^{\complement}$, os operadores $+^{\mathfrak{C}}$ e $\cdot^{\mathfrak{C}}$ são, respectivamente, a união e a interseção de conjuntos e a relação binária $<^{\mathfrak{C}}$ é definida pela inclusão $\subset$.

Atribuição

Uma **atribuição** associada a uma estrutura $\mathfrak{M} = \big(M, (c_i^{\mathfrak{M}})_{i=1}^{\ell}, (R_j^{\mathfrak{M}})_{j=1}^{m}, (F_k^{\mathfrak{M}})_{k=1}^{n}\big)$ é uma função

$$v : \{x_1, x_2, \dots\} \to M.$$

Dados uma estrutura $\mathfrak{M}$ e uma atribuição v, a **interpretação de termos** sob a atribuição é a única função $\bar{v}$ que estende a função v a todos os termos da linguagem, conforme as seguintes condições:

1. se x é variável, $\bar{v}(x) = v(x)$;
2. se c é uma constante, $\bar{v}(c) = c^{\mathfrak{M}}$;
3. se F é um símbolo funcional n-ário e $t_1, \dots, t_n$ são termos, então a interpretação do termo F $(t_1, \dots, t_n)$ é dada por $\bar{v}(F(t_1,\dots,t_n)) = F^{\mathfrak{M}}(\bar{v}(t_1),\dots,\bar{v}(t_n))$.

Exemplo 4.4. Com a $\mathscr{L}_N$-estrutura $\mathfrak{U}$ do exemplo 4.3 e com v tal que $v(x) = 1$ e $v(y) = 2$ o valor do termo $+(\cdot(0,x), y)$ é

$$\begin{aligned}\bar{v}(+(\cdot(0,x),y)) &= +^{\mathfrak{A}}(\cdot^{\mathfrak{A}}(\bar{v}(0),\bar{v}(x)),\bar{v}(y))\\ &= +^{\mathfrak{A}}(\cdot^{\mathfrak{A}}(0^{\mathfrak{A}},1),2)\\ &= +^{\mathfrak{A}}(\cdot^{\mathfrak{A}}(1,1),2)\\ &= +^{\mathfrak{A}}(1,2)\\ &= 2\end{aligned}$$

Para o termo $+(x,y)$ temos o valor

$$\bar{v}(+(x,y)) = +^{\mathfrak{A}}(\bar{v}(x),\bar{v}(y)) = +^{\mathfrak{A}}(1,2) = 2$$

O valor do termo 0 é $\bar{v}(0) = 0^{\mathfrak{A}} = 1$.

Exemplo 4.5. Com a $\mathscr{L}_N$-estrutura $\mathfrak{C}$ do exemplo 4.3 e com v tal que $v(x) = X$ e $v(y) = \varnothing$ o valor do termo $+(\cdot(0,x),y)$ é

$$\begin{aligned}\bar{v}(+(\cdot(0,x),y)) &= +^{\mathfrak{C}}(\cdot^{\mathfrak{C}}(\bar{v}(0),\bar{v}(x)),\bar{v}(y))\\ &= \cup(\cap(\varnothing,X),\varnothing)\\ &= \cup(\varnothing,\varnothing)\\ &= \varnothing.\end{aligned}$$

Para o termo $+(x,y)$ temos o valor

$$\bar{v}(+(x,y)) = +^{\mathfrak{C}}(\bar{v}(x),\bar{v}(y)) = \cup(X,\varnothing) = X.$$

Notemos que os termos usados como argumentos de $\bar{v}$ são símbolos da linguagem e a imagem de $\bar{v}$ são objetos do domínio da estrutura e, portanto, pertencem à metalinguagem.

Exercício 4.6. *Demonstre que que a extensão $\bar{v}$ de uma atribuição v a todos os termos de uma linguagem é única.*

Metateorema 4.7. *Seja $\mathfrak{M}$ uma estrutura para a linguagem de primeira ordem $\mathscr{L}$. Para todo termo t de $\mathscr{L}$, se v e w são duas atribuições que coincidem nas variáveis que ocorrem em t, então $\bar{v}(t) = \bar{w}(t)$.*

Demonstração. Por indução para termos. Se t é uma variável ou uma constante, o resultado $\bar{v}(t) = \bar{w}(t)$ é imediato. Se t é $Ft_1t_2\dots t_n$ e, por hipótese da indução, $\bar{v}(t_i) = \bar{w}(t_1)$ $(1 \leqslant i \leqslant n)$ então $\bar{v}(t) = F^{\mathfrak{M}}(\bar{v}(t_1),\dots,\bar{v}(t_n i)) = F^{\mathfrak{M}}(\bar{w}(t_1),\dots,\bar{w}(t_n i)) = \bar{w}(t)$ por definição. ■

Assim, o valor de um termo numa interpretação depende somente dos valores atribuídos às variáveis que ocorrem no termo.

Exercício 4.8. *Intuitivamente, a fórmula $\forall x\,(+(x,y) \doteq 0)$ da linguagem da aritmética é verdadeira no contexto do exemplo 4.4?*

Atribuição x-variante

Se v é uma atribuição na estrutura $\mathfrak{E}$, então definimos a atribuição $[v]_{x\rightsquigarrow a}$, para qualquer a no domínio E de $\mathfrak{E}$ pondo

$$[v]_{x_i\rightsquigarrow a}(x_j) = \begin{cases} a & \text{se } j = i \\ v(x_j) & \text{se } j \neq i. \end{cases}$$

Por exemplo, se $E = \mathbb{N}$ e $v(x_j) = j$ então $[v]_{x_3\rightsquigarrow 0}$ é

$$[v]_{x_3\rightsquigarrow 0}(x_j) = \begin{cases} 0 & \text{se } j = 3 \\ j & \text{se } j \neq 3. \end{cases}$$

4.2 Satisfazibilidade e valor-verdade

A ideia por trás da semântica da lógica de predicados é muito simples. Seguindo Tarski, nós assumimos que uma sentença é verdadeira em uma estrutura se esse é de fato o caso, se o "significado dentro de uma estrutura" atribuído aos símbolos formais é verdadeiro naquela estrutura. Sejam $\mathscr{L}$ um linguagem de primeira ordem, $\mathfrak{M}$ e v uma estrutura e uma atribuição para a linguagem $\mathscr{L}$, respectivamente. O par $(\mathfrak{M}, v)$ é chamado de **interpretação** a qual **satisfaz** a fórmula $\alpha \in \mathscr{L}$, denotado

$$(\mathfrak{M}, v) \vDash \alpha$$

nas seguintes circunstâncias

1. $(\mathfrak{M}, v) \vDash (t_1 \doteq t_2)$ se e só se $\bar{v}(t_1) = \bar{v}(t_2)$;
2. $(\mathfrak{M}, v) \vDash R(t_1, \dots, t_n)$ se e só se $(\bar{v}(t_1), \dots, \bar{v}(t_n)) \in R^{\mathfrak{M}}$;
3. $(\mathfrak{M}, v) \vDash \neg\gamma$ se e só se $(\mathfrak{M}, v) \nvDash \gamma$;
4. $(\mathfrak{M}, v) \vDash \gamma \to \beta$ se e só se $(\mathfrak{M}, v) \vDash \neg\gamma$ ou $(\mathfrak{M}, v) \vDash \beta$;
5. $(\mathfrak{M}, v) \vDash \forall x\, \beta$ se e só se para todo $a \in E$, $(\mathfrak{M}, [v]_{x\rightsquigarrow a}) \vDash \beta$

em que R é um símbolo relacional n-ário da linguagem, $t_1, \dots, t_n$ são termos, x é variável e γ e β fórmulas da linguagem. Das abreviaturas adotadas deduzimos que

6. $(\mathfrak{M}, v) \vDash \gamma \vee \beta$ se e só se $(\mathfrak{M}, v) \vDash \gamma$ ou $(\mathfrak{M}, v) \vDash \beta$
7. $(\mathfrak{M}, v) \vDash \gamma \wedge \beta$ se e só se $(\mathfrak{M}, v) \vDash \gamma$ e $(\mathfrak{M}, v) \vDash \beta$;
8. $(\mathfrak{M}, v) \vDash \exists x\, \gamma$ se e só se $(\mathfrak{M}, [v]_{x\rightsquigarrow a}) \vDash \gamma$ para algum $a \in E$.

Exemplo 4.9. Por exemplo, com $\mathfrak{U}$ do exemplo 4.3 de domínio $\{1,2,3\}$ e v tal que $v(y) = 2$.

$$\begin{aligned}
(\mathfrak{U}, v) \vDash \forall x\,(x + y \doteq 0) &\text{ sse para todo } a \in \{1,2,3\},\ (\mathfrak{U}, [v]_{x\rightsquigarrow a}) \vDash (x + y \doteq 0) \\
&\text{ sse para todo } a \in \{1,2,3\},\ \overline{[v]_{x\rightsquigarrow a}}(x + y) = \overline{[v]_{x\rightsquigarrow a}}(0) \\
&\text{ sse para todo } a \in \{1,2,3\},\ [v]_{x\rightsquigarrow a}(x) +^{\mathfrak{U}} [v]_{x\rightsquigarrow a}(y) = 1 \\
&\text{ sse para todo } a \in \{1,2,3\},\ a +^{\mathfrak{U}} 2 = 1
\end{aligned}$$

o que não é verdadeiro na estrutura pois $2 +^{\mathfrak{U}} 2 = 3$, logo a fórmula $\forall x\,(x + y \doteq 0)$ não é satisfeita por essa interpretação, ou seja

$$(\mathfrak{U}, v) \not\models \forall x\,(x + y = 1).$$

Exemplo 4.10. A linguagem $\mathscr{L}_F$ para a teoria dos corpos tem símbolos extralógicos $0, 1, +, \cdot$. Uma $\mathscr{L}_F$-estrutura é $\mathfrak{R} = (\mathbb{R}, 0^{\mathfrak{R}}, 1^{\mathfrak{R}}, +^{\mathfrak{R}}, \cdot^{\mathfrak{R}})$ com os significados usuais e tomamos a atribuição $v(x_n) = n + 1$. Então

$$(\mathfrak{R}, v) \models \forall x_1\,\big((0 \cdot x_1 \doteq x_3) \to (x_3 \doteq 0)\big)$$

pois $(\mathfrak{R}, v) \models \forall x_1\,\big((0 \cdot x_1 \doteq x_3) \to (x_3 \doteq 0)\big)$

sse para todo $a \in \mathbb{R}$, $(\mathfrak{R}, [v]_{x_1 \rightsquigarrow a}) \models \big((0 \cdot x_1 \doteq x_3) \to (x_3 \doteq 0)\big)$
sse para todo $a \in \mathbb{R}$, $(\mathfrak{R}, [v]_{x_1 \rightsquigarrow a}) \models \neg(0 \cdot x_1 \doteq x_3)$ ou $(\mathfrak{R}, [v]_{x_1 \rightsquigarrow a}) \models (x_3 \doteq 0)$
sse para todo $a \in \mathbb{R}$, $(\mathfrak{R}, [v]_{x_1 \rightsquigarrow a}) \models (0 \cdot x_1 \neq x_3)$ ou $(\mathfrak{R}, [v]_{x_1 \rightsquigarrow a}) \models (x_3 \doteq 0)$
sse para todo $a \in \mathbb{R}$, $\overline{[v]_{x_1 \rightsquigarrow a}}(0 \cdot x_1) \neq \overline{[v]_{x_1 \rightsquigarrow a}}(x_3)$ ou $\overline{[v]_{x_1 \rightsquigarrow a}}(x_3) = \overline{[v]_{x_1 \rightsquigarrow a}}(0)$
sse para todo $a \in \mathbb{R}$,

$$\overline{[v]_{x_1 \rightsquigarrow a}}(0) \cdot^{\mathfrak{R}} \overline{[v]_{x_1 \rightsquigarrow a}(x_1)} \neq \overline{[v]_{x_1 \rightsquigarrow a}}(x_3) \text{ ou } \overline{[v]_{x_1 \rightsquigarrow a}}(x_3) = \overline{[v]_{x_1 \rightsquigarrow a}}(0)$$

sse para todo $a \in \mathbb{R}$, $0^{\mathfrak{R}} \cdot^{\mathfrak{R}} a \neq 4$ ou $4 = 0^{\mathfrak{R}}$

isto é, a interpretação satisfaz a fórmula se, e somente se, em $\mathbb{R}$ temos $0 \neq 4$ ou $4 = 0$, portanto, a interpretação fornecida pela estrutura e pela atribuição satisfaz a fórmula.

Exemplo 4.11. Em $\mathscr{L}_O$ (exemplo 4.2), considere a estrutura $\mathscr{Q} = (\mathbb{Q}, <^{\mathscr{Q}})$ com $<^{\mathscr{Q}}$ o menor usual sobre o conjunto $\mathbb{Q}$ dos números racionais e seja v uma atribuição qualquer. Então

1. $(\mathscr{Q}, v) \models \forall x_1\,(\exists x_2\,(x_1 < x_2))$ e
2. $(\mathscr{Q}, v) \models \exists x_3\,(\exists x_4\,(x_3 < x_4 \to x_3 = x_4))$

Para o primeiro exemplo temos que $(\mathscr{Q}, v) \models \forall x_1\,(\exists x_2\,(x_1 < x_2))$

sse para todo $a \in \mathbb{Q}$, $(\mathscr{Q}, [v]_{x_1 \rightsquigarrow a}) \models \exists x_2\,(x_1 < x_2)$
sse para todo $a \in \mathbb{Q}$, para algum $b \in \mathbb{Q}$, $(\mathscr{Q}, [v]_{\substack{x_1 \rightsquigarrow a \\ x_2 \rightsquigarrow b}}) \models x_1 < x_2$
sse para todo $a \in \mathbb{Q}$, para algum $b \in \mathbb{Q}$, $\overline{[v]_{\substack{x_1 \rightsquigarrow a \\ x_2 \rightsquigarrow b}}}(x_1) <^{\mathfrak{Q}} \overline{[v]_{\substack{x_1 \rightsquigarrow a \\ x_2 \rightsquigarrow b}}}(x_2)$
sse para todo $a \in \mathbb{Q}$, para algum $b \in \mathbb{Q}$, $a <^{\mathfrak{Q}} b$

o que é verdadeiro na estrutura.

Agora, no segundo exemplo $(\mathscr{Q}, v) \models \exists x_3\,(\exists x_4\,(x_3 < x_4 \to x_3 \doteq x_4))$

sse para algum $a \in \mathbb{Q}$, $(\mathscr{Q}, [v]_{x_3 \rightsquigarrow a}) \vDash \exists x_4\, (x_3 < x_4 \to x_3 \doteq x_4)$

sse para algum $a \in \mathbb{Q}$, para algum $b \in \mathbb{Q}$, $(\mathscr{Q}, [v]_{\substack{x_3 \rightsquigarrow a \\ x_4 \rightsquigarrow b}}) \vDash (x_3 < x_4 \to x_3 \doteq x_4)$

sse para algum $a \in \mathbb{Q}$, para algum $b \in \mathbb{Q}$,

$(\mathscr{Q}, [v]_{\substack{x_3 \rightsquigarrow a \\ x_4 \rightsquigarrow b}}) \vDash \neg(x_3 < x_4)$ ou $\vDash (\mathscr{Q}, [v]_{\substack{x_3 \rightsquigarrow a \\ x_4 \rightsquigarrow b}})(x_3 \doteq x_4)$

sse para algum $a \in \mathbb{Q}$, para algum $b \in \mathbb{Q}$,

$[v]_{\substack{x_3 \rightsquigarrow a \\ x_4 \rightsquigarrow b}}(x_3) \geq^{\mathfrak{Q}} [v]_{\substack{x_3 \rightsquigarrow a \\ x_4 \rightsquigarrow b}}(4)$ ou $[v]_{\substack{x_3 \rightsquigarrow a \\ x_4 \rightsquigarrow b}}(x_3) = [v]_{\substack{x_3 \rightsquigarrow a \\ x_4 \rightsquigarrow b}}(x_4)$

sse para algum $a \in \mathbb{Q}$, para algum $b \in \mathbb{Q}$, $a \geq^{\mathfrak{Q}} b$ ou $a = b$

que é verdadeiro na estrutura.

Exemplo 4.12. Para qualquer $(\mathfrak{M}, v)$, se a variável x não ocorre no termo t então

$$(\mathfrak{M}, v) \vDash \exists x\, (x \doteq t).$$

$$\begin{aligned}
(\mathfrak{M}, v) \vDash \exists x\, (x = t) \text{ sse } & \text{ para algum } a \in M,\ (\mathfrak{M}, [v]_{x \rightsquigarrow a}) \vDash (x \doteq t) \\
\text{sse } & \text{ para algum } a \in M,\ [v]_{x \rightsquigarrow a}(x) = \overline{[v]_{x \rightsquigarrow a}}(t) \\
\text{sse } & \text{ para algum } a \in M,\ a = \overline{[v]_{x \rightsquigarrow a}}(t)
\end{aligned}$$

que é verdade pois, da definição, $\overline{[v]_{x \rightsquigarrow a}}(t) \in M$ e $\overline{[v]_{x \rightsquigarrow a}}(t) = \bar{v}(t)$ pois x não ocorre em t. Portanto, $(\mathfrak{M}, v) \vDash \exists x\, (x = t)$.

Metateorema 4.13. *Sejam $\mathfrak{M}$ uma estrutura para uma linguagem de primeira ordem $\mathscr{L}$. Para toda fórmula $\alpha \in \mathscr{L}$, se v e w são atribuições tais que $v(y) = w(y)$, para toda variável y que ocorre livre em α, então*

$$(\mathfrak{M}, v) \vDash \alpha \textit{ se, e somente se, } (\mathfrak{M}, w) \vDash \alpha.$$

Em particular, se α não tem variáveis livres, então $(\mathfrak{M}, v) \vDash \alpha$ se, e somente se, $(\mathfrak{M}, w) \vDash \alpha$ para quaisquer v e w.

Escrevemos

$$\mathfrak{M} \vDash \alpha$$

se $(\mathfrak{M}, v) \vDash \alpha$ para toda atribuição v é dizemos que α é **válida** em $\mathfrak{M}$.

Corolário 4.14. *Se α é uma sentença de $\mathscr{L}$ e $\mathfrak{M}$ é uma estrutura para $\mathscr{L}$, então $\mathfrak{M} \vDash \alpha$ ou $\mathfrak{M} \vDash \neg\alpha$.*

Demonstração do Teorema. A demonstração é por indução em fórmula. O teorema vale para fórmulas atômicas: se α é da forma $t_1 \doteq t_2$, então toda variável da fórmula é livre portanto $\bar{v}(t_1) = \bar{w}(t_1)$ e $\bar{v}(t_2) = \bar{w}(t_2)$. Se α é da forma $R(t_1, \dots, t_n)$, então toda variável da fórmula é livre portanto $\bar{v}(t_i) = \bar{w}(t_i)$ para todo i de modo que $(\bar{v}(t_1), \dots, \bar{v}(t_n)) = (\bar{w}(t_1), \dots, \bar{w}(t_n))$ portanto $(\bar{v}(t_1), \dots, \bar{v}(t_n)) \in R^{\mathfrak{M}}$ se, e só se, $(\bar{w}(t_1), \dots, \bar{w}(t_n)) \in R^{\mathfrak{M}}$ logo, em ambos os casos,

$$(\mathfrak{M}, v) \vDash \alpha \text{ se, e somente se, } (\mathfrak{M}, w) \vDash \alpha.$$

Se o teorema vale para α então vale para $\neg\alpha$: se $(\mathfrak{M}, v) \vDash \alpha$ se, e somente se, $(\mathfrak{M}, w) \vDash \alpha$, então $(\mathfrak{M}, v) \nvDash \alpha$ se, e somente se, $(\mathfrak{M}, w) \nvDash \alpha$ portanto $(\mathfrak{M}, v) \vDash \neg\alpha$ se, e somente se, $(\mathfrak{M}, w) \vDash \neg\alpha$.

Se o teorema vale para α e β então vale para $\alpha \to \beta$:

$$\begin{aligned} (\mathfrak{M}, v) \vDash \alpha \to \beta &\quad \text{sse} \\ (\mathfrak{M}, v) \vDash \neg\alpha \text{ ou } (\mathfrak{M}, v) \vDash \beta &\quad \text{sse} \\ (\mathfrak{M}, w) \vDash \neg\alpha \text{ ou } (\mathfrak{M}, w) \vDash \beta &\quad \text{sse} \\ (\mathfrak{M}, w) \vDash \alpha \to \beta & \end{aligned}$$

portanto $(\mathfrak{M}, v) \vDash \alpha \to \beta$ se, e somente se, $(\mathfrak{M}, w) \vDash \alpha \to \beta$.

Finalmente, se o teorema vale para α então vale para $\forall x\alpha$: suponha $(\mathfrak{M}, v) \vDash \forall x\alpha$. Fixado um $b \in E$, temos que $(\mathfrak{M}, [v]_{x\rightsquigarrow b}) \vDash \alpha$. Agora, se y é uma variável livre em α e $y \neq x$ então

$$[v]_{x\rightsquigarrow b}(y) = [w]_{x\rightsquigarrow b}(y)$$

pois $v(y) = w(y)$; se $y = x$

$$[v]_{x\rightsquigarrow b}(y) = [w]_{x\rightsquigarrow b}(y) = b.$$

Portanto, $(\mathfrak{M}, [w]_{x\rightsquigarrow b}) \vDash \alpha$ pois o teorema vale para α. Como b é arbitrário, o argumento vale para todo b, ou seja, $(\mathfrak{M}, w) \vDash \forall x\,\alpha$. A recíproca, se $(\mathfrak{M}, w) \vDash \forall x\,\alpha$ então $(\mathfrak{M}, v) \vDash \forall x\,\alpha$, é demonstrada com argumentação análoga.

Pelo Princípio da Indução para fórmulas, o teorema vale para toda fórmula de uma linguagem $\mathscr{L}$. ■

Demonstração do corolário. Seja α uma sentença e $\mathfrak{M}$ uma estrutura. Se $\mathfrak{M} \nvDash \alpha$, então para alguma atribuição v, $(\mathfrak{M}, v) \vDash \neg\alpha$. Como α não tem variáveis livres $(\mathfrak{M}, w) \vDash \neg\alpha$, para qualquer atribuição w. Portanto $\mathfrak{M} \vDash \neg\alpha$. A recíproca é análoga. ■

Exemplo 4.15. Seja $\mathfrak{D}$ uma estrutura cujo domínio D tenha pelo menos dois elementos. Então

$$\mathfrak{D} \vDash \forall x \exists y\,(x \neq y).$$

De fato, seja $a \in D$ um elemento arbitrário. Como D tem pelo menos 2 elementos

$$\text{dado } a \in D \text{, podemos escolher } b \in D \text{ com } b \neq a \text{ de modo que} \\ (\mathfrak{D}, [v]_{x\rightsquigarrow a, y\rightsquigarrow b}) \vDash x \neq y.$$

Como a foi arbitrário $(\mathfrak{D}, v) \vDash \forall x \exists y\,(x \neq y)$.

Se Γ é um conjunto de fórmulas da linguagem $\mathscr{L}$, escrevemos

$$\mathfrak{M} \vDash \Gamma$$

se $\mathfrak{M}) \vDash \alpha$ para toda fórmula $\alpha \in \Gamma$.

Exercício 4.16. *Prove que se* $\mathfrak{M} \vDash \{\alpha, \alpha \to \beta\}$ *então* $\mathfrak{M} \vDash \beta$.

Esboço da solução:. Seja v uma atribuição qualquer. Então $(\mathfrak{M}, v) \vDash \alpha$ e $(\mathfrak{M}, v) \vDash \neg\alpha$ (logo $(\mathfrak{M}, v) \nvDash \alpha$) ou $(\mathfrak{M}, v) \vDash \beta$. Então $(\mathfrak{M}, v) \vDash \beta$ para todo v. ■

Exercício 4.17. *Se* $\mathfrak{M} \vDash \alpha$ *então* $\mathfrak{M} \vDash \forall x\, \alpha$.

Solução. Se $\mathfrak{M} \vDash \alpha$ então $(\mathfrak{M}, v) \vDash \alpha$ para toda atribuição v, em particular, $(\mathfrak{M}, [v]_{x \rightsquigarrow a}) \vDash \alpha$ para todo a no domínio de $\mathfrak{M}$. ■

Exercício 4.18. *Verifique que para o contexto do exemplo 4.11 valem*

1. $\mathcal{Q} \vDash \forall x_1\, (\exists x_2\, (x_1 < x_2))$.
2. $\mathcal{Q} \vDash \exists x_3\, (\exists x_4\, (x_3 < x_4 \to x_3 \doteq x_4))$.

Esboço da solução:. $(\mathcal{Q}, v) \vDash \forall x_1\, (\exists x_2\, (x_1 < x_2))$ sse
$(\mathcal{Q}, [v]_{x_1 \rightsquigarrow a}) \vDash \exists x_2\, (x_1 < x_2)$ para todo $a \in \mathbb{Q}$, sse
$(\mathcal{Q}, [v]^{a,b}_{x_1,x_2}) \vDash x_1 < x_2$ para todo $a \in \mathbb{Q}$, para algum $b \in \mathbb{Q}$, sse
$[v]^{a,b^*}_{x_1,x_2}(x_1) <^{\mathcal{Q}} [v]^{a,b^*}_{x_1,x_2}(x_2)$ para todo $a \in \mathbb{Q}$, para algum $b \in \mathbb{Q}$, sse
$a < b$ para todo $a \in \mathbb{Q}$, para algum $b \in \mathbb{Q}$.
$(\mathcal{Q}, v) \vDash \exists x_3\, (\exists x_4\, (x_3 < x_4 \to x_3 = x_4))$ sse
$(\mathcal{Q}, [v]^{a}_{x_3}) \vDash \exists x_4\, (x_3 < x_4 \to x_3 = x_4)$ para algum $a \in \mathbb{Q}$, sse
$(\mathcal{Q}, [v]^{a,b}_{x_3,x_4}) \vDash (x_3 < x_4 \to x_3 = x_4)$ para algum $a \in \mathbb{Q}$, algum $b \in \mathbb{Q}$, sse
$[v]^{a,b^*}_{x_3,x_4}(x_3) <^{\mathcal{Q}} [v]^{a,b^*}_{x_3,x_4}(x_4) \to [v]^{a,b^*}_{x_3,x_4}(x_3) = [v]^{a,b^*}_{x_3,x_4}(x_4)$ para algum $a \in \mathbb{Q}$, para algum $b \in \mathbb{Q}$, sse
$a < b \to a = b$ para algum $a \in \mathbb{Q}$, para algum $b \in \mathbb{Q}$ ■

Agora, se vale

$$(\mathfrak{M}, v) \vDash \alpha \text{ para toda interpretação } (\mathfrak{M}, v)$$

então α é **universalmente válida** e escrevemos

$$\vDash \alpha$$

como, por exemplo, em $x \doteq x$. Para qualquer $\mathfrak{M}$ e qualquer v temos, por definição, que $(\mathfrak{M}, v) \vDash x \doteq x$ se, e só se, $\bar{v}(x) = \bar{v}(x)$, o que é sempre verdade. Notemos que $x \doteq y$ não é universalmente válida, pois basta tomar a estrutura canônica para a aritmética $\mathfrak{N}$ com $v(x) = 1$ e $v(y) = 2$. Tampouco $x \not\doteq y$ é válida, pois como antes basta tomar $v(x) = v(y) = 2$.

Exemplo 4.19. Para quaisquer $\mathfrak{M}$ e v vale $(\mathfrak{M}, v) \vDash \forall x\, (x \doteq x)$ sse para todo a no domínio da interpretação $(\mathfrak{M}, [v]_{x \rightsquigarrow a}) \vDash (x \doteq x)$. Mas $[v]_{x \rightsquigarrow a}(x) = [v]_{x \rightsquigarrow a}(x)$ para qualquer atribuição v e qualquer a no domínio M, portanto $(\mathfrak{M}, [v]_{x \rightsquigarrow a}) \vDash (x = x)$. Assim, $\vDash \forall x\, (x \doteq x)$.

Exemplo 4.20. Seja $\mathscr{L}$ uma linguagem de primeira ordem com símbolo relacional unário P e constante c. Então

$$\models P(c) \to \exists x P(x) \tag{4.1}$$

pois, por definição, para quaisquer $\mathfrak{M}$ e v temos $(\mathfrak{M}, v) \models P(c) \to \exists x P(x)$ se, e só se, para quaisquer $\mathfrak{M}$ e v temos $(\mathfrak{M}, v) \not\models P(c)$ ou $(\mathfrak{M}, v) \models \exists x P(x)$. Se $(\mathfrak{M}, v) \not\models P(c)$ temos $(\mathfrak{M}, v) \models P(c) \to \exists x P(x)$. Assuma que $(\mathfrak{M}, v) \models P(c)$. Porém $(\mathfrak{M}, v) \models \exists x P(x)$ se, e só se, para algum $a \in M$, $(\mathfrak{M}, [v]_{x \rightsquigarrow a}) \models P(x)$ e basta tomar $a = c$ e temos $(\mathfrak{M}, v) \models \exists x P(x)$. Como a interpretação foi arbitrária a equação (4.1) é universalmente válida.

Exemplo 4.21. A sentença $\forall x \forall y (x \doteq y)$ é falsa em qualquer interpretação com domínio formado por menos dois elementos pois, fixado $(\mathfrak{M}, v)$, se não for falsa nessa interpretação, então será verdadeira e se esse é o caso $(\mathfrak{M}, v) \models \forall x \forall y (x \doteq y)$ sse $(\mathfrak{M}, [v]_{x \rightsquigarrow a, y \rightsquigarrow b}) \models x = y$ para todo a e todo b. Se o universo do discurso tem pelo menos dois elementos então podemos tomar a e b distintos, o que torna a sentença falsa.

Exercício 4.22. *Verifique a validade universal* $\models \forall x \exists y (x \doteq y)$.

Na página 81 comentamos que argumentos como

Premissa	*O quadrado de qualquer inteiro é positivo*
Premissa	*9 é um quadrado*
Conclusão	*9 é positivo*

não são validados pela lógica proposicional. Agora temos, na linguagem da Aritmética,

Premissa	$\forall x (x \cdot x > 0)$
Premissa	$\exists x (x \cdot x \doteq SSSSSSSSS0)$
Conclusão	$SSSSSSSSS0 > 0$

pois, de fato, $\forall x (x \cdot x > 0), \exists x (x \cdot x \doteq SSSSSSSSS0) \models SSSSSSSSS0 > 0$. Para toda $\mathscr{L}_N$-estrutura $\mathfrak{M}$ tal que

$$\mathfrak{M} \models \exists x (x \cdot x \doteq SSSSSSSSS0), \forall x (x \cdot x > 0)$$

temos

$$\text{para algum } b \in M,\ b \cdot b = 9$$

e também

$$\text{para todo } a \in M,\ a \cdot a > 0$$

logo $b \cdot b > 0$ e se $b \cdot b = 9$, então $9 > 0$, ou seja, 9 é positivo.

Valor-verdade

Se a interpretação satisfaz uma fórmula, então ela é **verdadeira** naquela interpretação. Podemos definir formalmente uma valoração numa álgebra booleana $\hat{v}\colon \mathscr{L}_1 \to \{0,1\}$ pondo para cada fórmula α um valor-verdade de acordo com a interpretação $(\mathfrak{M}, v)$ definido recursivamente por

1. $\hat{v}(s \doteq t) = 1$ se, e somente se, $\bar{v}(s) = \bar{v}(t)$;
2. $\hat{v}(R(t_1,\dots,t_n)) = 1$ se, e somente se, $(\bar{v}(t_1),\dots,\bar{v}(t_n)) \in R^{\mathfrak{E}}$;
3. $\hat{v}(\neg\alpha) = 1 - \hat{v}(\alpha)$;
4. $\hat{v}(\beta \to \gamma) = \max\{1 - \hat{v}(\beta), \hat{v}(\gamma)\}$;
5. $\hat{v}(\forall x\alpha) = \min_{a\in E} \widehat{[v]_{x\rightsquigarrow a}}(\alpha)$.

Exercício 4.23. *Podemos dividir as fórmulas de uma linguagem de primeira ordem $\mathscr{L}$ em*

(i) primitivas*: são as fórmulas atômicas de $\mathscr{L}$ e as fórmulas da forma $\forall x\, \alpha$ de $\mathscr{L}$.*
(ii) não-primitivas: *são as fórmulas da forma $\neg\alpha$ e as fórmulas da forma $\alpha \to \beta$ (os outros conectivos são abreviações).*

Assim, qualquer fórmula de $\mathscr{L}$ é construída a partir das fórmulas primitivas usando os conectivos negação *e* implicação. *Denote por $\mathscr{VP}$ o conjunto das fórmulas primitivas. Agora, considerando a lógica proposicional e tomando para as variáveis proposicionais as fórmulas primitivas do conjunto $\mathscr{VP}$ temos que as fórmulas da linguagem $\mathscr{L}$ também são fórmulas da lógica proposicional. Por exemplo,* $(\forall y \neg P(y) \to \neg P(x)) \to (P(x) \to \neg\forall y \neg P(y))$ *é uma tautologia proposicional*

$\forall y \neg P(y)$	$P(x)$	$\neg\forall y \neg P(y)$	$\neg P(x)$	$(\forall y \neg P(y) \to \neg P(x)) \to (P(x) \to \neg\forall y \neg P(y))$
0	0	1	1	1
0	1	1	0	1
1	0	0	1	1
1	1	0	0	1

Por outro lado, $\forall x(P(x) \to P(x))$ não é tautologia (é uma fórmula atômica proposicional).

1. *Mostre que toda $\mathscr{L}$-estrutura que satisfaz $\forall x\, P(x)$ também satisfaz $P(a)$. Mostre que na semântica proposicional isso não vale, ou seja, $\forall x\, P(x) \not\models P(a)$.*
2. *Dada a interpretação $(\mathfrak{M}, v)$ para $\mathscr{L}$, defina uma interpretação na lógica proposicional definindo*
$$v : \mathscr{VP} \to \{0,1\}$$
que atribui um valor-verdade para cada fórmula primitiva pondo
$$v(\alpha) = 1 \textit{ se, e só se, } (\mathfrak{M}, v) \models \alpha.$$
Demonstre que a (única) atribuição $w : \mathscr{L} \to \{0,1\}$ que estende v satisfaz
$$w(\alpha) = 1 \textit{ se, e somente se, } (\mathfrak{M}, v) \models \alpha.$$

4.3 Consequência lógica

Sejam $\mathscr{L}$ uma linguagem de primeira ordem e $\Gamma \subset \mathscr{L}$ um conjunto de fórmulas. A fórmula α é **consequência lógica** (ou consequência semântica) de Γ, e escrevemos

$$\Gamma \vDash \alpha$$

quando para qualquer $\mathscr{L}$-estrutura $\mathfrak{M}$,

$$\text{se } \mathfrak{M} \vDash \Gamma \text{ então } \mathfrak{M} \vDash \alpha$$

ou seja, se $(\mathfrak{M}, v) \vDash \Gamma$ para toda atribuição v, então $(\mathfrak{M}, w) \vDash \Gamma$ para toda atribuição w. Caso Γ seja finito, escrevemos

$$\gamma_1, \gamma_1, \ldots, \gamma_n \vDash \alpha$$

e nesse caso temos um **argumento válido**.

Por exemplo, na linguagem da aritmética

$$x < y \vDash z < w. \tag{4.2}$$

De fato, seja $\mathfrak{A}$ tal que $\mathfrak{A} \vDash x < y$, isto é, para qualquer atribuição v na interpretação resulta que para todos a e b no domínio de $\mathfrak{A}$ temos $a <^{\mathfrak{A}} b$. Na estrutura $\mathfrak{A}$ vale $(\mathfrak{A}, u) \vDash z < w$ qualquer que seja a atribuição u pois $u(z), u(w) \in A$ logo $u(z) < u(w)$.

Exemplo 4.24. Do exercício 4.16 temos $\alpha, \alpha \to \beta \vDash \beta$.

Exercício 4.25. *Verifique que*

1. $\forall x\, \alpha, \forall x\, \alpha \to \beta \vDash \forall x\, \beta$
2. $\forall x\, \alpha \vDash [\alpha]_x^t$ *sempre que a substituição é admissível.*

Exemplo 4.26. A negação da sentença que formaliza o paradoxo de Russel na linguagem da Teoria dos Conjuntos, equação (3.1) na página 89, é universalmente válida

$$\vDash \neg \exists x \forall y\, (y \in x \leftrightarrow y \notin y).$$

Do exercício acima, item 2, temos

$$\forall y\, (y \in x \leftrightarrow y \notin y) \vDash y \in y \leftrightarrow y \notin y.$$

e como $y \in y \leftrightarrow y \notin y$ não é válida, temos $\nvDash \forall y\, (y \in x \leftrightarrow y \notin y)$ portanto

$$\nvDash \exists x \forall y\, (y \in x \leftrightarrow y \notin y)$$

ou seja $\vDash \neg \exists x \forall y\, (y \in x \leftrightarrow y \notin y)$.

Metateorema 4.27. *Sejam Γ um conjunto de fórmulas e α uma sentença e β uma fórmula, todos de uma linguagem de primeira ordem $\mathscr{L}$. Então*

$$\Gamma, \alpha \vDash \beta \textit{ se, e só se, } \Gamma \vDash \alpha \rightarrow \beta.$$

Demonstração. Primeiro, assumimos a hipótese que $\Gamma, \alpha \vDash \beta$ e provaremos $\Gamma \vDash \alpha \rightarrow \beta$. Seja $\mathfrak{M}$ uma $\mathscr{L}$-estrutura tal que $\mathfrak{M} \vDash \Gamma$ e temos dois casos pelo corolário 4.14

1. $\mathfrak{M} \vDash \alpha$: nesse caso, por hipótese vale $(\mathfrak{M}, v) \vDash \beta$ para qualquer atribuição v, então $(\mathfrak{M}, v) \vDash \neg\alpha$ ou $(\mathfrak{M}, v) \vDash \beta$, portanto, $(\mathfrak{M}, v) \vDash \alpha \rightarrow \beta$.
2. $\mathfrak{M} \nvDash \alpha$: nesse caso, para qualquer atribuição v, $(\mathfrak{M}, v) \vDash \neg\alpha$ ou $(\mathfrak{M}, v) \vDash \beta$, logo, $(\mathfrak{M}, v) \vDash \alpha \rightarrow \beta$.

Agora, assumimos que $\Gamma \vDash \alpha \rightarrow \beta$ e provaremos $\Gamma, \alpha \vDash \beta$. Suponha que $\mathfrak{M} \vDash \Gamma \cup \{\alpha\}$, então $\mathfrak{M} \vDash \Gamma$, portanto, $\mathfrak{M} \vDash \alpha \rightarrow \beta$, ou seja, $\mathfrak{M} \vDash \neg\alpha$ ou $\mathfrak{M} \vDash \beta$. Como, por hipótese, $\mathfrak{M} \vDash \alpha$, temos $\mathfrak{M} \vDash \beta$. ∎

A exigência de que α seja uma sentença é de fato necessária como mostra o seguinte exemplo. da equação (4.2) acima não podemos deduzir $\vDash (x < y) \rightarrow (z < w)$ pois essa não é universalmente válida. Considere o a estrutura canônica para a aritmética onde $<$ é interpretado como o “menor que” usual nos naturais. Com a atribuição $v(x) = v(w) = 1$ e $v(y) = v(z) = 0$ temos $(\mathfrak{N}, v) \nvDash (x < y) \rightarrow (z < w)$.

Equivalência lógica

Numa linguagem $\mathscr{L}$ de primeira ordem a fórmula α é **semanticamente equivalente** à fórmula β, o que denotamos por

$$\alpha \equiv \beta$$

se

$$\vDash \alpha \leftrightarrow \beta.$$

Por exemplo, são equivalências lógicas

$$\forall x \forall y \alpha \equiv \forall y \forall x \alpha$$

$$\forall x(\alpha \wedge \beta) \equiv \forall x \alpha \wedge \forall x \beta$$

$$\exists x \exists y \alpha \equiv \exists y \exists x \alpha$$

$$\exists x(\alpha \vee \beta) \equiv \exists x \alpha \vee \exists x \beta$$

$$\neg(\forall x\, \alpha) \equiv \exists x \neg\alpha$$

$$\neg(\exists x\, \alpha) \equiv \forall x \neg\alpha$$

4.4 Teoria e Modelo

Se Σ é um conjunto de sentenças tal que se $\alpha \in \Sigma$ então $\Sigma \vDash \alpha$, então Σ é dita um **teoria**. Se $\mathfrak{M}$ é uma estrutura para a linguagem $\mathscr{L}$, então a **teoria de** $\mathfrak{M}$ é o conjunto de todas as *sentenças* de $\mathscr{L}$ verdadeiras em $\mathfrak{M}$, ou seja

$$\mathrm{Th}(\mathfrak{M}) = \{\tau : \tau \text{ é uma sentença de } \mathscr{L} \text{ e } \mathfrak{M} \vDash \tau\}.$$

Uma teoria Σ é **axiomatizável** se existe um conjunto de fórmulas $\Gamma \subset \Sigma$ tal que para toda sentença α da teoria

$$\Gamma \vDash \alpha.$$

Por exemplo, a Aritmética é axiomatizável pois há um conjunto de axiomas desenvolvido por Giuseppe Peano cujas consequências lógicas são os teoremas da Aritmética.

Dizemos que a estrutura $\mathfrak{M}$ é uma **modelo** para uma teoria se para toda sentença α na teoria

$$\mathfrak{M} \vDash \alpha$$

e dizemos que α é **verdadeira** em $\mathfrak{M}$, caso contrário dizemos que α é **falsa** no modelo $\mathfrak{M}$.

Exemplo 4.28. Uma **ordem parcial** sobre um conjunto M é uma relação binária $\preceq$ com as seguintes propriedades, chamadas de **axiomas das ordens parciais**, formulados na linguagem $\mathscr{L}_O$

1. $\forall x(x \preceq x)$;
2. $\forall x \forall y(x \preceq y \land y \preceq x \to x \doteq y)$;
3. $\forall x \forall y \forall z(x \preceq y \land y \preceq z \to x \preceq z)$.

Um **conjunto parcialmente ordenado** é um modelo $\mathscr{O} = (M, \preceq)$ desses axiomas e a **teoria elementar das ordens parcias** é o conjunto das sentenças que são consequências lógicas desses axiomas.

Exemplo 4.29. Um **grafo** é um modelo $\mathscr{G} = (V, E)$ sobre um conjunto de vértices V e uma relação binária E para os seguintes **axiomas da teoria elementar dos grafos**, formulados na linguagem $\mathscr{L}_G$,

1. $\forall x, \neg E(x,x)$;
2. $\forall x \forall y\, (E(x,y) \to E(y,x))$.

Exercício 4.30. *Um vértice isolado de um grafo é um elemento v do universo que não é adjacente a nenhum outro elemento do universo. Expresse na linguagem da Teoria dos Grafos as sentença 'o grafo não tem vértice isolado'.*

Exercício 4.31. *Um triângulo em um grafo é qualquer conjunto de três vértices que são adjacentes dois a dois. Expresse na linguagem da Teoria dos Grafos as sentença 'o grafo tem triângulo'.*

4.5 Exercícios

1. Seja v uma atribuição associada a estrutura $\mathfrak{M}$ para uma linguagem $\mathscr{L}$. Suponha que para as variáveis x e y temos que $v(x) = v(y)$. Use indução para termos para demonstrar que se t é termo e s é obtido de t substituindo-se uma ou mais ocorrências de x por y então $\bar{v}(s) = \bar{v}(t)$.
2. Verifique que os axiomas dos sistemas dedutivos apresentados no capítulo 3.3 são verdades lógicas.
3. Considere a linguagem da aritmética $\mathscr{L}_N$ com a estrutura canônica $\mathfrak{N}$ do exemplo 4.3, item 2, e atribuição constante $v(x) = 2$ para toda variável.
   a) Verifique que $(\mathfrak{N}, s) \vDash x \doteq +(1,1)$.
   b) Diga para quais atribuições associadas a $\mathfrak{N}$ a seguinte fórmula é satisfeita:
      (b.1) $\forall x\,((\exists z(x \cdot z \doteq y)) \to \exists z\,((1+1)\cdot z \doteq x)))$
      (b.2) $(\exists x(x + x \doteq y)) \to (\exists y(y + x \doteq y))$
4. Seja $\mathscr{L}$ uma linguagem de primeira ordem com constante a, função unária G, relação unária R e relações binárias $\{P, Q\}$. Seja $\mathfrak{A}$ a estrutura definida por

   - $D := \mathbb{N}$
   - $a^{\mathfrak{A}} := 2$;
   - $G^{\mathfrak{A}}(n) := n+1$;
   - $R^{\mathfrak{A}}(n) := \{n \in \mathbb{N} \colon n \text{ é par}\}$;
   - $P^{\mathfrak{A}} := \{(n,m) \in \mathbb{N}\times\mathbb{N} \colon n \le m\}$;
   - $Q^{\mathfrak{A}} := \varnothing$.

   Para cada uma das sentenças abaixo, verifique se é satisfeita ou não na estrutura.

   a) $\exists x G(x) \wedge \forall x(G(x) \doteq x)$;
   b) $\exists x \exists y Q(x,y)$;
   c) $\neg R(a) \to \forall x \forall y Q(x,y)$;
   d) $\forall x(R(x) \to \forall x R(G(G(x)))$;
   e) $\forall x \exists y P(x,y)$;
   f) $\exists y \forall x P(x,y)$;
   g) $\exists y \forall x P(y,x)$;
   h) $\forall x\big(R(x) \vee \exists y\big(y \doteq G(x) \wedge R(y)\big)\big)$.

5. Seja $\mathscr{L}_F$ a linguagem dos corpos com constantes 0 e 1, símbolos funcionais $+$ e $\cdot$. Chamaremos de **axiomas de corpo** o seguinte conjunto de sentenças da linguagem $\mathscr{L}_F$:

   (C1) $0 \neq 1$;
   (C2) $\forall x\,(x + 0 \doteq x)$;
   (C3) $\forall x\,((x \neq 0) \to (x \cdot 1 \doteq x))$;
   (C4) $\forall x \forall y\,(x + y \doteq y + x)$;
   (C5) $\forall x \forall y\,(x \cdot y \doteq y \cdot x)$;
   (C6) $\forall x \forall y \forall z\,((x+y)+z \doteq x+(y+z))$;
   (C7) $\forall x \forall y \forall z\,((x \cdot y)\cdot z \doteq x \cdot (y \cdot z))$;
   (C8) $\forall x \exists y\,(x + y \doteq 0)$;
   (C9) $\forall x\,((x \neq 0) \to \exists y\,(x \cdot y \doteq 1))$;
   (C10) $\forall x \forall y \forall z\,(x\cdot(y+z) \doteq (x\cdot y)+(x\cdot z)$.

   (5.1) Considere a estrutura $\mathfrak{U}$ do exemplo 4.3, item 1. Verifique que $\mathfrak{U}$ satisfaz todos os axiomas de corpo.

   (5.2) Considere a estrutura do exercício anterior e v uma atribuição satisfazendo $v(x) = 1$, $v(y) = 2$ e $v(z) = 3$. Verifique quais das seguintes fórmulas abaixo são verdadeiras na interpretação $(\mathfrak{U}, v)$
   a) $x + y \doteq 0$;

b) $\forall y((y \neq 0) \to (y \cdot x \doteq y))$;
c) $\forall x(x \cdot 0 \doteq 0)$;

(5.3) Para cada fórmula α contendo variáveis livres do exercício anterior, considere o **fecho universal** de α a sentença $\forall x \forall y(\alpha)$. Verifique se essas sentenças são verdadeiras no modelo $\mathcal{N}$ do item 5.1.

(5.4) Verifique que a estrutura $\mathfrak{R} = (\mathbb{R}, 0, 1, +, \cdot)$ satisfaz os axiomas de corpo.

6. Seja $\mathscr{L}_G$ a linguagem dos grupos com constante e e símbolo funcional $\circ$. Chamamos de **axiomas de grupo** o seguinte conjunto Γ de sentenças da linguagem $\mathscr{L}_G$:
(G1) $\forall x\,((x \circ e = x) \wedge (e \circ x = x))$;
(G2) $\forall x \exists y\,(x \circ y = e)$;
(G3) $\forall x \forall y \forall z\,(x \circ (y \circ z) = (x \circ y) \circ z)$.
   a) Seja α a sentença $\forall x\,(x \circ x = e)$.
   Mostre que a sentença α é **independente** dos axiomas de grupo mostrando uma interpretação para $\{G1, G2, G3, \alpha\}$ e outra interpretação para $\{G1, G2, G3, \neg\alpha\}$.
   b) Tome $\mathscr{G}$ a seguinte estrutura para $\mathscr{L}_G$
   - $D := \{1, 2\}$;
   - $e^{\mathscr{G}} := 1$;
   -

$\circ^{\mathscr{G}}$	1	2
1	1	2
2	2	1

   Verifique se os axiomas são verdadeiros nesse modelo.

7. Demonstre usando indução para fórmula que se t é uma substituição admissível para x em α então

$$(\mathfrak{M}, v) \vDash [\alpha]_x^t \text{ sse } (\mathfrak{M}, [v]_{x \rightsquigarrow \bar{v}(t)}) \vDash \alpha.$$

8. Considere a linguagem de primeira ordem com o predicados unários r, p, o predicado binário q, as constantes a, b, c e os símbolos funcionais f unário g binário.
   a) Identifique quais das expressões a seguir são fórmulas.
      i. $r(a)$;
      ii. $r(f)$;
      iii. $r(g(x, f(a))) \wedge r(f(y)) \to x \doteq y$;
      iv. $r(x) \to \forall y(t(y))$;
      v. $\forall x(\exists y(r(f(x)) \to \neg r(g(y, x))))$
   b) Considere a estrutura $\mathscr{E}$ dada por
   - $E = \{1\}$;
   - $r^{\mathscr{E}} = p^{\mathscr{E}} = \{1\}$;
   - $q^{\mathscr{E}} = \{(1, 1)\}$;
   - $a^{\mathscr{E}} = b^{\mathscr{E}} = c^{\mathscr{E}} = 1$;
   - $f^{\mathscr{E}} : E \to E,\ f^{\mathscr{E}}(x) = 1$;
   - $g^{\mathscr{E}} : E \times E \to E,\ g^{\mathscr{E}}(x, y) = x$.

   Verificar se as sentenças a seguir são satisfeitas.

i. $\forall x_1(\exists x_2(\exists x_3(p(x_1) \to (r(x_2) \wedge r(x_3) \wedge (x_1 \doteq g(x_2, x_3))))))$.
ii. $\forall x_1(\exists x_2(\exists x_3(q(x_1, x_2) \to (r(x_2) \wedge r(x_3) \wedge (x_1 \doteq g(x_2, x_3))))))$.
iii. $\forall x_1(\exists x_2(p(x_1) \to (r(x_2) \wedge (x_1 \doteq g(x_2, a)))))$.
iv. $\forall x_1(\exists x_2(p(x_1) \to (r(x_2) \wedge (x_1 \doteq g(x_2, c)))))$.
v. $\exists x_1(\exists x_2(p(x_1) \to (r(x_2) \wedge (x_1 \doteq g(x_2, c)))))$.
vi. $\forall x_1(\exists x_2(q(x_1, x_2) \to (r(x_2) \wedge (x_1 \doteq g(x_2, a)))))$.
vii. $\forall x_1(\exists x_2(q(x_1, x_2) \to (r(x_2) \wedge (x_1 \doteq g(x_2, c)))))$.
viii. $\exists x_1(\exists x_2(q(x_1, x_2) \to (r(x_2) \wedge (x_1 \doteq g(x_2, a)))))$.
ix. $\forall x(r(x))$;
x. $\forall x(r(x) \to r(x))$;
xi. $\forall x(q(x,x) \to q(x,x))$;
xii. $\exists x(p(f(x)) \to r(x))$;
xiii. $\exists x(q(f(x), g(x,x)) \to r(x,x))$;
xiv. $\forall x(p(f(x)) \to r(x))$;
xv. $\forall x(\neg p(f(x)) \to r(x))$;
xvi. $\neg\forall x(p(f(x)) \to r(x))$;
xvii. $\forall x(q(f(x), x) \to r(x))$;
xviii. $\forall x(\neg q(f(x), x) \to r(x))$;
xix. $\neg\forall x(q(f(x), x) \to r(x))$;

c) Construa, se possível, uma estrutura para cada sentença φ acima de modo que $\mathscr{E} \not\models \varphi$.

d) Faça o mesmo para a estrutura $\mathscr{A}$ dada por
- $A = \{1, 2, 3, 4, \ldots\}$;
- $r^{\mathscr{A}} = \{1, 3, 5, \ldots\}$;
- $p^{\mathscr{A}} = \{2, 4, 6, \ldots\}$;
- $q^{\mathscr{A}} = \{(1,2), (3,4), (5,6), \ldots\}$;
- $a^{\mathscr{A}} = 1$;
- $b^{\mathscr{A}} = 2$;
- $c^{\mathscr{A}} = 3$;
- $f^{\mathscr{A}} : A \to A,\ f^{\mathscr{A}}(x) = x + 1$;
- $g^{\mathscr{A}} : A \times A \to A,\ g^{\mathscr{A}}(x, y) = x + y$.

9. Demonstre que a generalização de uma fórmula é válida se e somente se a fórmula é válida, ou seja, para uma fórmula α de uma linguagem de primeira ordem qualquer
$$\models \alpha \text{ se, e somente se} \models \forall x\, \alpha$$
qualquer que seja a variável x.

10. Deduza dos exercícios 9 e 4.23(c) que as tautologias da Lógica Proposicional são fórmulas válidas na Lógica de Predicados.

11. Demonstre que uma generalização para uma variável que não ocorre livre na fórmula é consequência lógica da própria fórmula, isto é, se x não ocorre livre em α então
$$\alpha \models \forall x\, \alpha.$$

12. Posto que $\neg\forall x\alpha$ é equivalente a $\exists x\neg\alpha$, e $\neg\exists x\alpha$ é equivalente a $\forall x\neg\alpha$, passe as sentenças dos axiomas para corpo para a negação, usando o símbolo de negação apenas na frente de subfórmulas atômicas.

5

Metateoremas da lógica Clássica

Referências

1. Rautenberg, Wolfgang (2010) A Concise Introduction to Mathematical Logic, 3ª edição, Universitext, Springer-Verlag London.
2. van Dalen, Dirk (2013) Logic and Structure, 5ª edição, Universitext, Springer-Verlag London.
3. Oliveira, Augusto Franco (2010) Lógica e Aritmética: uma introdução à lógica, matemática e computacional, 3ª edição, Gradiva.
4. Hodel, Richard E. (2013) An Introduction to Mathematical Logic. Dover Books on Mathematics.
5. Fajardo, Rogério A.S. (2017) Lógica matemática. Edusp. 111

Índice Remissivo