

Matemática Discreta

Aula 1

Sumário

Apresentação.

Capítulo 1: A lógica de primeira ordem e demonstração automática

- Introdução
- Lógica proposicional: Fórmula proposicionais, Interpretação de fórmulas, tautologia, fórmulas consistentes, fórmulas equivalentes.

Docente: Maria Elisa Carrancho Fernandes

Email: maria.elisa@ua.pt

Avaliação de Matemática Discreta:

1º teste 29 de Março

2º teste na época de exames

OT

2ª feira 18-19;

3ª feira 19-20 (online)

5ª feira 18-19

Programa

1. Lógica de primeira ordem e demonstração automática
2. Princípios de enumeração combinatória
3. Agrupamentos e Identidades Combinatórias
4. Recorrência e Funções Geradoras
5. Elementos de Teoria dos Grafos

O que é um proposição?

Na lógica proposicional, uma **proposição** é uma afirmação que apenas toma o valor verdadeiro ou falso, mas não os dois ao mesmo tempo. Temos então alguns exemplos de proposições:

- Um número primo ímpar p é soma de dois quadrados se e só se p tem o resto 1 na divisão por 4.
- $\sqrt{2}$ é um número racional.
- $1 + 1 = 3$ e 11 é um número primo.
- A hipótese de Riemann é falsa ou está a chover.
- Se o S. L. Benfica é campeão, então o F. C. Porto não é campeão.

A partir deste momento, podemos fazer a distinção entre dois tipos de proposições:

- **atómicas**: proposições onde o valor de verdade é dado pelo contexto ou escolhido livremente.
- **compostas**: proposições compostas por outras proposições, ligadas pelos conectivos, onde o valor de verdade depende do valor de verdade das componentes.

- \wedge representará a **conjunção** (« ... e ... »);
- \vee representará a **disjunção** (« ... ou ... »);
- \neg representará a **negação** (« não ... »);
- \rightarrow representará a **implicação** ou **condicional** (« Se ... então ... »);
- \leftrightarrow representará a **dupla implicação** ou **equivalência** (« ... se e só se ... »).

As **fórmulas proposicionais** podem então ser definidas indutivamente de acordo com as regras que abaixo se apresentam:

1. cada variável é uma fórmula e \perp and \top são fórmulas.

2. Se φ e ψ são fórmulas, então as expressões

$$(\neg\psi), \quad (\varphi \wedge \psi), \quad (\varphi \vee \psi), \quad (\varphi \rightarrow \psi), \quad (\varphi \leftrightarrow \psi)$$

são fórmulas.

Folha 0

1. Sejam p, q, r variáveis que representam as proposições

p : *Sou responsável;*

q : *Passo a Matemática Discreta;*

r : *Vou de férias para as Bermudas.*

Traduza as frases seguintes por meio de fórmulas proposicionais.

- a) Se passar a Matemática Discreta, vou de férias para as Bermudas.
- b) Para ir de férias para as Bermudas é suficiente que eu seja responsável.
- c) Passo a Matemática Discreta só se for responsável.
- d) Para passar a Matemática Discreta é necessário que eu seja responsável.
- e) Se passar a Matemática Discreta então vou de férias para as Bermudas caso seja responsável.

Definição 1.1.7. Uma **valoração** (ou **interpretação**) de um conjunto V de variáveis proposicionais é uma função $v: V \rightarrow \{0, 1\}$, onde 0 representa o valor lógico «falso» e 1 representa o valor lógico «verdadeiro».

Nota 1.1.8. Como visto anteriormente, os símbolos \perp e \top representam proposições atómicas especiais. Para qualquer valoração v , vamos convencionar $v(\top) = 1$ e $v(\perp) = 0$.

Exercício: Qual será o valor de verdade da seguinte formula?

$$((p \rightarrow (q \wedge r)) \leftrightarrow (\neg p \vee q))$$

Definição 1.1.13. Uma fórmula diz-se:

- uma **tautologia** (ou **fórmula válida**) quando tiver o valor lógico 1 para qualquer interpretação;
- uma **contingência** (ou **fórmula consistente**) se existir uma interpretação com valor lógico 1;
- uma **contradição** (ou **inconsistência**) quando não for uma consistência, ou seja, quando tiver valor lógico 0 para qualquer interpretação.

Definição 1.1.15. Duas fórmulas φ e ψ dizem-se **equivalentes lógicas** ($\varphi \equiv \psi$) quando a fórmula $\varphi \leftrightarrow \psi$ é uma tautologia.

Tautologias

$$(p \vee q) \equiv (q \vee p)$$

$$(p \wedge q) \equiv (q \wedge p)$$

$$((p \wedge q) \wedge r) \equiv (p \wedge (q \wedge r))$$

$$((p \vee q) \vee r) \equiv (p \vee (q \vee r))$$

$$(p \wedge p) \equiv p$$

$$(p \vee p) \equiv p$$

$$(p \wedge \top) \equiv p$$

$$(p \vee \perp) \equiv p$$

$$(p \wedge \perp) \equiv \perp$$

$$(p \vee \top) \equiv \top$$

$$(p \wedge (q \vee r)) \equiv (p \wedge q) \vee (p \wedge r)$$

$$(p \vee (q \wedge r)) \equiv (p \vee q) \wedge (p \vee r)$$

$$\neg(p \vee q) \equiv (\neg p \wedge \neg q)$$

$$\neg(p \wedge q) \equiv (\neg p \vee \neg q)$$

$$\neg\neg p \equiv p$$

Exercício: Existe uma formula φ com esta tabela de verdade?

p	q	r	φ
0	0	0	1
0	0	1	0
0	1	0	0
0	1	1	1
:	:	:	:

Definição 1.1.19. Uma fórmula φ é dita um **literal** se φ for uma variável ou a negação de uma variável.

Teorema 1.1.20. Para cada $j \in J$ (com J um subconjunto de índices), seja L_j um literal. Então, são equivalentes as seguintes afirmações:

- i) $\bigvee_{j \in J} L_j$ é uma tautologia.
- ii) $\bigwedge_{j \in J} L_j$ é uma contradição.
- iii) Existem índices distintos $j_1, j_2 \in J$ tais que $L_{j_1} = \neg L_{j_2}$.

Forma Normal Conjuntiva

Definição 1.1.21. Dizemos que uma fórmula φ está na **forma normal conjuntiva (FNC)** quando $\varphi = \bigwedge_{i \in I} \varphi_i$ (para algum subconjunto de índices I) e onde cada φ_i é da forma $\bigvee_{j \in J} L_j$ (para algum subconjunto de índices J), com L_j literais. Nestas circunstâncias, diremos que as componentes φ_i serão **\vee -cláusulas**.

Nota 1.1.22. Muitas das vezes, consideramos ainda a forma normal conjuntiva dual, a **forma normal disjuntiva (FND)**. Neste caso, uma fórmula φ estará nessa forma quando $\varphi = \bigvee_{i \in I} \varphi_i$, onde cada φ_i da forma $\bigwedge_{j \in J} L_j$, com L_j literais.

Exemplo 1.1.23. Consideremos as variáveis proposicionais p, q, r .

- $(p \vee q) \wedge (p \vee r) \wedge \neg r$ é uma FNC.
- $(p \wedge q) \vee (p \wedge r) \vee \neg r$ é uma FND.
- $p \wedge q \wedge r$ é uma FNC e uma FND.
- $(p \wedge (q \vee r)) \vee q$ não é nem FNC, nem FND.

Teorema 1.1.25. *Toda a fórmula da lógica proposicional é equivalente a uma fórmula na FNC (FND).*

Teorema 1.1.26. *Uma fórmula na FNC é uma tautologia se e só se cada uma das suas clausulas for uma tautologia. Dualmente, uma fórmula na FND é uma contradição se e só se cada uma das suas clausulas for uma contradição.*

Exercício: Coloque φ na FNC?

$$\varphi = ((p \leftrightarrow q) \rightarrow (r \rightarrow s)) \wedge (q \rightarrow \neg(p \wedge r))$$

Matemática Discreta

Aula 2

Folha 0

2. Usando tautologias apropriadas, transforme as seguintes fórmulas na forma normal conjuntiva.

- a) $p \vee (q \wedge (\neg p));$
- b) $\neg((\neg p) \wedge (\neg q));$
- c) $(p \wedge q) \vee (p \wedge (\neg q)).$
- d) $(q \wedge \neg p \wedge r) \vee (\neg p \wedge \neg q).$

Sumário

- Conjuntos de fórmulas consistentes.
- Consequência semântica.
- Dedução.
- O método de resolução (lógica proposicional)

Conjunto Consistente

Definição 1.1.29. Um conjunto de fórmulas $\{\varphi_1, \dots, \varphi_n\}$ dir-se-á **consistente** quando existir uma interpretação que é modelo de todas as fórmulas em $\{\varphi_1, \dots, \varphi_n\}$, i.e., se existir uma interpretação de tal forma a que todas as fórmulas do conjunto sejam verdadeiras.

Exemplo 1.1.30. Consideremos as variáveis proposicionais p, q e um conjunto de fórmulas $\Gamma = \{\neg p, p \rightarrow q, q\}$. Rapidamente conseguimos ver que Γ é consistente: basta considerar a valoração tal que $p \mapsto 0$ e $q \mapsto 1$.

Consequência Semântica

Definição 1.1.32. Uma fórmula ψ diz-se **consequência semântica** (ou **consequência lógica**) das fórmulas $\varphi_1, \dots, \varphi_n$ quando, para toda a valoração, se $\varphi_1, \dots, \varphi_n$ têm valor 1, então ψ tem valor 1. Neste caso, escrevemos $\varphi_1, \dots, \varphi_n \models \psi$.

Teorema 1.1.34. *Dadas fórmulas $\varphi_1, \dots, \varphi_n$ e ψ , temos que $\varphi_1, \dots, \varphi_n \models \psi$ se e só se $((\varphi_1 \wedge \dots \wedge \varphi_n) \rightarrow \psi)$ for uma tautologia.*

Exemplo 1.1.33. Vamos verificar que $q \vee \neg p$ é consequência de $p \vee q$ e $p \rightarrow q$, ou seja, que $p \vee q, p \rightarrow q \models q \vee \neg p$.

Consequência Sintática

Definição 1.1.36. Uma fórmula ψ diz-se **consequência sintáctica** das fórmulas $\varphi_1, \dots, \varphi_n$ se, a partir destas, existir uma **prova (dedução)** de ψ (por aplicação das regras de inferência anteriormente introduzidas). Neste caso, escrevemos $\varphi_1, \dots, \varphi_n \vdash \psi$.

Teorema da Correcção diz-nos que «tudo o que se prova é válido», i.e., que se $\Gamma \vdash \psi$, então $\Gamma \models \psi$. Já o Teorema da Completude diz-nos que «tudo o que é válido se consegue provar», ou seja, que se $\Gamma \models \psi$, então $\Gamma \vdash \psi$.

Teorema 1.1.42. Seja ψ uma fórmula e Γ um conjunto de fórmulas. Então $\Gamma \models \psi$ se e só se $\Gamma \cup \{\neg\psi\}$ é inconsistente.

$$\frac{\neg\psi \vee \theta \quad \psi \vee \varphi}{\theta \vee \varphi} \text{ (Res)}$$

Em particular, se tivermos $\theta = \perp$ e $\theta = \varphi = \perp$, conseguimos derivar, respectivamente

$$\frac{\neg\psi \quad \psi \vee \varphi}{\varphi} \quad \text{e} \quad \frac{\neg\psi \quad \psi}{\perp}$$

Teorema 1.1.43. Para cláusulas $\varphi_1, \dots, \varphi_n$, o conjunto $\Gamma = \{\varphi_1, \dots, \varphi_n\}$ é inconsistente se e só se $\Gamma \vdash \perp$.

Nota 1.1.44. Para verificar se $\varphi_1, \dots, \varphi_n \models \psi$ devemos:

1. converter as fórmulas $\varphi_1, \dots, \varphi_n$ na FNC.
2. negar a fórmula ψ e converter $\neg\psi$ na FNC.
3. aplicar a regra de resolução às cláusulas obtidas acima até:
 - obter \perp ;
 - não conseguirmos aplicar a regra de resolução (sem obter \perp).

Exercício: Vamos verificar $p \rightarrow q, q \rightarrow r \models p \rightarrow r$.

Folha 0

3. Utilizando o método de resolução, justifique que
- $p, p \rightarrow q \models q;$
 - $p \vee q, p \rightarrow r, q \rightarrow r \models r.$
4. Utilizando o método de resolução, verifique a correção de cada uma das seguintes deduções:
- Chove se e só se levo guarda-chuva. Hoje não levo guarda-chuva. Logo, hoje não chove.
 - Chove se levo guarda-chuva. Hoje não levo guarda-chuva. Logo, hoje não chove.
 - Se o mordomo cometeu o crime, então ele vai estar nervoso quando interrogado. O mordomo estava nervoso quando interrogado. Logo, o mordomo cometeu o crime.
 - r é uma condição suficiente para q . Além disso, verifica-se r ou a negação de p . Logo, se q não for verdadeiro, não se verifica p .
 - De $\neg(p \vee q)$ deduz-se $\neg p$.

Matemática Discreta

Aula 3

Sumário

Sintaxe e Semântica de lógica de primeira ordem

- Sintaxe: linguagem, termos, fórmulas interpretação.
- Variáveis livres e ligadas.

Folha 1

2. Exprima por meio de fórmulas bem formadas as seguintes afirmações:
- a) Todas as aves têm penas.
 - b) Todas as crianças são mais novas que os seus pais.
 - c) Todos os insectos são mais leves do que algum mamífero.
 - d) Nenhum número é menor do que zero.
 - e) Zero é menor do que qualquer número.
 - f) Alguns números primos não são pares.
 - g) Todo o número par é número primo.

Lógica de 1^a ordem

Definição 1.2.1. Um **alfabeto de 1^a ordem** consiste:

1. numa colecção de **variáveis**;
2. nos **símbolos** « \wedge , \vee , \rightarrow , \leftrightarrow , \neg , \top , \perp » da lógica proposicional;
3. nos **quantificadores**: os símbolos « \exists » (existe) e « \forall » (para todos);
4. no símbolo de **igualdade** « $=$ ».

Além dos pontos expostos acima, e dependendo do contexto, podemos ainda ter:

- uma colecção de **símbolos de constantes**;
- uma colecção de **símbolos de função** (cada símbolo de função tem uma **aridade** $n \in \mathbb{N}$ = número de argumentos);
- uma colecção de **símbolos de predicado (relação)** com $n \in \mathbb{N}$ argumentos;

Definição 1.2.3. Vamos introduzir o conceito de **termo** de forma recursiva:

- cada variável e cada símbolo de constante são termos;
- se f é um símbolo de função de aridade n e se t_1, \dots, t_n são termos, então $f(t_1, \dots, t_n)$ também é um termo.

Definição 1.2.5. Da mesma forma que fizemos para os termos, vamos agora introduzir, recursivamente, o conceito de **fórmula**. Comecemos com os **átomos** (ou **fórmulas atómicas**):

- $P(t_1, \dots, t_n)$ é um átomo, onde P é um símbolo de predicado com n argumentos e t_1, \dots, t_n são termos;
- $t_1 = t_2$ é um átomo, onde t_1, t_2 são termos;
- \perp e \top são átomos;

A partir daqui, e considerando os átomos como «elementos primitivos», podemos construir recursivamente as fórmulas a partir dos conectivos lógicos e dos quantificadores apresentados anteriormente:

- se φ e ψ são fórmulas, então

$$(\varphi \wedge \psi), \quad (\varphi \vee \psi), \quad (\varphi \rightarrow \psi), \quad (\neg\varphi), \quad \perp, \quad \top,$$

são fórmulas;

- se φ é uma fórmula e x é uma variável, então $\forall x \varphi$ e $\exists x \varphi$ são fórmulas.

Nota 1.2.7. Nas fórmulas da forma $\forall x\varphi$ (resp. $\exists x\varphi$), dizemos que a fórmula φ é o **alcance do quantificador** \forall (resp. \exists).

Definição 1.2.9. A ocorrência de uma variável numa fórmula diz-se **ligada** se esta estiver dentro do alcance de um quantificador utilizado para essa mesma variável. Por outro lado, a ocorrência de uma variável dir-se-á **livre** se não for ligada.

Nota 1.2.10. Uma variável numa fórmula φ dir-se-á livre quando ocorrer pelo menos uma vez livre em φ . Adicionalmente, diremos que φ é **fechada** quando esta não tiver variáveis livres.

Exemplo:

- (1) $(\forall x \exists y x < y) \wedge (a < x)$
- (2) $\forall x \exists y (x < y \wedge a < x)$

Folha 1

1. Indique quais as ocorrências livres e ligadas de cada uma das variáveis das seguintes fórmulas:

- a) $\exists y P(x, y)$
- b) $(\forall x (P(x) \rightarrow Q(x))) \rightarrow (\neg(P(x)) \vee Q(y))$
- c) $\exists x (P(y, z) \wedge \forall y (\neg Q(x, y) \vee P(y, z)));$
- d) $P(a, f(a, b));$
- e) $\exists x (P(x) \rightarrow \neg Q(x));$
- f) $\forall x ((P(x) \wedge C(x)) \rightarrow \exists y L(x, y)).$

NOTA. x, y, z, a, b são variáveis.

3. No que se segue, $c(x)$, $s(x)$ e $d(x)$ representam as afirmações « x é uma explicação clara», « x é satisfatória» e « x é uma desculpa», respectivamente. Admita que o universo do discurso para x é o conjunto de todos os textos em Português. Traduza as seguintes fórmulas bem formadas para linguagem comum:

- a) $\forall x \ c(x) \rightarrow s(x);$
- b) $\exists x \ d(x) \wedge \neg s(x);$
- c) $\exists x \ d(x) \wedge \neg c(x).$

7. Obtenha, na forma mais simplificada possível, a negação da seguinte fórmula

$$\forall y \exists x \ ((q(x) \rightarrow p(y)) \vee (p(y) \wedge q(x))) .$$

Matemática Discreta

Aula 4

Sumário

- Interpretação.
- Consequência semântica
- Fórmulas na forma normal.
- Regras para obter formas normais.

Qual o significado da formula $x = c$?

Definição 1.2.12. Uma **estrutura** \mathcal{M} para um alfabeto de 1^a ordem consiste num conjunto D (domínio) onde:

- a cada símbolo de constante a , associamos um **elemento** $a^{\mathcal{M}} \in D$;
- a cada símbolo de função f (de aridade n), associamos uma **função** $f^{\mathcal{M}}: D^n \rightarrow D$;
- a cada símbolo de predicado P (de aridade n), associamos um **subconjunto** $P^{\mathcal{M}} \subseteq D^n$.

Definição 1.2.13. Dada uma estrutura \mathcal{M} , uma **valoração** v em \mathcal{M} associará a cada variável x um elemento $v(x) \in D$. Adicionalmente, designamos o par (\mathcal{M}, v) por **interpretação**.

Qual o significado da formula $\exists x (x = c)$?

Definição 1.2.16. Dada uma interpretação (\mathcal{M}, v) de um alfabeto de 1^a ordem, definimos recursivamente o conceito de **validade** de uma fórmula em (\mathcal{M}, v) da seguinte forma:

- $(\mathcal{M}, v) \models t_1 = t_2$ quando $v(t_1) = v(t_2)$;
- $(\mathcal{M}, v) \models P(t_1, \dots, t_n)$ quando $(v(t_1), \dots, v(t_n)) \in P$;
- $(\mathcal{M}, v) \models \top$ e **não** $(\mathcal{M}, v) \models \perp$;
- $(\mathcal{M}, v) \models (\varphi \wedge \psi)$ quando $(\mathcal{M}, v) \models \varphi$ e $(\mathcal{M}, v) \models \psi$;
- $(\mathcal{M}, v) \models (\varphi \vee \psi)$ quando $(\mathcal{M}, v) \models \varphi$ ou $(\mathcal{M}, v) \models \psi$;
- $(\mathcal{M}, v) \models (\varphi \rightarrow \psi)$ quando $(\mathcal{M}, v) \models \varphi$ implicar $(\mathcal{M}, v) \models \psi$;
- $(\mathcal{M}, v) \models \exists x \varphi$ quando, para algum $a \in D$, $(\mathcal{M}, v^{\frac{x}{a}}) \models \varphi$; $v^{\frac{x}{a}}(y) = \begin{cases} v(y), & \text{se } y \text{ é diferente de } x, \\ a, & \text{se } y \text{ é igual a } x. \end{cases}$
- $(\mathcal{M}, v) \models \forall x \varphi$ quando, para todo o $a \in D$, $(\mathcal{M}, v^{\frac{x}{a}}) \models \varphi$.

Nota 1.2.17. Dizer que uma dada fórmula φ é **válida** numa interpretação (\mathcal{M}, v) é o mesmo que dizer que (\mathcal{M}, v) é um **modelo** para φ . Usualmente, denotamos esta relação por $(\mathcal{M}, v) \models \varphi$.

Exercício: Sejam \mathcal{M} uma estrutura com

• $D = \{1,2,3\}; R = \{(1,1), (1,2), (1,3), (2,2), (3,3), (3,2)\}; S = \{1,3\}$

e v uma valorarão com $v(x) = 3$ e $v(y) = 2$.

Verifique a validade das seguintes fórmulas:

(a) $R(x, y)$ (b) $S(y)$ (c) $\forall y (S(x) \wedge R(x, y))$ (d) $\exists x \forall y (S(x) \wedge R(x, y))$

10. Para cada fórmula seguinte determine, se possível, um modelo e uma interpretação em que a mesma seja não válida:

a) $\forall x (P(x, a) \rightarrow \neg Q(x, a))$, onde a denota um símbolo de constante;

Definição 1.2.22. Uma fórmula diz-se:

- uma **tautologia** (ou **fórmula válida**) quando for válida para qualquer interpretação;
- uma **contingência** (ou **fórmula consistente**) se existir uma interpretação para a qual seja válida;
- uma **contradição** (ou **inconsistência**) quando não for uma consistência, ou seja, quando for inválida para qualquer interpretação.

Definição 1.2.24. Duas fórmulas φ e ψ dizem-se **equivalentes** ($\varphi \equiv \psi$) quando $\varphi \leftrightarrow \psi$ é uma tautologia.

Definição 1.2.25. Uma fórmula ψ diz-se **consequência semântica** (ou **consequência lógica**) das fórmulas $\varphi_1, \dots, \varphi_n$ quando, para toda a interpretação (\mathcal{M}, v) , se $\varphi_1, \dots, \varphi_n$ são válidas em (\mathcal{M}, v) , então ψ é válida em (\mathcal{M}, v) . Neste caso, escrevemos $\varphi_1, \dots, \varphi_n \models \psi$.

Forma Normal Prenex

Definição 1.3.2. Uma fórmula da forma $Qx_1 \cdots Qx_n \varphi$, onde φ é uma fórmula sem quantificadores e Q denota « \exists » ou « \forall » diz-se na **forma normal prenex (FNP)**.

Nota 1.3.3. Relativamente a uma fórmula $Qx_1 \cdots Qx_n \varphi$ na FNP, é comum designarmos a parte inicial (« $Qx_1 \cdots Qx_n$ ») por **prefixo** e « φ » por **matriz** da fórmula.

- Mover as negações (« \neg ») para o interior das fórmulas:

$$\neg \forall x \varphi \equiv \exists x \neg \varphi \quad \text{e} \quad \neg \exists x \varphi \equiv \forall x \neg \varphi;$$

- Mover os quantificadores para o exterior das fórmulas:

- $(\forall x \varphi) \wedge (\forall x \psi) \equiv \forall x (\varphi \wedge \psi);$
- $(\exists x \varphi) \vee (\exists x \psi) \equiv \exists x (\varphi \vee \psi);$
- supondo que ψ não contém a variável x :

$$(\forall x \varphi) \wedge \psi \equiv \forall x (\varphi \wedge \psi), \quad (\exists x \varphi) \wedge \psi \equiv \exists x (\varphi \wedge \psi), \\ (\forall x \varphi) \vee \psi \equiv \forall x (\varphi \vee \psi), \quad (\exists x \varphi) \vee \psi \equiv \exists x (\varphi \vee \psi).$$

Exercício: Escreva as formulas seguintes na FNP.

- (a) $\forall x P(x) \rightarrow \exists x Q(x)$
- (b) $\forall x \forall y [(\exists x (P(x, z) \wedge P(y, z))) \rightarrow (\exists u Q(x, y, u))]$

11. Transforme as seguintes fórmulas na forma normal disjuntiva prenex e na forma normal conjuntiva prenex:

- a) $(\forall x S(x)) \rightarrow (\exists z P(z));$
- b) $\neg(\forall x (S(x) \rightarrow P(x)));$
- c) $\forall x (P(x) \rightarrow (\exists y Q(x, y)));$
- d) $\exists x (\neg(\exists y P(x, y)) \rightarrow (\exists z (Q(z) \rightarrow R(x))));$
- e) $\forall x \exists y \exists z ((\neg P(x, y) \wedge Q(x, z)) \vee R(x, y, z)).$

Matemática Discreta

Aula5

Sumário

- Forma normal de Skolem.
- Substituição.
- A composição de substituições.
- Unificação.

9. Considere um universo X com os objetos A , B e C (isto é, $X=\{A, B, C\}$) e uma linguagem onde α , β e γ são símbolos de constante, f é um símbolo de função com um argumento e R é um símbolo de predicado com dois argumentos. Considere a seguinte interpretação:

símbolos de constante: $\alpha \mapsto A$, $\beta \mapsto A$ e $\gamma \mapsto B$;

símbolo de função f : $f(A) = B$, $f(B) = C$, $f(C) = C$.

símbolo de predicado R : $\{(B, A), (C, B), (C, C)\}$.

Com esta interpretação, avalie as seguintes fórmulas:

a) $R(\alpha, \beta)$;

b) $\exists x f(x) = \beta$;

c) $\forall w R(f(w), w)$.

Forma Normal de Skolem

Definição 1.3.7. Uma fórmula diz-se na **forma normal de Skolem (FNS)** se for uma FNP, estando a matriz na FNC e sendo o prefixo composto apenas por quantificadores universais (« \forall »).

Exercício: Escreva as formulas seguintes na FNS.

(a) $\exists x \forall y \forall z \exists u \forall v \exists w P(x, y, z, u, v, w)$

(b) $\forall x \exists y \exists z ((\neg P(x, y) \wedge Q(x, z)) \vee R(x, y, z))$

Nota 1.3.9. As funções e constantes utilizadas para substituição das variáveis existentes (no procedimento acima) são ditas **funções de Skolem**.

12. Encontre a forma standard de Skolem das seguintes fórmulas:

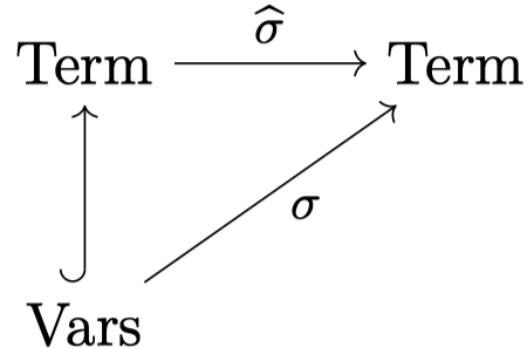
a) $\neg((\forall x P(x)) \rightarrow (\exists y P(y)))$

b) $\neg((\forall x P(x)) \rightarrow (\exists y \forall z Q(y, z)))$

c) $\forall x \exists y \exists z ((\neg P(x, y) \wedge Q(x, z)) \vee R(x, y, z))$

- no caso $\exists x_1 Q_2 x_2 \cdots Q_n x_n \varphi$:
 1. escolhemos um novo símbolo de constante (digamos c);
 2. substituimos todas as ocorrências livres de x_1 em $Q_2 x_2 \cdots Q_n x_n \varphi$ por c ;
 3. eliminamos $\exists x_1$ do prefixo.
- no caso $\forall x_1 \cdots \forall x_{k-1} \exists x_k Q_{k+1} x_{k+1} \cdots Q_n x_n \varphi$ ($k > 1$):
 1. escolhemos um novo símbolo de função (digamos f) de aridade $k - 1$;
 2. substituimos todas as ocorrências livres de x_k em $Q_{k+1} x_{k+1} \cdots Q_n x_n \varphi$ por $f(x_1, \dots, x_{k-1})$;
 3. eliminamos $\exists x_k$ do prefixo.

Substituição



Exemplo 1.4.6. Consideremos o termo $t = s(x, f(y, u), h(x, z))$ e a substituição

$$\theta = \{f(x, z)/x, g(y, f(x, y))/y, h(x, y)/z, v/u\}.$$

Exemplo 1.4.7. Vamos considerar as fórmulas $E_1 = F(x, y, g(z))$ e $E_2 = P(h(x), z, f(y))$ e a substituição $\theta = \{a/x, f(b)/y, c/z\}$.

14. Calcule $E\Theta$ em cada um dos seguintes casos:

a) $\Theta = \{a/x, f(z)/y, g(x)/z\}$, $E = P(h(x), z, f(z))$;

b) $\Theta = \{f(y)/x, a/y\}$, $E = F(a, h(a), x, h(y))$;

Definição 1.4.8. Consideremos duas substituições $\sigma, \theta : \text{Vars} \rightarrow \text{Term}$. Então, a **composta** de θ após σ é a função $\theta \Delta \sigma = \hat{\theta} \circ \sigma$.

Exemplo 1.4.10. $\theta = \{f(y)/x, z/y, x/u\}$

$$\sigma = \{a/x, g(x)/y, y/z\}$$

Unificador

Definição 1.4.14. Consideremos $\mathcal{E} = \{E_1, \dots, E_n\}$ um conjunto de expressões (termos, fórmulas). Uma substituição $\sigma: \text{Vars} \rightarrow \text{Term}$ diz-se um **unificador** de \mathcal{E} quando, para todas as expressões $E_1, \dots, E_n \in \mathcal{E}$, se tiver $E_1\sigma = \dots = E_n\sigma$.

Adicionalmente, dizemos que o conjunto \mathcal{E} de expressões é **unificável** quando existir um tal unificador.

Exemplo 1.4.15. • $\mathcal{E} = \{Q(x), Q(a)\}$ é unificável, com $\sigma = \{a/x\}$;

- $\mathcal{E} = \{R(x, y), Q(z)\}$ não é unificável;
- $\mathcal{E} = \{f(x), f(f(z))\}$ é unificável, com $\sigma = \{f(z)/x\}$;
- $\mathcal{E} = \{f(x), f(f(x))\}$ não é unificável;
- $\mathcal{E} = \{Q(a, y), Q(x, f(b))\}$ é unificável, com $\sigma = \{a/x, f(b)/y\}$.

Matemática Discreta

Aula 6

Sumário

- Obter o unificador mais geral.
- As regras da dedução: Resolvente binária e Fator. Exemplos.
- O algoritmo de resolução

Definição 1.4.16. Seja \mathcal{E} um conjunto de expressões. Um unificador σ de \mathcal{E} é dito **unificador mais geral (u.m.g.)** de \mathcal{E} quando, para cada unificador θ de \mathcal{E} , existir uma substituição λ tal que

$$\theta = \lambda \Delta \sigma,$$

ou seja, que cada unificador de \mathcal{E} se pode descrever como a composição de uma substituição com o unificador mais geral.

Definição 1.4.17. O **conjunto das diferenças**, \mathcal{D} , de um conjunto de expressões não vazio, \mathcal{E} , obtém-se determinando o primeiro símbolo (a contar da esquerda), no qual nem todas as expressões de \mathcal{E} têm exactamente os mesmos símbolos, extraíndo a sub-expressão que começa com o símbolo em causa e ocupa essa posição.

Exemplo 1.4.18. $\mathcal{E} = \{P(a), P(x)\} \quad \mathcal{D} = \{a, x\}$

Algoritmo: Determinação do u.m.g. de um conjunto \mathcal{E} (Robinson, 1965).

Entrada: conjunto (finito) de expressões $\mathcal{E} = \{E_1, \dots, E_n\}$;

Resultado: u.m.g. σ_k de \mathcal{E} (caso exista);

1 $k = 0$, $\mathcal{E}_0 = \mathcal{E}$ e $\sigma_0 = \varepsilon$;

2 **repetir até retornar algo**

3 **se** $|\mathcal{E}_k| = 1$ **então**

4 **retorna** σ_k ;

5 **fim**

6 determinar o conjunto $\mathcal{D}_k = \{D_1, \dots\}$ das diferenças de \mathcal{E}_k ;

7 **se** existir $p \in \text{Vars}$ e $t \in \text{Term}$ tal que $\{p, t\} \subseteq \mathcal{D}_k$ e p não ocorra em t
 então

8 $\sigma_{k+1} = (t/p) \Delta \sigma_k$;

9 $\mathcal{E}_{k+1} = \mathcal{E}_k(t/p)$;

10 $k = k + 1$;

11 **senão**

12 **retorna** « \mathcal{E} não é unificável»;

13 **fim**

Exemplo 1.4.19. Vamos considerar $\mathcal{E} = \{P(y, z), P(x, h(y)), P(a, h(a))\}$, onde x, y, z são variáveis, a é um símbolo de constante, h é um símbolo de função unária e P é um símbolo de predicado binário. Apliquemos então o algoritmo de Robinson para encontrar (caso exista) um u.m.g. para \mathcal{E} .

Exemplo 1.4.20. Consideremos $\mathcal{E} = \{P(h(x), z), P(x, h(y)), P(a, h(a))\}$, onde x, y, z são variáveis, a é um símbolo de constante, h é um símbolo de função unária e P é um símbolo de predicado binário. Vamos aplicar o alg. de Robinson para encontrar (caso exista) um u.m.g. para \mathcal{E} .

15. Para cada um dos seguintes conjuntos de fórmulas indique, justificando, se são ou não unificáveis. Em caso afirmativo, encontre um seu unificador mais geral. Tenha em atenção que « a » e « b » denotam constantes.

- a) $\{P(f(x), z), P(y, a)\};$
- b) $\{P(f(x), x), P(z, a)\};$
- c) $\{P(a, x, f(g(y))), P(b, h(z, w), f(w))\};$
- d) $\{S(x, y, z), S(u, g(v, v), v)\};$
- e) $\{P(x, x), P(y, f(y))\};$
- f) $\{Q(f(a), g(x)), Q(y, y)\};$
- g) $\{Q(f(x), y), Q(z, g(w))\}.$

Factor e Resolvente Binária

Definição 1.5.1. Se literais φ e ψ de uma cláusula $C = \varphi \vee \psi \vee \theta \vee \dots$ admitirem um u.m.g. σ , então $(\psi \vee \theta \vee \dots) \sigma$ será dito um **factor** de C .

Exemplo 1.5.2. $C = P(x) \vee P(f(y)) \vee \neg Q(x)$

Definição 1.5.3. Sejam $C_1 = \neg \psi \vee \theta \vee \dots$ e $C_2 = \varphi \vee \gamma \vee \dots$ cláusulas sem variáveis em comum. Se ψ e φ admitirem um u.m.g. σ , então a cláusula

$$(\theta \vee \dots \vee \gamma \vee \dots) \sigma$$

é dita uma **resolvente binária** de C_1 e C_2 .

Exemplo 1.5.4. $C_1 = P(x) \vee Q(x) \quad C_2 = \neg P(a) \vee R(x)$

Definição 1.5.5. Uma **resolvente** de duas cláusulas C_1 e C_2 é uma resolvente binária de (um factor de) C_1 e de (um factor de) C_2 .

Exemplo 1.5.6.

$$C_1 = P(x) \vee P(f(y)) \vee R(g(y))$$

$$C_2 = \neg P(f(g(a))) \vee Q(b)$$

19. Considere as seguintes fórmulas da lógica de primeira ordem:

F1: $\forall x (G(x) \rightarrow \forall y(P(y) \rightarrow L(x, y)))$

F2: $\exists x G(x)$

F3: $\exists x \forall y (P(y) \rightarrow L(x, y))$

Usando o princípio da resolução mostre que F3 é consequência de F1 e F2.

Matemática Discreta

Aula 7

Sumário

Princípios de enumeração combinatória (Capítulo 2).

- Princípio da Gaiola de Pombos e sua generalização.
- Princípio de Dirichlet.

Exercício de revisão: Princípio de resolução

Princípio da Gaiola de Pombos

Exemplo 2.2.2. Consideremos uma sala com 13 pessoas. Então existirão, pelo menos, duas pessoas a fazer anos no mesmo mês.

Exemplo 2.2.3. Consideremos 50 pessoas numa sala de $7m \times 7m$. Então, haverá duas pessoas que estão a uma distância inferior a $1.5m$.

De uma maneira matematicamente mais formal, podemos traduzir a ideia da seguinte forma: considerando um conjunto A e $(A_i)_{1 \leq i \leq m}$ uma família de subconjuntos de A (dois-a-dois distintos), com $A = \bigcup_{i=1}^m A_i$, se $|A| > m$, então $|A_i| > 1$, para algum $1 \leq i \leq m$.

Outra formulação possível prende-se com o conceito de injectividade de uma função: consideremos A, B dois conjuntos e $f: A \rightarrow B$ uma função; se $|A| > |B|$, então f não poderá ser injectiva (neste caso, a contraposição é mais óbvia: se $f: A \rightarrow B$ é injectiva, então $|A| \leq |B|$).

Folha 2

2. Mostre que num conjunto de cinco números inteiros positivos (arbitrários), existem pelo menos dois com o mesmo valor para o resto da divisão por 4.

Generalização

De uma maneira matematicamente mais formal, podemos traduzir a ideia da seguinte forma: considerando um conjunto A e $(A_i)_{1 \leq i \leq m}$ uma família de subconjuntos de A (dois-a-dois disjuntos), com $A = \bigcup_{i=1}^m A_i$; se $km < |A|$, então $|A_i| > k$, para algum $1 \leq i \leq m$.

1. A família Ferreira tem 13 filhos, para além de dois progenitores. Recorrendo ao princípio da gaiola dos pombos responda às seguintes questões:
 - a) Quantas pessoas desta família pode garantir que:
 - i. Nasceram no mesmo mês?
 - ii. Nasceram no mesmo dia da semana?
 - b) No próximo sábado, os Ferreira vão dar uma festa para a qual os filhos podem convidar os seus amigos mais próximos. Quantos amigos vão ser convidados por forma a garantir que pelo menos 3 dos convidados são amigos do mesmo filho dos Ferreira?

Exemplo 2.2.6. Num torneio em que participam $n \geq 2$ equipas de futebol, todas as equipas jogam uma vez umas com as outras. Vamos mostrar que em cada jornada, pelo menos duas equipas realizaram o mesmo número de jogos até esta jornada.

Folha 2

5. Mostre que num grupo de 20 pessoas escolhidas ao acaso existem pelo menos duas pessoas que têm o mesmo número de amigos dentro do grupo. Note que duas pessoas são consideradas amigas se houver uma relação de amizade recíproca estabelecida entre elas.

Folha 2

4. Mostre que dados 11 números no intervalo $]0, 1[$, haverá pelo menos dois deles cuja diferença menor que 0.1.

Princípio de Dirichlet

Teorema 2.2.4. *Para todos os $\alpha \in \mathbb{R}$ e $n \in \mathbb{N}$, $n \geq 1$, existem números inteiros p e q com $q \in \{1, \dots, n\}$ tal que $|q\alpha - p| < \frac{1}{n}$.*

21. Considere as seguintes afirmações, no universo dos animais:

- Os animais com pelos são mamíferos.
- Os ursos são animais com pelos.
- Os coelhos são mamíferos.
- O Winnie é um urso.
- O Bugsbunny é um coelho.
- O Sylvester é um animal com pelos.

a) Represente-as em lógica de primeira ordem.

b) Usando o Princípio de Resolução, responda às seguintes perguntas:

(i) O Winnie é mamífero?

(ii) Quais são os mamíferos?

(iii) Quem é que tem pelos?

Revisão: Princípio de resolução

Matemática Discreta

Aula 8

Sumário

Aplicações do princípio da gaiola de pombos.

O princípio da bijecção.

O princípio da adição e o princípio da multiplicação

Revisão: Exercício de revisão sobre o Princípio de Resolução.

Folha 2

6. Considere que p_1, p_2, \dots, p_n são números inteiros positivos.
- Mostre que se $p_1 + p_2 + \dots + p_n - n + 1$ objectos são colocados em n caixas, então existe um inteiro i entre 1 e n tal que a i -ésima caixa contém pelo menos p_i objectos.
 - Fazendo $p_1 = p_2 = \dots = p_n = r \in \mathbb{N}$ o que se pode afirmar?
7. Durante o mês de Janeiro, o João bebeu 42 cafés. Dado que o João bebe pelo menos um café por dia, mostre que num certo número de dias consecutivos o João bebeu exatamente 17 cafés.

Princípio da bijeção

O **princípio da bijecção** é outra das importantes ferramentas da combinatória que nos auxilia na contagem de elementos. Este diz-nos basicamente que se A e B são conjuntos finitos e se existe uma função bijectiva $f: A \rightarrow B$, então $|A| = |B|$. Tipicamente utilizamos este princípio quando é mais fácil contar os elementos de um destes conjuntos.

Exemplo 2.3.1. Existe uma bijecção entre o conjunto C dos números naturais com 4 algarismos em $A = \{1, 2, \dots, 9\}$ e o conjunto A^4 . De facto, se pensarmos na função $f: A^4 \rightarrow C$ que a cada quádruplo (a_1, a_2, a_3, a_4) faz corresponder $a_1 10^3 + a_2 10^2 + a_3 10 + a_4$, obtemos a bijecção pretendida.

Exemplo 2.3.2. Vamos determinar o número de subconjuntos de $X = \{1, \dots, n\}$. Se considerarmos $\mathcal{P}(X)$ como o conjunto dos subconjuntos de X e \mathbb{B}^n como o conjunto das sequências binárias de comprimento n , conseguimos ver que a função

$$f: \mathcal{P}(X) \longrightarrow \mathbb{B}^n$$

$$A \longmapsto f(A) = x_1 \dots x_n, \quad \text{onde} \quad x_i = \begin{cases} 1, & i \in A, \\ 0, & i \notin A. \end{cases}$$

é uma bijecção.

Exercício: De quantas maneiras é possível escrever 10 como uma soma com quatro números inteiros não negativos?

Princípio da adição e da multiplicação

Exemplo: Quantos números existem com 4 algarismos distintos? E se um dos algarismos for o 5?

O **princípio da adição** diz-nos que, para A_1, \dots, A_n conjuntos finitos dois-a-dois disjuntos (i.e., tais que $A_i \cap A_j = \emptyset$, quando $i \neq j$), temos

$$\left| \bigcup_{i=1}^n A_i \right| = \sum_{i=1}^n |A_i|.$$

Por outro lado, o **princípio da multiplicação** diz-nos que, para A_1, \dots, A_n conjuntos finitos, a cardinalidade do produto entre estes é igual ao produto das cardinalidades de todos, i.e.,

$$|A_1 \times A_2 \times \cdots \times A_n| = |A_1| \cdot |A_2| \cdot \cdots \cdot |A_n|.$$

23. São conhecidos os seguintes factos:

- Todo e qualquer cavalo é mais rápido do que todo e qualquer galgo;
- Existe pelo menos um galgo que é mais rápido do que todo e qualquer coelho;
- Para todos e quaisquer x , y e z , se x é mais rápido do que y e y é mais rápido do que z , então x é mais rápido do que z .
- Roger é um coelho;
- Harry é um cavalo.

a) Usando os predicados

- $\text{Cavalo}(x)$ representa « x é um cavalo»;
- $\text{Galgo}(x)$ representa « x é um galgo»;
- $\text{Coelho}(x)$ representa « x é um coelho»;
- $\text{MaisRápido}(x, y)$ representa « x é mais rápido do que y »;

represente os factos conhecidos na lógica de primeira ordem.

b) Mostre, usando resolução, que Harry é mais rápido do que Roger.

Revisão: Princípio de resolução