

Matemática para a Computação I

Notas de Aula

Valdigleis S. Costa

Universidade Federal do Rio Grande do Norte – UFRN

Centro de Ciências Exatas e da Terra – CCET

Departamento de Informática e Matemática Aplicada – DIMAP

15 de setembro de 2025

Copyright © 2019-2025 Linus van Pelt

Este texto NÃO possui qualquer tipo de vínculo editorial, e não possui fins lucrativos.

Página pessoal do autor <https://linus.pagina>

Este material é licenciado sob a Licença Atribuição-NãoComercial-CompartilhaIgual 3.0 Não Adaptada (CC BY-NC-SA 4.0). Você pode obter uma cópia da licença acessando a página:

<https://creativecommons.org/licenses/by-nc-sa/4.0/legalcode.pt>

ou enviando uma carta para Creative Commons, 444 Castro Street, Suite 900, Mountain View, California, 94041, USA.

Este tomo foi escrito com base em uma coleção de notas de aulas do autor, o mesmo foi redigido usando um *template* desenvolvido pelo próprio autor. Este texto foi escrito com o conjunto de macros L^AT_EX (em sua versão 2) e compilado usando as ferramentas LuaL^AT_EX e BibT_EX, tais ferramentas fornecidas pelas distribuições T_EXLive e MacT_EX, respectivamente nos sistemas operacionais *Unix-like*: **Debian** e no **Mac OS X**, para edição foram usados os *softwares* livres de edição textual **Vim** (versão 0.10.1), além disso, o sistema de controle de versão adotado é o **Git** (versão 2.34.1).

Release compilado em 15 de setembro de 2025 (732 minutos após a meia-noite).

Sumário

I Lógica e Demonstrações

1	Introdução à Lógica	3
1.1	O que é Lógica?	3
1.2	Um Pouco de História	4
1.3	Argumentos, Proposições e Predicados	6
1.4	Conectivos, Quantificadores e Negação	7
1.5	Representação Simbólica	9
1.6	Lógica e Ciência da Computação	10
1.7	Questionário	11
2	Lógica Proposicional	15
2.1	A Linguagem Proposicional	15
2.2	Sistema Dedutivo	17
2.3	Sistema Axiomático L	31
2.4	Sistema Semântico	33
2.5	Corretude e Completude	40
2.6	Questionário	46
3	Lógicas e Teoria de Primeira Ordem	51
4	Demonstrações	53
4.1	Introdução	53
4.2	Demonstrando Implicações	55
4.3	Demonstração por Absurdo	58
4.4	Demonstrando Generalizações	60
4.5	Demonstrando Existência e Unicidade	61
4.6	Demonstração Guiada por Casos	64
4.7	Outras Formas de Representação de Provas	65
4.8	Demonstração de Suficiência e Necessidade	66
4.9	Refutações	66
4.10	Questionário	67
	Referências Bibliográficas	74

Parte I

Lógica e Demonstrações

Introdução à Lógica

“Se você sabe que está morto, você está morto.

Mas se você sabe que está morto, você não está morto, portanto você não sabe se está morto ou não.”

Zenão de Cítio (334-262 a.C.)

1.1 O que é Lógica?

Antes de apresentar uma descrição histórica da lógica, este texto começa pela árdua tarefa de apresentar de forma sucinta uma resposta para a pergunta, “**o que é a lógica?**”. Como dito em [8, 17], a palavra lógica e suas derivações são familiares a quase todas (se não todas) as pessoas, de fato, é comum durante o cotidiano do dia a dia as pessoas recorrerem ao uso do termo lógica ou de seus derivados, sendo que na maioria das vezes seu uso está ligada à ideia de obviedade (ou certeza), por exemplo, nas frases:

- (a) É lógico que vou na festa.
- (b) É lógico que ciência da computação é um curso difícil.
- (c) Logicamente o Vasco não pode ganhar o título da primeira divisão nacional em 2021.
- (d) Logicamente se eu tomar banho, vou ter que me molhar.

Essa forma de usar os derivados da palavra lógica enquanto entidades para transmissão de certeza pode ser usada como gatilho “fácil e preguiçoso” para enunciar que a lógica se trata de uma ciência (ou disciplina) acerca das certezas sobre os fatos do mundo real.

Existem outras respostas comumente encontradas na literatura acadêmica (ver [1, 8, 40]) para o que seria a lógica, entre essas respostas, esta aquela que descreve a lógica como sendo um mecanismo utilizado durante o raciocínio estruturado e correto¹, isto é, uma ferramenta do raciocínio que possibilita a inferência de conclusões a partir de premissas [1, 17, 31], por exemplo, dado as premissas:

- (a) Toda quinta-feira é servido peixe no almoço.
- (b) Hoje é quarta-feira.

¹ Em [38] diz que a lógica se preocupa com a avaliação de argumentos, e em separar os argumentos bons dos ruins.

O raciocínio munido da “ferramenta de inferência” contida na lógica permite deduzir a afirmação: **Amanhã será servido peixe no almoço**, como conclusão. Note que esta segunda resposta estabelece que a lógica é um tipo de procedimento mental capaz de transformar (informações) as entradas (as premissas) nas saídas (a conclusão), usando uma ferramenta de inferência.

Essas duas formas de encarar a lógica não estão totalmente erradas, entretanto, também não exibem de forma completa o real significado do que seria a lógica em si. Uma terceira resposta para a pergunta “O que é a lógica?” aparece na edição de 1953 da *Encyclopædia Britannica* na seguinte forma: “*Logic is the systematic study of the structure of propositions and of the general conditions of valid inference by a method which abstracts from the content or matter of the propositions and deals only with their logical form*”. Note que essa resposta utiliza-se de autorreferência², pois a mesma tenta definir o que é a lógica em função do termo “forma lógica”.

Apesar dessa definição recursiva, a resposta da *Encyclopædia Britannica* apresenta duas características muito marcantes para a apresentação da lógica enquanto ciência (ou disciplina) nos dias atuais. A primeira característica é a validade das afirmações derivadas (ou concluídas) pelos mecanismos de inferência. A segunda característica é a importância da forma de representação (a escrita) dos termos lógicos.

A validade remonta a ideia de um significado dual (verdadeiro e falso) para as afirmações, ou seja, fornece indícios da existência de interpretações das afirmações, e isto significa que existem diferentes significados para as afirmações a depender de um fator que pode ser chamado de contexto, por exemplo, considere a seguinte afirmação:

“O atual presidente americano é um democrata”.

Note que o contexto temporal muda drasticamente o valor lógico interpretativo (semântico) dessa afirmação, pois em 2021 essa afirmação pode ser interpretada como verdadeira, porém no ano de 2019 a mesma era falsa. Assim, os valores interpretativos (semânticos) dentro do universo da lógica não são imutáveis, isto é, os valores das interpretações da lógica são passíveis de mudança a depender do contexto.

Dado então estes componentes sintáticos e semânticos pode-se concluir a partir das definições linguísticas que a **lógica é uma linguagem**, entretanto, vale salientar que não é uma linguagem natural como o português, como será visto nos próximos capítulos a lógica é uma linguagem formal [9], no sentido de que todas as construções linguísticas possuem uma forma precisa e sem ambiguidade determinada por uma gramática geradora [33, 35], pode-se inclusive estabelecer que a lógica é a linguagem da ciência da inferência racional, ou seja, a linguagem usada para representar argumentos, inferência e conclusões sobre um certo universo do discurso.

1.2 Um Pouco de História

A história do desenvolvimento da lógica remonta até a Grécia antiga e a nomes como: Aristóteles (384-322 a.C.), Sócrates (469-399 a.C.), Zenão de Eléia (490-420 a.C.), Parmênides (515-445 a.C.), Platão (428-347 a.C.), Eudemo de Rodes (350-290 a.C.), Teofrasto de Lesbos (378-287 a.C.), Euclides de Megara (435-365 a.C.) e Eubulides de Mileto³ (384-322 a.C.). De fato, o nome lógica vem do termo grego *logike*, cunhado por Alexandre de Afrodísias no fim do século II depois de Cristo. Como explicado em [1], os mais antigos registros sobre o estudo da lógica como uma disciplina (ciência) são encontrados exatamente na obra de Aristóteles intitulado como “*T da metafísica*”. Todavia, após seu desenvolvimento inicial dado pelos gregos antigos, a lógica permaneceu quase que intocada⁴ por mais de 1800 anos.

Os primeiros a profanar a santidade da lógica de forma contundente, abalando as estruturas da ideia de que a lógica era uma ciência completa, no sentido de que não havia nada novo a se fazer, estudar ou provar. Foram os matemáticos George Boole (1815-1864) e Augustus De Morgan (1806-1871), que introduziram a moderna ideia da lógica como uma ciência simbólica, isto é, eles semearam os conceitos iniciais que depois iriam convergir para as ideias da lógica enquanto linguagem formal apresentadas

² Autorreferência é um fenômeno que ocorre na língua natural e nas linguagens formais, tal fenômeno consiste em uma oração ou fórmula que se refere a si mesma de forma direta ou através de alguma sub-frase ou fórmula intermediária, ou ainda por meio de alguma codificação.

³ A quem é creditado o paradoxo do mentiroso.

⁴ Aqui não está sendo levada em conta as tentativas de Gottfried Wilhelm Leibniz (1646-1716) de desenvolver uma linguagem universal através da precisão matemática.

pelo matemático e filósofo alemão Gottlob Frege (1848-1925), que via a lógica como uma linguagem, que continha em seu interior todo o rigor da matemática.

Ainda no século XIX os maiores defensores das ideias de Frege, os britânicos Alfred Whitehead (1861-1947) e Bertrand Russell (1872-1970), usaram muitas de suas ideias e sua linguagem na publicação monumental em três volumes intitulada “*Principia Mathematica*” [4], que é ainda hoje considerada por muitos o maior tratado matemático do século XIX. Como dito em [8], outro influenciado por Frege que apresentou importantes contribuições foi filósofo austríaco Ludwig Wittgenstein (1889-1951), que em seu “*Tractatus Logico-Philosophicus*” apresentou pela primeira vez a lógica proposicional através das tabelas verdade. Muitos autores, como é o caso de [1], consideram que a lógica moderna se iniciou verdadeiramente com a publicação do *Principia*, de fato, alguns usam exatamente a visão de Whitehead que diz: “A lógica atual está para a lógica aristotélica como a matemática moderna está para a aritmética das tribos primitivas”.

Outra vertente emergente na lógica do século XIX era aquela apoiada puramente por interesses matemáticos, isto é, a visão da lógica não apenas como linguagem, mas também como um objeto algebrizável (um cálculo). Tal escola de lógica encontra alguns de seus expoentes nos nomes de: Ernst Zermelo⁵ (1871-1953), Thoralf Skolem (1887-1963), Ludwig Fraenkel-Conrad (1910-1999), John von Neumann (1903-1957), Arend Heyting (1898-1980) entre outros. Uma das grandes contribuições feitas por essa escola foi incluir uma formulação explícita e precisa das regras de inferência no desenvolvimento de sistemas axiomáticos.

Uma ramificação desta escola “matemática” ganhou força na Polônia sobre a tutela e liderança do lógico e filósofo Jan Łukasiewicz (1878-1956), o foco da escola polonesa era como dito em [8], analisar os sistemas axiomáticos da lógica proposicional, lógica modal e das álgebras booleanas. Foi esta escola que primeiro considerou interpretações alternativas da linguagem (da lógica) e questões da meta-lógica, tais como: consistência, correteza e completude. Por fim, foi na escola polonesa que houve pela primeira vez duas visões separadas sobre a lógica, uma em que a lógica era vista puramente como uma linguagem, e a segunda visão que via a lógica puramente como um cálculo [8].

Instigado pelo problema número dois da lista Hilbert (1862-1943), o jovem matemático e lógico austríaco Kurt Gödel (1906-1978) fez grandes contribuições para a lógica, inicialmente ele provou o teorema da completude para a lógica de primeira ordem em sua tese de doutorado em 1929, tal resultado estabelece que uma fórmula de primeira ordem é dedutível se e somente se ela é universalmente válida [8]. Outra contribuição monumental de Gödel são seus teoremas da incompletude [26], em especial o primeiro que deu uma resposta negativa ao problema número dois da lista Hilbert, de forma sucinta o resultado de Gödel estabelece que não pode haver uma sistematização completa da Aritmética, ou seja, sempre vão existir sentenças verdadeiras, porém indemonstráveis [1, 38].

Outros contemporâneos de Gödel também contribuíram fortemente para a lógica, Alfred Tarski (1901-1983) foi o responsável pela matematização do conceito de verdade como correspondência [1, 58], já o francês Jacques Herbrand (1908-1931) introduziu as funções recursivas e apresentou os resultados hoje chamados de teoria de Herbrand. Entre os resultados de Herbrand se encontra o teorema que relaciona um conjunto insatisfatível de fórmulas da lógica de primeira ordem com um conjunto insatisfatível de fórmulas proposicionais.

Outra enorme revolução matemática do século XX que foi escrita na linguagem da lógica foi a prova da independência entre a hipótese do *continuum*⁶ e o axioma da escolha da teoria de conjuntos de Zermelo-Fraenkel ou teoria dos conjuntos axiomática, como também é chamada.

De forma sucinta pode-se então concluir que a lógica uma ciência nascida na Grécia antiga se desenvolveu de forma exponencial após o século XIX, e que seu desenvolvimento foi em boa parte guiado por matemáticos, de fato, pode-se dizer que a lógica contemporânea se caracteriza pela tendência da matematização da lógica [7]. Muitos outros estudiosos, além dos que foram aqui mencionados, também apresentaram resultados diretos em lógica ou em área correlatas, como a teoria da prova e a teoria

⁵ Zermelo junto com Fraenkel desenvolveu o sistema formal hoje conhecido como teoria axiomática dos conjuntos.

⁶ A hipótese do *continuum* é uma conjectura proposta por Georg Cantor e que fazia parte da lista inicial de 10 problemas estabelecida por David Hilbert. Esta conjectura consiste no seguinte enunciado: **Não existe nenhum conjunto com cardinalidade maior que a do conjunto dos números inteiros e menor que a do conjunto dos números reais.**

da recursão, tornando a lógica e suas ramificações e aplicações um dos assuntos dominantes nos séculos XX e XXI.

1.3 Argumentos, Proposições e Predicados

Como qualquer outra disciplina para entender de fato o que é a lógica deve-se estudar a mesma [17], antes de qualquer coisa é bom saber que diferente de outras ciências, a lógica não apresentar fronteiras bem definidas, na verdade, como dito em [40], a lógica pode ser compreendida como a tênue linha que separa as ciências da filosofia e da matemática, no que diz respeito a isto, este manuscrito irá se debruçar primariamente sobre os aspectos matemáticos da lógica.

É sabido que para se estudar uma ciência deve-se saber quais são as entidades fundamentais de interesse dessa ciência, no caso da lógica, estas entidades fundamentais são os argumentos em um discurso.

Definição 1.1 (Argumento) Um argumento é par formado por dois componentes básicos, a saber:

- (1) Um conjunto de frases declarativas, em que cada frase é chamada de premissa.
- (2) Uma frase declarativa, chamada de conclusão.

Para representar um argumento pode-se como visto em [17, 40] usar uma organização de linhas, por exemplo, para representar um argumento que possua n premissas primeiro serão distribuídas nas n primeiras linhas as tais premissas do argumento ⁷ Como dito em [38] de onde a linha $n + 1$ é usado o símbolo \therefore para separar as premissas da conclusão ⁷, sendo esta última colocada na linha $n + 2$.

Exemplo 1.3.1 A construção:

Toda quarta-feira é servida sopa para as crianças.
Hoje é quinta-feira.
 \therefore
Ontem as crianças tomaram sopa.

É um argumento.

As frases declarativas usadas para construção de argumentos são aquelas que, como dito em [40], enunciam como as entidades em um certo discurso são ou poderiam ter sido, em outras palavras, as frases declarativas falam sobre as propriedades das entidades.

Exemplo 1.3.2 As frases:

- A lua é feita de queijo.
- O Flamengo é um time carioca.

São ambas frases declarativas. Por outro lado, as frases:

- Que horas são?
- Forneça uma resposta para o exercício.
- Faça exatamente o que eu mandei.
- Cuidado!

Não são frases declarativas.

Uma forma de identificar se uma frase é declarativa é verificada se a mesma admite ser classificada como verdadeira ou falso. Na lógica, as frases declarativas podem ser “tipadas” com dois rótulos: **proposições** e **predicados**.

Definição 1.2 (Proposição) Uma proposição é uma frase declarativa sobre as propriedades de indivíduos específicos em um discurso.

Exemplo 1.3.3 São exemplos de proposições:

- (a) $3 < 5$.
- (b) A lua é feita de queijo.
- (c) Albert Einstein era francês.
- (d) O Brasil é penta campeão de futebol masculino.


Definição 1.3 (Predicados) Predicados são frases declarativas sobre as propriedades de indivíduos não específicos em um discurso.

Pela Definição 1.3 pode-se entender que um predicado fala das propriedades de indivíduos sem explicitamente dar nomes a tais indivíduos.

Exemplo 1.3.4 São exemplos de predicados:

- (a) Para qualquer $x \in \mathbb{N}$ tem-se que $x < x + 1$.
- (b) Para todo $x \in \mathbb{R}$ sempre existem dois números $y_1, y_2 \in \mathbb{R}$ tal que $y_1 < x < y_2$.
- (c) Existe algum professor cujo nome da mãe é Maria de Fátima.
- (d) Há um estado brasileiro que não tem litoral.

Agora note que nas frases (a) e (b) do Exemplo 1.3.4 o símbolo x se torna um mecanismo que faz o papel dos números naturais e reais respectivamente, mas sem ser os próprios números em si, o mesmo vale para y_1 e y_2 . Similarmente, na frase (c) o termo **professor** representa todo um conjunto de pessoas, mas nunca sendo uma pessoa em particular, já na frase (d) o termo **estado brasileiro** representa novamente todos os indivíduos de um conjunto, mas ele nunca é um indivíduo particular. Os termos em um predicado que tem essa capacidade de representação são chamados de **variáveis do predicado**.

 **Atenção** Um predicado que tem suas variáveis substituídas (ou instanciadas) por valores específicos ou concretos se torna uma proposição.

Exemplo 1.3.5 Considere o predicado: “**Existe algum professor cujo nome da mãe é Maria de Fátima**”. Se for atribuído o valor **Valdigleis** no lugar da variável **professor** será gerado a proposição: **O nome da mãe de Valdigleis é Maria de Fátima**.

Exemplo 1.3.6 Considere o predicado: Para todo $x \in \mathbb{N}$, tem-se que $x > x + 1$. Ao atribuir o valor 2 a variável x teremos a proposição $2 > 2 + 1^a$.

^aObviamente se for feita a avaliação do termo $2 + 1$, poderia ser escrito a proposição como $2 > 3$.

1.4 Conectivos, Quantificadores e Negação

As proposições e os predicados podem ser classificados em duas categorias: simples ou composto. Uma proposição (ou predicado) é dita(o) composta(o) sempre que for possível dividi-la (o) proposição (predicado) em proposições (predicados) menores. E no caso contrário é dito que a proposição (ou predicado) é simples (ou atômicas).

Definição 1.4 (Conectivos) Conectivos são termos linguísticos que fazem a ligação entre as proposições ou (e) predicados.

⁸ Idioma aqui diz respeito a linguagem natural (português, por exemplo) que tem papel de meta-linguagem para falar sobre a lógica.

Os principais conectivos são: a conjunção, a disjunção e a implicação. E a depender do idioma⁸ mais de um termo da linguagem pode representar um determinado conectivos.

A seguir são listados os termos na língua portuguesa que são conectivos, ressaltamos que o símbolo _____ será usado como meta-variável para representar a posição de proposições (ou predicados).

Conectivo	Termo em Português
Conjunção	_____ e _____
	_____ mas _____
	_____ também _____
	_____ além disso _____
Disjunção	_____ ou _____
Implicação	Se _____, então _____
	_____ implica _____
	_____ logo, _____
	_____ só se _____
	_____ somente se _____
	_____ segue de _____
	_____ é uma condição suficiente para _____
Basta	_____ para _____
	_____ é uma condição necessária para _____

Tabela 1.1: Termos em português que representamos conectivos.

Exemplo 1.4.1

Usando as proposições do Exemplo 1.3.3 e os predicados do Exemplo 1.3.4 pode-se criar:

- (a) $3 < 5$ e para qualquer $x \in \mathbb{N}$ tem-se que $x < x + 1$.
- (b) Há um estado brasileiro que não tem litoral ou O Brasil é penta campeão de futebol masculino.
- (c) Se para todo $x \in \mathbb{R}$ sempre existem dois números $y_1, y_2 \in \mathbb{R}$ tal que $y_1 < x < y_2$, então Albert Einstein era francês.
- (e) Se a lua é feita de queijo ou $3 < 5$, então há um estado brasileiro que não tem litoral.

Neste exemplo, os conectivos estão destacados na cor teal.

Como já mencionado antes um predicado não especifica diretamente os indivíduos, em vez disso, usa variáveis para não mencionar os indivíduos especificamente. Essas variáveis por sua vez, estão conectadas a termos da linguagem que determinam a quantidade de elementos que podem vir a ser atribuído a tais variáveis, tais termos são chamados de quantificadores. Os quantificadores por sua vez, podem ser “tipados” em duas categorias: universais e existenciais.

Quando uma variável é ligada a um quantificador universal significa que o predicado será verdadeiro se para a atribuição de cada um dos elementos do universo discurso a proposição gerada com a atribuição é também verdadeira, no caso contrário o predicado é falso. Por outro lado, quando uma variável é ligada a um quantificador existencial significa que tal predicado será verdadeiro se para pelo menos um dos elementos do discurso ao ser atribuído a variável gera uma proposição verdadeira, e no caso contrário o predicado será falso.

De forma similar aos conectivos os quantificadores também são “representados” por termos da língua portuguesa como mostrado na tabela 1.2. Anteriormente já foi dito que na lógica as proposições e predicados podem ser interpretados como sendo verdadeiros ou falsos, dito isto, para qualquer proposição ou predicado sempre é possível obter uma proposição ou predicado com um valor de interpretação oposta, isto

é, se a proposição (ou predicado) original for verdadeira a proposição (ou predicado) oposta será falsa, ou vice-versa. Esse operador que gerar as proposições (ou predicados) opostas(os) é chamado de negação e a Tabela 1.3 exibe como os termos na língua portuguesa podem ser usados para representar a negação.

Quantificador	Termo em Português
Universal	Para todo(a) _____
	Para qualquer _____
	Para cada _____
Existencial	Existe _____
	Existe algum _____
	Há um _____
	Para algum _____
	Para um _____

Tabela 1.2: Termos em português que representamos quantificadores.

Termos em português
Não _____
É falso que _____
Não é verdade que _____

Tabela 1.3: Termos em português para designar a negação de uma proposição ou predicado.

1.5 Representação Simbólica

A lógica simbólica é o estudo das propriedades lógica sem se preocupar com o que cada proposição e(ou) predicado de fato enuncia, em tal perspectiva as abstrações simbólicas capturam as características formais (sintaxe e semântica) das proposições e predicados, além de, representar de forma sucinta e precisa as abordagens para a inferência lógica aplicada a qualquer argumento [4, 28].

Definição 1.5 Na lógica simbólica, as letras maiúsculas do alfabeto latino com ou sem indexação representam proposições simples.

Além dos símbolos usados para representar as proposições, é necessário, como destacado em [30] apresentar representações simbólicas para os conectivos e a negação, as representações usadas neste documento estão listadas a seguir.

Objeto	Notação
Negação	\neg
Conjunção	\wedge
Disjunção	\vee
Implicação	\Rightarrow

Tabela 1.4: Notação simbólica para os conectivos e a negação.

Exemplo 1.5.1 Dado duas proposições:

(1) “Hoje é quarta-feira”

(2) “Julia foi ao parque”

pode-se representar ambas respectivamente por Q e J , assim a conjunção de (1) e (2), é simbolicamente representada por $Q \wedge J$. Além disso, a implicação de que

Julia não foi ao parque com o fato de hoje não ser quarta-feira, é representada por $\neg J \Rightarrow \neg Q$.

Exemplo 1.5.2 A proposição “**A formatura é amanhã ou no sábado**”, pode ser simbolicamente representada por $A \vee S$.

Já para os quantificadores existencial e universal, os mesmos são representados como exposto na tabela a seguir, ressaltando que no caso x é uma variável da linguagem de primeira ordem e o $[\text{_____}]$ imediatamente inserido após a simbolização do quantificador diz respeito ao escopo do mesmo (isso será melhor discutido no capítulo próprio do assunto), dentro do escopo está representado o predicado, a representação do predicado pode conter símbolos de conectivos, além de, símbolos para constantes, funções, relações e variáveis.

Objeto	Notação
Quantificador existencial	$(\exists x)[\text{_____}]$
Quantificador universal	$(\forall x)[\text{_____}]$

Tabela 1.5: Notação simbólica para os quantificadores.

Exemplo 1.5.3 O predicado: “**Existe um gato que mora na casa de Hugo,**”, pode ser representado por $(\exists x)[g(x) \wedge h(x)]$, x denota a variável do discurso, $g(x)$ é a relação que denota que x é um gato, $h(x)$ denota a relação de morar na casa de Hugo.

Exemplo 1.5.4 O clássico predicado^a: “**Todos os homens são mortais,**”, pode ser representado por $(\forall x)[h(x) \Rightarrow m(x)]$. Aqui x é novamente a variável usada para simbolizar de forma genérica os elementos no discurso, $h(x)$ simboliza o fato de x ser homem e $m(x)$ ser mortal.

^aAlguns textos, como [15], costumam creditar a Aristóteles a criação de tal predicado.

1.6 Lógica e Ciência da Computação

Para finalizar este capítulo introdutório, é conveniente falar mesmo que de forma superficial sobre os tipos de lógica. A lógica, assim como a física, pode ser dividida em duas categorias ou tipos bem definidos, a saber, clássicas e as não clássicas. Como mencionado em [8, 21], as lógicas clássicas são aquelas que apresentam a característica de obedecer aos seguintes princípios:

- **Princípio da não contradição:** Qualquer proposição (ou predicado) não pode ser verdadeira(o) e falsa(o) ao mesmo tempo;
- **Princípio do terceiro excluído:** Toda(o) proposição (ou predicado) só pode ser falsa(o) ou verdadeira(o), não existe uma terceira possibilidade.

Logo a lógica clássica é bi-valorada [21], ou seja, as interpretações sobre as proposições e predicados só podem ser valoradas por dois valores, a saber: verdadeiro ou falso. E por sua vez, a própria lógica clássica é subdividida em duas partes, sendo estas: a lógica proposicional e a lógica de primeira ordem (ou lógica dos predicados).

Como respeito a aplicações, a lógica clássica tem um papel fundamental e central para a Ciência da Computação, uma vez que, todos os computadores são construídos pela combinação de circuitos digitais e estes por sua vez implementam operações da lógica proposicional [1, 23]. Outra área de destaque da aplicação da lógica dentro da Ciência da Computação é no campo de Inteligência Artificial, onde a mesma é o principal formalismo de representação do conhecimento e, portanto, é muito útil no desenvolvimento de sistemas especialistas e sistemas multi-agentes [8], algumas outras áreas de aplicação da lógica clássica são:

- Banco de dados: através da descrição de consultas e no relacionamento das tabelas em bancos de dados dedutivos.

- Ontologias web: como uma linguagem para descrever ontologias e representar o conhecimento.
- Engenharia de software: usada como formalismo para especificação e verificação formal das propriedades dos sistemas⁹.

As lógicas não clássicas, por sua vez, podem se apresentar de duas formas. (1) não obedecem a algum dos princípios apresentados acima ou (2) estendem a lógica clássica através de teoremas e meta-teoremas (formalizados nos capítulos futuros) não válidos para as lógicas clássicas. Como exemplos de lógicas não clássicas estão: lógica intuicionista [37], lógica paraconsistente [20], lógicas multivaloradas [8, 38], lógicas modais [38] e lógicas temporais [27, 29, 39]. Com respeito a aplicações relacionadas à Ciência da Computação tem-se, por exemplo:

- A utilização da lógica modal para a verificação das propriedades de sistemas e software [29].
- A lógica temporal usada para especificação e verificação de programas concorrentes [39] e também para especificar circuitos síncronos [27].
- As lógicas multi-valoradas usadas para lidar com a simulação e representação de incertezas presente no raciocínio aproximado [8], principalmente na área de reconhecimento de padrões.

Obviamente, como dito em [8], existem muitas outras lógicas não clássicas que têm aplicações ou ainda servem de fundamentação para diversas áreas, ou disciplinas da computação. Porém, como esta parte do texto é apenas uma introdução, não cabe neste escopo se debruçar tão profundamente assim neste assunto. Em capítulos futuros, as lógicas não clássicas (em especial a modal) serão estudadas mais a fundo em capítulos futuros deste documento.

⁹ Em especial sistemas críticos como software para controle aéreo são exemplo de sistemas cujas propriedades deve ser especificadas e verificadas com alta precisão matemática dado a importância do mesmo para a manutenção da vida humanas que dependem dele.

1.7 Questionário

Questão 1.1

Examine cada uma das frases declarativas abaixo e diga se as mesmas são proposições ou predicados e também diga se são simples ou compostas, justifique suas respostas no caso de proposição (ou predicado) composta(o).

- Existe um gato amarelo.
- Alguns patos são marrons.
- Não é verdade que o gato de Júlio é amarelo.
- O Flamengo joga hoje.
- Todos os ratos têm olhos azuis.
- 4 é o menor número composto pelo produto de primos.
- Meu cachorro é branco, alguns outros são vermelhos.
- Alguns gatos são cinzas, mas meu gato não é cinza. Além disso, Tadeu tem um gato preto ou Sormany tem um rato amarelo.
- Os carros são amarelos se e somente se eles não são italianos.
- Se todos os jogadores da seleção jogam na Europa ou Neymar está machucado, então o Brasil não vence a Argentina.
- Basta mais um ponto na carteira de motorista para Sormany perder a aposta ou Juca terá que pagar o almoço.

- (l). Se Lucas é irmão de Pedro, então Natalia vai casar com Gabriel e Francisco não voltará para a Espanha.
- (m). Se $\frac{10^2}{50} = 2!$, então $\pi - 2x = 0$ para todo $x \in \mathbb{C}$.
- (n). Se a terra é plana e existe chip nas vacinas, então o Brasil vai conquistar o país de Juvenal.
- (o). A bola é preta.
- (p). Eu tirei foto com meu avô hoje.
- (q). $3 < 5$ segue do fato de que o voto no papel é mais rápido que o voto eletrônico.
- (r). O sorvete ser de uva segue do fato de Juliane estar grávida.
- (s). Bill escreveu o DOS em 1978 é condição necessária para *Apple Inc.* ter lançado o *Apple 2*.
- (t). Se o Cruzeiro é um time da primeira divisão, então todo pato come macarrão ou não é o caso de Patricia ser professora de matemática.

Questão 1.2

Determine as frases simples (ou atômicas) que compõem as proposições e predicados que se seguem.

- (a). Juca não irá à festa, mas Pedro irá ou Flaviana irá.
- (b). Fui com a minha família ontem ao parque e me diverti muito.
- (c). Juca vai com a família ou irá sozinho, mas se Anabel aparecer no parque, então Juca e Paula não vão se divertir.
- (d). Se Paulo chegou, então ele está na sala. Mas não é verdade que Paulo chegou.
- (e). Valdi toca clarinete somente se Katia tocar flauta ou Shizue sabe desenhar com carvão.
- (f). Eu sou aluno da computação somente se eu passei em Matemática discreta. Mas eu não passei em Introdução à programação ou reprovei todas as disciplinas do primeiro período.
- (g). Para qualquer navio no porto, existe um marinheiro bêbado no bar ou todos os soldados estão dormindo na praia.
- (h). Se Romero tivesse vindo ver o filme, então Katia teria ido para a sorveteria com ele. Mas Romero foi para a praia com Julinha.
- (i). Todos os números primos são números ímpares ou o número π é o pode ser escrito como produto de números primos.
- (j). Vou à padaria e, se estiver fazendo frio, então Juliane vai tomar sopa.
- (k). Não é verdade que a terra é esférica e não existem pessoas morando em Recife.
- (l). Shizue e Valdi foram para o Chile, mas Luiza também foi.
- (m). Basta que eu tire 8 em Matemática discreta para eu ter uma noite de festa.
- (n). A gripe é uma condição suficiente para ser declarado morto.
- (o). Se para toda flor existe um vaso, então os jardins de Jaçanã são cheios de cerejeiras.
- (p). Se ontem choveu a noite toda e hoje é meu aniversário de 14 anos, então se Pedro vai à Califórnia, então Tom e Frajola são amigos do Manda-chuva.

- (q). Não é verdade que Shizue sabe desenhar com carvão, mas sabe desenhar com lápis e pincel.
- (r). Se o Catatau comeu o mel e o Puffy saiu para passear, então o Jack ou Jerry é vizinho do Mickey.
- (s). Para todo homem existe uma mulher que é sua mãe ou Valdi toca clarinete.
- (t). Existe um carro amarelo e, se todas as bicicletas são roxas, então não é verdade que existem motos que são azuis.

Lógica Proposicional

“Ou a matemática é muito grande para a mente humana, ou a mente humana é mais do que uma máquina.”

Kurt Gödel

2.1 A Linguagem Proposicional

Este capítulo tem como objetivo apresentar ao leitor o cálculo proposicional, ou seja, o estudo da lógica proposicional, em seus dois aspectos já bem estabelecido por matemáticos e filósofos, isto é, sua sintaxe e sua semântica¹. Assim esse capítulo começa com a formalização da linguagem da lógica proposicional, isto é, a linguagem proposicional. A seguir é apresentado formalmente a noção de alfabeto proposicional.

¹ O aspecto pragmático da lógica, por ainda se encontrar em um estágio primitivo de seu desenvolvimento, do ponto de vista matemático, não será abordado neste texto, para este assunto ver [52, 54].

Definição 2.1

(Alfabeto Proposicional) O alfabeto proposicional corresponde ao conjunto enumerável $\Sigma = \Sigma_s \cup \Sigma_o \cup \Sigma_p \cup \{\perp\}$ onde:

- $\Sigma_s = \{A, \dots, P, Q, R, P_1, Q_{12}, \dots\}$ é um conjunto enumerável, chamado conjunto dos átomos;
- $\Sigma_o = \{\wedge, \vee, \neg, \Rightarrow\}$ é o conjunto dos símbolos operacionais^a;
- $\Sigma_p = \{(\, , \,)\}$ é o conjunto dos símbolos de pontuação e
- \perp é o símbolo do absurdo.

^aTambém é comum encontrar na literatura (ver [40]) a nomenclatura conjunto de conectivos.

Em algumas outras obras tais como [15] também é mencionado o símbolo \Rightarrow para designar a tautologia, entretanto, como explicado no próprio texto de [15], tal símbolo é apenas um açúcar sintático para a expressão $(\neg \perp)$.

Definição 2.2

(Linguagem Proposicional) Dado o alfabeto proposicional Σ , a linguagem proposicional, denotada por \mathcal{L} , é menor conjunto de fórmulas bem formadas (fbf) indutivamente gerado, tal que cada fbf $\phi \in \mathcal{L}$ é construído pela gramática:

$$\phi ::= x \mid (\neg \phi) \mid (\phi \wedge \phi) \mid (\phi \vee \phi) \mid (\phi \Rightarrow \phi)$$

onde $x \in \Sigma_s \cup \{\perp\}$.

Exemplo 2.1.1

Dado $P, Q, R, S, T \in \Sigma_s \cup \{\perp\}$ tem-se que:

(a) P

- (b) $(P \wedge Q)$
 (c) $(R \Rightarrow S)$
 (d) $((Q \vee S) \Rightarrow T)$

são todas palavras da linguagem \mathcal{L} . Por outro lado, as palavras:

- (e) $P \wedge$
 (f) $\Rightarrow Q$
 (g) $P \vee \wedge Q$

não são palavras da linguagem \mathcal{L} , pois nenhuma é uma fbf.

Na prática, o número das parênteses incomoda bastante, assim sempre que possível é interessante remover o excesso deles. E para remover os parênteses mais externos de qualquer fórmula, para isso se considera como dito em [59], a precedência dos símbolos dos conectivos da linguagem proposicional, sendo tal precedência expressa a seguir.

Ordem	Conectivo
1	\neg
2	\wedge
3	\vee
4	\Rightarrow

Tabela 2.1: Tabela de precedência dos conectivos proposicionais.

Ou seja, a Tabela 2.1 descreve que o símbolo \neg tem precedência maior do que \wedge , sendo que \wedge tem precedência maior do que \vee e, por fim, \vee tem precedência maior do que \Rightarrow .

Exemplo 2.1.2

Usando a precedência dos conectivos da linguagem proposicional tem-se a seguinte tabela de simplificações de fbfs:

Fbf	Fbf simplificada
$(\neg(\neg(\neg(\neg P))))$	$\neg\neg\neg\neg P$
$((P \vee Q) \Rightarrow (R \wedge (\neg S)))$	$P \vee Q \Rightarrow R \wedge \neg S$
$((P \wedge Q) \vee R)$	$P \wedge Q \vee R$

É possível enriquecer² a linguagem proposicional adicionando mais símbolos operacionais no alfabeto da mesma, essa introdução é feita utilizando o conceito de abreviação. Uma abreviação na lógica formal consiste na ação de usar um novo símbolo para criar uma nova palavra não presente originalmente na linguagem proposicional, mas que representa uma palavra da linguagem.

Um exemplo do que foi descrito no paragrafo anterior é o símbolo \Rightarrow , que na verdade é uma abreviação para a palavra $(\neg \perp)$, outro exemplo de abreviação, como dito em [40], é o uso do símbolo \Leftrightarrow , usando tal símbolo como um Conectivo lógico, tem-se que $\alpha \Leftrightarrow \beta$ é a abreviação da palavra $((\alpha \Rightarrow \beta) \wedge (\beta \Rightarrow \alpha))$ com $\alpha, \beta \in \mathcal{L}$, vale salientar que o símbolo \Leftrightarrow também pode ser usado para representa uma relação de equivalência semântica [8, 21, 23].

De fato, muitos dos símbolos operacionais que foram tomados como símbolos básicos do alfabeto proposicional (Definição 2.1) poderiam ser removidos, pois como muito bem explicado em [8, 40] a lógica proposicional pode ser definida sobre a linguagem que contém apenas os símbolos operacionais de \Rightarrow e \neg , os demais símbolos podem ser obtidos via abreviação sem qualquer perda no estudo da lógica proposicional, para mais detalhes ver [8].

² No sentido de adicionar mais símbolos ao alfabeto.

2.2 Sistema Dedutivo

A ideia de sistemas dedutivos para a lógica formal remonta aos trabalhos publicados³ no ano de 1934 pelo matemático e filósofo alemão Gerhard Gentzen (1909-1945) e pelo lógico polonês Stanisław Jakowski (1906-1965). Existem diversos sistemas dedutivos para a lógica proposicional, cada um possuindo suas próprias características, vantagens e desvantagens, no entanto, todos os sistemas dedutivos compartilham a característica em comum de possuírem um conjunto finito de regras de inferência, esse conjunto de regras de inferência é também chamado de sistema regras ou sistema de dedução [21].

³ Esses trabalhos podem ser encontrados re-editados respectivamente em [57] e [34].

O sistema dedutivo introduzido por Gentzen e Jakowski é conhecido por dedução natural, aqui ele será apresentado de forma similar a exposição feita em [40]. O conjunto de regras de inferência da dedução natural é composto pelas regras: de introdução e eliminação de conectivos, regra de reiteração, introdução de hipóteses e a regra do absurdo. Entretanto, antes de apresentar as regras do sistema de dedução natural e conveniente apresentar o conceito de demonstração, para isso deve-se escolher uma notação para as provas da dedução natural.

Existem diversas formas de se escrever (ou representar) uma demonstração no sistema de dedução natural, entre elas destacam-se as árvores de prova de Gentzen [8], o estilo linear [17, 45] e o estilo de Fitch [24, 40].

Neste texto será adotado o estilo de Fitch como modelo padrão para a escrita das demonstrações do sistema de dedução natural para a lógica proposicional, assim é conveniente apresentar de forma sucinta o estilo de Fitch. O estilo de Fitch foi introduzido pelo lógico americano Frederic Brenton Fitch (1908-1987) e corresponde a diagramas hierárquicos formados por linhas e barras (verticais e horizontais) que representam o raciocínio para a partir de um conjunto de premissas se obter uma determinada conclusão ou objetivo (em inglês *goal*).

O diagrama de Fitch é organizado por linhas numeradas, onde cada linha i pode conter uma única palavra de \mathcal{L} , sendo essa palavra uma premissa ou sendo ela obtida pela aplicação de alguma regra de inferência sobre uma ou mais linhas anteriores a linha i .

As barras verticais nos diagramas de Fitch são usadas de duas formas:

- (1) Para separar a demonstração em escopos, sendo que um escopo consiste de uma sequência de várias linhas (ou passos) para demonstrar uma conclusão.
- (2) Como um mecanismo para saber quais palavras de \mathcal{L} estão ativas⁴ na prova, como explicado em [40].

⁴ Uma palavra de \mathcal{L} está ativa em uma demonstração, enquanto o escopo da mesma está aberto na demonstração.

As barras horizontais no diagrama de Fitch indicam a divisão entre as afirmações que estamos assumindo (nossas premissas e (ou) hipóteses) e as palavras que se seguem delas, sejam conclusões intermediárias ou nosso objetivo final. No caso das hipóteses a barra horizontal também cria um novo “escopo”, isto é, adiciona uma indentação em relação ao escopo anterior, vale salientar que cada escopo é na verdade uma prova para um (sub-)objetivo.

Por fim, é comum na notação dos diagramas de Fitch escrever mais à direita de cada linha a regra de inferência que gerou a palavra na linha, ou o fato da palavra ser uma premissa ou hipótese. Agora pode-se apresentar formalmente o conceito de prova que será adotado neste capítulo.

Definição 2.3

(Prova) Uma prova para $\alpha \in \mathcal{L}$ consiste de um diagrama de Fitch como uma quantidade finita de linhas, de forma que a última linha contém a palavra α e cada linha i anterior contém uma palavra $\beta_i \in \mathcal{L}$ tal que β_i ou é uma premissa ou é obtida via aplicação de alguma regra de inferência.

Agora pode-se definir precisamente o conceito de relação de consequência sintática sobre a linguagem \mathcal{L} .

Definição 2.4 (Consequência Sintática) Seja \mathcal{L} a linguagem proposicional, dado $\alpha \in \mathcal{L}$ e $\Gamma \subseteq \mathcal{L}$, diz-se que α é consequência sintática de Γ , denotado por $\Gamma \vdash \alpha$, sempre que existir uma prova de α a partir do conjunto de premissas Γ .

A seguir são apresentadas as regras de inferência do sistema de dedução natural, aqui será iniciada pelas regras que não envolvem diretamente os símbolos operacionais, isto é, que não age diretamente para eliminar ou introduzir os elementos de Σ_o na demonstração.

Definição 2.5 (Regra das premissas) Se $\Gamma = \{\alpha_1, \dots, \alpha_n\}$ é um conjunto finitos de premissas, então a regra das premissas fixa que a construção do diagrama de Fitch para uma prova de $\Gamma \vdash \alpha$ dispões nas n primeiras linhas do diagrama as n premissas contidas Γ , onde na linha i se encontra a premissa α_i , além disso, existe uma barra vertical contínua^a a esquerda das premissas e após a linha n há uma barra horizontal separando as premissas do resto da prova, ou seja:

1		α_1	Premissa
\vdots		\vdots	
n		α_n	Premissa
\vdots		\vdots	

^aCada linha vertical contínua é um escopo dentro da demonstração.

Exemplo 2.2.1 A prova de $\{P, Q\} \vdash P \wedge Q$ pode ser iniciada usando a regra das premissas de forma que é obtido o seguinte diagrama inicial:

1		P	Premissa
2		Q	Premissa



Atenção

Obviamente, uma vez que, Γ é um conjunto seu elementos não possuem uma ordem explícita, assim não existe diferença entre o diagrama do Exemplo 2.2.1 com um diagrama em que Q esteja na linha 1, e P na linha 2.

Seguindo com as regras mais básicas do sistema de dedução natural tem-se a regra de reiteração, repetição, copia ou clonagem, aqui esta regra será denotada apenas por REI.

Definição 2.6 (Regra da reiteração) Em uma demonstração sempre é possível repetir uma palavra $\beta \in \mathcal{L}$ que já foi obtida em uma linha i durante a prova, desde que o escopo que contém β ainda esteja ativo^a. Na notação de Fitch tem-se:

\vdots		\vdots	
i		β	
\vdots		\vdots	
n		β	REI, i
\vdots		\vdots	

^aA noção de escopo ativo diz respeito se uma (sub-)prova foi concluída ou ainda está em desenvolvimento, este conceito será melhor trabalhado mais adiante.

Exemplo 2.2.2

Em uma prova de $\{P, Q\} \vdash P \wedge (P \wedge Q)$ após aplicar a regra das premissas pode-se aplicar a regra de reiteração na linha 1 e com isso é obtido uma segunda “instância” da proposição P :

1	P	Premissa
2	Q	Premissa
3	P	REI, 1

Agora que já foram apresentadas as regras que não agem diretamente sobre os símbolos operacionais (de conectivos) pode-se dá sequência no texto apresentando as regras de inferência do sistema de dedução natural que atuam diretamente sobre os símbolos.

Atenção A partir deste ponto serão apresentadas as regras de introdução e eliminação dos operadores (conectivos), assim sempre que o símbolo vier seguindo de I significa que a regra é de introdução, e quando vier seguido de E a regra será de eliminação.

Definição 2.7

(Regra $\wedge I$) Se em uma prova foram deduzidas as palavras $\alpha, \beta \in \mathcal{L}$ nas linhas i e j respectivamente, então pode-se deduzir a palavra $\alpha \wedge \beta$ em uma linha k com $i < j < k$, na notação do diagrama de Fitch tem-se:

\vdots	\vdots	
i	α	
\vdots	\vdots	
j	β	
\vdots	\vdots	
k	$\alpha \wedge \beta$	$\wedge I, i, j$
\vdots	\vdots	

A regra de introdução da conjunção impõe que a palavra que está na linha i seja fixada à esquerda do símbolo \wedge e a palavra na linha j seja fixada à direita do símbolo \wedge . Entretanto, isso pode ser facilmente contornado, imagine que na linha i aparece a palavra β e apenas na linha j (com $i < j$) se encontra o α , mas se deseja obter a palavra $\alpha \wedge \beta$, bem pela Definição 2.7 não seria possível, entretanto, sempre se pode usar a regra descrita na Definição 2.6 para copiar β para uma linha $j + k$, e então obter após isso a palavra $\alpha \wedge \beta$.

Exemplo 2.2.3

Para concluir a prova de $\{P, Q\} \vdash P \wedge Q$ iniciada no Exemplo 2.2.1 basta aplicar a regra de introdução da conjunção nas linhas 1 e 2, como pode ser visto a seguir.

1	P	Premissa
2	Q	Premissa
3	$P \wedge Q$	$\wedge I, 1, 2$

Exemplo 2.2.4 | A prova de $\{P, Q, S\} \vdash S \wedge (P \wedge Q)$ é dada por:

1	P	Premissa
2	Q	Premissa
3	S	Premissa
4	$P \wedge Q$	$\wedge I, 1, 2$
5	$S \wedge (P \wedge Q)$	$\wedge I, 3, 4$

A próxima regra é a eliminação da conjunção, tal regra possui duas formas o que contrasta com a regra da introdução da conjunção que possui apenas uma única forma, note que o operador \wedge combina duas palavras $\alpha, \beta \in \mathcal{L}$, assim quando tal operador for removido deve-se optar por qual das duas palavras será mantida como uma conclusão (intermediária ou final) da prova. A seguir é definida formalmente a regra de eliminação de conjunção.

Definição 2.8 (Regra $\wedge E$) Se em uma prova for deduzida a palavra $\alpha \wedge \beta$ na linha i , então pode-se deduzir a palavra α ou então a palavra β em uma linha j com $i < j$, na notação do diagrama de Fitch tem-se:

\vdots	\vdots		\vdots	\vdots	
i	$\alpha \wedge \beta$		i	$\alpha \wedge \beta$	
\vdots	\vdots		\vdots	\vdots	
		ou			
j	α	$\wedge E, i$	j	β	$\wedge E, i$
\vdots	\vdots		\vdots	\vdots	

Agora será aberto um parêntese na apresentação das regras de inferência dos símbolos operacionais para que possa ser discutido neste texto a noção de prova hipotética. As provas hipotéticas são muito importantes dentro do sistema de dedução natural, tais provas com dito em [40], podem ser pensadas como sendo um ambiente (ou escopo) de subprova em que além das premissas que iniciaram a prova são assumidas outras informações na forma de hipóteses.

Como argumentado em [17, 40], uma prova hipotética surge quando a regra de introdução hipótese é aplicada, e ao se introduzir essa nova hipótese na prova é gerado um novo escopo dentro da prova que se estava demonstrando, isto é, é criada uma subprova que terá seu próprio objetivo.

Definição 2.9 (Regra de introdução de hipótese) Dado uma demonstração com n passos, se for necessário assumir uma hipótese $\beta \in \mathcal{L}$ no passo $n + 1$, então é inserida a hipótese β junto com uma barra vertical de escopo, e abaixo de β é inserida a barra horizontal de separação para destacar a hipótese, aqui será usado a palavra **Assuma** para referenciar a regra de introdução de hipótese^a.

\vdots	\vdots	
n	\vdots	
$n + 1$	β	Assuma
\vdots	\vdots	

^aNa literatura em língua inglesa é comum o uso do termo *Assumption*.

Como dito em [21], uso da regra de inferência de introdução de hipótese está intimamente ligada ao uso da regra de introdução da implicação definida a seguir, por isso a necessidade de apresentá-la antes da regra de introdução da implicação.

Definição 2.10

(Regra $\Rightarrow I$) Se partindo de uma suposição hipotética α na linha m for possível deduzir um certo β na linha n com $m < n$, então no escopo externo da prova hipotética é concluído na linha $n + 1$ que $\alpha \Rightarrow \beta$, na notação dos diagrama de Fitch tem-se:

\vdots	\vdots	
m	α	Assuma
\vdots	\vdots	
n	β	
$n + 1$	$\alpha \Rightarrow \beta$	$\Rightarrow I, m-n$
\vdots	\vdots	

Note que a regra de introdução da implicação pode ser vista como um mecanismo que desativa um escopo de prova, isto é, quando a mesma é aplicada um escopo de prova terá sido completado e assim estará desativado.

Exemplo 2.2.5

Para provar que a $P \Rightarrow P$ é consequência sintática de um conjunto vazio de premissas utiliza-se a combinação das regras de introdução de hipótese, reiteração e da introdução da implicação como pode ser visto pelo diagrama a seguir.

1	P	Assuma
2	P	REI, 1
3	$P \Rightarrow P$	$\Rightarrow I, 1-2$



Atenção

Ao desativar um escopo de prova todas as palavras contidas entre as linhas i e j , que forma a prova, não podem mais ser utilizadas na sequência da demonstração, isso ocorre pela razão de tais palavras só existirem no escopo “local” da subprova que foi concluída, ou seja, as palavras internas a uma subprova são similares a variáveis internas a um sub-programa, isto é, só existem dentro do escopo em que foram criadas ou derivadas.

Aproveitando o Exemplo 2.2.5, antes de seguir o texto com a próxima regra de inferência é interessante introduzir ao leitor a ideia de teorema, este conceito é extremamente importante no estudo de qualquer lógica e o mesmo é descrito formalmente a seguir.

Definição 2.11

(Teorema) Seja \mathcal{L} uma linguagem formal^a e seja \vdash uma relação de consequência sintática sobre \mathcal{L} , uma palavra $\alpha \in \mathcal{L}$ é dita ser um teorema sempre que $\emptyset \vdash \alpha$ ^b.

^aA palavra formal aqui diz respeito a ideia de sabe-se precisamente a forma de todas as palavras contidas na linguagem.

^bÉ também comum encontrar na literatura a notação $\vdash \alpha$ em vez de $\emptyset \vdash \alpha$.



Atenção

Dizer que α é um teorema, significa que α é uma consequência direta do próprio sistema sintático da linguagem, isto é, que α é consequência das próprias regras de inferência, sem que haja a necessidade da existência de premissas.

Usando apenas as regras de inferência apresentadas até este ponto do texto no próximo exemplo será mostrado um clássico teorema da linguagem proposicional.

Exemplo 2.2.6 Para qualquer $\alpha, \beta \in \mathcal{L}$ tem-se o seguinte diagrama de Fitch:

1	$\alpha \wedge \beta$	Assuma
2	β	$\wedge E, 1$
3	α	$\wedge E, 1$
4	$\beta \wedge \alpha$	$\wedge I, 2, 3$
5	$(\alpha \wedge \beta) \Rightarrow (\beta \wedge \alpha)$	$\Rightarrow I, 1-4$

Portanto, para qualquer $\alpha, \beta \in \mathcal{L}$ tem-se que $\vdash \alpha \wedge \beta \Rightarrow \beta \wedge \alpha$, ou seja, a palavra $(\alpha \wedge \beta) \Rightarrow (\beta \wedge \alpha)$ é um teorema da linguagem \mathcal{L} .

Prosseguindo com a apresentação das regras de inferência do sistema de dedução natural a seguir será definida formalmente a regra de eliminação da implicação, também conhecida como *modus ponens*, que surge da expressão em latim, *modus ponendo ponens*, que em português pode ser traduzido como: **o modo de afirmar, afirmando**.

Definição 2.12 (Regra $\Rightarrow E$) Se em uma prova na linha i existe uma palavra α e em uma linha j existe uma palavra $\alpha \Rightarrow \beta$ com $i < j$, então na linha k tal que $j < k$ é possível deduzir a palavra β , em diagrama tem-se:

i	α	
\vdots	\vdots	
j	$\alpha \Rightarrow \beta$	
\vdots	\vdots	
k	β	$\Rightarrow E, i, j$
\vdots	\vdots	

Exemplo 2.2.7 A prova de $\{P \Rightarrow Q, P \wedge R\} \vdash Q$ é dado pelo seguinte diagrama:

1	$P \Rightarrow Q$	Premissa
2	$P \wedge R$	Premissa
3	P	$\wedge E, 2$
4	$P \Rightarrow Q$	REI, 1
5	Q	$\Rightarrow E, 3, 4$



Atenção

O leitor deve ficar atento ao fato de que a Definição 2.12 especifica que o termo hipotético α deve aparecer na prova antes do termo condicional $\alpha \Rightarrow \beta$, para que se possa aplicar a regra $\Rightarrow E$.

A próxima regra de inferência do sistema de dedução natural que será apresentada neste texto é chamada de regra de introdução do absurdo, a mesma é utilizada para introduzir na demonstração o símbolo do absurdo (\perp), de fato, é comum na literatura em língua inglesa principalmente na área de lógica algébrica achar o símbolo do absurdo sendo chamado *bottom*.



Atenção

O \perp não é um operador de fato, entretanto, é uma palavra tão importante que no estudo da lógica tem uma regra de introdução própria.

Definição 2.13

(Regra de introdução do absurdo ($\perp I$)) Se na linha i de uma prova existe uma palavra β e no mesmo escopo de prova na linha j existe uma palavra $\neg\beta$ com $i < j$, então na linha k desta prova é deduzido \perp com $j < k$, em diagrama tem-se:

\vdots	\vdots	
i	β	
\vdots	\vdots	
j	$\neg\beta$	
\vdots	\vdots	
k	\perp	$\perp I, i, j$
\vdots	\vdots	

Exemplo 2.2.8

Uma prova de $\{P \wedge Q, R \wedge \neg P\} \vdash \perp$ é dado pelo seguinte diagrama:

1	$P \wedge Q$	Premissa
2	$R \wedge \neg P$	Premissa
3	P	$\wedge E, 1$
4	$\neg P$	$\wedge E, 2$
5	\perp	$\perp I, 3, 4$

Definição 2.14

(Regra $\neg I$) Se existe uma subprova iniciada com α na linha i que deduz \perp em uma linha j tal que $i < j$, então pode-se fechar a subprova e na linha $j + 1$ introduzir a palavra $\neg\alpha$. Em notação de diagrama de Fitch tem-se:

\vdots	\vdots	
i	α	
\vdots	\vdots	
j	\perp	
$j + 1$	$\neg\alpha$	$\neg I, i-j$
\vdots	\vdots	

Exemplo 2.2.9

Uma prova de $\{P \Rightarrow \neg Q, Q\} \vdash \neg P$ é descrita pelo diagrama a seguir.

1	$P \Rightarrow \neg Q$	Premissa
2	Q	Premissa
3	P	Assuma
4	$P \Rightarrow \neg Q$	REI, 1
5	Q	REI, 2
6	$\neg Q$	$\Rightarrow E, 3, 4$
7	\perp	$\perp I, 5, 6$
8	$\neg P$	$\neg I, 3-7$

Definição 2.15 (Regra $\neg E$) Sempre que existir uma palavra $\neg\neg\alpha$ em uma linha i , então em uma linha j pode-se deduzir α com $i < j$. Em notação de diagrama tem-se:

\vdots	\vdots	
i	$\neg\neg\alpha$	
\vdots	\vdots	
j	α	$\neg E, i$
\vdots	\vdots	

E possível interpretar esta regra como representado a ideia de que negar uma palavra (argumento) duas vezes é o mesmo que afirmar tal palavra (argumento).

Exemplo 2.2.10 O seguinte resultado $\vdash (P \wedge \neg P) \Rightarrow Q$ é um dos mais famosos e controversos teoremas envolvendo o operador de implicação, para detalhes ver [40], na demonstração pode-se ver o uso da regra de eliminação da negação para provar tal teorema.

1	$P \wedge \neg P$	Assuma
2	$\neg Q$	Assuma
3	$P \wedge \neg P$	REI, 1
4	P	$\wedge E, 3$
5	$\neg P$	$\wedge E, 3$
6	\perp	$\perp I, 4, 5$
7	$\neg\neg Q$	$\neg I, 2-6$
8	Q	$\neg E, 7$
9	$(P \wedge \neg P) \Rightarrow Q$	$\Rightarrow I, 1-8$

Por fim, serão agora apresentadas as regras de introdução e eliminação para a disjunção para o sistema de dedução natural. Pela regra de eliminação da disjunção é um pouco mais complicada.

Definição 2.16 (Regra $\vee E$) Dado $\alpha \vee \beta$ na i -ésima linha se for possível deduz γ a partir de α e β como hipótese, então na linha n tal que $i < n$ é deduzida a palavra γ , ou seja:

i	$\alpha \vee \beta$	
\vdots	\vdots	
j	α	
\vdots	\vdots	
$j + l_1$	γ	
k	β	
\vdots	\vdots	
$k + l_2$	γ	
\vdots	\vdots	
n	γ	$\vee E, i, (j-j+l_1, k-k+l_2)$

Exemplo 2.2.11

A prova de $\vdash ((P \vee Q) \wedge \neg P) \Rightarrow Q$ usa a regra de eliminação da disjunção.

1	$(P \vee Q) \wedge \neg P$	Assuma
2	$P \vee Q$	$\wedge E, 1$
3	$\neg P$	$\wedge E, 1$
4	P	Assuma
5	$\neg Q$	Assuma
6	P	REI, 4
7	$\neg P$	REI, 3
8	\perp	$\perp I, 6, 7$
9	$\neg\neg Q$	$\neg I, 5-8$
10	Q	$\neg E, 9$
11	Q	Assuma
12	Q	REI, 11
13	Q	$\vee E, 2, (4-10, 11-12)$
14	$((P \vee Q) \wedge \neg P) \Rightarrow Q$	$\Rightarrow I, 1-13$

A próxima regra é reponsável por introduzir a disjunção, em alguma obras tais como [15] é mencionado que ela também é conhecida como regra aditiva, por ser capaz de introduzir símbolos que não estava inicialmente expostos no conjunto de premissas. A introdução da disjunção apesar de apresentar duas formas de aplicação, é muito mais simples que a regra remoção apresentada anteriormente.

Definição 2.17

(Regra $\vee I$) Se em uma prova aparece na linha i uma palavra α , então em uma linha j tal que $i < j$ pode-se deduzir para algum $\beta \in \mathcal{L}$ uma das seguintes palavras: $\alpha \vee \beta$ ou $\beta \vee \alpha$, ou seja:

\vdots	\vdots			\vdots	\vdots		
i	α			i	α		
\vdots	\vdots		ou	\vdots	\vdots		
j	$\alpha \vee \beta$	$\vee I, i$		j	$\beta \vee \alpha$	$\vee I, i$	
\vdots	\vdots			\vdots	\vdots		

Exemplo 2.2.12

A prova de $\{P, (Q \wedge S)\} \vdash S \vee \neg P$ é dada por:

1	P	Premissa
2	$Q \wedge S$	Premissa
3	S	$\wedge E, 2$
4	$S \vee \neg P$	$\vee I, 3$

Exemplo 2.2.13

| Uma simples prova da relação de consequência sintática $\{\neg S \Rightarrow (P \wedge Q), \neg S\} \vdash$

$Q \vee \neg R$ utilizando a regra de introdução da disjunção pode ser vista a seguir.

1	$\neg S$	Premissa
2	$\neg S \Rightarrow (P \wedge Q)$	Premissa
3	$P \wedge Q$	$\Rightarrow E, 1, 2$
4	Q	$\wedge E, 3$
5	$Q \vee \neg R$	$\vee I, 4$

Para prosseguir serão apresentadas as propriedades do sistema dedutivo, os próximos resultados são meta-teoremas do sistema em si, isto é, são resultados da natureza do sistema dedutivo em si e não palavras que podem ser deduzidas de um conjunto vazio de hipóteses.

Teorema 1 (Teorema da dedução) Seja $\Gamma \subseteq \mathcal{L}$ e $\alpha, \beta \in \mathcal{L}$. Se $\Gamma \cup \{\alpha\} \vdash \beta$, então $\Gamma \vdash \alpha \Rightarrow \beta$.

Prova Suponha que $\Gamma \cup \{\alpha\} \vdash \beta$, assim existe um diagrama da forma:

1	δ_1	Premissa
\vdots	\vdots	
m	δ_m	Premissa
$m+1$	α	Premissa
\vdots	\vdots	
n	β	

com $\delta_i \in \Gamma$ para todo $i \leq m$. Assim pode-se iniciar uma nova prova a partir das premissas $\delta_1, \dots, \delta_m$ do conjunto Γ , em seguida é iniciada uma subprova hipotética tomando α como hipótese, ou seja, começa-se a desenvolver o seguinte diagrama:

1	δ_1	Premissa
\vdots	\vdots	
m	δ_m	Premissa
$m+1$	α	Assuma

Em seguida usando a regra REI é possível “copiar” todas as premissas para o escopo da subprova, atualizando o diagrama para a forma:

1	δ_1	Premissa
\vdots	\vdots	
m	δ_m	Premissa
$m+1$	α	Assuma
$m+1+1$	δ_1	REI, 1
\vdots	\vdots	
$2m+1$	δ_m	REI, m

Agora basta desenvolver a subprova utilizando exatamente a mesma sequência de regras utilizadas^a na prova original de $\Gamma \cup \{\alpha\} \vdash \beta$, e assim será possível deduzir a

palavra β na subprova após n linhas depois da última premissa copiada com REI, ou seja, o diagrama fica com a seguinte forma:

1	δ_1	Premissa
\vdots	\vdots	
m	δ_m	Premissa
$m + 1$	α	Assuma
$m + 1 + 1$	δ_1	REI, 1
\vdots	\vdots	
$2m + 1$	δ_m	REI, m
\vdots	\vdots	
$2m + n + 1$	β	

Portanto, utilizando a regra de introdução da implicação entre as linhas $m + 1$ e $2m + n + 1$, é obtida na linha $2m + n + 2$ a palavra $\alpha \Rightarrow \beta$, ou seja, tem-se o seguinte diagrama:

1	δ_1	Premissa
\vdots	\vdots	
m	δ_m	Premissa
$m + 1$	α	Assuma
$m + 1 + 1$	δ_1	REI, 1
\vdots	\vdots	
$2m + 1$	δ_m	REI, m
\vdots	\vdots	
$2m + n + 1$	β	
$2m + n + 2$	$\alpha \Rightarrow \beta$	$\Rightarrow I, m + 1 - 2m + n + 1$

O que mostra que, $\Gamma \vdash \alpha \Rightarrow \beta$, concluindo assim a prova. \square

^aVale destacar que obviamente devem ser atualizadas as informações sobre as linhas de aplicação das regras, com respeito as linha do novo diagrama.

O resultado que se segue é uma consequência direta do Teorema da dedução.

Corolário 1 Seja $\Gamma \subseteq \mathcal{L}$ tal que $\Gamma = \{\alpha_1, \dots, \alpha_n\}$ e $\beta \in \mathcal{L}$. Se $\Gamma \vdash \beta$, então $\vdash \alpha_1 \Rightarrow (\dots (\alpha_n \Rightarrow \beta))$.

Prova A prova deste corolário consiste simplesmente de n aplicações do Teorema da dedução (Teorema 1). \square

Teorema 2 Seja $\Gamma \subseteq \mathcal{L}$ e $\alpha, \beta \in \mathcal{L}$. Se $\Gamma \vdash \alpha \Rightarrow \beta$, então $\Gamma \cup \{\alpha\} \vdash \beta$.

Prova A prova deste teorema apresenta uma simetria com o raciocínio apresentado pela prova do Teorema da dedução, assim sendo, a prova deste teorema irá ficar como exercício ao leitor. \square

Durante a prova do Teorema 3 a seguir, o símbolo Σ irá denotar o somatório e não o alfabeto proposicional.

Teorema 3 (Transitividade de \vdash) Seja $\Gamma \subseteq \mathcal{L}$ e $\alpha_1, \dots, \alpha_n, \beta \in \mathcal{L}$. Se $\Gamma \vdash \alpha_1, \dots, \Gamma \vdash \alpha_n$ e $\{\alpha_1, \dots, \alpha_n\} \vdash \beta$, então $\Gamma \vdash \beta$.

Prova Assuma que para todo $1 \leq i \leq n$ tem-se que $\Gamma \vdash \alpha_i$, ou seja, para cada α_i existe um diagrama da forma:

1	δ_1	Premissa
\vdots	\vdots	
m	δ_m	Premissa
\vdots	\vdots	
k_i	α_i	

com $\delta_c \in \Gamma$ para todo $1 \leq c \leq m$ e $k_i \in \mathbb{N}$ tal que $k_i > m$. Além disso, assuma também que $\{\alpha_1, \dots, \alpha_n\} \vdash \beta$, ou seja, assuma que existe um diagrama da forma:

1	α_1	Premissa
\vdots	\vdots	
n	α_n	Premissa
\vdots	\vdots	
l	β	

Assim é possível construir um novo diagrama em que as linhas de 1 até m contém exatamente as premissas que formam o conjunto Γ . Além disso, as linhas de $m + 1$ até k_1 serão idênticas as linhas do diagrama para a prova de $\Gamma \vdash \alpha_1$. Seguindo a construção deste novo diagrama para cada $2 \leq j \leq n$, as linha de $m + 1$ até k_j dos diagramas da prova de $\Gamma \vdash \alpha_j$ são dispostas sequencialmente no novo diagrama da mesma forma que estão em seus diagramas originais^a, assim o novo diagrama possui neste momento a seguinte forma:

1	δ_1	Premissa
\vdots	\vdots	
m	δ_m	Premissa
\vdots	\vdots	
k_1	α_1	
\vdots	\vdots	
$m + \sum_{i=1}^n (k_i - m)$	α_n	

Aplicando então a regra REI n vezes pode-se copiar as palavras $\alpha_1, \dots, \alpha_n$ para as linhas de $m + \sum_{i=1}^n (k_i - m) + 1$ até $m + \sum_{i=1}^n (k_i - m) + n$, atualizando assim o novo

diagrama para a forma:

1	δ_1	Premissa
\vdots	\vdots	
m	δ_m	Premissa
\vdots	\vdots	
k_1	α_1	
\vdots	\vdots	
$m + \sum_{i=1}^n (k_i - m)$	α_n	
$\left(m + \sum_{i=1}^n (k_i - m)\right) + 1$	α_1	REI, k_1
\vdots	\vdots	
$\left(m + \sum_{i=1}^n (k_i - m)\right) + n$	α_n	REI, $m + \sum_{i=1}^n (k_i - m)$

Agora basta repetir no novo diagrama todas as linhas de n até l do diagrama da prova de $\{\alpha_1, \dots, \alpha_n\} \vdash \beta$ exatamente como estão dispostas, atualizando apenas as referência das aplicações das regra de dedução natural, assim o diagrama assumi a forma:

1	δ_1	Premissa
\vdots	\vdots	
m	δ_m	Premissa
\vdots	\vdots	
k_1	α_1	
\vdots	\vdots	
$m + \sum_{i=1}^n (k_i - m)$	α_n	
$\left(m + \sum_{i=1}^n (k_i - m)\right) + 1$	α_1	REI, k_1
\vdots	\vdots	
$\left(m + \sum_{i=1}^n (k_i - m)\right) + n$	α_n	REI, $m + \sum_{i=1}^n (k_i - m)$
\vdots	\vdots	
$\left(m + \sum_{i=1}^n (k_i - m)\right) + n + l$	β	

E tal diagrama é exatamente a prova de $\Gamma \vdash \beta$, o que conclui a demonstração. \square

^aExceto pelo fato de que a referência das linhas de aplicação das regras de dedução natural precisam ser atualizadas para as linhas do novo diagrama

Seguindo com a apresentação das propriedades do sistema dedutivo, a seguir serão exposto duas diferente formas de apresentar e demonstrar a noção de monotonicidade de \vdash .

Teorema 4 (Teorema da monotonicidade (versão 1)) Sejam Γ_1 e Γ_2 dois subconjuntos de \mathcal{L} e seja $\alpha \in \mathcal{L}$. Se $\Gamma_1 \vdash \alpha$, então $\Gamma_1 \cup \Gamma_2 \vdash \alpha$.

Prova Sem perda de generalidade assuma que $\Gamma_1 = \{\alpha_1, \dots, \alpha_m\}$ e que $\Gamma_2 = \{\beta_1, \dots, \beta_n\}$ com $\Gamma_1 \cap \Gamma_2 = \emptyset$. Agora suponha que $\Gamma_1 \vdash \alpha$, logo existe um diagrama na forma:

1	α_1	Premissa
\vdots	\vdots	
m	α_m	Premissa
\vdots	\vdots	
k	α	

Agora é claro que é possível construir um novo diagrama em que além das premissas $\alpha_1, \dots, \alpha_m$ são também usadas as premissas do conjunto Γ_2 , de forma que este diagrama inicialmente seja da forma:

1	α_1	Premissa
\vdots	\vdots	
m	α_m	Premissa
$m + 1$	β_1	Premissa
\vdots	\vdots	
$m + n$	β_n	Premissa

Agora basta atualizar^a este diagrama repetindo todas as linhas de $m + 1$ até a linha k do diagrama da prova de $\Gamma_1 \vdash \alpha$, e dessa forma o novo diagrama será atualizado para a forma:

1	α_1	Premissa
\vdots	\vdots	
m	α_m	Premissa
$m + 1$	β_1	Premissa
\vdots	\vdots	
$m + n$	β_n	Premissa
\vdots	\vdots	
$m + n + (k - m + 1)$	α	

Mas tal diagrama é exatamente uma prova de $\Gamma_1 \cup \Gamma_2 \vdash \alpha$. \square

^aA atualização deve indexar corretamente a aplicação das provas com respeito as linhas do novo diagrama.

Para prosseguir é necessário antes considerar a definição de conjunto das palavras deduzíveis apresentada a seguir.

Definição 2.18 Seja $\Gamma \subseteq \mathcal{L}$ o conjunto de todas as palavras deduzíveis de Γ , denotada por $Th(\Gamma)$, é o conjunto de todas as palavras que são consequência sintática de Γ , ou seja, $Th(\Gamma) = \{\alpha \in \mathcal{L} \mid \Gamma \vdash \alpha\}$.

Teorema 5 Para qualquer que seja $\Gamma \subseteq \mathcal{L}$ tem-se que $Th(\Gamma)$ é infinito.

Prova Não é difícil verificar que $Th(\Gamma) \neq \emptyset$ para qualquer que seja $\Gamma \subseteq \mathcal{L}^a$, dessa forma existe pelo menos um $\alpha \in Th(\Gamma)$. Agora escolhendo qualquer $\beta \in \mathcal{L}$ considere agora uma palavra $\alpha \vee \beta$, e uma vez que, $\Gamma \vdash \alpha$, é claro pela regra de introdução da disjunção que $\Gamma \vdash \alpha \vee \beta$, e portanto, $\alpha \vee \beta \in Th(\Gamma)$. Uma vez que existem infinitos $\beta \in \mathcal{L}$ tem-se que $Th(\Gamma)$ é infinito. \square

^aO leitor pode treinar seu raciocínio de construção de provas demonstrando essa afirmação.

Teorema 6 (Teorema da monotonicidade (versão 2)) Sejam Γ_1 e Γ_2 dois subconjuntos de \mathcal{L} . Se $\Gamma_1 \subset \Gamma_2$, então $Th(\Gamma_1) \subset Th(\Gamma_2)$.

Prova Suponha que $\Gamma_1 \subset \Gamma_2$, agora para qualquer $\alpha \in Th(\Gamma_1)$, uma vez que, $\Gamma_1 \vdash \alpha$ pelo Teorema 4 tem-se que $\Gamma_1 \cup \Gamma_2 \vdash \alpha$, entretanto, pelas propriedades da união de conjuntos, como $\Gamma_1 \subset \Gamma_2$ tem-se que $\Gamma_2 = \Gamma_1 \cup \Gamma_2$, e portanto, $\Gamma_2 \vdash \alpha$, consequentemente, $\alpha \in Th(\Gamma_2)$. E assim tem-se que $Th(\Gamma_1) \subset Th(\Gamma_2)$. \square

Teorema 7 (Teorema da compacidade) $\Gamma \vdash \alpha$ se, e somente se, existe um conjunto finito $\Gamma_0 \subseteq \Gamma$ tal que $\Gamma_0 \vdash \alpha$.

Prova (\Rightarrow) Assuma que $\Gamma \vdash \alpha$ assim existe uma diagrama de Fitch que prova tal afirmação, mas uma vez que, um diagrama tem um número finito de linhas tem-se que existe n premissas de Γ usadas no diagrama, e portanto, existe um Γ_0 que é formado exatamente pelas premissas usadas, o que implica que Γ_0 é finito e $\Gamma_0 \vdash \alpha$, e além disso, por definição de subconjunto é claro que $\Gamma_0 \subseteq \Gamma$.
 (\Leftarrow) Suponha que $\Gamma_0 \subseteq \Gamma$ e que $\Gamma_0 \vdash \alpha$ pelo Teorema 6 tem-se que todo $\alpha \in Th(\Gamma_0)$ é tal que $\alpha \in Th(\Gamma)$, mas assim por definição $\Gamma \vdash \alpha$ o que completa a prova. \square

Teorema 8 (Teorema do ponto fixo) $Th(\Gamma) = Th(Th(\Gamma))$ para qualquer Γ .

Prova Primeiro note que para qualquer $\alpha \in Th(\Gamma)$, uma vez que, usando a regra REI pode-se demonstrar que $\{\alpha\} \vdash \alpha$, dessa forma tem-se que $\alpha \in Th(Th(\Gamma))$, e portanto, $Th(\Gamma) \subset Th(Th(\Gamma))$. Por outro lado, suponha por absurdo que $Th(Th(\Gamma)) \not\subset Th(\Gamma)$, assim existe um $\alpha \in Th(Th(\Gamma))$ tal que $\alpha \notin Th(\Gamma)$, mas por definição α necessariamente deve ser deduzidas de um conjunto de premissas $\{\beta_1, \dots, \beta_n\} \subset Th(\Gamma)$, e nessas condições pelo Teorema 6 tem-se que $\alpha \in Th(\Gamma)$ o que contradiz a hipótese, e portanto, $Th(Th(\Gamma)) \subset Th(\Gamma)$. Agora uma vez que, $Th(\Gamma) \subset Th(Th(\Gamma))$ e $Th(Th(\Gamma)) \subset Th(\Gamma)$, tem-se que $Th(\Gamma) = Th(Th(\Gamma))$, completando assim a prova. \square

2.3 Sistema Axiomático L

Uma abordagem alternativa para o sistema de dedução natural são os chamados sistemas axiomáticos¹, esses sistemas introduzidos inicialmente pelo matemático alemão David Hilbert (1862-1943), consistem em adotar um conjunto finito de axiomas e um número reduzido de regras de inferência [40, 53]. Antes de prosseguir para definir precisamente a noção de sistemas axiomáticos é necessário antes falar sobre provas para o sistemas axiomáticos.

Definição 2.19 [30] Uma prova de uma palavra α em um sistema axiomático T é uma sequência com n linhas, cada linha possui tem 3 informações: (1) o número da linha, (2) uma palavra da linguagem do sistema axiomático T e (3) se a palavra contida na linha é

¹Em algumas referências como por exemplo [8, 30] é usado o termo teorias formais em vez de sistemas axiomáticos.

uma premissa, uma instância de axioma ou a regra de inferência e as linhas usadas para obter tal palavra.

Note que a Definição 2.19 menciona a noção de linguagem do sistema T , isso faz referência ao fato de que cada sistema axiomático considera apenas um subconjunto de conectivos lógicos apresentados na Definição 2.1, assim as palavras que ocorrem na linguagem do sistema axiomático é restrita as palavras com tais conectivos. Vale ressaltar que isso não diminui o poder de dedução dos sistemas axiomáticos, pois como explicado em [8], existe uma relação entre os conectivos que torna sempre possível obter um usando os outros, isso é possível usando abreviações como descrito a seguir.

Definição 2.20 Seja Σ_s da mesma forma que apresentado na Definição 2.1 para todo $\alpha, \beta \in \Sigma_s \cup \{\perp\}$ são estabelecidas as seguintes abreviações:

- $\alpha \wedge \beta \equiv_{abr} \neg(\neg\alpha \vee \neg\beta)$.
- $\alpha \vee \beta \equiv_{abr} \neg(\neg\alpha \wedge \neg\beta)$.
- $\alpha \Rightarrow \beta \equiv_{abr} \neg\alpha \vee \beta$.
- $\neg\alpha \equiv_{abr} \alpha \Rightarrow \perp$.

Assim as abreviações podem ser vistas como um homomorfismo da linguagem \mathcal{L} para a linguagem \mathcal{L}_T de algum sistema axiomático T . A seguir são formalizados os conceitos de sistema axiomático e de consequência para o sistema axiomático.

Definição 2.21 (Sistema axiomático) Um sistema axiomático T é uma estrutura da forma $\langle \mathcal{L}_T, Axi, Reg \rangle$ onde:

- \mathcal{L}_T é a linguagem do sistema axiomático.
- Axi é um conjunto finito de axiomas, de forma que todas as instâncias de Axi são um suconjunto de \mathcal{L}_T .
- Reg é um conjunto de regras de inferência.

Definição 2.22 (Consequência em sistemas axiomáticos) Seja T um sistema axiomático e seja $\Gamma \subseteq \mathcal{L}_T$ e $\alpha \in \mathcal{L}_T$, é dito que α é consequência sintática de Γ no sistema T , denotado por $\Gamma \vdash_T \alpha$, se existir uma prova partindo das premissas em Γ que deduza α .

A seguir é apresentado o sistema axiomático conhecido como sistema L o mesma é definida sobre a linguagem $\mathcal{L}_{\Rightarrow}$, ou como também é conhecida linguagem implicativa.

Definição 2.23 (Linguagem $\mathcal{L}_{\Rightarrow}$) Dado o conjunto $\Sigma_s \cup \{\perp\}$, a linguagem $\mathcal{L}_{\Rightarrow}$ é o menor conjunto indutivamente gerado pelas regras:

- (a) Se $\alpha \in \Sigma_s \cup \{\perp\}$, então $\alpha \in \mathcal{L}_{\Rightarrow}$.
- (b) Se $\alpha \in \mathcal{L}_{\Rightarrow}$, então $(\neg\alpha) \in \mathcal{L}_{\Rightarrow}$.
- (c) Se $\alpha, \beta \in \mathcal{L}_{\Rightarrow}$, então $(\alpha \Rightarrow \beta) \in \mathcal{L}_{\Rightarrow}$.

O leitor mais atento pode notar que a linguagem implicativa é na verdade a linguagem \mathcal{L} sem a conjunção e a disjunção, ou seja, \mathcal{L} é reescrita usando abreviações.

Definição 2.24 (Sistema L) [42] O sistema L é a estrutura $\langle \mathcal{L}_{\Rightarrow}, Axi, \{\Rightarrow E\} \rangle$ onde:

$$Axi = \left\{ \begin{array}{l} \alpha \Rightarrow (\beta \Rightarrow \alpha), \\ (\alpha \Rightarrow (\beta \Rightarrow \gamma)) \Rightarrow ((\alpha \Rightarrow \beta) \Rightarrow (\alpha \Rightarrow \gamma)), \\ (\neg\beta \Rightarrow \neg\alpha) \Rightarrow ((\neg\beta \Rightarrow \alpha) \Rightarrow \beta) \end{array} \right\}$$

Para ficar melhor de justificar durante as demonstrações no sistema L são adotados os seguintes apelidos para os axiomas do sistema:

$$(A_1) \quad \alpha \Rightarrow (\beta \Rightarrow \alpha).$$

$$(A_2) \quad (\alpha \Rightarrow (\beta \Rightarrow \gamma)) \Rightarrow ((\alpha \Rightarrow \beta) \Rightarrow (\alpha \Rightarrow \gamma)).$$

$$(A_3) \quad (\neg\beta \Rightarrow \neg\alpha) \Rightarrow ((\neg\beta \Rightarrow \alpha) \Rightarrow \beta).$$

Exemplo 2.3.1 Uma prova de $\vdash_L P \Rightarrow P$ é dada por:

- | | | |
|----|---|------------------------|
| 1. | $P \Rightarrow ((P \Rightarrow P) \Rightarrow P)$ | Instância de A_1 |
| 2. | $(P \Rightarrow ((P \Rightarrow P) \Rightarrow P)) \Rightarrow ((P \Rightarrow (P \Rightarrow P)) \Rightarrow (P \Rightarrow P))$ | Instância de A_2 |
| 3. | $P \Rightarrow (P \Rightarrow P)$ | Instância de A_1 |
| 4. | $(P \Rightarrow (P \Rightarrow P)) \Rightarrow (P \Rightarrow P)$ | $(\Rightarrow E) 1, 2$ |
| 5. | $P \Rightarrow P$ | $(\Rightarrow E) 3, 4$ |

Para simplificar mais ainda a escrita das demonstrações é comum evitar ficar escrevendo na justificativa “instância de . . .”, em vez disso, coloca-se apenas o identificador do axioma, o próximo exemplo já faz uso dessa simplificação.

Exemplo 2.3.2 Uma prova de $\{\neg P \Rightarrow \neg P, \neg P \Rightarrow P\} \vdash_L P$ é dada por:

- | | | |
|----|--|------------------------|
| 1. | $\neg P \Rightarrow \neg P$ | Premissa |
| 2. | $\neg P \Rightarrow P$ | Premissa |
| 3. | $(\neg P \Rightarrow \neg P) \Rightarrow ((\neg P \Rightarrow P) \Rightarrow P)$ | A_3 |
| 4. | $(\neg P \Rightarrow P) \Rightarrow P$ | $(\Rightarrow E) 1, 3$ |
| 5. | P | $(\Rightarrow E) 2, 4$ |

O Teorema da dedução (Teorema 1) e os demais meta-teoremas provados na seção anterior para linguagem \mathcal{L} usando a dedução natural são válidos para qualquer sistema axiomático T e sua linguagem [8]. O próximo exemplo, mostra como empregar o uso do Teorema da dedução durante uma demonstração no sistema L .

Exemplo 2.3.3 Uma prova de $\{P \Rightarrow Q, Q \Rightarrow R, P\} \vdash_L R$ é detalhada a seguir:

- | | | |
|----|-------------------|------------------------|
| 1. | $P \Rightarrow Q$ | Premissa |
| 2. | $Q \Rightarrow R$ | Premissa |
| 3. | P | Premissa |
| 4. | Q | $(\Rightarrow E) 1, 3$ |
| 5. | R | $(\Rightarrow E) 2, 4$ |

Agora pela prova acima e pelo Teorema da dedução (no sistema L) tem-se que $\{P \Rightarrow Q, Q \Rightarrow R\} \vdash_L P \Rightarrow R$.

2.4 Sistema Semântico

A semântica da lógica proposicional foi descrita inicialmente pelo matemático inglês George Boole (1815-1864) em seu trabalho [11, 12], entretanto, Alfred Tarski⁵

⁵ O artigo de Tarski pode ser consultado na versão re-editada em [58].

⁶ Clássica aqui diz respeito a lógica como apresentada pelo matemático, lógico e filósofo alemão Gottlob Frege (1848-1925).

(1901-1983) apresentou uma formulação mais rigorosa para computar os valores lógicos das palavras da linguagem proposicional em 1936.

A semântica é responsável por introduzir significado para as palavras de uma linguagem formal, no caso da linguagem proposicional clássica⁶, as palavras podem ter seu significado como verdadeiro ou falso. Antes de apresentar formalmente o conceito de semântica da linguagem proposicional é necessário definir a ideia de função de valoração.

Definição 2.25

(Valoração) Uma valoração dos símbolos proposicionais é uma função total $\rho : \Sigma_s \rightarrow \{0, 1\}$.

O conjunto $\{0, 1\}$ na Definição 2.25 é chamado de conjunto dos valores de representação de verdade, em muitas apresentações de lógica usam V e F para representar os dois valores de verdade (a saber, verdadeiro e falso) em vez de usar 0 e 1.

Neste texto, entretanto, se optou por usar 1 (verdade) e 0 (falso), para assim, evitar confusão com variáveis em fórmulas e metavariables em regras de inferência, que podem ocorrer ao usar V e F. A opção pelo uso de 1 e 0, é particularmente interessante para cientistas e engenheiros de computação, uma vez que, tais valores tem uso comum no design de circuitos digitais [14, 32, 36] e em discussões sobre design e arquitetura de computadores [47, 56], duas áreas intimamente ligadas a lógica clássica.

A semântica da linguagem proposicional como destacado em [40] se baseia na noção de interpretação⁷, sendo que, uma interpretação nada mais é do que a extensão de uma dada valoração ρ para a linguagem proposicional, usando alguma álgebra booleana [11, 12], sendo está última também chamada de espaço das valorações [5].

⁷ A definição de semântica apresentada aqui é equacional, ou seja, sempre existe uma equação que determina o valor semântico de qualquer $\alpha \in \mathcal{L}$.

Definição 2.26

(Interpretação) Dada uma valoração ρ , uma interpretação é uma função total $I_\rho : \mathcal{L} \rightarrow \{0, 1\}$ definida para todo $\alpha, \beta \in \mathcal{L}$ recursivamente como:

- Se $\alpha = \perp$, então $I_\rho(\alpha) = 0$.
- Se $\alpha \in \Sigma_s$, então $I_\rho(\alpha) = \rho(\alpha)$.
- $I_\rho(\neg\alpha) = 1 - I_\rho(\alpha)$.
- $I_\rho(\alpha \wedge \beta) = \min(I_\rho(\alpha), I_\rho(\beta))$.
- $I_\rho(\alpha \vee \beta) = \max(I_\rho(\alpha), I_\rho(\beta))$.
- $I_\rho(\alpha \Rightarrow \beta) = \max(1 - I_\rho(\alpha), I_\rho(\beta))$.

Exemplo 2.4.1

Considere uma valoração ρ tal que $\rho(P) = 0, \rho(Q) = 1$ e $\rho(R) = 1$ o valor de significado da palavra $\neg(P \Rightarrow (R \wedge Q))$ é calculado por:

$$\begin{aligned} I_\rho(\neg(P \Rightarrow (R \wedge Q))) &= 1 - I_\rho(P \Rightarrow (R \wedge Q)) \\ &= 1 - \max(1 - I_\rho(P), \min(I_\rho(R), I_\rho(Q))) \\ &= 1 - \max(1 - \rho(P), \min(\rho(R), \rho(Q))) \\ &= 1 - \max(1 - 0, \min(1, 1)) \\ &= 1 - \max(1, 1) \\ &= 0 \end{aligned}$$

Outra forma de apresentar a semântica para a lógica proposicional é através do uso de tabelas verdade [25], em um primeiro momento pode-se pensar que, a noção de semântica por tabelas verdades e a definição de semântica equacional apresentada na Definição 2.26 não tem similaridade, entretanto, isso não é verdade! Pois, como dito em [40], as leis expressas nas tabelas verdades são derivadas das equações de álgebras booleanas, assim também podem ser derivadas das equações da Definição 2.26, uma vez que tais equações formam uma álgebra booleana [15].



Atenção

De fato, uma vez que, o número n de variáveis em qualquer $\alpha \in \mathcal{L}$ é finita e o número de valores verdade são apenas dois, então o número de linhas em qualquer tabela verdade é exatamente igual a 2^n . Onde cada linha da tabela representa uma interpretação I_p .

Definição 2.27 Seja $\alpha, \beta \in \mathcal{L}$, a tabela verdade da conjunção possui a seguinte forma:

α	β	$\alpha \wedge \beta$
0	0	0
0	1	0
1	0	0
1	1	1

Definição 2.28 Seja $\alpha, \beta \in \mathcal{L}$, a tabela verdade da disjunção possui a seguinte forma:

α	β	$\alpha \vee \beta$
0	0	0
0	1	1
1	0	1
1	1	1

Definição 2.29 Seja $\alpha, \beta \in \mathcal{L}$, a tabela verdade da implicação possui a seguinte forma:

α	β	$\alpha \Rightarrow \beta$
0	0	1
0	1	1
1	0	0
1	1	1

Definição 2.30 Seja $\alpha \in \mathcal{L}$, a tabela verdade da negação possui a seguinte forma:

α	$\neg \alpha$
0	1
1	0

Antes de prosseguir para explicar a construção das tabelas verdade e explicar sua relação com a Definição 2.26 é conveniente introduzir alguns conceitos chaves.

Definição 2.31 (Conjunto de sub-palavras) Seja $\alpha \in \mathcal{L}$ o conjunto das sub-palavras de α , denotado por Sub_α , é o conjunto gerado pelas seguintes regras:

R1. Se $\alpha \in \Sigma_s \cup \{\perp\}$, então $Sub_\alpha = \{\alpha\}$.

R2. Se $\alpha = \neg \beta$, então $Sub_\alpha = \{\neg \beta\} \cup Sub_\beta$.

R3. Se $\alpha = \beta \bullet \gamma$ com $\bullet \in \{\wedge, \vee, \Rightarrow\}$, então $Sub_\alpha = \{\beta \bullet \gamma\} \cup Sub_\beta \cup Sub_\gamma$.

Exemplo 2.4.2 Considere a palavra $(P \Rightarrow \neg Q) \vee S$, tem-se que:

$$\begin{aligned}
 Sub_{(P \Rightarrow \neg Q) \vee S} &= \{(P \Rightarrow \neg Q) \vee S\} \cup Sub_{P \Rightarrow \neg Q} \cup Sub_S \\
 &= \{(P \Rightarrow \neg Q) \vee S\} \cup (\{P \Rightarrow \neg Q\} \cup Sub_P \cup Sub_{\neg Q}) \cup \{S\} \\
 &= \{(P \Rightarrow \neg Q) \vee S, S\} \cup (\{P \Rightarrow \neg Q\} \cup \{P\} \cup (\{\neg Q\} \cup Sub_Q)) \\
 &= \{(P \Rightarrow \neg Q) \vee S, S\} \cup (\{P \Rightarrow \neg Q, P\} \cup (\{\neg Q\} \cup \{Q\})) \\
 &= \{(P \Rightarrow \neg Q) \vee S, S\} \cup (\{P \Rightarrow \neg Q, P\} \cup \{\neg Q, Q\}) \\
 &= \{(P \Rightarrow \neg Q) \vee S, S\} \cup \{P \Rightarrow \neg Q, P, \neg Q, Q\} \\
 &= \{(P \Rightarrow \neg Q) \vee S, S, P \Rightarrow \neg Q, P, \neg Q, Q\}
 \end{aligned}$$

Para realizar a construção da tabela verdade de uma fórmula α , deve-se indexar as colunas da tabela com os elementos de Sub_α , assim uma tabela verdade para uma fórmula α terá exatamente $\#Sub_\alpha$ colunas.

Como os elementos de Sub_α não possuem uma ordenação, em geral é usado a regra de distribuir as palavras da esquerda para à direita de forma crescente de acordo com o tamanho das mesmas ordenadas pela ordem lexicográfica de Σ_s , assim as palavras mais à esquerda sempre terão tamanho 1, enquanto que a palavra mais à direita será sempre a maior palavra, isto é, a própria palavra α .

Exemplo 2.4.3 Seguindo as regras mencionados no parágrafo anterior, a tabela para a palavra $(P \Rightarrow \neg Q) \vee S$ terá exatamente 6 colunas, uma vez que, $\#Sub_{(P \Rightarrow \neg Q) \vee S} = 6$, e pode ser da forma:

P	Q	S	$\neg Q$	$P \Rightarrow \neg Q$	$(P \Rightarrow \neg Q) \vee S$
-----	-----	-----	----------	------------------------	---------------------------------

Uma vez que as colunas são inseridas e indexadas pelas palavras de Sub_α , o próximo passo é preencher as demais linhas, onde na linha i de coluna indexada por β estará disposto o valor de $I_{\rho_i}(\beta)$, onde ρ_i é a i -ésima valoração que atribuiu diferentes valores para as variáveis da palavra α . É usado a ordem lexicográfica das palavras do código binário com palavras de tamanho n onde n é o número de átomos α , para determinar a ordenação das valorações ρ .

Exemplo 2.4.4 Considere a tabela iniciada no Exemplo 2.4.3, agora usando a regra de ordenar as valorações ρ usando a ordem lexicográfica do código binário, tem-se a seguinte ordem para as valorações:

	P	Q	S	$\neg Q$	$P \Rightarrow \neg Q$	$(P \Rightarrow \neg Q) \vee S$
ρ_1	0	0	0			
ρ_2	0	0	1			
ρ_3	0	1	0			
ρ_4	0	1	1			
ρ_5	1	0	0			
ρ_6	1	0	1			
ρ_7	1	1	0			
ρ_8	1	1	1			

Agora basta computar os valores usando a Definição 2.26, ficando então a tabela com a seguinte forma final:

	P	Q	S	$\neg Q$	$P \Rightarrow \neg Q$	$(P \Rightarrow \neg Q) \vee S$
ρ_1	0	0	0	1	1	1
ρ_2	0	0	1	1	1	1
ρ_3	0	1	0	0	1	1
ρ_4	0	1	1	0	1	1
ρ_5	1	0	0	1	1	1
ρ_6	1	0	1	1	1	1
ρ_7	1	1	0	0	0	0
ρ_8	1	1	1	0	0	1

Não é necessário identificar as linhas em uma tabela verdade, isso foi feito no exemplo anterior apenas para ficar mais didático.

Exemplo 2.4.5 Para a palavra $P \Rightarrow ((\neg P) \wedge Q)$ tem-se a seguinte tabela verdade.

P	Q	$\neg P$	$\neg P \wedge Q$	$P \Rightarrow ((\neg P) \wedge Q)$
0	0	1	0	1
0	1	1	1	1
1	0	0	0	0
1	1	0	0	0

Como muito bem exposto em [21, 23], as propriedades semânticas das palavras de \mathcal{L} , permitem construir três categorias ou classes, apresentadas a seguir

Definição 2.32 (Tautologia) Uma palavra $\alpha \in \mathcal{L}$ é uma tautologia quando para toda interpretação I_ρ tem-se que $I_\rho(\alpha) = 1$.

Definição 2.33 (Contradição) Uma palavra $\alpha \in \mathcal{L}$ é uma contradição quando para toda interpretação I_ρ tem-se que $I_\rho(\alpha) = 0$.

Exemplo 2.4.6 As palavras $P \vee \neg P$ e $P \wedge \neg P$ são respectivamente uma tautologia e uma contradição, como pode ser visto nas tabelas abaixo.

P	$\neg P$	$P \vee \neg P$
0	1	1
1	0	1

P	$\neg P$	$P \wedge \neg P$
0	1	0
1	0	0

Proposição 1 Para todo $\alpha \in \mathcal{L}$ tem-se que α é uma tautologia se e somente se $\neg\alpha$ é uma contradição.

Prova Trivial. \square

Definição 2.34 (Contingência) Uma palavra $\alpha \in \mathcal{L}$ é uma contingência quando não é uma tautologia e nem uma contradição.

Usando a noção de interpretação é possível definir formalmente a noção de palavra satisfatível.

Definição 2.35 (Palavra satisfatível) Uma palavra $\alpha \in \mathcal{L}$ é dita satisfatível quando existe uma interpretação I_ρ tal que $I_\rho(\alpha) = 1$.

Proposição 2 Uma palavra $\alpha \in \mathcal{L}$ é satisfatível se, e somente se, α é uma contingência ou uma tautologia.

Prova Trivial. \square

Exemplo 2.4.7 A palavra $P \Rightarrow Q$ é satisfatível pois existe uma interpretação I_ρ com a valoração ρ definido $\rho(Q) = 1$, e é claro pela Definição 2.26 que tal interpretação torna o significado da palavra $P \Rightarrow Q$ como sendo verdadeiro, isto é, $I_\rho(P \Rightarrow Q) = 1$.

Definição 2.36 (Conjunto satisfatível) Um conjunto $\Gamma \subseteq \mathcal{L}$ é dito satisfatível se existe uma interpretação I_ρ tal que para todo $\alpha \in \Gamma$ tem-se que $I_\rho(\alpha) = 1$.

Exemplo 2.4.8 O conjunto $\Gamma = \{P, Q, \neg P \vee Q\}$ é satisfatível pois a interpretação I_ρ tal que $I_\rho(P) = 1$ e $I_\rho(Q) = 1$ é capaz de satisfazer todas as palavras de Γ .

Definição 2.37 (Conjunto Contraditório) Um conjunto $\Gamma \subseteq \mathcal{L}$ é dito contraditório se não existe nenhuma interpretação I_ρ que satisfaça Γ .

Exemplo 2.4.9 O Conjunto $\Gamma = \{\neg\neg P, \neg P\}$ é contraditório, pois não existe nenhuma interpretação^a capaz de satisfazer todas as palavras em Γ .

^aProvar essa afirmação é um ótimo exercício para o leitor.

Definição 2.38 (Modelo) Seja $\Gamma \subseteq \mathcal{L}$, se Γ é satisfatível para uma certa interpretação I_ρ . Então é dito que I_ρ é um modelo para Γ .

Pode-se então agora formalizar a ideia de consequência do ponto de vista semântico, a consequência semântica é o mecanismo que determina se uma conclusão (ou tese) segue (ou é consequência) de um conjunto de premissas, formalmente isto é definido como se segue.

Definição 2.39 (Consequência Semântica) Seja $\Gamma \subseteq \mathcal{L}$ e $\alpha \in \mathcal{L}$, é dito que α é consequência semântica de Γ , denotado por $\Gamma \models \alpha$, sempre que todo modelo I_ρ de Γ , for também um modelo para o conjunto unitário $\{\alpha\}$.

Quando α é uma tautologia verifica-se que $\emptyset \models \alpha$, isto é, α é consequência semântica do conjunto vazio. Este fato também pode ser denotado por $\models \alpha$.

Exemplo 2.4.10 Seja $\Gamma = \{P, \neg P \vee Q\}$ tem-se que $\Gamma \models Q \vee \neg Q$, para verificar isso primeiro considere a seguinte tabela verdade^a:

P	Q	$\neg P$	$\neg P \vee Q$
0	0	1	1
0	1	1	1
1	0	0	0
1	1	0	1

Note que, a linha em destaque é a única em que P e $\neg P \vee Q$ são ambos verdadeiras, assim tal linha é o **único** modelo de Γ , isto é, tem-se que o modelo de Γ é a interpretação I_ρ tal que $I_\rho(P) = 1$ e $I_\rho(Q) = 1$, pois com essa interpretação todas as palavras do conjunto Γ são satisfeitas. Agora assumindo esse mesmo modelo tem-se que:

Q	$\neg Q$	$Q \vee \neg Q$
1	0	1

E assim $\{Q \vee \neg Q\}$ também é satisfeito pelo mesmo modelo, como pode ser observado pela tabela verdade acima. Assim de fato tem-se que $\Gamma \models Q \vee \neg Q$.

^aAqui as tabelas verdades das palavras $\neg P$ e $\neg P \vee Q$ foram claramente concatenadas e reorganizadas.

Exemplo 2.4.11 Dado o conjunto $\Gamma = \{P, Q \vee R\}$ tem-se que $\neg P \wedge R$ não é consequência semântica de Γ , denotado por $\Gamma \not\models \neg P \wedge R$, pois se Γ é satisfatível para I_ρ tem-se que $I_\rho(P) = 1$, mas isso implicada que $I_\rho(\neg P) = 0$, e portanto, $I_\rho(\neg P \wedge R) = 0$, consequentemente, $\Gamma \not\models \neg P \wedge R$.

Como para a consequência sintática a consequência semântica pode ser vista como uma relação no sentido usual da teoria dos conjunto, ou seja, tem-se que $\models \subseteq \wp(\mathcal{L}) \times \mathcal{L}$.

Teorema 9 (Teorema da refutação) Seja $\Gamma \subseteq \mathcal{L}$ e $\alpha \in \mathcal{L}$. $\Gamma \models \alpha$ se, e somente se, $\Gamma \cup \{\neg\alpha\}$ não é satisfatível.

Prova (\Rightarrow) Suponha que $\Gamma \models \alpha$ acontece, assim para todo I_ρ que satisfaz Γ tem-se que $I_\rho(\alpha) = 1$, mas pelo Definição 2.26 tem-se que $I_\rho(\neg\alpha) = 0$, e portanto, nenhum I_ρ será capaz de satisfazer $\Gamma \cup \{\neg\alpha\}$.

(\Leftarrow) Suponha que $\Gamma \cup \{\neg\alpha\}$ não é satisfatível, assim para qualquer interpretação I_ρ que satisfaça Γ obrigatoriamente não pode satisfazer $\{\neg\alpha\}$, ou seja, $I_\rho(\neg\alpha) = 0$,

mas pela Definição 2.26 tem-se que $I_\rho(\alpha) = 1$, e portanto, $\Gamma \models \alpha$. \square

Teorema 10 (Teorema da dedução (semântico)) Para todo $\alpha, \beta \in \mathcal{L}$ tem-se que $\{\alpha\} \models \beta$ se, e somente se, $\models \alpha \Rightarrow \beta$.

Prova (\Rightarrow) Suponha que $\{\alpha\} \models \beta$, assim para toda interpretação I_ρ tal que $I_\rho(\alpha) = 1$ tem-se que $I_\rho(\beta) = 1$, logo pela Definição 2.26 tem-se que $I_\rho(\alpha \Rightarrow \beta) = 1$, e portanto, é modelo de $\{\alpha \Rightarrow \beta\}$, assim por vacuidade é claro que $\models \alpha \Rightarrow \beta$.
 (\Leftarrow) Suponha que $\models \alpha \Rightarrow \beta$, assim existe um modelo I_ρ tal que $I_\rho(\alpha \Rightarrow \beta) = 1$, de fato existe $I_\rho(\alpha) = I_\rho(\beta) = 1$, mas por esta interpretação é também modelo para $\{\alpha\}$ e $\{\beta\}$, portanto, conclui-se que $\{\alpha\} \models \beta$. \square

Corolário 2 Para todo $\alpha_1, \dots, \alpha_{n-1}, \alpha_n, \beta \in \mathcal{L}$ tem-se que $\{\alpha_1, \dots, \alpha_{n-1}, \alpha_n\} \models \beta$ se, e somente se, $\{\alpha_1, \dots, \alpha_{n-1}\} \models \alpha_n \Rightarrow \beta$.

Prova (\Rightarrow) Suponha que $\{\alpha_1, \dots, \alpha_{n-1}, \alpha_n\} \models \beta$, assim existe um modelo I_ρ para $\{\alpha_1, \dots, \alpha_{n-1}, \alpha_n\}$ e $\{\beta\}$, logo por definição tem-se para todo $i \leq n$ que $I_\rho(\alpha_i) = I_\rho(\beta) = 1$, consequentemente $I_\rho(\alpha_n) \leq I_\rho(\beta)$, dessa forma tem-se que $I_\rho(\alpha_n \Rightarrow \beta) = 1$, assim I_ρ é um modelo para $\{\alpha_n \Rightarrow \beta\}$, e portanto, $\{\alpha_1, \dots, \alpha_{n-1}\} \models \alpha_n \Rightarrow \beta$.
 (\Leftarrow) Suponha que $\{\alpha_1, \dots, \alpha_{n-1}\} \models \alpha_n \Rightarrow \beta$ logo existe um modelo I_ρ que satisfaz $\{\alpha_1, \dots, \alpha_{n-1}\}$ e $\{\alpha_n \Rightarrow \beta\}$, assumamos que este modelo é tal que $I_\rho(\alpha_n) = I_\rho(\beta) = 1$, assim claramente tem-se que este modelo satisfaz $\{\alpha_1, \dots, \alpha_{n-1}, \alpha_n\}$ e também satisfaz $\{\beta\}$, portanto, $\{\alpha_1, \dots, \alpha_{n-1}, \alpha_n\} \models \beta$. \square

Proposição 3 Dado $\Gamma \subseteq \mathcal{L}$ tal que $\Gamma = \{\alpha_1, \dots, \alpha_n\}$ e $\beta \in \mathcal{L}$ tem-se que $\Gamma \models \beta$ se, e somente, se $\models \alpha_1 \Rightarrow (\dots (\alpha_n \Rightarrow \beta))$.

Prova A demonstração desse resultado pode ser verificada com n aplicações de Corolário 2. \square

Um aspecto semântico importante do sistema axiomático L é exposto pelos dois resultados a seguir.

Teorema 11 Todos os axiomas do sistema axiomática L são tautologias.

Prova Trivial, basta o leitor construir as tabelas verdades. \square

Corolário 3 O conjunto de axiomas do sistema axiomática L é satisfatível.

Prova Direto Teorema 11 e da definição de conjunto satisfatível. \square

Outro importante aspecto semântico entre as palavras de \mathcal{L} é a noção de equivalência semântica definida formalmente a seguir.

Definição 2.40 (Equivalência semântica) Dado $\alpha, \beta \in \mathcal{L}$ é dito que α e β são equivalentes, denotado^a por $\alpha \equiv \beta$, quando para toda interpretação I_ρ tem-se que $I_\rho(\alpha) = I_\rho(\beta)$.

^aTambém pode ser usado o símbolo \Leftrightarrow em vez de \equiv .

Exemplo 2.4.12 As palavras $\alpha \Rightarrow \beta$ e $\neg\alpha \vee \beta$ são semanticamente equivalentes como pode ser a seguir.

P	Q	$\neg P$	$P \Rightarrow Q$	$\neg P \vee Q$
0	0	1	1	1
0	1	1	1	1
1	0	0	0	0
1	1	0	1	1

Em alguns textos (como [8]) é feita uma distinção entre lógica proposicional e a linguagem proposicional, isso acontece pois nesse tipo de texto é empregada a visão da lógica proposicional como sendo a ciência que estuda o raciocínio proposicional correto (ou verdadeiro), assim as palavras que não são tautologias não são diretamente interessantes no estudo da lógica proposicional nesta visão, entretanto, considerar o estudo da linguagem proposicional como um todo ou apenas de suas tautologias não há qualquer diferença⁸ como apontado pelos professores Aho e Ullman em [3].

2.5 Corretude e Completude

Antes de introduzir os conceitos e resultados de completude e corretude é conveniente antes, apresentar algumas noções sobre o sistema sintático e o sistema semântico, apresentados nas seções anteriores.

A ideia apresentada nas demonstrações do sistema sintático é o uso das regras de inferência para **derivar** palavras da linguagem proposicional, assim o sistema sintático, através da relação \vdash , pode ser visto como um sistema de reescrita [6]. Por outro lado, como discutido anteriormente o sistema semântico apresenta o mecanismo (a relação \models) para **validar** o significado das palavras da linguagem proposicional. Agora é momento em que o leitor perspicaz faz o questionamento: “As relações \vdash e \models interagem de alguma forma?”. A resposta a esse questionamento é afirmativa e tais interações acontecem exatamente através da corretude e da completude como será mostrado nesta seção, a Figura 2.1 a seguir ilustra as interações mencionadas neste parágrafo.

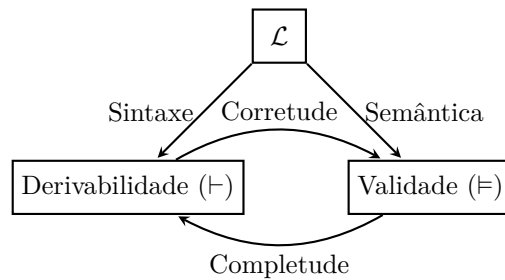


Figura 2.1: Relacionamento das estruturas que compõem a lógica proposicional.

Este texto irá prosseguir primeiro mostrando que a lógica proposicional é correta, isto é, será demonstrado o teorema da corretude. De forma amigável tal teorema pode ser interpretado da seguinte forma, se existir uma prova de $\Gamma \vdash \alpha$, isto é, se for possível deduzir α a partir das premissas em Γ , isso significa que todo modelo de Γ é também um modelo para o conjunto $\{\alpha\}$.

Teorema 12 (Teorema da Corretude) Para qualquer conjunto finito $\Gamma \subseteq \mathcal{L}$ e qualquer $\alpha \in \mathcal{L}$ se $\Gamma \vdash \alpha$, então $\Gamma \models \alpha$.

Prova Para o caso em que Γ é vazio a prova é trivial por vacuidade e não será apresentada aqui, quando Γ não é vazio a prova será feita por indução sobre o tamanho dos diagramas do sistema dedutivo, ou seja, a quantidade de linhas dos diagramas, em que serão aplicadas as regras do sistema de dedução natural.

(B)ase: Na base da indução estão as demonstrações cujo diagrama tem apenas uma linha, ou seja, obrigatoriamente o diagrama é da forma:

1 | α Premissa

Ou seja, $\Gamma = \{\alpha\}$, agora trivialmente é claro que $\Gamma \models \alpha$.

(H)ipótese indutiva: Assuma que para qualquer prova com n linhas de $\Gamma \vdash \alpha$ tem-se que $\Gamma \models \alpha$, sendo $n \in \mathbb{N}$.

(P)asso indutivo: Dado uma prova de $\{a_1, \dots, \alpha_n\} \vdash \alpha$ com um número de linhas maior que n é necessário analisar cada aplicação das regras do sistema dedutivo que finalizou a prova de forma separada.

- Para a **regra das premissas**, uma vez que, a prova de $\Gamma \vdash \alpha$ tem $n + 1$ linhas, Γ deverá ser obrigatoriamente da forma $\Gamma = \{\alpha_1, \dots, \alpha_n, \alpha_{n+1}\}$ e $\alpha = \alpha_{n+1}$, assim tem-se que tal diagrama é da forma:

1	α_1	Premissa
\vdots	\vdots	
n	α_n	Premissa
$n + 1$	α_{n+1}	Premissa

agora dado que é impossível você ter um modelo para $\{\alpha_1, \dots, \alpha_n, \alpha_{n+1}\}$ que não seja modelo de $\{\alpha_{n+1}\}$ trivialmente tem-se que $\Gamma \models \alpha$, concluindo esta etapa da prova.

- Para a **regra de reiteração**, uma vez que, a prova de $\Gamma \vdash \alpha$ tem $n + 1$ linhas, significa assumido sem perda de generalidade, que o conjunto de premissas é da forma $\Gamma = \{\alpha_1, \dots, \alpha_i\}$, tem-se que a prova de $\Gamma \vdash \alpha$ é da forma,

1	α_1	Premissa
\vdots	\vdots	
i	α_i	Premissa
\vdots	\vdots	
n	α	
$n + 1$	α	REI, n

mas isso implica que existe uma prova com n passos para $\Gamma \vdash \alpha$, e por (H), sabe-se que para tal prova condicional que $\Gamma \models \alpha$, dado que o conjunto de premissas é o mesmo para a prova com $n + 1$ passos pode-se concluir novamente que $\Gamma \models \alpha$.

- Para a \wedge I, uma vez que, a prova de $\Gamma \vdash \alpha$ tem $n + 1$ linhas, tem-se que obrigatoriamente α é uma palavra $\beta \wedge \gamma$, e assim a prova de $\Gamma \vdash \alpha$ é um diagrama da forma,

1	α_1	Premissa
\vdots	\vdots	
i	α_i	Premissa
\vdots	\vdots	
j	β	
\vdots	\vdots	
k	γ	
\vdots	\vdots	
$n + 1$	$\beta \wedge \gamma$	\wedge I, $j; k$

mas isso implica que existe uma prova de $\Gamma \vdash \beta$ e outra para $\Gamma \vdash \gamma$, em que a maior das duas teria no máximo n linhas, e assim por (H), tem-se

que $\Gamma \models \beta$ e $\Gamma \models \gamma$, para qualquer modelo I_ρ de $\{\beta, \gamma\}$ tem-se por definição que este também seria um modelo para $\{\beta \wedge \gamma\}$, e portanto, $\Gamma \models \beta \wedge \gamma$, ou seja, $\Gamma \models \alpha$ concluído assim, essa etapa da prova.

- Para a regra $\wedge\mathbf{E}$, uma vez que, a prova de $\Gamma \vdash \alpha$ possui $n + 1$ linhas, tem-se que obrigatoriamente α é uma palavra β (ou γ), sem perda de generalidade assuma que α com sendo β , e assim a prova de $\Gamma \vdash \alpha$ é um diagrama da forma,

1	α_1	Premissa
\vdots	\vdots	
i	α_i	Premissa
\vdots	\vdots	
n	$\beta \wedge \gamma$	
$n + 1$	β	$\wedge\mathbf{E}, n$

assim existe uma prova com n linhas para $\Gamma \vdash \beta \wedge \gamma$, logo por **(H)**, tem-se que $\Gamma \models \beta \wedge \gamma$, mas é fácil notar pela Definição 2.26 que todo modelo de $\beta \wedge \gamma$ é modelo de β (e também de γ), o que implica que é impossível que exista um modelo para Γ que não seja modelo de β , concluído essa etapa da prova.

- Para a regra $\Rightarrow\mathbf{I}$, considere que α é a palavra $\beta \Rightarrow \gamma$, além disso, assuma inicialmente que exista uma prova de $\Gamma \cup \{\beta\} \vdash \gamma$ com exatamente n linhas, assim por **(H)**, tem-se que $\Gamma \cup \{\beta\} \models \gamma$. Dito isso, pelo Teorema 1, existe uma prova de $\Gamma \vdash \beta \Rightarrow \gamma$, sendo que tal prova tem mais de n linhas (vê a demonstração do Teorema 1). Suponha agora por absurdo que exista um modelo I_ρ de Γ que não é modelo de $\beta \Rightarrow \gamma$, assim tem-se que $I_\rho(\beta \Rightarrow \gamma) = 0$, mas isso só é possível, quando $I_\rho(\beta) = 1$ e $I_\rho(\gamma) = 0$, ou seja, só possível se I_ρ é um modelo para $\Gamma \cup \{\beta\}$ mas não é um modelo para γ , o que é um absurdo, e portanto, $I_\rho(\gamma)$ deve ser igual a 1, implicado que $I_\rho(\beta \Rightarrow \gamma) = 1$, e portanto, sendo modelo para $\{\beta \Rightarrow \gamma\}$, possibilitando concluir que $\Gamma \models \beta \Rightarrow \gamma$, o que completa mais um ponto da prova.
- Para a regra $\Rightarrow\mathbf{E}$, considere que existe uma prova de $\Gamma \vdash \alpha$ com $n + 1$ linhas da forma,

1	α_1	Premissa
\vdots	\vdots	
i	α_i	Premissa
\vdots	\vdots	
j	β	
\vdots	\vdots	
n	$\beta \Rightarrow \alpha$	
$n + 1$	α	$\Rightarrow\mathbf{E}, j, n$

assim existe uma prova de $\Gamma \vdash \beta$ e uma prova de $\Gamma \vdash \beta \Rightarrow \alpha$ com no máximo n linhas, assim por **(H)**, tem-se que $\Gamma \models \beta$ e $\Gamma \models \beta \Rightarrow \alpha$, assim pela semântica da implicação é impossível que exista um modelo de Γ que não seja modelo de α , concluído mais um passo para a demonstração.

- Para a regra $\neg\mathbf{I}$, considere que existe uma prova de $\Gamma \vdash \alpha$ onde α é uma palavra da forma $\neg\beta$ com $n + 1$ linhas da forma,

1	α_1	Premissa
\vdots	\vdots	
i	α_i	Premissa
\vdots	\vdots	
j	β	Premissa
\vdots	\vdots	
n	\perp	
$n + 1$	$\neg\beta$	$\neg\mathbf{I}, j-n$

entretanto, pela definição da regra $\neg\mathbf{I}$, essa prova só existe se, existirem duas provas $\Gamma \vdash \beta \Rightarrow \gamma$ e $\Gamma \vdash \beta \Rightarrow \neg\gamma$ com n ou menos linhas, e assim por **(H)**, tem-se que, $\Gamma \models \beta \Rightarrow \gamma$ e $\Gamma \models \beta \Rightarrow \neg\gamma$. Agora suponha por absurdo que exista um modelo I_ρ de Γ que não é modelo para $\{\neg\beta\}$, assim obrigatoriamente, I_ρ será modelo de $\{\beta\}$, o que é um absurdo, visto que $\Gamma \models \beta \Rightarrow \gamma$ e $\Gamma \models \beta \Rightarrow \neg\gamma$, e portanto, tem-se que $\Gamma \models \neg\beta$, isto é, $\Gamma \models \alpha$, o que termina essa etapa da prova.

- Para a regra $\neg\mathbf{E}$, considere que existe uma prova de $\Gamma \vdash \alpha$ com $n + 1$ linhas, mas tal prova é exatamente da forma:

1	α_1	Premissa
\vdots	\vdots	
i	α_i	Premissa
\vdots	\vdots	
n	$\neg\neg\alpha$	
$n + 1$	α	$\neg\mathbf{E}, n$

logo existe uma prova com exatamente n linhas de $\Gamma \vdash \neg\neg\alpha$, e assim por **(H)**, tem-se que, $\Gamma \models \neg\neg\alpha$, logo todo modelo de Γ é modelo para $\{\neg\neg\alpha\}$, agora pelas definições 2.26 e 2.38 é claro que todo modelo de $\{\neg\neg\alpha\}$ será também modelo de $\{\alpha\}$, consequentemente, $\Gamma \models \alpha$, concluindo mais uma etapa da demonstração.

- Para a regra $\vee\mathbf{I}$, considere que existe uma prova de $\Gamma \vdash \alpha$ com $n + 1$ linhas onde α é uma palavra da forma $\beta \vee \gamma$, assim sem perda de generalidade, existe uma prova de exatamente n linha de $\Gamma \vdash \beta$, logo por **(H)**, tem-se que, $\Gamma \models \beta$, e pelas definições 2.26 e 2.38 é claro que todo modelo de $\{\beta\}$ será também modelo de $\{\beta \vee \gamma\}$, consequentemente, $\Gamma \models \beta \vee \gamma$, ou seja, $\Gamma \models \alpha$, concluindo assim, mais uma etapa da demonstração.
- Para a regra $\vee\mathbf{E}$, considere que exista uma prova de $\Gamma \vdash \alpha$ com $n + 1$

linhas, agora pela definição da regra $\forall E$ a prova de $\Gamma \vdash \alpha$ será da forma:

1	α_1	Premissa
\vdots	\vdots	
i	α_i	Premissa
\vdots	\vdots	
j	$\beta \vee \gamma$	
k	β	
\vdots	\vdots	
$k+l$	α	
m	γ	
\vdots	\vdots	
n	α	
$n+1$	α	$\forall E, j, (k-k+l, m-n)$

mas de tal prova fica evidente que existe três provas $\Gamma \vdash \beta \vee \gamma$, $\Gamma \vdash \beta \Rightarrow \alpha$ e $\Gamma \vdash \gamma \Rightarrow \alpha$ com n ou menos linhas, logo por **(H)**, tem-se que, $\Gamma \models \beta \vee \gamma$, $\Gamma \models \beta \Rightarrow \alpha$ e $\Gamma \models \gamma \Rightarrow \alpha$. Agora suponha por absurdo que exista um modelo I_ρ de Γ que não é modelo de $\{\alpha\}$, mas como $\Gamma \models \beta \Rightarrow \alpha$ e $\Gamma \models \gamma \Rightarrow \alpha$ tem-se então pela Definição 2.26 que obrigatoriamente, $I_\rho(\beta) = I_\rho(\gamma) = 0$, o que é um absurdo, uma vez que, por **(H)** tem-se que $\Gamma \models \beta \vee \gamma$, conseqüentemente, $\Gamma \models \alpha$.

Agora desde que $\Gamma \vdash \alpha$ implica que $\Gamma \models \alpha$ por todos os casos descritos em **(B)**, **(H)** e **(P)**, pode-se concluir que a sentença, para qualquer conjunto finito $\Gamma \subseteq \mathcal{L}$ e qualquer $\alpha \in \mathcal{L}$ se $\Gamma \vdash \alpha$, então $\Gamma \models \alpha$, é de fato verdadeira. \square

Para tratar da questão da completude, ou seja, para poder exibir um teorema da completude para a lógica proposicional, antes é necessário adicionar mais alguns conceitos para a sintaxe da linguagem.

Definição 2.41 (Conjunto consistente) Um conjunto $\Gamma \subseteq \mathcal{L} - \{\perp\}$ é consistente se, e somente se, para nenhum $\alpha \in \mathcal{L} - \{\perp\}$ tem-se que $\Gamma \vdash \alpha \wedge \neg \alpha$.

Definição 2.42 (Conjunto inconsistente) Um conjunto $\Gamma \subseteq \mathcal{L} - \{\perp\}$ é inconsistente se, e somente se, existe $\alpha \in \mathcal{L} - \{\perp\}$ tal que $\Gamma \vdash \alpha \wedge \neg \alpha$.

Definição 2.43 (Conjunto maximamente consistente) Um conjunto $\Gamma \subseteq \mathcal{L} - \{\perp\}$ é dito maximamente consistente se, e somente se, para todo $\alpha \in \mathcal{L} - \{\perp\}$ as duas condições a seguir são satisfeitas:

- (a) Γ é consistente;
- (b) $\alpha \in \Gamma$ e $\neg \alpha \notin \Gamma$ ou $\neg \alpha \in \Gamma$ e $\alpha \notin \Gamma$.

Agora como dito em [40] um conjunto maximamente consistente tem a propriedade de ser o maior possível sem ser inconsistente.

Teorema 13 Qualquer conjunto consistente Γ pode ser entendido para um conjunto maximamente consistente Γ_∞ .

Prova | Antes de qualquer coisa lembre-se que a linguagem \mathcal{L} é também recursivamente enumerável (detalhes em [3]), portanto, $\mathcal{L} - \{\perp\}$ é também um conjunto recursivamente enumerável, assim as palavras de $\mathcal{L} - \{\perp\}$ podem ser distribuídas em uma sequência ordenada $\{\alpha_i\}_{i \in \mathbb{N}}$, dito isto, suponha que Γ é um conjunto consistente e defina indutivamente os seguintes conjuntos:

$$\begin{aligned}\Gamma_0 &= \Gamma \\ \Gamma_1 &= \begin{cases} \Gamma_0 \cup \{\alpha_1\}, & \text{se } \Gamma_0 \cup \{\alpha_1\} \text{ é consistente} \\ \Gamma_0 \cup \{\neg\alpha_1\}, & \text{senão.} \end{cases} \\ \Gamma_{n+1} &= \begin{cases} \Gamma_n \cup \{\alpha_{n+1}\}, & \text{se } \Gamma_n \cup \{\alpha_{n+1}\} \text{ é consistente} \\ \Gamma_n \cup \{\neg\alpha_{n+1}\}, & \text{senão.} \end{cases}\end{aligned}$$

obviamente por esta construção, para qualquer que seja $i \in \mathbb{N}$ tem-se que Γ_i será consistente. Agora considere o conjunto:

$$\Gamma_\infty = \bigcup_{i \in \mathbb{N}} \Gamma_i$$

suponha por absurdo que Γ_∞ não é um conjunto consistente, assim existe um α tal que $\Gamma_\infty \vdash \alpha \wedge \neg\alpha$, assumamos que $\alpha \wedge \neg\alpha$ corresponde a palavra α_j da sequência ordenada $\{\alpha_i\}_{i \in \mathbb{N}}$, portanto, é obvio que $\Gamma_j \vdash \alpha \wedge \neg\alpha$, o que é uma contradição, uma vez que, Γ_j é consistente, consequentemente, Γ_∞ é consistente. De forma trivial, pela construção de Γ_∞ tem-se que este atende a condição (b) da Definição 2.43. Desde que, Γ_∞ é consistente e atende a condição (b), tem-se que Γ_∞ é um conjunto maximamente consistente, o que conclui a prova. \square

Teorema 14 | Qualquer conjunto maximamente consistente Γ tem um modelo.

Prova | Ver a demonstração em [40]. \square

Lema 1 | Para todo $\alpha \in \mathcal{L}$ se $\models \alpha$, então $\vdash \alpha$.

Prova | Assumamos por absurdo que α é uma tautologia e que $\Gamma = Th(\emptyset)$ de forma que $\alpha \notin \Gamma$, logo $\Gamma \cup \{\neg\alpha\}$ é um conjunto consistente. Agora pelo Teorema 13 existe um conjunto maximamente consistente Γ_∞ gerado a partir de $\Gamma \cup \{\neg\alpha\}$ e pelo Teorema 14 existe um modelo I_ρ para o conjunto Γ_∞ , e assim por definição $I_\rho(\neg\alpha) = 1$, mas desde que α é uma tautologia tem-se que $I_\rho(\alpha) = 1$, o que é uma contradição, portanto, α é um teorema, ou seja, $\vdash \alpha$. \square

Teorema 15 | Para quaisquer $\alpha_1, \dots, \alpha_n, \alpha \in \mathcal{L}$ se $\{\alpha_1, \dots, \alpha_n\} \models \alpha$, então $\{\alpha_1, \dots, \alpha_n\} \vdash_L \alpha$.

Prova | Suponha que $\{\alpha_1, \dots, \alpha_n\} \models \alpha$ assim pela Proposição 3 tem-se que $\models \alpha_1 \Rightarrow (\dots(\alpha_n \Rightarrow \alpha))$ dessa forma pela Lema 1 tem-se que $\vdash_L \alpha_1 \Rightarrow (\dots(\alpha_n \Rightarrow \alpha))$, agora aplicando n vezes o Teorema 2 tem-se que $\{\alpha_1, \dots, \alpha_n\} \vdash_L \alpha$, o que completa a prova. \square

Vale destacar que a completude apresentada pelo teorema acima é a chamada completude fraca pois o conjunto de premissas Γ é um conjunto finito, entretanto, este resultado pode ser estendido para um conjunto de premissas infinito com mencionado em [40].

2.6 Questionário

Questão 2.1 Usando o sistema dedutivo da lógica proposicional demonstre as seguintes relações de consequência.

- (a). $\vdash P \Rightarrow (Q \Rightarrow P)$
- (b). $\{P \Rightarrow Q, Q \Rightarrow R\} \vdash P \Rightarrow R$
- (c). $\{P \Rightarrow (Q \Rightarrow R), P \Rightarrow Q\} \vdash P \Rightarrow R$
- (d). $\{(P \Rightarrow Q) \Rightarrow (P \Rightarrow R)\} \vdash P \Rightarrow (Q \Rightarrow R)$
- (e). $\{P \Rightarrow (P \Rightarrow Q)\} \vdash P \Rightarrow Q$
- (f). $\{P \Rightarrow (Q \Rightarrow R)\} \vdash Q \Rightarrow (P \Rightarrow R)$
- (g). $\{P \Rightarrow (Q \Rightarrow (R \Rightarrow S))\} \vdash R \Rightarrow (Q \Rightarrow (P \Rightarrow S))$
- (h). $\{(P \Rightarrow Q) \Rightarrow R\} \vdash P \Rightarrow (Q \Rightarrow R)$
- (i). $\{P \wedge Q\} \vdash Q \wedge P$
- (j). $\{P \wedge (Q \wedge R)\} \vdash (P \wedge Q) \wedge R$
- (k). $\{P \Rightarrow R\} \vdash (P \wedge Q) \Rightarrow R$
- (l). $\{P \Rightarrow Q\} \vdash (R \wedge P) \Rightarrow (Q \wedge R)$
- (m). $\{P \Rightarrow (Q \Rightarrow R)\} \vdash (P \wedge Q) \Rightarrow R$
- (n). $\{(P \wedge Q) \Rightarrow R\} \vdash P \Rightarrow (Q \Rightarrow R)$
- (o). $\{(P \Rightarrow Q) \Rightarrow R\} \vdash (P \wedge Q) \Rightarrow R$
- (p). $\{P \wedge (Q \Rightarrow R)\} \vdash (P \Rightarrow Q) \Rightarrow R$
- (q). $\{(P \Rightarrow Q) \wedge (P \Rightarrow R)\} \vdash P \Rightarrow (Q \wedge R)$
- (r). $\{P \Rightarrow (Q \wedge R)\} \vdash (P \Rightarrow Q) \wedge (P \Rightarrow R)$
- (s). $\{P \vee P\} \vdash P$
- (t). $\{P \vee Q\} \vdash Q \vee P$
- (u). $\{P \vee (Q \vee R)\} \vdash (P \vee Q) \vee R$
- (v). $\{(Q \vee (P \vee R)) \vee P\} \vdash R \vee (P \vee Q)$
- (w). $\{P \Rightarrow Q\} \vdash P \Rightarrow (Q \vee R)$
- (x). $\{(P \vee Q) \Rightarrow R\} \vdash P \Rightarrow R$
- (y). $\{P \vee Q, P \Rightarrow R, Q \Rightarrow S\} \vdash R \vee S$
- (z). $\{P \Rightarrow R, Q \Rightarrow R\} \vdash (P \vee Q) \Rightarrow R$

Questão 2.2 Demonstre usando o sistema dedutivo da lógica proposicional as relações de consequência.

- (a). $\{P \Rightarrow Q\} \vdash (R \vee P) \Rightarrow (Q \vee R)$
- (b). $\{P \wedge (Q \vee R)\} \vdash (P \wedge Q) \vee (P \wedge R)$
- (c). $\{(P \wedge Q) \vee (P \wedge R)\} \vdash P \wedge (Q \vee R)$

- (d). $\{P \vee (Q \wedge R)\} \vdash (P \vee Q) \wedge (P \vee R)$
- (e). $\{(P \vee Q) \wedge (P \vee R)\} \vdash P \vee (Q \wedge R)$
- (f). $\{P \wedge Q\} \vdash P \vee Q$
- (g). $\{P \wedge Q\} \vdash P \Rightarrow Q$
- (h). $\{P\} \vdash P \wedge (P \vee Q)$
- (i). $\{P \vee (P \wedge Q)\} \vdash P$
- (j). $\{P \wedge \perp\} \vdash Q$
- (k). $\{\neg P\} \vdash P \Rightarrow \perp$
- (l). $\{P \Rightarrow \perp\} \vdash \neg P$
- (m). $\{P\} \vdash \neg\neg P$
- (n). $\{\neg\neg\neg P\} \vdash \neg P$
- (o). $\{\neg\neg P\} \vdash P$
- (p). $\{P, \neg P\} \vdash Q$
- (q). $\{P \Rightarrow Q, P \Rightarrow \neg Q\} \vdash \neg P$
- (r). $\{\neg\neg P \Rightarrow Q, \neg\neg P \Rightarrow \neg Q\} \vdash \neg P$
- (s). $\{\neg P \Rightarrow Q, \neg P \Rightarrow \neg Q\} \vdash P$
- (t). $\vdash P \vee \neg P$
- (u). $\{P \Rightarrow Q, \neg P \Rightarrow Q\} \vdash Q$
- (v). $\vdash (P \Rightarrow \neg P) \Rightarrow \neg P$
- (w). $\vdash (\neg P \Rightarrow P) \Rightarrow P$
- (x). $\{\neg P \Rightarrow \neg Q, Q\} \vdash P$
- (y). $\{\neg(P \wedge Q), P\} \vdash \neg Q$
- (z). $\{\neg(P \wedge Q), Q\} \vdash \neg P$

Questão 2.3

Usando o sistema dedutivo da lógica proposicional prove que:

- (a). $\{\neg(P \wedge \neg Q), P\} \vdash Q$
- (b). $\{\neg(\neg P \wedge Q), Q\} \vdash P$
- (c). $\{\neg(P \wedge (Q \wedge R)), Q\} \vdash \neg(P \wedge R)$
- (d). $\{\neg(P \wedge T \wedge Q), \neg(R \wedge \neg T \wedge S)\} \vdash \neg(P \wedge Q \wedge R \wedge S)$
- (e). $\{P \vee Q, \neg P\} \vdash Q$
- (f). $\{\neg P \vee Q, P\} \vdash Q$
- (g). $\{P \vee Q, \neg Q\} \vdash P$
- (h). $\{P \vee \neg Q, Q\} \vdash P$
- (i). $\{P \vee (T \vee Q), R \vee (\neg T \vee S)\} \vdash (P \vee Q) \vee (R \vee S)$
- (j). $\{\neg P\} \vdash \neg(P \wedge Q)$
- (k). $\{\neg Q\} \vdash \neg(P \wedge Q)$

- (l). $\{P\} \vdash \neg(\neg P \wedge Q)$
- (m). $\{Q\} \vdash \neg(P \wedge \neg Q)$
- (n). $\{\neg(P \vee Q)\} \vdash \neg P$
- (o). $\{\neg(P \vee Q)\} \vdash \neg Q$
- (p). $\{\neg(\neg P \vee Q)\} \vdash P$
- (q). $\{\neg(P \vee \neg Q)\} \vdash Q$
- (r). $\{P \Rightarrow Q\} \vdash \neg P \vee Q$
- (s). $\{\neg P \Rightarrow Q\} \vdash P \vee Q$
- (t). $\{P \Rightarrow Q\} \vdash \neg(P \wedge \neg Q)$
- (u). $\{P \Rightarrow \neg Q\} \vdash \neg(P \wedge Q)$
- (v). $\{P, \neg Q\} \vdash \neg(P \Rightarrow Q)$
- (w). $\{\neg(P \Rightarrow Q)\} \vdash P$
- (x). $\{\neg(P \Rightarrow Q)\} \vdash \neg Q$
- (y). $\{\neg(P \Rightarrow \neg Q)\} \vdash Q$
- (z). $\{\neg P \wedge \neg Q\} \vdash \neg(P \vee Q)$

Questão 2.4 Usando o sistema dedutivo demonstre que:

- (a). Se $\{\alpha, \beta\} \vdash \gamma$, então $\{\neg(\alpha \Rightarrow \neg\beta)\} \vdash \gamma$
- (b). $\{\alpha\} \vdash \neg\neg(\alpha \Rightarrow \neg\beta) \Rightarrow \neg\beta$
- (c). Se $\vdash \alpha \Rightarrow \beta$ e $\vdash \alpha \Rightarrow \gamma$, então $\vdash \alpha \Rightarrow \neg(\beta \Rightarrow \neg\gamma)$
- (d). Se $\Gamma \vdash \alpha$, então $\Gamma \vdash \neg\alpha \Rightarrow \beta$
- (e). Se $\Gamma_1 \vdash \alpha$ e $\Gamma_2 \vdash \alpha \Rightarrow \beta$, então $\Gamma_1 \cup \Gamma_2 \vdash \beta$
- (f). Se $\Gamma \vdash \alpha \Rightarrow \beta$ e $\Gamma \vdash \neg\alpha \Rightarrow \gamma$, então $\Gamma \vdash \beta$ ou $\Gamma \vdash \gamma$
- (g). Se $\Gamma \vdash \beta$ ou $\Gamma \vdash \gamma$, então $\Gamma \vdash \neg\beta \Rightarrow \gamma$
- (h). Se $\Gamma \vdash \alpha$ ou $\Gamma \vdash \beta$, então $\Gamma \vdash \neg(\neg\alpha \wedge \neg\beta)$

Questão 2.5 Considerando o sistema axiomático L demonstre as seguintes relações de consequência.

- (a). $\{\alpha\} \vdash_L \beta \Rightarrow (\neg\alpha \Rightarrow \gamma)$
- (b). $\vdash_L (\beta \Rightarrow \alpha) \Rightarrow ((\neg\alpha \Rightarrow \beta) \Rightarrow \alpha)$
- (c). $\{\alpha, \beta\} \vdash_L \neg(\alpha \Rightarrow \neg\beta)$
- (d). $\{\neg(\alpha \Rightarrow \neg\beta)\} \vdash_L \beta$
- (e). $\{\neg(\alpha \Rightarrow \neg\beta)\} \vdash_L \alpha$
- (f). $\vdash_L (\neg\alpha \Rightarrow \beta) \Rightarrow (\neg\beta \Rightarrow \alpha)$
- (g). $\{P, \neg P\} \vdash_L Q$
- (h). $\{P \Rightarrow Q, P \Rightarrow \neg Q\} \vdash_L \neg P$
- (i). $\{\neg\neg P \Rightarrow Q, \neg\neg P \Rightarrow \neg Q\} \vdash_L \neg P$
- (j). $\{\neg P \Rightarrow Q, \neg P \Rightarrow \neg Q\} \vdash_L P$

Questão 2.6 Exiba as tableas verdades para as palavras a seguir.

- (a). $P \Rightarrow (Q \vee (R \Rightarrow P))$
- (b). $\neg(P \Rightarrow \neg(P \Rightarrow Q))$
- (c). $(P \Rightarrow Q) \Rightarrow R \Rightarrow R$
- (d). $P \Rightarrow (Q \Rightarrow P)$
- (e). $P \Leftrightarrow (\neg P \Leftrightarrow \neg(P \vee Q))$
- (f). $P \Rightarrow ((Q \wedge \neg R) \Rightarrow S)$
- (g). $((P \wedge Q) \vee (R \wedge S)) \Rightarrow (((\neg R \wedge S) \Rightarrow (S \vee \neg R)) \wedge ((S \vee \neg R) \Rightarrow (\neg R \wedge S)))$
- (h). $\perp \Rightarrow (\neg(P \vee \neg P) \wedge S)$
- (i). $(X \wedge \perp) \Rightarrow (P \Leftrightarrow \neg P)$
- (j). $\neg(\neg Q \vee \neg \neg T) \Rightarrow (R \Leftrightarrow \neg Z)$
- (k). $((P \vee Q) \wedge \neg P) \Rightarrow Q$
- (l). $(P \Rightarrow (Q \Rightarrow R)) \Rightarrow ((P \Rightarrow Q) \Rightarrow (P \Rightarrow R))$
- (m). $(P \Rightarrow P) \Rightarrow P$
- (n). $((\neg Q) \Rightarrow (\neg P)) \Rightarrow \neg(P \Rightarrow Q)$
- (o). $\neg \neg \neg P \Rightarrow \neg(Q \Leftrightarrow \neg \neg R)$
- (p). $\neg(P \wedge Q) \wedge (Q \wedge \neg \neg P)$
- (q). $(\neg R \wedge T) \vee ((S \vee \neg X) \wedge (P \vee (Q \Rightarrow \perp)))$
- (r). $(P \wedge (Q \wedge R)) \Rightarrow (R \wedge (P \wedge Q))$
- (s). $(P \Rightarrow Q) \Leftrightarrow (\neg \neg Q \vee \neg P)$
- (t). $(P \wedge Q) \Leftrightarrow \neg(Q \Rightarrow \neg P)$

Questão 2.7 Verifique se as seguintes palavras da linguagem proposicional são *equivalentes* (isto é, se têm a mesma tabela de verdade). Para cada item explique sua resposta ou preferir, mostre tautologias/contingências usando tabelas verdades ou transforme as fórmulas usando equivalências lógicas.

- (a). $p \wedge q$ e $q \wedge p$
- (b). $p \vee (q \wedge r)$ e $(p \vee q) \wedge (p \vee r)$
- (c). $p \Rightarrow q$ e $\neg p \vee q$
- (d). $p \Rightarrow q$ e $(p \Rightarrow q) \wedge (q \Rightarrow p)$
- (e). $\neg(p \vee q)$ e $\neg p \wedge \neg q$
- (f). $\neg(p \wedge q)$ e $\neg p \vee \neg q$
- (g). $p \wedge (q \vee r)$ e $(p \wedge q) \vee r$
- (h). $p \Rightarrow q$ e $\neg q \Rightarrow \neg p$
- (i). $p \Rightarrow (q \Rightarrow r)$ e $(p \wedge q) \Rightarrow r$
- (j). $(p \vee q) \Rightarrow r$ e $(p \Rightarrow r) \wedge (q \Rightarrow r)$

- (k). $p \Rightarrow q$ e $(p \vee q) \wedge \neg(p \wedge q)$
- (l). $\neg\neg p$ e p
- (m). $p \vee (q \wedge \neg q)$ e p
- (n). $p \wedge (p \Rightarrow q)$ e $p \wedge q$
- (o). $(p \Rightarrow q) \vee (q \Rightarrow p)$ e $\Rightarrow p$

Questão 2.8

Demonstre ou refute as afirmações a seguir.

- (a). O conjunto $\{\neg(\neg P \vee \neg Q) \Rightarrow Q, \neg R \vee S, \neg P\}$ tem um único modelo.
- (b). O conjunto $\{P \vee (Q \vee R), \neg P \Rightarrow (Q \vee R), Q \Rightarrow \neg(R \vee P)\}$ tem exatamente 3 diferentes modelos.
- (c). O conjunto $\{\neg P \wedge Q, P \Rightarrow Q, \neg Q \vee (\neg P \vee R)\}$ não possui um modelo.
- (d). O conjunto $\{Q \Rightarrow \neg R, P \Rightarrow (R \vee Q), S, T\}$ não possui um modelo.
- (e). Qualquer valoração é um modelo para o conjunto $\{Q \vee \neg Q, P \Rightarrow P, \neg(\neg R \wedge R)\}$.
- (f). Não existe modelos para o conjunto $\{P \wedge Q, Q \vee \neg P, Q \Rightarrow \neg S\}$.
- (g). O conjunto $\{P \Rightarrow \perp, \neg\neg Q \Rightarrow \neg P\}$ não tem nenhum modelo.
- (h). $\{\neg(P \vee Q) \Rightarrow R\} \models \neg P \Rightarrow R$
- (i). $\{P \vee Q, P \Rightarrow \neg R, \neg Q \Rightarrow S\} \models R \vee \neg S$
- (j). $\{P \Rightarrow R, Q \Rightarrow R\} \models (P \vee Q) \Rightarrow R$
- (k). $\{\neg\neg P \Rightarrow Q\} \models (R \vee P) \Rightarrow (Q \vee R)$
- (l). $\{P \wedge (Q \vee R)\} \models \neg(\neg P \vee \neg Q) \vee (P \wedge R)$
- (m). $\{(P \wedge Q) \vee (P \wedge R)\} \models P \wedge (Q \vee R)$
- (n). $\{P \vee (Q \wedge R)\} \models (P \vee Q) \wedge (P \vee R)$
- (o). $\{(P \vee Q) \wedge (P \vee R)\} \models \neg\neg P \vee (Q \wedge R)$
- (p). $\{\neg P, \neg\neg Q\} \models \neg P \Rightarrow Q$
- (q). $\{\neg P, \neg Q\} \models \neg(P \vee \neg Q)$
- (r). $\{\neg P, Q\} \models \neg(\neg P \Rightarrow Q)$
- (s). $\{P \Rightarrow \neg Q, \neg P, \neg Q \Rightarrow \neg\neg P\} \models \neg Q$
- (t). $\{\neg P \Rightarrow Q, \neg(Q \wedge P), \neg Q\} \models \neg P$

Lógicas e Teoria de Primeira Ordem

Escreve depois. . .

Demonstrações

“Mais um colchão, mais uma demonstração”.

Paul Erdős

“Um matemático é uma máquina que transforma café em teoremas”.

Paul Erdős

4.1 Introdução

Desde que, as demonstrações são figuras de interesse central no cotidiano dos matemáticos, cientistas da computação e engenheiros de software, em especial aqueles que trabalham com métodos formais, este texto irá fazer uma breve pausa no estudo da teoria dos conjuntos, para apresentar um pouco de teoria da prova ao leitor.

Este capítulo começa então com o seguinte questionamento: “Do ponto de vista da ciência da computação, qual a importância das demonstrações?” Bem, a resposta a essa pergunta pode ser dada de dois pontos de vista, um teórico (purista) e um prático (aplicado ou de engenharia).

Na perspectiva de um cientista da computação puro, as demonstrações de teoremas, proposições, lema, corolários e propriedades são a principal ferramenta para investigar os limites dos diferentes modelos de computação propostos [33, 35], assim sendo é de suma importância que o estudante de graduação em ciência da computação receba em sua formação pelo menos o básico para dominar a “arte” de provar teoremas, sendo assim preparado para o estudo e a pesquisa pura em computação e(ou) matemática.

Já na visão prática, só existe uma forma segura de garantir que um *software* está livre de erros, essa “tecnologia” é exatamente a demonstração das propriedades do *software*.

É claro que, mostrar que um *software* não possui erros exige que o *software* seja visto através de um certo nível de formalismo e rigor matemático, mas após essa modelagem, demonstrações podem garantir que um *software* não apresentará erros (quando bem especificado), e assim se algo errado ocorrer foi por fatores externos, tais como defeito no *hardware* por exemplo, e não por falha ou erros com a implementação. Este conceito é o cerne de uma área da engenharia de *software* [51], chamada métodos (ou especificações) formais, sendo essa área o ponto crucial no desenvolvimento de *softwares* para sistemas críticos [55]. Isto já mostra a grande importância de programadores e engenheiros de *software* terem em sua formação as bases para o domínio das técnicas de demonstração.

Nas próximas seções deste documento serão descritas as principais técnicas de

demonstração de interesse de matemáticos, cientistas da computação e engenheiros formais de *software*.



Atenção

Para o leitor que nunca antes teve contato com a lógica matemática, recomenda-se que antes de estudar este capítulo, o leitor deve fazer pelo menos uma leitura superficial em obras como [21, 30, 40].

Para poder falar sobre métodos de demonstração e poder então descrever como os matemáticos, lógicos e cientistas da computação justificam propriedades usando apenas a argumentação matemática, será necessário fixar algumas nomenclaturas e falar sobre alguns conceitos importantes.

Definição 4.1

(Asserção) Uma **asserção** é qualquer frase declarativa que possa ser expressa na linguagem da lógica simbólica.

Os métodos (ou estratégias) de demonstrações apresentadas neste documento seguem as ideias e a ordem de apresentação similar ao que foi exposto em [61]. Em [61] antes de apresentar as provas formais, era necessário a construção de um rascunho de prova, este rascunho possui similaridades com as demonstrações em provadores de teoremas tais como Coq [10, 49] e Lean [46], isto é, existe uma separação clara entre dados (hipótese) e os objetivos (em inglês *Goal*) que se quer demonstrar.

Neste documento por outro lado, não será utilizado a ideia de um rascunho de prova, em vez disso, será usado aqui a noção de **diagrama de blocos** [13]. Aqui tais diagramas serão encarados como as demonstrações em si, assim diferente de [61] não haverá a necessidade de escrever um texto formal após o diagrama da prova ser completado.

Sobre o diagrama de blocos é conveniente explicar sua estrutura, ele consiste de uma série de linhas numeradas de 1 até m , em cada linha está uma informação, sendo esta uma hipótese assumida como verdadeira ou deduzida a partir das informações anteriores a ela ou ainda um resultado (ou definição) válido(a) conhecido(a). Um diagrama de bloco representa uma prova, porém, uma prova pode conter n subprovas. Cada **prova** é delimitada no diagrama por um **bloco**, assim se existe uma subprova p' em uma prova p , significa que o diagrama de bloco de p' é interno ao diagrama de bloco de p . Na linha abaixo de todo bloco sempre estará a conclusão que se queria demonstrar, isto é, abaixo de cada bloco está a asserção que tal bloco demonstra.

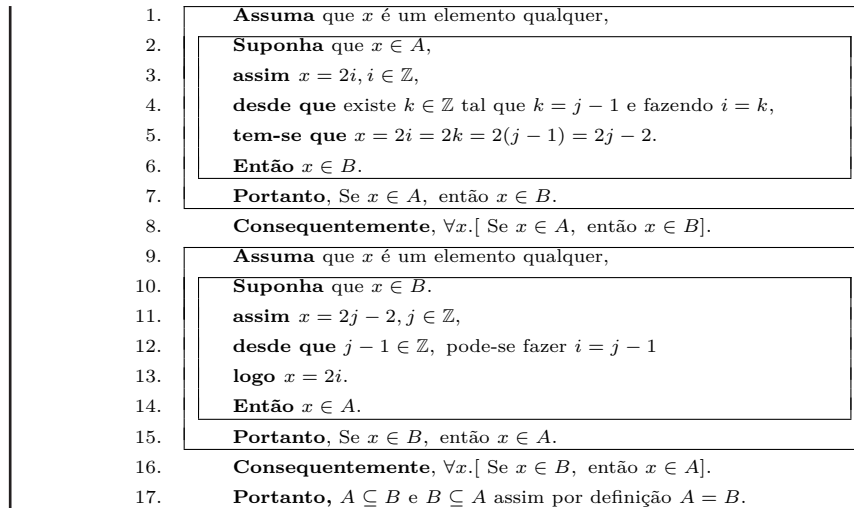
Cada linha no diagrama começa com algum termo reservado (em um sentido similar ao de palavra reservada de linguagem de programação [2, 16]) escrito em negrito¹, esses termos reservados tem três naturezas distintas: inicialização de bloco, ligação e conclusão de blocos. Tais palavras podem variar a depender do material sobre demonstrações que o leitor possa encontrar na literatura neste documento serão usando os seguintes conjuntos de palavras:

- Termos de inicialização de bloco: **Suponha**, **Deixe ser**, **Assuma** e **Considere**;
- Termos de ligação: **mas**, **tem-se que**, **então**, **assim**, **logo**, **além disso**, **desde que** e **dessa forma**;
- Termos de conclusão de bloco: **Portanto**, **Dessa forma**, **Consequentemente**, **Por contrapositiva** e **Logo por contrapositiva**.

Exemplo 4.1.1

Demonstre a asserção: Dado $A = \{x \in \mathbb{Z} \mid x = 2i, i \in \mathbb{Z}\}$ e $B = \{x \in \mathbb{Z} \mid x = 2j - 2, j \in \mathbb{Z}\}$ tem-se que $A = B$.

¹ A escrita dos termos reservados em negrito em geral será usada para que o leitor consiga identificar o que é informação último da prova e o que é apenas um artifício textual para dá melhor entendimento a demonstração.



Neste momento o exemplo anterior serve apenas para esboçar a ideia de um diagrama de bloco para uma demonstração, note que fica evidente que a depender da situação alguns termos de ligação são melhores que outros, e o mesmo também é válido para os termos de inicialização e conclusão de bloco.

Aqui não será detalhando a aplicação dos métodos de demonstração usado na demonstração do Exemplo 4.1.1, mas nas próximas seções serão apresentados cada um dos métodos de demonstração, e seguida será gradativamente apresentados exemplos para esboçar ao leitor como é usado o diagrama de blocos e relação a cada método de demonstração.

Como o leitor pode ter notado pelo diagrama de bloco no Exemplo 4.1.1, é possível enxergar o diagrama como ambiente muito similar a ideia de um programa imperativo em uma linguagem de programação estruturada (como Pascal ou C), no sentido de que, uma demonstração pode ser visto como a combinação de diversos blocos, em que os blocos respeito uma hierarquia e podem está aninhados entre si, a hierarquia dos bloco é determinar por uma indentação².

² Indentação é um termo utilizando em código fonte de um programa, serve para ressaltar, identificar ou definir a estrutura do algoritmo.

4.2 Demonstrando Implicações

Este documento irá iniciar a apresentação dos métodos de demonstração a partir das estratégias usadas para demonstrar a implicação, isto é, as estratégias usadas para provar asserção da forma: “se α , então β ”.

Definição 4.2

(Prova Direta (PD)) Dado uma asserção da forma: “se α , então β ”. A metodologia de prova direta para tal asserção consiste em supor α como sendo verdade e a partir disto deduzir β .

Esta estratégia é provavelmente a técnicas mais famosa e usada dentre todos os métodos de demonstração que existem, um conhecedor de lógica pode notar facilmente que tal estratégia nada mais é do que a regra de dedução natural chamada de introdução da implicação[40].

No que diz respeito ao diagrama tal estratégia consistem em: (1) criar um bloco, e dentro deste bloco na primeira linha irá conter a afirmação de que α está sendo assumido com uma hipótese verdadeira; (2) nas próximas n linhas irão acontecer as deduções necessárias até que na linha $n + 2$ seja deduzido o β e o bloco é fechado e (3) na linha $n + 3$ será adicionada a conclusão do bloco. A seguir serão apresentados exemplos do uso do método de demonstração direto para implicações e seu uso junto com o diagrama de bloco.

Exemplo 4.2.1

Será Provado a asserção, “**Se x é ímpar, então $x^2 + x$ é par**”, usando **PD**. A prova começa abrindo um bloco e inserido na primeira linha a hipótese de que o

antecedente x é um número ímpar é verdadeira, ou seja, tem-se:

1. Suponha que x é um número ímpar
- 2.

em seguida pode-se na linha 2 deduzir a forma de x , mudando o diagrama para:

1. Suponha que x é um número ímpar,
2. logo $x = 2k + 1, k \in \mathbb{Z}$,
- 3.

agora nas próximas duas linhas pode-se deduzir respectivamente as formas (ou valores) de x^2 e $x^2 + x$, assim o diagrama é atualizado para:

1. Suponha que x é um número ímpar,
2. logo $x = 2k + 1, k \in \mathbb{Z}$,
3. assim $x^2 = 4k^2 + 4k + 1, k \in \mathbb{Z}$,
4. dessa forma $x^2 + x = 2((2k^2 + 2k) + k + 1), k \in \mathbb{Z}$.
- 5.

note que $x^2 + x = 2((2k^2 + 2k) + k + 1)$ pode ser reescrito (por substituição) como $x^2 + x = 2j$ com $j = (2k^2 + 2k) + k + 1$, essa dedução é inserida na linha de número 5 atualizando o diagrama para:

1. Suponha que x é um número ímpar,
2. logo $x = 2k + 1, k \in \mathbb{Z}$,
3. assim $x^2 = 4k^2 + 4k + 1, k \in \mathbb{Z}$,
4. dessa forma $x^2 + x = 2((2k^2 + 2k) + k + 1), k \in \mathbb{Z}$.
5. logo $x^2 + x = 2j$ com $j = (2k^2 + 2k) + k + 1, k \in \mathbb{Z}$.
- 6.

assim pode-se então deduzir a partir da informação na linha de número 5 que $x^2 + x$ é um número par, assim o diagrama muda para a forma:

1. Suponha que x é um número ímpar,
2. logo $x = 2k + 1, k \in \mathbb{Z}$,
3. assim $x^2 = 4k^2 + 4k + 1, k \in \mathbb{Z}$,
4. dessa forma $x^2 + x = 2((2k^2 + 2k) + k + 1), k \in \mathbb{Z}$.
5. logo $x^2 + x = 2j$ com $j = (2k^2 + 2k) + k + 1, k \in \mathbb{Z}$,
6. então $x^2 + x$ por definição é um número par.
- 7.

note porém que a informação na deduzida na linha de número 6 é exatamente o consequente da implicação que se queria deduzir. Portanto, o objetivo interno ao bloco foi atingido, pode-se então fechar o bloco introduzindo abaixo dele a conclusão do bloco, ou seja, na linha de número 7 é escrito que o antecedente de fato implica no consequente, assim o diagrama fica da forma:

1. Suponha que x é um número ímpar,
2. logo $x = 2k + 1, k \in \mathbb{Z}$,
3. assim $x^2 = 4k^2 + 4k + 1, k \in \mathbb{Z}$,
4. dessa forma $x^2 + x = 2((2k^2 + 2k) + k + 1), k \in \mathbb{Z}$.
5. logo $x^2 + x = 2j$ com $j = (2k^2 + 2k) + k + 1, k \in \mathbb{Z}$,
6. então $x^2 + x$ por definição é um número par.
7. **Portanto**, Se x é ímpar, então $x^2 + x$ é par.

assim o objetivo a ser demonstrado foi atingido e, portanto, a prova está completa.

Na demonstração apresentada no Exemplo 4.2.1 as justificativas da evolução do diagrama fora apresentadas passo a passo e separadas do diagrama, isso foi adotado nesse primeiro exemplo para detalhar a evolução da demonstração ao leitor, entretanto, isso não é o padrão, o normal (que será adotado) é que a justificativa (caso necessário³) da dedução de uma linha seja inserida a direita da informação deduzida, destacada em azul. Além disso, nas justificativas das provas as palavras definição, associatividade, comutatividade serão abreviadas para DEF, ASS, COM respetivamente.

³ Quando a justificativa for trivial, não é necessário.

Exemplo 4.2.2 | Demonstração da asserção: Se $x = 4k$, então x é múltiplo de 2.

1.	Suponha que $x = 4k, k \in \mathbb{Z}$,	Hipótese
2.	assim $x = (2 \cdot 2)k, k \in \mathbb{Z}$,	Reescrita da linha 1
3.	 dessa forma $x = 2(2k), k \in \mathbb{Z}$.	ASS da multiplicação
4.	logo $x = 2i$, com $i = 2k, k \in \mathbb{Z}$.	Reescrita da linha 3
5.	então x é múltiplo de 2.	DEF de múltiplo de 2
6.	Portanto , Se $x = 4k$, então x é múltiplo de 2.	PD (linhas 1-6)

O leitor deve ter notado nos Exemplos 4.2.1 e 4.2.2 as demonstrações sempre iniciam das hipótese que estão sendo assumidas, isto é, os antecedentes das implicações, isso ocorrer por que nenhuma informação adicional (necessária) é apresentada como premissa, há caso entretanto, que as premissas são importantes para o desenvolvimento da prova, como será visto no próximo exemplo.

Exemplo 4.2.3 | Demonstração da asserção: Dado m inteiro maior ou igual que 5 e n um número impar maior que 0. Se $m = 2i + 1$, então $m + n \geq 6$.

1.	$m \geq 5, m \in \mathbb{Z}$	Premissa
2.	$n = 2j + 1, j \in \mathbb{Z}^+$	Premissa
3.	Suponha que $m = 2i + 1$,	Hipótese
4.	assim $m + n = 2(i + j + 1)$	
5.	desde que $m \geq 5$ tem-se que $i \geq 2$,	
6.	mas como $n \in \mathbb{Z}_+$ tem-se que $j \geq 0$,	
7.	assim $i + j + 1 \geq 3$,	Direto das linhas 5 e 6
8.	logo $2(i + j + 1) \geq 6$	
9.	então $m + n \geq 6$.	Reescrita da linha 8
10.	Portanto , Se $m = 2i + 1$, então $m + n \geq 6$.	PD (linhas 3-9)

Exemplo 4.2.4 | Demonstração da asserção: Dado $m, n \in \mathbb{R}$ e $3m + 2n \leq 5$. Se $m > 1$, então $n < 1$.

1.	$m, n \in \mathbb{R}$	Premissa
2.	$3m + 2n \leq 5$	Premissa
3.	Suponha que $m > 1$,	Hipótese
4.	assim $3m > 3$,	
5.	desde que $3m \leq 5 - 2n$,	
6.	tem-se que $3 < 3m \leq 5 - 2n$	Direto das linhas 4 e 5
7.	logo $3 < 5 - 2n$,	
8.	assim $3 + 2n < 5$,	
9.	então $n < 1$.	
10.	Portanto , Se $n > 1$, então $n < 1$.	PD (linhas 3-10)

Além do método de prova direta asserções que são implicações podem ser provadas por um segundo método, chamado método da contrapositiva (ou contraposição). Como dito em [43], o método da contrapositiva se baseia na equivalência semântica⁴ da expressão “Se α , então β ” com a expressão “Se não β , então não α ”. Formalmente o método de demonstração por contrapositiva é como se segue.

⁴ Para um entendimento sobre equivalência semântica ver [21, 30].

Definição 4.3

(Prova por contrapositiva (PCP)) Dado uma asserção da forma: “se α , então β ”. A metodologia de prova por contrapositiva para tal asserção consiste em demonstrar usando PD a asserção “se não β , então não α ”, em seguida concluir (ou enunciar) que a veracidade de “se α , então β ” segue da veracidade de “se não β , então não α ”.

Agora em termos do diagrama de blocos o método PCP apresenta o seguinte raciocínio de construção do diagrama: (1) abrir um bloco com a primeira linha em branco; (2) realizar em um bloco (interno) a demonstração de que “se não β , então não α ” e (3) após a conclusão deste segundo bloco, o primeiro bloco é fechado, e sua conclusão consiste na informação “se α , então β ” e a justificativa de tal informação é simplesmente a conclusão PCP das linhas i - j , onde i - j diz respeito ao intervalo contendo as linhas do bloco e da conclusão da prova de “se não β , então não α ”.



Atenção

Vale salientar que a linha em branco no início dos próximos exemplos é apenas um **fator estético** adotado, para tornar a leitura do diagrama da demonstração mais agradável. Esse recurso pode voltar a ser usado em exemplos futuros. É mais conveniente escrever, por exemplo apenas $l2$, do que ter que escrever linhas 2 nas justificativas, assim o l nas justificativas a partir deste ponto deve ser lido como “linha” ou “linhas” no caso de ser $lx - y$ onde x e y são os números.

Exemplo 4.2.5 Demonstração da asserção: Se $n! > (n + 1)$, então $n > 2$.

1.		
2.	Suponha que $n \leq 2$,	Hipótese
3.	assim $n = 0, n = 1$ ou $n = 2$	Direto da $l2$
4.	logo $n! = 1$ ou $n! = 2$,	Da $l3$ e da DEF de fatorial
5.	então $n! \leq (n + 1)$ com $n \leq 2$.	Direto de $l3$ e $l4$
6.	Portanto , Se $n \leq 2$, então $n! \leq (n + 1)$.	PD ($l2 - 5$)
7.	Por contrapositiva , Se $n! > (n + 1)$, então $n > 2$.	PCP ($l2 - 6$)

Exemplo 4.2.6 Demonstração da asserção: Se $n \neq 0$, então $n + c \neq c$.

1.		
2.	Suponha que $n + c = c$,	Hipótese
3.	assim $n + c - c = c - c$	
4.	logo , $n + 0 = 0$,	
5.	então $n = 0$.	
6.	Portanto , Se $n + c = c$, então $n = 0$.	PD ($l2 - 5$)
7.	Logo por contrapositiva , Se $n \neq 0$, então $n + c \neq c$.	PCP ($l2 - 6$)

Exemplo 4.2.7 Demonstração da asserção: Dado três números $x, y, z \in \mathbb{R}$ com $x > y$. Se $xz \leq yz$, então $z \leq 0$.

1.	$x, y, z \in \mathbb{R}$,	Premissa
2.	$x > y$,	Premissa
3.		
4.	Suponha que $z > 0$,	Hipótese
5.	então $xz > yz$,	Das $l2$ e $l4$ e da MON ^a da \cdot em \mathbb{R}
6.	Portanto , Se $z > 0$, então $xz > yz$.	PD ($l2-5$)
7.	Por contrapositiva , Se $xz \leq yz$, então $z \leq 0$.	PCP ($l3 - 6$)

^aMON aqui é a abreviatura de monotonicidade.

Exemplo 4.2.8 Demonstração da asserção: Se n^2 é par, então n é par.

1.		
2.	Suponha que n não é par,	Hipótese
3.	logo $n = 2k + 1$ com $k \in \mathbb{Z}$,	DEF de paridade
4.	assim $n^2 = 4k^2 + 4k + 1$ com $k \in \mathbb{Z}$,	
5.	dessa forma $n^2 = 2j + 1$ com $j = 2k^2 + 2k$,	Reescrita de $l4$
6.	então n^2 não é par	DEF de paridade
7.	Portanto , Se n não é par, então n^2 não é par.	PD ($l2-6$)
8.	Logo por contrapositiva , Se n^2 é par, então n é par.	PCP ($l2-6$)

4.3 Demonstração por Absurdo

⁵ *Reductio ad absurdum* em latim.

O método de demonstração por redução ao absurdo⁵ (ou por contradição) tem por objetivo provar que a asserção α junto com as premissas (se houverem) é verdadeira a partir da prova de que a suposição de que a asserção “não α ” seja verdadeira junto das mesmas premissas (mencionadas anteriormente) gera um absurdo (ou contradição). O fato deste absurdo seja gerado, permite concluir que suposição de que a asserção “não α ” seja verdadeira é ridícula, ou seja, “não α ” tem que ser falsa e, portanto, a asserção α tem que ser verdadeira.

Definição 4.4

(Prova por Redução ao Absurdo (RAA)) A metodologia para uma demonstração por redução ao absurdo de uma asserção α , consiste em supor que não α é uma hipótese verdadeira, então deduzir um absurdo (ou contradição). Em seguida concluir que dado que a partir de não α foi produzido um absurdo pode-se afirma que α é verdadeiro.

Em termos do diagrama de blocos o método RAA consiste nos seguintes passo: (1) abrir um bloco cuja primeira linha é vazia; (2) iniciar um bloco interno em que na primeira linha deste bloco o termo de inicialização do bloco (já listados anteriormente) é seguida da expressão “por absurdo” e da asserção não α ; (3) em seguida nas próximas n linhas irão acontecer as deduções necessárias até que na linha $n + 2$ seja deduzido o absurdo (ou uma contradição) e o bloco é fechado, inserido na linha $n + 3$ a informação de que “Se não α , então \perp ” e é fechado o bloco externo e (4) na linha $n + 4$ será adicionada a conclusão do bloco externo, contendo algo como “Portanto, α é verdadeiro”.



Atenção

Aqui como em muitos outros materiais será usado o símbolo \perp^a para denotar o absurdo.

^aEste símbolo também costuma ser usado na teoria de reticulados para representar o bottom nos reticulados.

O leitor um pouco mais atento perceberá que provar o asserção P usando RAA, é na verdade, realizar uma demonstração para uma asserção da seguinte forma $\neg P \Rightarrow \perp$.

Exemplo 4.3.1

Demonstração da asserção: $\sqrt{2} \notin \mathbb{Q}$.

1.		
2.	Assuma por absurdo que $\sqrt{2} \in \mathbb{Q}$,	Hipótese
3.	logo existem $a, b \in \mathbb{Z}$ tal que $\sqrt{2} = \frac{a}{b}$ e $\text{mdc}(a, b) = 1$	
4.	logo $a^2 = 2b^2$, ou seja, a^2 é par,	
5.	dessa forma $a = 2i$ com $i \in \mathbb{Z}$,	De l4 e do Exemplo 4.2.8
6.	logo $b^2 = 2i^2$ com $i \in \mathbb{Z}$,	
7.	dessa forma $b = 2j$ com $j \in \mathbb{Z}$,	De l6 e do Exemplo 4.2.8
8.	assim $\text{mdc}(a, b) \geq 2$,	De l5 e l7
9.	mas $\text{mdc}(a, b) = 1$ e $\text{mdc}(a, b) \geq 2$ é um absurdo.	Direto de l3 e l8
10.	Portanto , Se $\sqrt{2} \in \mathbb{Q}$, então \perp .	PD (l2-10)
11.	Consequentemente , $\sqrt{2} \notin \mathbb{Q}$.	RAA (l2-11)

Exemplo 4.3.2

Demonstração da asserção: Não existe solução inteira positiva não nula para a equação diofantina^a $x^2 - y^2 = 1$.

1.		
2.	Assuma por absurdo $\exists x, y \in \mathbb{Z}_+^*$ com $x^2 - y^2 = 1$,	Hipótese
3.	assim $\min(x, y) = 1$ e $(x - y)(x + y) = 1$,	
4.	logo $x - y = x + y = 1$ ou $x - y = -1$ e $x + y = -1$,	Por $x, y \in \mathbb{Z}_+^*$
5.	com $x - y = 1$ e $x + y = 1$ tem-se $x = 1$ e $y = 0$,	
6.	assim $\min(x, y) \neq 1$,	De l5
7.	com $x - y = -1$ e $x + y = -1$ segue $x = -1$ e $y = 0$,	
8.	assim $\min(x, y) \neq 1$,	De l7
9.	mas $\min(x, y) = 1$ e $\min(x, y) \neq 1$ é um absurdo.	De l3, l6 e l8.
10.	Portanto , Se $\exists x, y \in \mathbb{Z}_+^*$ tal que $x^2 - y^2 = 1$, então \perp .	PD (l2-10)
11.	Portanto , não $\exists x, y \in \mathbb{Z}_+^*$ tal que $x^2 - y^2 = 1$.	RAA (l2-10)

^aEquações diofantinas são equações polinomiais, que permite a duas ou mais variáveis assumirem apenas valores inteiros.

Equações diofantinas tem papel central para computação, assim vale mencionar aqui que um importante resultado sobre essas equações, e que possui forte impacto computabilidade, foi demonstrado pelos trabalhos de Julia Robinson (1919–1985) e Yuri Matiyasevich(1947–.) [41]. Tal resultado apresentou de forma precisa uma solução

⁶ Apresentada por David Hilbert (1862–1943) em 1900 no primeiro ICM.

ao décimo problema da lista de Hilbert⁶, de forma sucinta o resultado diz que não existe um algoritmo universal para determinar se uma equação diofantina tem raízes inteiras.

Exemplo 4.3.3

Demonstração da asserção: Se $3n + 2$ é ímpar, então n é ímpar.

1.	
2.	Suponha por absurdo que $3n + 2$ é ímpar e n é par, Hipótese
3.	logo $n = 2k, k \in \mathbb{Z}$, DEF de paridade
4.	dessa forma $3n + 2 = 2(3k + 1), k \in \mathbb{Z}$,
5.	assim $3n + 2$ é par, DEF de paridade
6.	mas $3n + 2$ ser ímpar e $3n + 2$ ser par, é um absurdo. De l2 e l5
7.	Portanto , se $3n + 2$ é ímpar e n é par, então \perp . PD (l2-7)
8.	Portanto , se $3n + 2$ é ímpar, então n é ímpar. RAA (l2-8)

4.4 Demonstrando Generalizações

Antes de falar sobre o método usado para demonstrar generalizações deve-se primeiro reforçar ao leitor o que são generalizações. Uma generalização é qualquer asserção que contenha em sua formação expressões das formas:

- (a) Para todo _____.
- (b) Para cada _____.
- (c) Para qualquer _____.

Exemplo 4.4.1

A seguintes asserções são generalizações.

- (a) Todos os cachorros são mamíferos.
- (b) Todos os números inteiros possuem um inverso aditivo.
- (c) Todos os times de futebol pernambucanos são times brasileiros.

Nos termos da lógica uma asserção é uma generalização sempre que o quantificador universal é o quantificador mais externo a da asserção.

Agora que o leitor está a par do que é uma generalização, pode-se prosseguir o texto deste documento apresentando formalmente o método de demonstração para generalizações.

Definição 4.5

(Prova de Generalizações (PG)) Para provar uma asserção da forma, “ $(\forall x)[P(x)]$ ”, em que $P(x)$ é uma asserção acerca da variável x . Deve-se assumir que a variável x assume como valor um objeto qualquer no universo do discurso de que trata a generalização, em seguida, provar que a asserção $P(x)$ é verdadeira, usando as propriedades disponível de forma genérica para os objetos do universo do discurso.

Em termos do diagrama, a prova de uma generalização começa inserido na primeira linha de um bloco a informação de que x é um objeto genérico (ou qualquer) do discurso, em seguida deve ser provado $P(x)$ é verdadeiro, caso seja necessário deve ser aberto um novos blocos para as subprovas, após demonstrar que $P(x)$ é verdadeiro para um x genérico do discurso, o bloco externo (aberto para a prova da generalização) é fechado e pode-se apresentar a conclusão de que todo objeto x do discurso $P(x)$ é verdadeiro.

Note que esse raciocínio de demonstração garante (com explicado em [61]) que a asserção P é universal sobre o universo do discurso, ou seja, garante a universalidade da asserção P .

Exemplo 4.4.2

Demonstração da asserção: $(\forall x \in \{4n \mid n \in \mathbb{N}\})[x \text{ é par}]$.

1.	Assuma que $x \in \{4n \mid n \in \mathbb{N}\}$	Hipótese
2.	dessa forma $x = 4n, n \in \mathbb{N}$,	DEF do discurso
3.	logo $x = (2 \cdot 2)n, n \in \mathbb{N}$,	Reescrita de l2
4.	dessa forma $x = 2(2n), n \in \mathbb{N}$,	ASS da \cdot
5.	assim $x = 2k, k \in \mathbb{N}$,	
6.	então x é par.	DEF de paridade
7.	Portanto , com $x \in \{4n \mid n \in \mathbb{N}\}$, tem-se que x é par.	
8.	Consequentemente , $(\forall x \in \{4n \mid n \in \mathbb{N}\})[x \text{ é par}]$.	PG (l1-7)

Exemplo 4.4.3 Demonstração da asserção: $(\forall X, Y \subseteq \mathbb{U})[\text{se } X \neq \emptyset, \text{ então } (X \cup Y) \neq \emptyset]$.

1.	Considere dois conjuntos quaisquer $X, Y \subseteq \mathbb{U}$	Hipótese
2.	Suponha que $X \neq \emptyset$,	Hipótese
3.	logo existe pelo menos um $x \in X$,	
4.	desde que $x \in X$ tem-se que $x \in (X \cup Y)$,	
5.	então $(X \cup Y) \neq \emptyset$.	
6.	Consequentemente , Se $X \neq \emptyset$, então $X \cup Y \neq \emptyset$.	PD (l2-5)
7.	Portanto , $(\forall X, Y \subseteq \mathbb{U})[\text{se } X \neq \emptyset, \text{ então } (X \cup Y) \neq \emptyset]$.	PG (l1-6)

Um erro que muitos iniciantes frequentemente cometem ao tentar provar enunciados de generalização é utilizar uma (ou mais) propriedade(s) de um elemento genérico x para provar $P(x)$, entretanto esta(s) propriedade(s) usada(s) não é (são) compartilhada(s) por todos os elementos de \mathbb{U} , isto é, apenas um subconjunto de \mathbb{U} apresenta a(s) propriedade(s) usadas, para mais detalhes sobre este tipo de erro podem ser consultados em [61].

Exemplo 4.4.4 Demonstração da asserção: $(\forall n \in \mathbb{Z})[\text{se } n > 2, \text{ então } n^2 > n + n]$.

1.	Assuma que n é um número inteiro,	Hipótese
2.	Suponha que $n > 2$,	Hipótese
3.	logo $n \cdot n > 2x$,	MON ^a da \cdot em \mathbb{Z}
4.	então $n^2 > n + n$.	Reescrita de l3
5.	Dessa forma , se $n > 2$, então $x^2 > n + n$.	PD (l2-4)
6.	Portanto , $(\forall n \in \mathbb{Z})[\text{se } n > 2, \text{ então } x^2 > n + n]$.	PG (l1-5)

^aComo antes MON significa monotonicidade.

Exemplo 4.4.5 Prova da asserção: Dado $(\forall n \in \mathbb{Z})[3(n^2 + 2n + 3) - 2n^2 \text{ é um quadrado perfeito}]$.

1.	Assuma que n é um número inteiro,	Hipótese
2.	Desde que $3(n^2 + 2n + 3) - 2n^2 = 3n^2 + 6n + 9 - 2n^2$,	
3.	mas $3n^2 + 6n + 9 - 2n^2 = n^2 + 6n + 9$,	
4.	assim $3(n^2 + 2n + 3) - 2n^2 = n^2 + 6n + 9$	De l2 e l3
5.	mas $n^2 + 6n + 9 = (n + 3)^2$,	
6.	logo $3(n^2 + 2n + 3) - 2n^2 = (n + 3)^2$,	
7.	Dessa forma , $3(n^2 + 2n + 3) - 2n^2$ é um quadrado perfeito.	Direto de l2-6
8.	Portanto , $(\forall n \in \mathbb{Z})[3(n^2 + 2n + 3) - 2n^2 \text{ é um quadrado perfeito}]$.	PG (l1-7)

4.5 Demonstrando Existência e Unicidade

Antes de falar sobre o método de demonstração existencial deve-se primeiro reforçar ao leitor o que é um enunciado existencial. Um enunciado de uma sentença do tipo existencial é qualquer asserção que inicia usando as expressões das forma seguir:

- (a) Existe um(a) _____.
- (b) Há um(a) _____.

Agora sobre a metodologia para demonstrar (provar) a existência de um objeto com um determinada propriedade, ou seja, provar que um certo objeto x satisfaz uma propriedade P , é especificada pela definição a seguir.

Definição 4.6

(Prova de existência (PE)) Para provar uma asserção da forma “ $(\exists x)[P(x)]$ ”, em que $P(x)$ é uma asserção sobre a variável x . Deve-se exibir^a um elemento específico “ a ” pertencente ao universo do discurso, e mostrar que a asserção $P(x)$ é verdadeira quando x é instanciado como sendo exatamente o elemento a , ou seja, deve-se mostrar que $P(a)$ é verdadeira.

^aOu seja, deve-se instanciar o x para algum objeto concreto do discurso.

Em relação ao diagrama de bloco, uma demonstração de existência, isto é, uma prova de uma asserção $(\exists x)[P(x)]$, irá se comportar de forma muito semelhante a uma demonstração de generalidade, as únicas mudanças significativas é que tal método inicia seu bloco com a declaração de que será atribuído um objeto **específico** em vez de considerar a variável genérica a x , ou seja, é realizado uma instanciação de um elemento. Além disso, a conclusão do bloco externo deve ser exatamente a $(\exists x)[P(x)]$, ou seja, a conclusão deverá ser a asserção existencial.

Exemplo 4.5.1

Demonstração da asserção: $(\exists n \in \mathbb{N})[n = n^2]$.

- | | | |
|----|---|--------------------------------|
| 1. | Deixe ser $n = 1$ | Instanciação |
| 2. | logo $n \cdot n = 1 \cdot n$, | MON de \cdot em \mathbb{N} |
| 3. | assim $n^2 = n$, | Reescrita da l2 |
| 4. | então $n = n^2$, | Reescrita da l3 |
| 5. | Portanto , $(\exists n \in \mathbb{N})[n = n^2]$. | PE (l1-4) |

Exemplo 4.5.2

Demonstração da asserção: $(\exists a, b \in \mathbb{I})[m^n \in \mathbb{Q}]$.

- | | | |
|-----|--|------------------|
| 1. | Deixe ser $a = \sqrt{2}$ e $b = \sqrt{2}$ | Instanciação |
| 2. | logo $a, b \in \mathbb{I}$, | Do Exemplo 4.3.1 |
| 3. | Se $\sqrt{2}^{\sqrt{2}} \in \mathbb{Q}$, | |
| 4. | então não há mais nada a ser demonstrado. | |
| 5. | Consequentemente , se $\sqrt{2}^{\sqrt{2}} \in \mathbb{Q}$, então $a^b \in \mathbb{Q}$. | PD de l3-4 |
| 6. | Se $\sqrt{2}^{\sqrt{2}} \notin \mathbb{Q}$, | |
| 7. | logo $\sqrt{2}^{\sqrt{2}} \in \mathbb{I}$, | |
| 8. | assim fazendo $c = a^b$ tem-se que $c \in \mathbb{I}$, | |
| 9. | então $c^b = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = 2$. | |
| 10. | Portanto , se $\sqrt{2}^{\sqrt{2}} \notin \mathbb{Q}$, então $c^b \in \mathbb{Q}$ com $c \in \mathbb{I}$, $c = a^b$. | PD de l6-9 |
| 11. | Portanto , $(\exists m, n \in \mathbb{I})[m^n \in \mathbb{Q}]$. | PE (l1-10) |

Exemplo 4.5.3

Demonstração da asserção: $(\exists X \subseteq \mathbb{U})[(\forall Y \subseteq \mathbb{U})[X \cup Y = Y]]$.

- | | | |
|-----|--|-------------------------------|
| 1. | Deixe ser $X = \emptyset$, | Instanciação |
| 2. | Assuma que $Y \subseteq \mathbb{U}$ | Hipótese |
| 3. | logo $y \in Y$ tem-se que $y \in (\emptyset \cup Y)$ | DEF de união |
| 4. | assim $Y \subseteq (X \cup Y)$, | De l1 e l3 |
| 5. | | |
| 6. | Suponha por absurdo que $(\emptyset \cup Y) \not\subseteq Y$ | Hipótese |
| 7. | assim tem-se que existe $z \in (\emptyset \cup Y)$ e $z \notin Y$, | |
| 8. | dessa forma $z \in \emptyset$, | De l7 |
| 9. | desde que $X = \emptyset$ é um absurdo que $z \in X$, | De l1 e da DEF de \emptyset |
| 10. | Portanto , se $(X \cup Y) \not\subseteq Y$, então \perp . | Conclusão da PD (l6-9) |
| 11. | Consequentemente , $(X \cup Y) \subseteq Y$. | Conclusão RAA (l6-10) |
| 12. | Dessa forma , $(X \cup Y) = Y$. | Direto de l4 e l11 |
| 13. | Portanto , $(\exists X \subseteq \mathbb{U})[(\forall Y \subseteq \mathbb{U})[X \cup Y = Y]]$. | PE (l1-12) |

O leitor que tenha domínio sobre a teoria ingênua dos conjuntos sabe que $(\emptyset \cup X) = X$, para qualquer conjunto X , assim poderia escrever uma prova bem mais curta (fica como exercício) do que a demonstração mostrada no Exercício 4.5.3.

Agora vale ressaltar uma importante questão, a prova de existência não garante que um único elemento do discurso satisfaça uma determinada propriedade, note que

no Exemplo 4.5.1 poderia ser substituído 1 pelo número natural 0 sem haver qualquer perca para a demonstração.

De fato, o que a prova de existência garante é que **pelo menos um** elemento dentro do discurso satisfaz a propriedade que está sendo avaliada. Uma demonstração que garante que **um e apenas um** elemento em todo discurso satisfaz uma certa propriedade é chamada de demonstração de unicidade.

Antes de falar sobre o método de demonstração de unicidade deve-se primeiro reforçar ao leitor o que é um enunciado existencial de unicidade. Basicamente tal tipo de enunciado consiste de um enunciado de existência que adiciona os termos “único” ou “apenas um” na uma sentença do tipo existencial ficando da formas:

(a) Existe apenas um(a) _____.

(b) Há apenas um(a) _____.

(c) Há somente um(a) _____.

ou ainda,

(a) Existe um(a) único(a) _____.

(b) Há um(a) único(a) _____.



Atenção

Deste ponto em diante sempre que possível será substituído a escrita “se P , então Q ” pela notação da lógica simbólica $P \Rightarrow Q$.

Definição 4.7

(Prova de unicidade (PU)) Uma prova de unicidade consiste em provar uma asserção da forma “ $(\exists x)[P(x) \wedge (\forall y)[P(y) \Rightarrow x = y]]$ ”, em que P é uma asserção sobre os elementos do discurso. Para tal primeiro deve-se demonstrar que a asserção “ $(\exists x)[P(x)]$ ” é verdadeira, e depois prova que a generalização $(\forall y)[P(y) \Rightarrow x = y]$ também é verdadeira.

Com respeito ao diagrama de blocos, uma demonstração de unicidade apresenta um diagrama similar ao de uma prova de existência, entretanto, internamente ao bloco da demonstração irá existir uma subprova para a asserção $(\forall y)[P(y) \Rightarrow x = y]$, sendo esta subprova responsável por mostrar a unicidade. Por fim após fechar o bloco mais externo deve-se enunciar a conclusão.



Atenção

Como dito em [40], é comum representar a unicidade como $(\exists!x)[P(x)]$ em vez de $(\exists x)[P(x) \wedge (\forall y)[P(y) \Rightarrow x = y]]$.

Exemplo 4.5.4

Demonstração da asserção: $(\exists!x \in \mathbb{N})[x + x = x \wedge (\forall y \in \mathbb{N})[y + y = y \Rightarrow x = y]]$.

1.	Deixe ser $x = 0$,	Instanciação
2.	logo $x + 0 = 0 + 0$,	
3.	assim $x + 0 = 0$,	
4.	dessa forma $x + x = x$.	De l1 e l3
5.	Suponha que $y \in \mathbb{N}$,	Hipótese
6.	Assuma que $y + y = y$,	Hipótese
7.	logo $y = y - y$,	
8.	assim $y = 0$,	
9.	então $y = x$,	Reescrita de l8
10.	Consequentemente, $y + y = y \Rightarrow x = y$.	PD (l6-9)
11.	Portanto, $(\forall y \in \mathbb{N})[y + y = y \Rightarrow x = y]$,	PG (l5-10)
12.	logo $x + x = x \wedge (\forall y \in \mathbb{N})[y + y = y \Rightarrow x = y]$.	Direto de l4 e l11
13.	Portanto, $(\exists x \in \mathbb{N})[x + x = x \wedge (\forall y \in \mathbb{N})[y + y = y \Rightarrow x = y]]$.	PU (l2-13)

Exemplo 4.5.5

Demonstração da asserção: $(\forall x \in \mathbb{Z})[(\exists!y \in \mathbb{Z})[x + y = 0]]$.

1.	Assuma que $x \in \mathbb{Z}$,	Hipótese
2.	Deixe ser $y = -x$,	Instanciação
3.	logo $x + y = x + (-x)$,	
4.	mas $x + (-x) = 0$,	
5.	então $x + y = 0$.	
6.	$(\exists y \in \mathbb{Z})[x + y = 0]$.	PE (I2-5)
7.	Assuma que $z \in \mathbb{Z}$,	Hipótese
8.		
9.	Suponha por absurdo que $x + z = 0$ e $z \neq y$,	Hipótese
10.	desde que $x + y = 0$ tem-se que $x + z = x + y$,	
11.	mas assim $z = y$, o que contradiz é um absurdo.	
12.	Consequentemente , se $x + z = 0$ e $z \neq -x$, então \perp .	PD (I8-10)
13.	Portanto , se $x + z = 0$, então $x = y$.	RAA (I8-11)
14.	Dessa forma $(\forall z \in \mathbb{Z})[x + z = 0 \Rightarrow z = y]$.	PG (I7-13)
15.	Portanto , $(\forall x \in \mathbb{Z})[(\exists! y \in \mathbb{Z})[x + y = 0]]$.	PU (I2-13)

4.6 Demonstração Guiada por Casos

Para realizar uma demonstração guiada por casos (ou simplesmente demonstração por casos) a estratégia empregada consiste em demonstrar cobrindo todos os casos possíveis que as premissas α_i em um enunciado podem assumir, formalmente esta metodologia de demonstração é definida como se segue.

Definição 4.8

(Prova por Casos (PPC)) Uma prova por caso, consiste em provar um enunciado da forma: Se α_1 ou \dots ou α_n , então β . Para isso é realizado os seguintes passos:

- Supor α_1 (e apenas ela) verdadeira, e demonstrar β .
- \vdots
- Supor α_n (e apenas ela) verdadeira, e demonstrar β .

A justificativa da validade da metodologia da prova por casos é que um enunciado que tenha a forma $(\alpha_1 \vee \dots \vee \alpha_n) \Rightarrow \beta$ será verdadeiro quando a conjunção da forma $(\alpha_1 \Rightarrow \beta) \wedge \dots \wedge (\alpha_n \Rightarrow \beta)$ for verdadeira, e para isso deve-se provar a validade de $(\alpha_i \Rightarrow \beta)$ para todo $1 \leq i \leq n$. Dessa forma o leitor pode notar facilmente que uma prova por casos nada mais é do que provar uma série de n implicações (se for necessário releia a Seção 4.2).

Com respeito ao diagrama de blocos uma prova por casos consiste de um diagrama que possui em seu interior n provas da forma $\alpha_i \Rightarrow \beta$ com $1 \leq i \leq n$, após todas as sub-provas serem apresentadas a última linha no diagrama mais externo irá expressar uma sentença da forma $(\alpha_1 \Rightarrow \beta) \wedge \dots \wedge (\alpha_n \Rightarrow \beta)$, então o diagrama será fechado e será escrita a conclusão do diagrama. O exemplo a seguir ilustram esse procedimento.

Exemplo 4.6.1 | Demonstração da asserção: Dado $n \in \mathbb{N}$. Se $n \leq 2$, então $n! \leq n + 1$.

1.	$n \in \mathbb{N}$	— Premissa
2.	Assuma que $n = 0$,	Hipótese
3.	desde que $0! = 1$	
4.	assim $0! \leq 1$	
5.	mas $1 = n + 1$	
6.	então $n! \leq n + 1$	
7.	Portanto , se $n = 0$, então $n! \leq n + 1$	PD (l2 – 5)
8.	Assuma que $n = 1$,	Hipótese
9.	desde que $n! = 1$	
10.	assim $n! < 2$	
11.	mas $2 = n + 1$	
12.	então $n! < n + 1$	
13.	Portanto , se $n = 1$, então $n! < n + 1$	PD (l7 – 11)
14.	Assuma que $n = 2$,	Hipótese
15.	desde que $n! = 2$	
16.	logo $n! < 3$	
17.	mas $3 = n + 1$	
18.	então $n! < n + 1$	
19.	Portanto , se $n = 2$, então $n! < n + 1$	PD (l7 – 11)
20.	Portanto , Dado $n \in \mathbb{N}$. Se $n \leq 2$, então $n! \leq n + 1$.	PPC (l1 – 19)

Exemplo 4.6.2

Demonstração da asserção: Se $x \in \mathbb{Z}$, então x^2 tem a mesma paridade de x .

1.		
2.	Assuma que $x = 2i$ com $i \in \mathbb{Z}$,	Hipótese
3.	logo $x^2 = 2(2i^2)$, com $i \in \mathbb{Z}$	
4.	então x é par	DEF de paridade
5.	Portanto , se x é par, então x^2 é par	PD (l2 – 4)
6.	Assuma que $x = 2i + 1$ com $i \in \mathbb{Z}$,	Hipótese
7.	logo $x^2 = 4i^2 + 4i + 1$, com $i \in \mathbb{Z}$	
8.	assim $x^2 = 2(2i^2 + 2i) + 1$, com $i \in \mathbb{Z}$	Reescrita
9.	então x^2 é ímpar	DEF de paridade
10.	Portanto , se x é ímpar, então x^2 é ímpar	PD (l6 – 9)
11.	Portanto , se $x \in \mathbb{Z}$, então x^2 tem a mesma paridade que x .	PPC (l1 – 10)

4.7 Outras Formas de Representação de Provas

Durante este capítulo foram apresentadas diversas metodologias para se realizar demonstrações, e para representar as provas (demonstrações) usando tais metodologias foi empregado o uso de representação por diagrama de blocos. Este documento utilizou-se dessa representação por ela ser mais amigável ao leitor iniciante na tarefa de provar teoremas.

Existem diversas outras formas de representar a demonstração de um teorema, por exemplo, em [60], se usa o conceito de tabuleiro do “jogo” da demonstração para representar as demonstrações. Por fim, vale destacar a representação das demonstrações por meio de texto formal, que consiste basicamente em descrever a prova usando um texto utilizando o máximo de formalismo matemático possível, o exemplo a seguir ilustra a representação em texto formal.

Exemplo 4.7.1

A representação por texto formal da demonstração da asserção: “Se n é par, então n^2 é par”, pode ser da seguinte forma.

Prova

Suponha que n é par, logo $n = 2k$ para algum $k \in \mathbb{Z}$, dessa forma tem-se que $n^2 = n \cdot n = 2k \cdot 2k = 4k^2 = 2(2k^2)$, mas desde que a multiplicação e potenciação são fechadas em \mathbb{Z} tem-se que existe $r \in \mathbb{Z}$ tal que $r = 2k^2$ e, portanto, $n^2 = 2r$, consequentemente, n^2 é par. \square

A representação por texto formal é em geral a maneira utilizada de fato no meio acadêmico, para mais exemplos dessa representação veja [18, 19, 22, 44, 48] e com texto em inglês é sugerido a leitura de [50, 61]. A partir deste ponto será adotado

a escrita de demonstração em texto formal, ficando assim a representação por bloco “confinada” as seções anteriores deste capítulo.

4.8 Demonstração de Suficiência e Necessidade

Na matemática (em também na computação) é comum encontrar enunciados (sejam proposições, lemas, teoremas ou propriedades de programas) da forma: “ P se, e somente se, Q ”. Provar esse tipo de enunciado consiste em provar duas sentenças implicativas em separado, sendo elas: “Se P , então Q ” e “Se Q , então P ”. A primeira sentença recebe o nome de **condição suficiente**, sua prova costuma ser rotulada no texto formal da demonstração por (\Rightarrow) . Já a segunda implicação é nomeada como **condição necessário** e na demonstração sua prova é geralmente rotulada por (\Leftarrow) . A seguir serão apresentados alguns exemplos de demonstrações deste tipo.

Exemplo 4.8.1 Considere a seguinte sentença sobre números inteiros:

n é par se, e somente se, n^2 é par”.

para demonstrar tal afirmação como mencionada anteriormente é necessário provar as condições: suficiente e necessária, a seguir é apresentado como isso será feito.

Prova (\Rightarrow) A condição suficiente é trivialmente uma conclusão obtida direta do Exemplo 4.6.2. (\Leftarrow) A prova da condição necessária foi realizada no Exemplo 4.2.8. \square

Exemplo 4.8.2 Considere a seguinte sentença sobre números inteiros:

x é divisível por 6 se, e somente se, x é divisível por 2 e por 3”.

como no exemplo anterior para demonstrar tal afirmação é preciso provar as condições, suficiente e necessária, de forma separada, e isto é feito a seguir.

Prova (\Rightarrow) Suponha que x é divisível por 6, logo existe um $i \in \mathbb{Z}$ tal que $x = 6i$, mas deste que i é um inteiro podemos reescrever x como $x = 2(3i)$ e $x = 3(2i)$, agora fazendo $j = 3i$ e $k = 2i$ tem-se que $x = 2j$ e $x = 3k$ e, portanto, por definição x é divisível por 2 e por 3. (\Leftarrow) Suponha que x é divisível por 2 e por 3, ou seja, existem $i, j \in \mathbb{Z}$ tal que $x = 2i$ e $x = 3j$, mas disso tem-se que x é par e assim por transitividade da igualdade $3j$ também é par, e disso pode-se concluir que j é um número par (a prova disso fica como exercício ao leitor), dessa forma tem-se que $j = 2n$ para algum $n \in \mathbb{Z}$ e, assim tem-se que, $x = 3j = 3(2n) = 6n$, consequentemente, x é divisível por 6. \square

Exemplo 4.8.3 Considere a seguinte sentença sobre conjuntos:

$X \cup Y \neq \emptyset$ se, e somente se, $X \neq \emptyset$ ou $Y \neq \emptyset$ ”.

como no exemplo anterior para demonstrar tal afirmação é preciso provar as condições, suficiente e necessária, de forma separada, e isto é feito a seguir.

Prova (\Rightarrow) Suponha que $X \cup Y \neq \emptyset$, logo existe um a tal que $a \in X \cup Y$, mas pela definição de união tem-se que $a \in X$ ou $a \in Y$ e, portanto, $X \neq \emptyset$ ou $Y \neq \emptyset$. (\Leftarrow) Trivial, ficando com exercício ao leitor. \square



Atenção

Em alguns textos [60, 9] a condição suficiente é chamada de “ida”. Por sua vez, a condição necessária é chamada de “volta”.

4.9 Refutações

Escrever depois. . .

4.10 Questionário

Questão 4.1

Demonstre as seguintes asserções.

- (a). Dado $a, b \in \mathbb{R}$. Se $a < b < 0$, então $a^2 > b^2$.
- (b). Dado $a, b \in \mathbb{R}$. Se $0 < a < b$, então $\frac{1}{b} < \frac{1}{a}$.
- (c). Dado $a \in \mathbb{R}$. Se $a^3 > a$, então $a^5 > a$.
- (d). Sejam $(A - B) \subseteq (C \cap D)$ e $x \in A$. Se $x \notin D$, então $x \in B$.
- (e). Sejam $a, b \in \mathbb{R}$. Se $a < b$, então $\frac{a+b}{2} < b$.
- (f). Dado $x \in \mathbb{R}$ e $x \neq 0$. Se $\frac{\sqrt[3]{x}+5}{x^2+6} = \frac{1}{x}$, então $x \neq 8$.
- (g). Sendo $a, b, c, d \in \mathbb{R}$ com $0 < a < b$ e $d > 0$. Se $ac \geq bd$, então $c > d$.
- (h). Dado $x, y \in \mathbb{R}$ e $3x + 2y \leq 5$. Se $x > 1$, então $y < 1$.
- (i). Sejam $x, y \in \mathbb{R}$. Se $x^2 + y = -3$ e $2x - y = 2$, então $x = -1$.
- (j). Se $n \in \mathbb{Z}$ e $n \in \{x \mid 4 \leq x \leq 12, x \text{ não é primo}\}$, então n é a soma de dois números primos.
- (k). Dado $n \in \mathbb{N}$. Se $n \leq 3$, então $n! \leq 2^n$.
- (l). Dado $n \in \mathbb{N}$. Se $2 \leq n \leq 4$, então $n^2 \geq 2^n$.
- (m). Se n é um inteiro par, então $n^2 - 1$ é ímpar.
- (n). Seja $n_0 \in \mathbb{N}$ e $n_1 = n_0 + 1$. Tem-se que $n_0 n_1$ é par.
- (o). Se $n \in \mathbb{Z}$, então $n^2 + n$ é par.
- (p). Se $n \in \mathbb{Z}$ e n é par, então n^2 é divisível por 4.
- (q). Para todo $n \in \mathbb{Z}$ o número $3(n^2 + 2n + 3) - 2n^2$ é um quadrado perfeito.
- (r). Dado $n \in \mathbb{Z}$. Se $x > 0$, então $x + 1 > 0$.
- (s). Se n é ímpar, então n é a diferença de dois quadrados.
- (t). Se $3n + 5 = 6k + 8$ com $k \in \mathbb{Z}$, então n é ímpar.
- (u). Se n é par, então $3n + 2 = 6k + 2$ com $k \in \mathbb{Z}$.
- (v). Se $x^2 + 2x - 3 = 0$, então $x \neq 2$.
- (w). Dado $n, n_0, n_1 \in \mathbb{Z}$. Se n_0 e n_1 são ambos múltiplos de n , então $n_0 + n_1$ é também múltiplo n .
- (x). Dado $x, y \in \mathbb{Z}$. Se xy não é múltiplo por n tal que $n \in \mathbb{Z}$, então $x + y$ é múltiplo de n .
- (y). Dado $m, n, p \in \mathbb{Z}$. Se m é múltiplo de n e n é múltiplo de p , então m é múltiplo de p .
- (z). Se x é ímpar, então $x^2 - x$ é par.

Questão 4.2

Prove que se A e $(B - C)$ são disjuntos, então $(A \cap B) \subseteq C$.

Questão 4.3 Prove que se $A \subseteq (B - C)$, então A e C são disjuntos.

Questão 4.4 Dado $x \in \mathbb{R}$ prove que:

- (a). Se $x \neq 1$, então existe $y \in \mathbb{R}$ tal que $\frac{y+1}{y-2} = x$.
- (b). Se existe um $y \in \mathbb{R}$ tal que $\frac{y+1}{y-2} = x$, então $x \neq 1$.

Questão 4.5 Considere que \mathbb{P} e $\overline{\mathbb{P}}$ representam respectivamente o conjunto dos números inteiros pares e ímpares, assim demonstre as seguintes asserções.

- (a). Para todo $x, y \in \overline{\mathbb{P}}$ tem-se que $x - y \in \mathbb{P}$.
- (b). Para todo $x, y \in \mathbb{P}$ e todo $z \in \overline{\mathbb{P}}$ tem-se que $(x + y) + z \in \overline{\mathbb{P}}$.
- (c). A soma de três elementos consecutivos de $\overline{\mathbb{P}}$ é um número múltiplo de 3.

Questão 4.6 Prove que $\sqrt{3} \notin \mathbb{Q}$.

Questão 4.7 Demonstre que: para todo $n \in \mathbb{Z}$, se $5n$ é ímpar, então n é ímpar.

Questão 4.8 Demonstre que $x^2 = 4y + 3$ não tem solução inteira.

Questão 4.9 Prove que todo número primo maior que 3 é igual a $6k + 1$ ou igual a $6k - 1$.

Questão 4.10 Considerando o conjunto dos números inteiros demonstre as seguintes asserções.

- (a). Para todo x, y, z se x divide y e x divide z , então x divide $y + z$.
- (b). Para todo x, y, z se xy divide yz e $z \neq 0$, então x divide y .

Questão 4.11 Considerando o conjunto \mathbb{R} como universo do discurso demonstre as asserções a seguir:

- (a). $(\forall x)[(\exists!y)[x^2y = x - y]]$.
- (b). $(\exists!x)[(\forall y)[xy + x - 4 = 4y]]$.
- (c). $(\forall x)[x \neq 0 \wedge x \neq 1 \Rightarrow (\exists!y)[\frac{y}{x} = y - x]]$.
- (d). $(\forall x)[x \neq 0 \Rightarrow (\exists!y)[(\forall z)[zy = \frac{z}{x}]]]$

Questão 4.12 Seja \mathbb{U} um conjunto qualquer, demonstre as seguintes asserções:

- (a). $(\exists!A \in \wp(\mathbb{U}))[(\forall B \in \wp(\mathbb{U}))[A \cup B = B]]$.
- (b). $(\exists!A \in \wp(\mathbb{U}))[(\forall B \in \wp(\mathbb{U}))[A \cap B = B]]$.

Questão 4.13 Demonstre as condições suficientes e necessárias das asserções a seguir.

- (a). Dado $x \in \mathbb{Z}$ tem-se que x é par se, e somente se, $3x + 5$ é ímpar.
- (b). Dado $x \in \mathbb{Z}$ tem-se que x é ímpar se, e somente se, $3x + 9$ é par.

- (c). Dado $x \in \mathbb{Z}$ tem-se que $x^3 + x^2 + x$ é par se, e somente se, x é par.
- (d). Dado $x \in \mathbb{Z}$ tem-se que $x^2 + 4x + 5$ é ímpar se, e somente se, x é ímpar.
- (e). Seja $x \in \mathbb{N}$ tem-se que x é ímpar se, e somente se, x^3 é ímpar.
- (f). Sejam $x, y \in \mathbb{R}$ tem-se que $x^3 + x^2y = y^2 + xy$ se, e somente se, $y = x^2$ ou $y = -x$.
- (g). Sejam $x, y \in \mathbb{R}$ tem-se que $(x + y)^2 = x^2 + y^2$ se, e somente se, $x + y = x$ ou $x + y = y$.
- (h). Dado $x \in \mathbb{Z}$ tem-se que x é múltiplo de 16 se, e somente se, x é múltiplo de 2, 4, 8 e seu dobro é múltiplo de 32.
- (i). Sejam $x, y \in \mathbb{Z}$ tem-se que $x = \text{mdc}(x, y)$ se, e somente se, $y = xn$ para algum $n \in \mathbb{Z}$.
- (j). Sejam $x, y \in \mathbb{Z}$ tem-se que $y = \text{mmc}(x, y)$ se, e somente se, y é múltiplo de $x = yn$ para algum $n \in \mathbb{Z}$.

Questão 4.14

Para cada asserção a seguir apresente uma demonstração (no caso da asserção ser verdadeira) ou uma refutação (no caso da asserção ser falsa).

- (a). Se $x, y \in \mathbb{R}$, então $|x + y| = |x| + |y|$.
- (b). Existe $x \in \mathbb{R}$ tal que $|x| = |\sqrt{x}|$.
- (c). Se $n \in \mathbb{Z}$ e $n^5 - n$ é par, então n é par.
- (d). Para todo natural n , o inteiro da forma $2n^2 - 4n + 31$ é primo.
- (e). Para todo natural n_1 e n_2 primos, o inteiro da forma $2n_1 + (n_2 - 1) + 1$ é ímpar.
- (f). Não existe nenhum número inteiro n tal que $2n^2 - 1$ seja par.
- (g). Se A e B são conjuntos quaisquer, então $\wp(A) - \wp(B) \subseteq \wp(A - B)$.
- (h). Se A e B são conjuntos quaisquer e $A \cap B = \emptyset$, então $\wp(A) - \wp(B) \subseteq \wp(A - B)$.
- (i). Se $x, y, z \in \mathbb{N}$ tal que xy, yz e xz tem a mesma paridade, então $x, y, z \in \mathbb{P}$ ou $x, y, z \in \overline{\mathbb{P}}$.
- (j). Existe um conjunto $X \subseteq \mathbb{Z}$ tal que $X \cap \mathbb{N} \neq \emptyset$ mas $X \not\subseteq \mathbb{N}$.
- (k). Existe um conjunto X tal que $\mathbb{R} \subseteq X$ e $\emptyset \in X$.
- (l). Existem dois conjuntos X_1 e X_2 com $X_1 \neq X_2, X_1 \neq \emptyset$ e $X_2 \neq \emptyset$ tal que $\mathbb{Z}_+ \subseteq X_1 \cap X_2$ mas $\mathbb{Z} \not\subseteq X_1 \cup X_2$.
- (m). Para todo $x, y \in \mathbb{Q}$ com $x < y$, existe um número irracional z para o qual $x < z < y$.
- (n). Existe um natural n tal que $\sqrt{n+1} = p$ e p é primo.
- (o). Existem dois números primos p_1 e p_2 tal que $p_1 + p_2 = 53$.
- (p). Existem dois números primos p_1 e p_2 tal que $p_1 - p_2 = 1000$.
- (q). Existem dois números primos p_1 e p_2 tal que $p_1 - p_2 = 97$.
- (r). Existem dois números primos p_1 e p_2 tal que $p_1 < p_2$ e $2p_1 + p_2^2$ é ímpar.
- (s). Dado $x, y \in \mathbb{R}$, se $x^3 < y^3$, então $x < y$.
- (t). Para todo $x \in \mathbb{R}$ tem-se que $2^x \geq x + 1$.
- (u). Existem $x, y \in \mathbb{Z}$ tal que $42x + 7y = 1$.
- (v). Se existe $x \in \mathbb{N}$ para todo $y \in \mathbb{N}$ tal que $x - y \in \mathbb{Z}$ e $x - y \notin \mathbb{N}$, então $x = 0$.

Referências Bibliográficas

- [1] J. M. Abe. *Introdução à Lógica para a Ciência da Computação*. Arte & Ciência, 2002.
- [2] A. V. AHO, M. S. LAM, R. SETHI, and J. D. ULLMAN. *Compiladores: Princípios, Técnicas e ferramentas*. Editora Pearson, 2 edition, 2007.
- [3] A. V. Aho and J. D. Ullman. *Foundations of Computer Science*. Computer Science Press, Inc., 1992.
- [4] W. AN and B. Russell. *Principia Mathematica*, 1910.
- [5] J. Avigad. Handbook of proof theory. In *Studies in Logic and the Foundations of Mathematics*, ch. Citeseer, 1998.
- [6] M. Ayala-Rincón and F. L. C. de Moura. *Fundamentos da Programação Lógica e Funcional – O princípio de Resolução e a Teoria de Reescrita*. Editora UnB, 2014.
- [7] J. M. Barreto, M. Roiseberg, M. A. F. Almeida, and K. Callozos. *Fundamentos de Matemática Aplicada à Informática*. <http://www.inf.ufsc.br/~mauro.roisenberg/ine5381/leituras/apostila.pdf>, Universidade Federal de Santa Catarina, ???–2021. Work in progress.
- [8] B. Bedregal and B. M. Acióly. *Introdução à lógica clássica para a ciência da computação*. Notas de Aula, 2007.
- [9] B. Bedregal, B. M. Acióly, and A. Lyra. *Introdução à Teoria da Computação: Linguagens Formais, Autômatos e Computabilidade*. Editora UnP, Natal, 2010.
- [10] Y. Bertot and P. Castéran. *Interactive Theorem Proving and Program Development: CoqArt: The Calculus of Inductive Constructions*. Springer Science & Business Media, 2013.
- [11] G. Boole. *An Investigation of the Laws of Thought: On which are Founded the Mathematical Theories of Logic and Probabilities*, volume 2. Walton and Maberly, 1854.
- [12] G. Boole. *The Laws of Thought*. Dover, New York (original edition 1854), 1957.
- [13] K. Broda, J. Ma, G. Sinnadurai, and A. Summers. Pandora: A reasoning toolbox using natural deduction style. *Logic Journal of the IGPL*, 15(4):293–304, 2007.
- [14] F. G. Capuano. *Elementos de eletrônica digital*. Saraiva Educação SA, 2018.
- [15] J. Carmo, P. Gouveia, and F. M. Dionísio. *Elementos de Matemática Discreta*. College Publications, 2013.
- [16] K. Cooper and L. Torczon. *Construindo Compiladores*, volume 1. Elsevier Brasil, 2017.

- [17] I. M. Copi. *Introdução à Lógica*. Mestre Jou, 1981.
- [18] V. S. Costa. Linguagens Lineares Fuzzy. Master's thesis, Programa de Pós-graduação em Sistemas e Computação, Universidade Federal do Rio Grande do Norte, UFRN, Natal, RN, 2016.
- [19] V. S. Costa. *Autômatos Fuzzy Hesitantes Típicos: Teoria e Aplicações*. PhD thesis, Programa de Pós-graduação em Sistemas e Computação, Universidade Federal do Rio Grande do Norte, UFRN, Natal, RN, 2020.
- [20] J. I. da Silva Filho. Lógica Paraconsistente e Probabilidade Pragmática no Tratamento de Incertezas. *Revista Seleção Documental*, (9):16–27, 2008.
- [21] E. de Alencar Filho. *Iniciação à Lógica Matemática*. NBL Editora, 2002.
- [22] A. A. de Lima. *Conjuntos fuzzy multidimensionais*. PhD thesis, Programa de Pós-graduação em Sistemas e Computação, Universidade Federal do Rio Grande do Norte, UFRN, Natal, RN, 2019.
- [23] J. N. de Souza. *Lógica para Ciência da Computação e Áreas Afins*. Elsevier Brasil, 2008.
- [24] F. B. Fitch. Symbolic Logic, An Introduction. *American Journal of Physics*, 21(3):237–237, 1953.
- [25] J. L. Gersting. *Fundamentos Matemáticos para Ciência da Computação*. Grupo-Gen LTC, 2021.
- [26] K. Gödel. Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I. *Monatshefte für mathematik und physik*, 38(1):173–198, 1931.
- [27] J. Halpern, Z. Manna, and B. Moszkowski. A hardware Semantics Based on Temporal Intervals. In *International Colloquium on Automata, Languages, and Programming*, pages 278–291. Springer, 1983.
- [28] A. G. Hamilton. *Logic for Mathematicians*. Cambridge University Press, 1988.
- [29] D. Harel et al. First-order Dynamic Logic. *Lecture Notes Computer Sciences*, (9):133, 1979.
- [30] L. Hegenberg. *Lógica: Cálculo Sentencial, Cálculo de Predicados, Cálculo com Igualdades*. GEN, 31 edition, 2012.
- [31] W. Hodges et al. *A Shorter Model Theory*. Cambridge university press, 1997.
- [32] B. Holdsworth and C. Woods. *Digital logic design*. Elsevier, 2002.
- [33] J. E. Hopcroft, R. Motwani, and J. D. Ullman. *Introduction to Automata Theory, Languages and Computation*. Pearson Education India, USA, 31 edition, 2008.
- [34] S. Jaskowski. On the rules of supposition in formal logic in the series. *Studia Logica: Wydawnictwo Poswiecone Logice i jej Historii*, 1934.
- [35] P. Linz. *An Introduction to Formal Languages and Automata*. Jones & Bartlett Learning, New York, 2006.
- [36] A. C. d. Lourenço, E. C. A. CRUZ, S. R. FERREIRA, and S. C. JÚNIOR. Circuitos digitais. *Sao Paulo, Erica*, 6, 1996.
- [37] C. A. Lungarzo. La Consistencia de la Lógica Intuicionista. *Tarea*, 3:119–132, 1972.
- [38] P. D. Magnus, T. Button, A. Thomas-Bolduc, R. Zach, and R. Trueman. *forall x: Calgary. An Introduction to Formal Logic*. Fall 2020, 2020.

- [39] Z. Manna and A. Pnueli. The Modal Logic of Programs. In *International Colloquium on Automata, Languages, and Programming*, pages 385–409. Springer, 1979.
- [40] J. P. Martins. *Lógica e Raciocínio*. College Publications, 2014.
- [41] Y. V. Matiyasevich, J. V. Matijasevič, Ū. V. Matiâsevič, Y. V. Matiyasevich, Y. V. Matiyasevich, M. R. Garey, and A. Meyer. *Hilbert’s tenth problem*. MIT press, 1993.
- [42] E. Mendelson. *Introduction to Mathematical Logic*. CRC press, 2009.
- [43] P. B. Menezes. *Matemática Discreta para Computação e Informática*, volume 2. Bookman, 2010.
- [44] T. R. B. Milfont. *Grafos fuzzy intervalares n-dimensionais*. PhD thesis, Programa de Pós-graduação em Sistemas e Computação, Universidade Federal do Rio Grande do Norte, UFRN, Natal, RN, 2021.
- [45] C. A. Mortari. *Introdução à Lógica*. Unesp, 2001.
- [46] L. d. Moura, S. Kong, J. Avigad, F. v. Doorn, and J. v. Raumer. The lean theorem prover (system description). In *International Conference on Automated Deduction*, pages 378–388. Springer, 2015.
- [47] M. J. Murdocca and V. P. Heuring. *Introdução à arquitetura de computadores*. Elsevier, 2001.
- [48] R. E. B. Paiva. *Uma extensão de overlaps e naBL-Álgebras para reticulados*. PhD thesis, Programa de Pós-graduação em Sistemas e Computação, Universidade Federal do Rio Grande do Norte, UFRN, Natal, RN, 2019.
- [49] B. C. Pierce, C. Casinghino, M. Gaboardi, M. Greenberg, C. Hrițcu, V. Sjöberg, and B. Yorgey. *Matemática Fundacional para Computação*. <https://softwarefoundations.cis.upenn.edu/>, University of Pennsylvania, 2007.
- [50] A. J. Pinheiro. *On algebras for interval-valued fuzzy logic*. PhD thesis, Programa de Pós-graduação em Sistemas e Computação, Universidade Federal do Rio Grande do Norte, UFRN, Natal, RN, 2019.
- [51] R. Pressman and B. Maxim. *Engenharia de Software*. McGraw Hill Brasil, 81 edição edition, 2016.
- [52] D. A. Rodrigues. *Sobre a Lógica da Verdade Pragmática em Cálculo de Sequentes*. PhD thesis, Universidade Estadual Paulista, São Paulo, Brasil, 2021.
- [53] A. Sernadas and C. Sernadas. *Fundamentos de Lógica e Teoria da Computação*. College Publications, 2012. Coleção: Cadernos de Lógica e Computação.
- [54] H. G. d. Silva. *A Lógica da Verdade Pragmática em um Sistema de Tableaux*. PhD thesis, Universidade Estadual Paulista, São Paulo, Brasil, 2018.
- [55] I. Sommerville. *Software Engineering*. Pearson, 91 edição edition, 2011.
- [56] W. Stallings. *Arquitetura e Organização de Computadores 8a Edição*. São Paulo: Prentice Hall do Brasil, 2010.
- [57] M. E. Szabo et al. *The Collected Papers of Gerhard Gentzen*, volume 74. North-Holland Amsterdam, 1969.
- [58] A. Tarski. *Logic, Semantics, Metamathematics: Papers From 1923 To 1938*. Hackett Publishing, 1983.

- [59] S. I. to Logic. Operator Precedence. Acessado em 25 de Agosto de 2024 na página http://intrologic.stanford.edu/dictionary/operator_precedence.html, 2023.
- [60] T. Tsouanas. *Matemática Fundacional para Computação*. <http://www.tsouanas.org/fmcbook>, Universidade Federal do Rio Grande do Norte, 2017–2021. Work in progress.
- [61] D. J. Velleman. *How to prove it: A structured approach*. Cambridge University Press, 2019.