2. Noção de lógica e técnicas de demonstração

Introdução

* Lógica matemática é uma ferramenta fundamental na definição de conceitos computacionais.
* Com base no estudo da inteligência artificial são imprescindíveis conhecimentos de lógica matemática
* A lógica permite definir a noção de Teorema

Lógica

* Lógica booleana ou lógica de Boole → estudo dos princípios e métodos usados para distinguir sentenças verdadeiras de falsas (George Boole → inglês, 1815 - 1864, um dos precursores do estudo da lógica)

* Definição (proposição): uma proposição é uma construção (sentença, frase, pensamento) à qual se pode atribuir juízo (verdadeiro - V ou falso F). Notação: p.

* Para uma dada proposição p, denota-se por $V(p)$ o valor verdade (V ou F) de p.
* Proposições atômicas → são aquelas que não podem ser separadas em proposições mais simples.
* Conectivos: são operadores lógicos que permitem construir proposições mais complexas, a partir de proposições atômicas. Principais conectivos: e, ou, não, se-então e se-somente-se.

* Definição (conectivo não): dada uma proposição lógica p, o significado (semântica) da Negação $\neg p$ (ou $\sim p$) é dada pela tabela-verdade

p	$\neg p$
V	F
F	V

* Definição (conectivo e - conjunção): Dadas duas proposições lógicas p e q, a semântica da conjunção $p \wedge q$ é dada pela tabela verdade:

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

* Definição (conectivo ou - disjunção): Dadas duas proposições lógicas p e q, a semântica da disjunção p ou q é dada pela TV:

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

* Definição (conectivo se-então - condição): Dadas duas proposição lógicas p e q, a semântica da condição $p \rightarrow q$ é dada pela TV:

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

* Definição (conectivo se-somente-se - bicondição): Dadas duas proposições lógicas p e q, a semântica da Bicondição $p \leftrightarrow q$ é dada pela T.V:

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

* Fórmulas lógicas → são as palavras da linguagem lógica. É uma sentença lógica corretamente construída sobre o alfabeto cujos símbolos são conectivos ($\wedge$, $\vee$, $\rightarrow$, etc), parenteses, identificadores (p, q, r, etc), constantes, etc

* Para n fórmulas atômicas (não constantes), → a tabela verdade (T.V) terá 2^n linhas para expressar todas as combinações possíveis de valores lógicos.

* Definição (Tautologia e Contradição): Seja W uma fórmula. Então:
— W é dita uma tautologia se W é V para todas as combinações possíveis de valores de sentenças variáveis
— W é dita uma contradição se W é F para todas as combinações possíveis de valores de sentenças variáveis

* Definição (relação de implicação): Sejam p e q duas fórmulas. Então p implica q ($p \Rightarrow q$) se e somente se $p \rightarrow q$ é uma tautologia

— A relação de implicação está diretamente relacionada com o conceito de teorema

* Definição (relação de equivalência): Sejam p e q duas fórmulas. Então p é equivalente a q ($p \Leftrightarrow q$) se e somente se $p \leftrightarrow q$ é uma tautologia

— A relação de equivalência permite definir a noção de "mesmo significado" entre duas fórmulas (sintaticamente) diferentes
— Alternativamente, p é equivalente a q se a tabela verdade da fórmula p é igual a tabela verdade de q.

— Bicondição x condição: $\underbrace{p \leftrightarrow q \Leftrightarrow (\overset{\text{"ida"}}{p \rightarrow q}) \wedge (\overset{\text{"volta"}}{q \rightarrow p})}$

uma bicondição: p se e somente se q é equivalente a se p então q e se q então p (duas condições)

mesmas tabelas verdades

— Contraposição: $p \rightarrow q \Longleftrightarrow \neg q \rightarrow \neg p$
— Redução ao absurdo: $p \rightarrow q \Leftrightarrow p \wedge \neg q \rightarrow F$

* Definição (proposição sobre um conjunto): Seja A um conjunto, uma proposição sobre A é uma proposição cujo valor lógico depende do elemento $x \in A$ considerado

— Uma proposição p que descreve alguma propriedade de um elemento $x \in A$ é usualmente denotada por: $p(x)$

— <u>Conjunto verdade de p:</u> $\{x \in A \,/\, p(x) \text{ é verdadeira}\}$

— <u>Conjunto falsidade de p:</u> $\{x \in A \,/\, p(x) \text{ é falsa}\}$

— Uma proposição p sobre A é uma:

- <u>Tautologia</u> se $p(x)$ é verdadeira para qualquer $x \in A$, ou seja, o conjunto verdade é A.
- <u>Contradição</u> se $p(x)$ é falsa para qualquer $x \in A$, ou seja, o conjunto falsidade é A.

* Definição (<u>quantificador universal, quantificador existencial</u>): Seja $p(x)$ uma proposição lógica sobre um conjunto A. Então:

— <u>Quantificador universal</u>: a proposição $(\forall x \in A)\, p(x)$ é:

- V, se o conjunto verdade for igual ao conjunto A;
- F, caso contrário

— Quantificador existencial: a proposição $(\exists x)\, p(x)$ é:

- V, se o conjunto verdade for não vazio;
- F, caso contrário

— Existe pelo menos um x; existe um único x: $\exists! x$

$$(\exists! x)\, p(x) \Leftrightarrow (\exists x)\, p(x) \wedge (\forall x)(\forall y)((p(x) \wedge p(y) \rightarrow x = y))$$

— Negação de proposições quantificadas:

$$\neg((\forall x \in A)\, p(x)) \Leftrightarrow (\exists x \in A)\, \neg p(x)$$

$$\neg((\exists x \in A)\, p(x)) \Leftrightarrow (\forall x \in A)\, \neg p(x)$$

Técnicas de demonstração

* Um <u>Teorema</u> é uma proposição do tipo:

$$p \rightarrow q$$

a qual prova-se ser V sempre (tautologia), ou seja, que:

$$\underset{\text{hipótese}}{p} \Rightarrow \underset{}{q} \leftarrow \text{tese ou conclusão}$$

— Corolário → teorema que é consequência quase direta de um outro já demonstrado
— Lema → é um teorema auxiliar que possui um resultado importante para a prova de um outro.
— Um teorema pode ser visto com um algoritmo que, prova-se, sempre funciona.
— Definição intuitiva de algoritmo (procedimento efetivo ou função computável): Uma sequência finita de instruções, as quais podem ser realizadas mecanicamente, em um tempo finito.
— Principais técnicas de demonstrações para provar que $p \to q$ é uma tautologia ($p \Rightarrow q$): prova direta, prova por contraposição, prova por redução ao absurdo (ou prova por absurdo) e prova por indução
— Para mostrar que $(\forall x \in A)\, p(x)$ → é necessário provar que $p(x)$ é V para todo o $x \in A$ (não basta provar para um $a \in A$)
— Para mostrar que $(\exists x \in A)\, p(x)$ → basta provar que existe pelo menos um $a \in A$ tal que $p(a)$ é V.
— Demonstrar $p \Leftrightarrow q$ é provar $(p \Rightarrow q) \wedge (q \Rightarrow p)$

* Definição (prova direta): Uma prova é dita prova direta ou demonstração direta quando pressupõe V a hipótese e, a partir desta, prova ser V a tese (conclusão)

* Definição (prova por contraposição): Uma prova é dita prova por contraposição ou demonstração por contraposição quando, para provar $p \Rightarrow q$, prova-se $\neg q \Rightarrow \neg p$, pois são formas equivalentes (a prova $\neg q \Rightarrow \neg p$ é feita por prova direta.

* Definição (prova por redução ao absurdo): Uma prova é dita prova por redução ao absurdo ou prova por absurdo quando a prova $p \Rightarrow q$ consiste em supor a hipótese p V, supor a negação da tese $\neg q$ V e concluir uma contradição (F)

— A prova por contraexemplo é um tipo de prova onde para demonstrar que $(\forall x \in A)\, p(x)$, mostra-se que $(\exists a \in A) \sim p(x)$ (ou seja, encontra-se um exemplo que viola a afirmação $(\forall x \in A)\, p(x)$. É um tipo que demonstração por absurdo (ocorre $q \wedge \neg q$ que é uma contradição)

* Algumas implicações importantes:

— Adição: $p \Rightarrow p \vee q$

— Simplificação: $p \wedge q \Rightarrow p$

* Algumas equivalências importantes

— Idempotência: $p \wedge p \Leftrightarrow p$; $p \vee p \Leftrightarrow p$

— Comutativa: $p \wedge q \Leftrightarrow q \wedge p$; $p \vee q \Leftrightarrow q \vee p$

— Associativa: $p \wedge (q \wedge r) \Leftrightarrow (p \wedge q) \wedge r$; $p \vee (q \vee r) \Leftrightarrow (p \vee q) \vee r$

— Distributiva: $p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r)$; $p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r)$

— Dupla negação: $\neg\neg p \Leftrightarrow p$

— De Morgan: $\neg(p \wedge q) \Leftrightarrow \neg p \vee \neg q$; $\neg(p \vee q) \Leftrightarrow \neg p \wedge \neg q$

— Absorção: $p \wedge (p \vee q) \Leftrightarrow p$; $p \vee (p \wedge q) \Leftrightarrow p$

* Conectivos EXOR e NAND:

x	y	x EXOR y	x NAND y
V	V	F	F
V	F	V	V
F	V	V	V
F	F	F	V

* Todos os conectivos podem ser expressos usando-se somente os conectivos $\neg$ e $\wedge$