

# LÓGICA E PROVA

RAUL H.C.LOPES

## 1. INTRODUÇÃO

Estas notas contêm uma formalização da lógica clássica de primeira ordem, fortemente baseada em igualdade e, por isso, comumente identificada como lógica equacional<sup>1</sup> em [2]. Alguns dos axiomas e regras de inferência introduzidos no texto de Gries Schneider [2] são apresentadas abaixo. O sistema de dedução natural também é apresentado. Ao longo do curso de *Técnicas de Busca e Ordenação* você pode usar os sistemas de prova de lógica equacional, Dedução Natural, Sequent Calculus, ou sistema de Hilbert. O importante é que use um sistema de forma coerente e apresente referência para as fontes de suas regras para que não restem dúvidas sobre quaisquer passos de suas provas.

Estas notas contêm exercícios que deverão ser entregues até à data estabelecida na página da disciplina.

**Notação 1.** O símbolo  $\triangleq$  é usado para introduzir nomes como abreviações de fórmulas, ou seja, introduzir nomes/símbolos via definiçãoológica. Por exemplo,

$$P \triangleq 0 \leq k \leq m \wedge S = (+i : 0 \leq i < k : v.i)$$

introduz o símbolo  $P$  como nome para a fórmula

$$0 \leq k \leq m \wedge S = (+i : 0 \leq i < k : v.i)$$

**Notação 2.** A definição indutiva do conjunto de fórmulas da lógica clássica pode ser encontrada em textos como [2] ou [3]. Vale notar que serão usados:

- $(\neg p)$ : negação de  $p$ .
- $(p \wedge q)$ : conjunção de  $p$  e  $q$ .
- $(p \vee q)$ : disjunção de  $p$  e  $q$ .
- $(p \Rightarrow q)$ :  $p$  implica  $q$ .
- $(p = q)$ : equivalência lógica.
- $(\forall x : Px : Qx)$ : quantificação universal: para todo  $x$ , satisfazendo  $(Px)$ ,  $(Qx)$  vale.

---

<sup>1</sup> Veja a página de David Gries para uma introdução a *equational logic*.

- $(\exists x : Px : Qx)$ : *quantificação existencial: existe algum  $x$ , satisfazendo  $(Px)$ , tal que  $(Qx)$  vale.*

**Notação 3.** *Como é usual em textos de teoria da prova, o símbolo  $\vdash$  é usado para denotar uma relação de conseqüência lógica ou dedutibilidade. Assim*

- $\Gamma \vdash \alpha$  *denota que, da conjunção das premissas contidas em  $\Gamma$ ,  $\alpha$  pode ser provada.*
- $\vdash \alpha$  *denota que  $\alpha$  é um teorema da lógica.*

**Notação 4.** *As seguintes regras, essencialmente retiradas de [1] e usadas tanto por Curry<sup>2</sup> quanto por Church, poderão ser usadas para reduzir o número de parêntesis usados em expressões aritméticas e lógicas.*

- *operadores aritméticos são mais fortes do que operadores relacionais. Assim*

$$1 + 2 = 3$$

*obviamente é uma abreviação de*

$$(1 + 2) = 3$$

- *dentre os operadores relacionais, negação é o mais forte, seguido de conjunção e disjunção e, por último, implicação e igualdade.*
- *ponto (.) e dois pontos (:) podem ser usados como marcadores para reduzir a número de parêntesis. Fim e início de expressão são marcadores com zero pontos. As regras básicas para seu uso neste texto são:*

- (1) *um marcador com mais pontos tem mais força do que um marcador com menos pontos.*

$$\text{rev.}\hat{x}\hat{y} ::= \text{rev}\hat{y}\hat{x}$$

*abrevia*

$$(\text{rev}(\hat{x}\hat{y})) = (\text{rev}(\hat{y}\hat{x}))$$

- (2) *um marcador à esquerda de um operador delimita uma expressão que se estende para a esquerda até um marcador de mais alta prioridade.*

$$x + f.y$$

*abrevia*

$$x + f(y)$$

---

<sup>2</sup>Aliás, se você tem interesse sério em **Ciência da Computação**, cedo ou tarde deveria ler [1].

- (3) *um marcador à direita de um operador delimita uma expressão que se estende para a direita até um marcador de mais alta prioridade.*
- (4) *a expressão delimitada por um marcador respeita os tipos da expressão envolvida.*

$$\text{rev}.\perp = \perp$$

abrevia

$$\text{rev}(\perp) = \perp$$

e não

$$\text{rev}(\perp = \perp)$$

*que violaria o fato de rev mapeia seqüências para seqüências.*

- (5) *um ponto amarrado a um operador relacional tem mais força do que um ponto ligado operador funcional.*

$$\text{rev}.x \text{ .}=. \text{rev}.y$$

abrevia

$$\text{rev}(x) = \text{rev}(y)$$

- (6) *um marcador mais à esquerda tem mais prioridade do que um marcador mais á direita.*

$$p \Rightarrow . q \Rightarrow . r \Rightarrow s$$

abrevia

$$p \Rightarrow (q \Rightarrow (\Rightarrow s))$$

IMPORTANTE: Estas notas não substituem o conhecimento que você adquiriu na disciplina de **Noções de lógica**.

**Definição 1.** *A seguir são apresentados teoremas da lógica de primeira ordem que são usados em diversas provas ao longo deste documento. Note que:*

- *Equivalência lógica de duas proposições é representada pela igualdade das mesmas<sup>3</sup> escrevendo*

$$p = q$$

*é usado em lugar de*

$$p \equiv q$$

---

<sup>3</sup> Textos clássicos de lógica, por exemplo [3], preferem o uso de um símbolo distinto, no caso ( $\equiv$ ) para representar equivalência lógica. Essa também é tendência seguida por [2]. É interessante notar, no entanto, que este último texto liga os sucessivos passos de uma prova, que são equivalências lógicas, usando igualdade. Por isso, eu prefiro seguir a tradição da lógica de alta ordem e tratar equivalência como igualdade de proposições.

- Regras de inferência são frequentemente introduzidas usando a notação:

$$\frac{\Gamma_0 \vdash \alpha_1, \quad \Gamma_1 \vdash \alpha_1}{\Lambda \vdash \beta}$$

que abrevia o raciocínio: se  $\Gamma_0$  é um conjunto de hipóteses a partir do qual se pode provar  $\alpha_0$  e  $\Gamma_1$  é outro conjunto de hipóteses do qual se pode provar  $\alpha_1$ , então do conjunto de hipóteses  $\Lambda$  é possível provar (deduzir)  $\beta$ .

Para exemplo mais concreto, observe a seguinte regra, apresentada como Introdução da Conjunção no sistema de Dedução Natural.

$$\frac{\vdash p, \quad \vdash q}{\vdash p \wedge q}$$

que diz que

- se  $p$  é um teorema da lógica e  $q$  é um teorema da lógica, então  $(p \wedge q)$  é um teorema da lógica;
- ou, lendo de baixo para cima, para provar que  $(p \wedge q)$  é verdadeiro (ou seja,  $\vdash (p \wedge q)$ ), prove que  $p$  é verdadeiro (ou seja,  $\vdash p$ ) e prove que  $q$  é verdadeiro (ou seja,  $\vdash q$ ).

## 2. LÓGICA VIA IGUALDADE

Nesta seção, são introduzidos os axiomas da formalização da lógica clássica usada por Dijkstra, Scholten e outros a partir dos anos 1980 e que se caracteriza por uma apresentação de provas baseada em igualdade, implicação e transitividade das mesmas e de relações da aritmética. O sistema formal chamado de lógica **E** é introduzido e detalhado nos capítulos 4 e 5 de [2].

Na apresentação das regras e axiomas da lógica valem:

- $p, q, r$  denotam fórmulas da lógica: termos de tipo (valor) booleano;
- $a, b, c, x, y, z$  denotam termos arbitrários.

**2.1. Axiomas e regras de inferência.** Os axiomas estabelecem as propriedades fundamentais de igualdade e dos valores lógicos: *true* e *false*.

- $\frac{\vdash p}{\vdash p[x := E]}$  **<substituição>**
- $\frac{\vdash a = b}{\vdash E[x := a] = E[x := b]}$  **<Leibniz>**
- $\vdash x = x$  **<reflexividade(=)>**
- $\frac{\vdash x = y}{\vdash y = x}$  **<simetria(=)>**

- $\frac{\vdash x = y, \quad \vdash y = z}{\vdash x = z}$  **transitividade(=)**
- $\frac{\vdash p, \quad \vdash p = q}{\vdash q}$  **(equanimidade)**
- $\vdash (p = q) = r \text{ .} \equiv \text{.} p = (q = r)$  **(associatividade(=))**
- $\vdash p = q = q = p$  **(simetria(=))**

A simetria da igualdade de proposições permite, pelo axioma da associatividade, deduzir

$$\vdash ((p = q) = q) = p$$

e também

$$\vdash p = (q = (q = p))$$

- $\vdash \text{true} = q = q$  **(identidade(=))**
- $\vdash \text{false} = \neg \text{true}$  **(definição(false))**
- $\vdash \neg(p = q) = (\neg p = q)$  **(distributividade( $\neg, =$ ))**

**Exercício 1.** Prove os seguintes teoremas usando apenas os axiomas já apresentados.

- (1)  $\vdash \text{true}$
- (2)  $\vdash \neg p = q \text{ .} \equiv \text{.} p = \neg q$
- (3)  $\vdash \neg \neg p = p$
- (4)  $\vdash \neg p = p = \text{false}$

Os axiomas a seguir definem as constantes lógicas  $\vee$  e  $\wedge$ .

- $\vdash (p \vee q) \vee r \text{ .} \equiv \text{.} p \vee (q \vee r)$  **(associatividade( $\vee$ ))**
- $\vdash (p \vee q) = (q \vee p)$  **(simetria( $\vee$ ))**
- $\vdash p \vee (q = r) \text{ .} \equiv \text{.} (p \vee q) = (p \vee r)$  **(distributividade( $\vee, =$ ))**
- $\vdash p \vee p = p$  **(idempotente( $\vee$ ))**
- $\vdash p \vee \neg p$  **(Excluded Middle)**
- $\vdash p \wedge q = p = q = p \vee q$  **(Golden Rule)**

**Exercício 2.** Prove os seguintes teoremas, usando apenas os axiomas já apresentados.

- (1)  $\vdash p \vee \text{true} = \text{true}$  **(Zero( $\vee$ ))**
- (2)  $\vdash p \vee \text{false} = p$  **(identidade( $\vee$ ))**
- (3)  $\vdash p \vee (q \vee r) = (p \vee q) \vee (p \vee r)$  **(lrdist( $\vee, \vee$ ))**
- (4)  $\vdash p \vee q = p \vee \neg q = p$
- (5)  $\vdash p \wedge \neg p = \text{false}$

**Exercício 3.** Defina e prove as seguintes para a conjunção: simetria, associatividade, idempotência, identidade, zero, distributividade de:  $\wedge$  sobre  $\wedge$ ,  $\wedge$  sobre  $\vee$  e  $\vee$  sobre  $\wedge$ .

**Exercício 4.** Prove as seguintes leis, usando as regras já apresentadas.

- (1)  $\vdash \neg(p \wedge q) = \neg p \vee \neg q$
- (2)  $\vdash p = q .=. (p \wedge q) \vee (\neg p \wedge q)$
- (3)  $\vdash p = q \wedge (r = p) .=. (p = q) \wedge (r = q)$

Os axiomas a seguir definem implicação( $\Rightarrow$ ).

- $\vdash p \Rightarrow q = p \vee q = q$  **\langle definição( $\Rightarrow$ ) \rangle**
- $\vdash (q \Leftarrow p) = (p \Rightarrow q)$  **\langle Conseqüência \rangle**
- $\vdash p \Rightarrow q = \neg p \vee q$  **\langle lrdéf( $\Rightarrow$ ) \rangle**
- $\vdash p \Rightarrow q = \neg q \Rightarrow p$  **\langle Contrapositiva \rangle**

**Exercício 5.** Prove os seguintes teoremas sobre implicação, frequentemente usados no processo de prova.

- (1)  $\vdash p \Rightarrow (q \Rightarrow r) .=. (p \Rightarrow q) \Rightarrow (p \Rightarrow r)$
- (2)  $\vdash p \Rightarrow (q = r) .=. (p \Rightarrow q) = (p \Rightarrow r)$
- (3)  $\vdash p \wedge q \Rightarrow r \quad p \Rightarrow (q \Rightarrow r)$
- (4)  $\vdash p \Rightarrow \text{false} .=. \neg p$
- (5)  $\vdash \text{false} \Rightarrow p .=. \text{true}$

**Exercício 6.** Defina e prove sobre reflexividade, transitividade, antissimetria, identidade e zero à direita da implicação.

**Exercício 7.** Os teoremas a seguir são muito usados no desenvolvimento de provas em geral. Prove-sos.

- (1)  $\vdash p \Rightarrow p \vee q$  **\langle Weakening \rangle**
- (2)  $\vdash p \wedge q \Rightarrow p$  **\langle Weakening \rangle**
- (3)  $\vdash p \wedge q \Rightarrow p \vee q$  **\langle Weakening \rangle**
- (4)  $\vdash p \vee (q \wedge r) \Rightarrow p \vee q$  **\langle Weakening \rangle**
- (5)  $\vdash p \wedge q \Rightarrow p \wedge (q \vee r)$  **\langle Weakening \rangle**
- (6)  $\vdash p \wedge (p \Rightarrow q) \Rightarrow q$  **\langle Modus Ponens \rangle**
- (7)  $\vdash (p \Rightarrow r) \wedge (\neg \Rightarrow r) = r$  **\langle Análise de caso \rangle**
- (8)  $\vdash (p \Rightarrow r) \wedge (q \Rightarrow r) = (p \vee q \Rightarrow r)$
- (9)  $\vdash (p \Rightarrow q) \wedge (q \Rightarrow p) = p = q$
- (10)  $\vdash (p \Rightarrow q) \Rightarrow (p \vee q \Rightarrow q \vee r)$  **\langle Monotonicidade( $\wedge$ ) \rangle**
- (11)  $\vdash (p \Rightarrow q) \Rightarrow (p \wedge r \Rightarrow q \wedge r)$  **\langle Monotonicidade( $\wedge$ ) \rangle**
- (12)  $\vdash \neg(p \vee q) = \neg p \wedge \neg q$

### 3. DEDUÇÃO NATURAL

Uma alternativa para sistemas de prova com um número elevado de axiomas como o que foi apresentado na seção anterior é o sistema de dedução natural, inventado por Gentzen [4]. Neste sistema, os axiomas válidos são introduzidos através de regras de inferência que estabelecem o significado das constantes lógicas.

**Exercício 8.** Use as regras de inferência do sistema de dedução natural, apresentadas em aula, e prove os teoremas da seção 2.

#### 4. CONCLUSÃO?

Estas notas representam um rascunho inicial de um curso de uso de lógica para prova de propriedades de programas. Elas são necessariamente incompletas e precisam de muitas correções e adições em termos de:

- novos exemplos;
- novos exercícios;
- validações usando algum assistente de prova.

Agradeço contribuições nesse sentido.

#### REFERÊNCIAS

1. Haskell B. Curry, *Foundations of mathematical logic*, Dover Publications, Inc., 1977.
2. David Gries and Fred B. Schneider, *A logical approach to discrete mathematics*, Springer-Verlag, 1993.
3. Stephen Cole Kleene, *Introduction to metamathematics*, North-Holland Publishing CO., 1964.
4. M. Szabo (ed.), *The collected papers of Gerhard Gentzen*, North-Holland, Amsterdam, 1969.