Matemática Discreta 2023/2024

Departamento de Matemática, Universidade de Aveiro

Sumário 1

Apresentação da UC.

Capítulo 1: A lógica de primeira ordem e demonstração automática

Proposições, conectivos, formulas;

Valoração; tabelas de verdade; tautologia, contingência, contradição.

Equivalentes lógicos.

Docentes

- António Jorge Monteiro Neves, Gab. 11.3.9, jorgeneves@ua.pt
- Maria Elisa Carrancho Fernandes, Gab. 11.3.44, maria.elisa@ua.pt
- Paula Cristina Roque da Silva Rama, Gab. 11.3.31, prama@ua.pt
- Alexandre Leite de Castro Madeira, Gab. 11.3.17, madeira@ua.pt
- Nelson José Rodrigues Faustino, Gab. 11.2.14, nfaust@ua.pt

6 Orientação Tutorial (OT)

6.1 Aulas OT

As aulas **OT (Orientação Tutorial)** funcionam nos seguintes horários:

- **OT1/OT2**: Segundas, 18h-19h, Sala 11.1.30;
- **OT3**: Terças, 19h-20h, Sala 11.1.31;
- **OT4/OT5**: Quintas, 18h-19h, Sala 11.1.28;

Nota importante:

Os alunos devem **avisar o respetivo docente (por email) se tencionam frequentar a aula OT**, até **às 14h do mesmo dia**.

9 Avaliação

9.1 Avaliação Discreta (AD)

Inicialmente, no PACO todos os alunos estão associados à **AD**, a qual inclui quatro elementos de avaliação, **MiniTeste 1 (MT1), Teste 1 (T1), MiniTeste 2 (MT2), Teste 2 (T2)**, tendo como objetivo motivar a aprendizagem dos estudantes de forma faseada por tópicos da matéria, avaliando-a de acordo com a seguinte calendarização:

- **MT1 (10%):** nas aulas **de 11 a 15 de março**, avaliando tópicos de **1LPO**;
- **T1 (40%):** **12 de abril** **(sexta-feira, 16h30m)**, sobre **1LPO, 2PEC, 3AIC**;
- **MT2 (10%):** nas aulas **de 13 a 17 de maio**, sobre **4RFG**;
- **T2 (40%):** na data da época normal de exames (11 a 24 de junho) a fixar pelo Conselho Pedagógico, avaliando tópicos de **4RFG e 5ETG**;

Classificação Final de AD (NAD)

A nota **NAD** será o arredondamento às unidades do valor calculado pela fórmula:

$$\mathbf{NAD} = \max(\mathbf{NCMT}, \mathbf{NSMT}),$$

onde

$$\mathbf{NCMT} = \mathbf{0.1\ MT1} + \mathbf{0.4\ T1} + \mathbf{0.1\ MT2} + \mathbf{0.4\ T2}$$

$$\mathbf{NSMT} = \mathbf{0.5\ T1} + \mathbf{0.5\ T2}$$

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

Capítulo 1

Lógica de Primeira Ordem e Demonstração Automática

1.1 Elementos da Lógica Proposicional

Fórmulas

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 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 ... »).

- « … mas … » pode ser substituido por « … e … »;
- « … só se … » pode ser substituido por « … implica … » ou « Se … então … »;
- « … excepto se … » pode ser substituido por « … ou … ».

A Maria foi à praia mas não foi tomar banho no mar.

A Maria vai à praia só se o tempo melhorar.

A Maria vai à praia excepto se começar a chover.

Uma **fórmula (bem formada)** é uma sequência finita de símbolos de um determinado alfabeto que é parte de uma linguagem formal. No caso da lógica proposicional, as fórmulas (bem formadas) são ditas **fórmulas proposicionais** e o alfabeto a considerar é composto pelos símbolos relativos aos conectivos $\wedge, \vee, \rightarrow, \neg, \leftrightarrow, \perp, \top$ e uma escolha de variáveis proposicionais (diferentes destes símbolos), tipicamente denotados por $p, q, r, \ldots$. As fórmulas proposicionais podem então ser definidas recursivamente 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

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

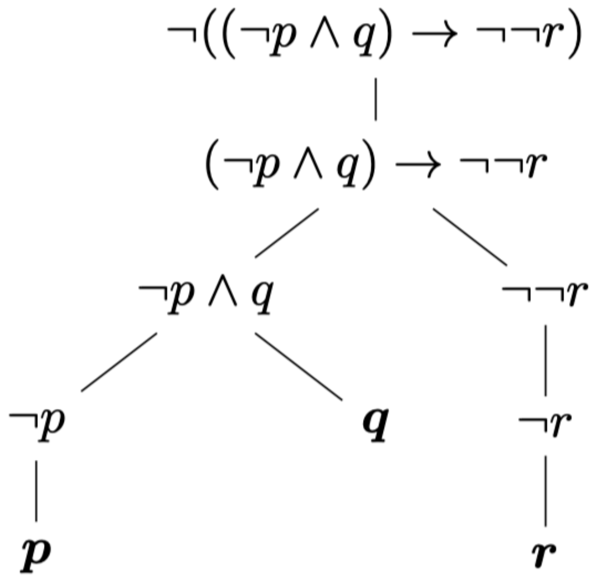
são fórmulas.

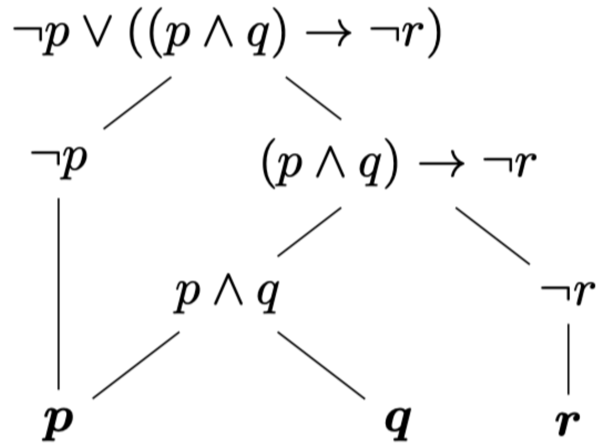
Exemplo 1.1.4. Se considerarmos p, q e r três variáveis, podemos ter os seguintes exemplos de fórmulas:

- $\bot,\ \top,\ p,\ q,\ r, \ldots$
- $p \vee q,\ p \to \bot,\ \neg\bot, \ldots$
- $(p \wedge q) \leftrightarrow q,\ (p \to q) \to (p \vee q), \ldots$
- $(p \wedge q) \to ((p \vee q) \to q), \ldots$

No entanto, se considerarmos o mesmo conjunto de variáveis, as sequências $(\bot\top)$, (pqr), $p\neg$, $p \leftrightarrow \vee$, $(\top \to)$, $(p \wedge q) \to r)$ ou $(p\wedge \to q)$ não são fórmulas.

Exemplo 1.1.5. As expressões $\neg((\neg p \wedge q) \rightarrow \neg\neg r)$ e $\neg p \vee ((p \wedge q) \rightarrow \neg r)$ são fórmulas. Efectivamente, se considerarmos as variáveis p, q, r, podemos seguir as árvores de construcção ilustradas abaixo.





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.

Semântica, Validade e Equivalência

Definição 1.1.6. Uma **valoração** (ou **interpretação**) de um conjunto V de variáveis proposicionais é uma função $v\colon V \to \{0,1\}$, 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 $v(\perp) = 0$.

- se tivermos uma valoração $v\colon V \to \{0,1\}$, onde $V = \{p, q, r\}$, tal que $p, r \mapsto 1$ e $q \mapsto 0$, qual será o valor de verdade da seguinte fórmula?

$$((p \to (q \land r)) \leftrightarrow (\neg p \lor q))$$

tabela de verdade

φ	$\neg\varphi$
0	1
1	0

φ	ψ	$\varphi \wedge \psi$
0	0	0
0	1	0
1	0	0
1	1	1

φ	ψ	$\varphi \rightarrow \psi$
0	0	1
0	1	1
1	0	0
1	1	1

φ	ψ	$\varphi \leftrightarrow \psi$
0	0	1
0	1	0
1	0	0
1	1	1

$$v(\bot) = 0$$
$$v(\top) = 1$$
$$v(\varphi \wedge \psi) = v(\varphi) \wedge v(\psi)$$
$$v(\varphi \vee \psi) = v(\varphi) \vee v(\psi)$$
$$v(\varphi \to \psi) = v(\varphi) \to v(\psi)$$
$$v(\varphi \leftrightarrow \psi) = v(\varphi) \leftrightarrow v(\psi)$$
$$v(\neg\varphi) = \neg v(\varphi)$$

Exemplo 1.1.10. Suponhamos que $V = \{p, q\}$ e que temos uma valoração $v \colon V \to \{0, 1\}$ tal que $p \mapsto 1$ e $q \mapsto 0$. Então,

$$v(\neg p \to (p \vee q)) = ?$$

Definição 1.1.12. Uma fórmula diz-se:

- uma **tautologia** (ou **fórmula válida**) quando tiver o valor lógico 1 para <u>cada</u> 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 <u>cada</u> interpretação.

Exemplo 1.1.13. As fórmulas $(p \wedge q) \rightarrow q$ e $(p \wedge q) \rightarrow p$ são tautologias.

Definição 1.1.14. As fórmulas φ e ψ dizem-se **equivalentes lógicas** ($\varphi \equiv \psi$) quando φ e ψ tem o mesmo valor lógico, para cada valoração.

Nota 1.1.15. $\varphi \equiv \psi$ se e só se a fórmula $\varphi \leftrightarrow \psi$ é uma tautologia.

Exemplo 1.1.16. Temos que $(\neg p \vee q) \equiv (p \to q) \equiv (\neg q \to \neg p)$.

Exemplo 1.1.17. Dadas três variáveis proposicionais p, q, r e as fórmulas $\varphi = p \wedge (q \vee r)$ e $\psi = (p \wedge q) \vee r$, verifica-se que $\varphi \not\equiv \psi$.

Tautologias

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Leis de De Morgan

Exemplo 1.1.18. Consideremos as variáveis proposicionais p, q, r e uma fórmula φ, unicamente dependente destas. Apresentamos abaixo a tabela de verdade relativa a φ.

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

$\varphi = ?$

Sumário 2

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

Formas Normais

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 $L_{j_1} = \neg L_{j_2}$.*

Definição 1.1.21. Dizemos que a fórmula φ está na **forma normal conjuntiva** (**FNC**) quando $\varphi = \bigwedge_{i\in I} \varphi_i$ (para algum conjunto de índices I) e onde cada φ_i é da forma $\bigvee_{j\in J} L_j$ (para algum conjunto 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.*

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) $(q \wedge \neg p \wedge r) \vee (\neg p \wedge \neg q)$.

Definição 1.1.29. Um conjunto de fórmulas $\{\varphi_1, \ldots, \varphi_n\}$ dir-se-á **consistente** quando existir uma interpretação que é modelo de todas as fórmulas em $\{\varphi_1, \ldots, \varphi_n\}$, 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 $\Gamma = \{\neg p, p \to q, q\}$. Rapidamente conseguimos ver que Γ é consistente: basta considerar a valoração tal que $p \mapsto 0$ e $q \mapsto 1$.

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 $\varphi_1, \dots, \varphi_n \models \psi$.

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

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 $((\varphi_1 \wedge \cdots \wedge \varphi_n) \to \psi)$ for uma tautologia.*

regras de inferência

$$\frac{\varphi \qquad \psi}{\varphi \wedge \psi}\,(\wedge\mathcal{I}) \qquad \frac{\varphi \wedge \psi}{\varphi}\,(\wedge\mathcal{E}_1) \qquad \frac{\varphi \wedge \psi}{\psi}\,(\wedge\mathcal{E}_2)$$

$$\frac{\varphi}{\varphi \vee \psi}\,(\vee\mathcal{I}_1) \qquad \frac{\psi}{\varphi \vee \psi}\,(\vee\mathcal{I}_2) \qquad \frac{\varphi \vee \psi \qquad \boxed{\begin{array}{c}\varphi\\ \vdots\\ \theta\end{array}} \qquad \boxed{\begin{array}{c}\psi\\ \vdots\\ \theta\end{array}}}{\theta}\,(\vee\mathcal{E})$$

$$\frac{\boxed{\begin{array}{c}\varphi\\ \vdots\\ \psi\end{array}}}{\varphi \to \psi}\,(\to \mathcal{I}) \qquad \frac{\varphi \qquad \varphi \to \psi}{\psi}\,(\to \mathcal{E})$$

$$\frac{\perp}{\varphi}\,(\perp\mathcal{E}) \qquad \frac{}{\varphi \vee \neg\varphi}\,(\mathrm{EM})$$

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

Teorema 1.1.39 (Correção). *Toda a consequência sintática do cálculo proposicional é também uma consequência semântica.*

Teorema 1.1.40 (Completude). *Toda a consequência semântica do cálculo proposicional é também uma consequência sintáctica.*

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

regra de resolução:

$$\boxed{\dfrac{\neg\psi \vee \theta \qquad \psi \vee \varphi}{\theta \vee \varphi}\ (\mathrm{Res})}$$

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

$$\boxed{\dfrac{\neg\psi \qquad \psi \vee \varphi}{\varphi}} \quad \text{e} \quad \boxed{\dfrac{\neg\psi \qquad \psi}{\bot}}$$

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

Nota 1.1.45. Para verificar se $\varphi_1, \ldots, \varphi_n \vDash \psi$ devemos:

1. converter as fórmulas $\varphi_1, \ldots, \varphi_n$ 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 $\perp$).

Exemplo 1.1.46. Vamos verificar $p \to q, q \to r \vDash p \to r$.

Exemplo 1.1.47. Será que $p, p \to q, \neg(r \land \neg q) \models r$?

Sumário 3

- Resolução de exercícios de aplicação do método de resolução.
- Alfabeto de 1ª ordem: variáveis, símbolos, quantificares, predicados e funções.
- Termos.
- Alcance de um quantificado; variáveis livres e ligadas.
- Tradução de formulas para a linguagem corrente e vice-versa.

Folha 0

3. Utilizando o método de resolução, justifique que

   a) $p,\, p \to q \models q$;

   b) $p \vee q,\, p \to r,\, q \to r \models r$.

4. Utilizando o método de resolução, verifique a correção de cada uma das seguintes deduções:

   a) Chove se e só se levo guarda-chuva. Hoje não levo guarda-chuva. Logo, hoje não chove.

   b) Chove se levo guarda-chuva. Hoje não levo guarda-chuva. Logo, hoje não chove.

   c) 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.

   d) 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.

   e) De $\neg(p \vee q)$ deduz-se $\neg p$.

1.2 Sintaxe e Semântica de lógica de primeira ordem

$$\forall x \forall y\ ((\mathrm{par}(x) \wedge \mathrm{par}(y)) \to \mathrm{par}(x+y))$$

$$\forall x\ (\mathrm{gato}(x) \to \mathrm{garras}(x))$$

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

1. numa colecção de **variáveis**;
2. nos **símbolos** «$\wedge, \vee, \to, \leftrightarrow, \neg, \top, \bot$» 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 coleção de **símbolos de constantes**;
- uma coleção de **símbolos de função** (cada símbolo de função tem uma **aridade** $n \in \mathbb{N}$ — o número de argumentos);
- uma coleção de **símbolos de predicado** (ou **relação**) (cada símbolo de predicado tem uma **aridade** $n \in \mathbb{N}$ — o número de 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 $t_1, \ldots, t_n$ são termos, então $f(t_1, \ldots, t_n)$ também é um termo.

Exemplo 1.2.4. Consideremos uma linguagem com as variáveis x, y, z, um símbolo constante a, um símbolo de função unária i e um símbolo de função binária m. Então, as seguintes expressões são termos:

- x, y, z, a;
- $i(a), i(x), m(z, y), m(a, z), \ldots$;
- $m(i(x), x), i(m(z, a)), m(m(a, y), i(x)), \ldots$.

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**):

- $P(t_1, \ldots, t_n)$ é um átomo, onde P é um símbolo de predicado com n argumentos e $t_1, \ldots, t_n$ 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.

Exemplo 1.2.6.

$$\underbrace{\forall x, y, z\ \underbrace{\overbrace{(x<y)}^{\text{fórmula}} \to \overbrace{(\underbrace{x+z}_{\text{termo}} < \underbrace{y+z}_{\text{termo}})}^{\text{fórmula}}}_{\text{fórmula}}}_{\text{fórmula}}$$

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. $\exists$).

Exemplo 1.2.8. No que se segue, gato e garras são símbolos de função unária e a é um símbolo de constante.

- $\forall x \; (\text{gato}(x) \to \text{garras}(x))$
- $(\forall x \; \exists y \; x < y) \wedge (a < x)$
- $\forall x \; \exists y \; (x < y \wedge a < x)$

o alcance de «∀» / alcance de «∃»

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.

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) $(\forall x\, (P(x) \to Q(x))) \to (\neg(P(x)) \vee Q(y))$

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

   d) $P(a, f(a, b))$;

   e) $\exists x\, (P(x) \to \neg Q(x))$;

   f) $\forall x\, ((P(x) \wedge C(x)) \to \exists y L(x, y))$.

NOTA. x, y, z, a, b são variáveis.

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.

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) $\exists x \; d(x) \; \wedge \; \neg \; c(x)$.

Sumário 4

- Estrutura, valoração, interpretação e modelo.
- Validade de uma formula
- Formas normais
- Forma normal prenex

O que significa, por exemplo, a fórmula $x = c$?

Definição 1.2.12. Uma **estrutura** $\mathcal{M}$ para um alfabeto de 1ª 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** $f^{\mathcal{M}} \colon D^n \to D$;
- 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**.

Dada agora uma interpretação $(\mathcal{M}, v)$ de uma linguagem, é comum definirmos (de forma recursiva - à semelhança da lógica proposicional) a interpretação dos termos:

$$v(f(t_1, \ldots, t_n)) = f(v(t_1), \ldots, v(t_n)) \in D.$$

Exemplo 1.2.14. Consideremos a linguagem com um símbolo de função binária f e um símbolo de constante a. Para a interpretação $(\mathcal{M}, v)$, com $D = \mathbb{Z}$ e

$$f^{\mathcal{M}} \colon D^2 \to D \quad \text{tal que} \quad (n, m) \mapsto |n| - |m|, \quad a^{\mathcal{M}} = 0, \quad v(x) = -2 \quad \text{e} \quad v(y) = 1,$$

temos:

- $v(f(f(x, a), f(y, f(x, a)))) =$?

O que significa, por exemplo, a fórmula $x = c$?

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 $(\mathcal{M}, v) \vDash \varphi$.

O que significa, por exemplo, a fórmula $\exists x\ x = c$?

$$v^{\frac{x}{a}}(y) = \begin{cases} v(y), & \text{se } y \text{ é diferente de } x, \\ a, & \text{se } y \text{ é igual a } x. \end{cases}$$

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

- $(\mathcal{M}, v) \vDash t_1 = t_2$ quando $v(t_1) = v(t_2)$;
- $(\mathcal{M}, v) \vDash P(t_1, \ldots, t_n)$ quando $(v(t_1), \ldots, v(t_n)) \in P$;
- $(\mathcal{M}, v) \vDash \top$ e **não** $(\mathcal{M}, v) \vDash \bot$;
- $(\mathcal{M}, v) \vDash (\varphi \wedge \psi)$ quando $(\mathcal{M}, v) \vDash \varphi$ e $(\mathcal{M}, v) \vDash \psi$;
- $(\mathcal{M}, v) \vDash (\varphi \vee \psi)$ quando $(\mathcal{M}, v) \vDash \varphi$ ou $(\mathcal{M}, v) \vDash \psi$;
- $(\mathcal{M}, v) \vDash (\varphi \to \psi)$ quando $(\mathcal{M}, v) \vDash \varphi$ implicar $(\mathcal{M}, v) \vDash \psi$;
- $(\mathcal{M}, v) \vDash \exists x\, \varphi$ quando, para algum $a \in D$, $(\mathcal{M}, v^{\frac{x}{a}}) \vDash \varphi$;
- $(\mathcal{M}, v) \vDash \forall x\, \varphi$ quando, para todo o $a \in D$, $(\mathcal{M}, v^{\frac{x}{a}}) \vDash \varphi$.

Exercício: Sejam $\mathscr{M}$ 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) $\exists x \forall y (S(x) \wedge R(x, y))$

Folha 1

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

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 $\varphi_1, \dots, \varphi_n \vDash \psi$.

Exemplo 1.2.27. O nosso objectivo será fazer a dedução de

$$\frac{\text{Todos os gatos têm garras} \qquad \text{Tom é um gato}}{\text{Tom tem garras}}$$

1.3 Formas Normais

Definição 1.3.1. Na lógica de 1ª ordem, uma fórmula φ é dita um **literal** se for um átomo ou uma negação de um átomo.

- φ está na FNC se $\varphi = \bigwedge_{i \in I} \varphi_i$, onde cada $\varphi_i = \bigvee_{j \in J} L_j$ e cada L_j é um literal;

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 designamos a parte inicial («$Qx_1 \cdots Qx_n$») por **prefixo** e «φ» por **matriz** da fórmula.

É agora absolutamente legítimo perguntarmos de que forma podemos obter/transformar uma dada fórmula na sua FNP.

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

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

- 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:

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

Exemplo 1.3.4. Vamos transformar a fórmula $(\forall x \ P(x)) \to (\exists x \ Q(x))$ para a forma normal prenex.

Exemplo 1.3.5. Vamos transformar a fórmula

$$\forall x \, \forall y \, (\exists z (P(x,z) \wedge P(y,z))) \to (\exists u \, Q(x,y,u))$$

para a forma normal prenex.

Folha 1

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

$$\forall y \, \exists x \ \left(\left(\ q(x) \to p(y) \ \right) \ \vee \ \left(\ p(y) \wedge q(x) \ \right) \ \right) \ .$$

Sumário 5

- Forma normal de Skolem.
- Substituição.

Folha 1

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

a) $(\forall x\, S(x)) \to (\exists z\, P(z))$;

b) $\neg(\forall x\, (S(x) \to P(x)))$;

c) $\forall x\, (P(x) \to (\exists y\, Q(x, y)))$;

d) $\exists x\, (\neg(\exists y\, P(x, y)) \to (\exists z\, (Q(z) \to R(x))))$;

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

Forma Normal de Skolem e Eliminação dos Quantificadores «∃»

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 («∀»).

Exemplo 1.3.10. Vamos aplicar o procedimento descrito anteriormente por forma a obter a FNS da fórmula

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

Exemplo 1.3.11. Vamos obter a FNS da fórmula

$$\forall x\, \exists y\, \exists z\, ((\neg P(x, y) \land Q(x, z)) \lor R(x, y, z)).$$

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

- 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 $f(x_1, \ldots, x_{k-1})$;
  3. eliminamos $\exists x_k$ do prefixo.

Folha 1

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

1.4 Unificação

Substituições

$$
\begin{tikzcd}
\mathrm{Term} \arrow[r, "\widehat{\sigma}"] & \mathrm{Term} \\
\mathrm{Vars} \arrow[u, hook] \arrow[ur, "\sigma"'] &
\end{tikzcd}
$$

- **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 $\theta = \{a/x, f(b)/y, c/z\}$.

Folha 1

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 $\sigma, \theta \colon \mathrm{Vars} \to \mathrm{Term}$. Então, a **composta** de θ após σ é a função $\theta \vartriangle \sigma = \widehat{\theta} \circ \sigma$.

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

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

Sumário 6

- Unificação.
- Unificador mais geral.
- As regras da dedução: Resolvente binária e Fator. Exemplos.
- O algoritmo de resolução

Unificadores

Definição 1.4.14. Consideremos $\mathcal{E} = \{E_1, \ldots, E_n\}$ um conjunto de expressões (termos, fórmulas). Uma substituição $\sigma\colon \text{Vars} \to \text{Term}$ diz-se um **unificador** de $\mathcal{E}$ quando, para todas as expressões $E_1, \ldots, E_n \in \mathcal{E}$, se tiver $E_1\sigma = \cdots = E_n\sigma$.
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 $\sigma = \{a/x, f(b)/y\}$.

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

$$\theta = \lambda \vartriangle \sigma,$$

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, extraindo 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 $\mathcal{E} = \{E_1, \ldots, E_n\}$;

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

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

repetir até retornar algo

  se $|\mathcal{E}_k| = 1$ **então**

    retorna σ_k;

  fim

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

  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**

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

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

    $k = k + 1$;

  senão

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

  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 $\mathcal{E}$.

Folha 1

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) $\{Q(f(x), y), Q(z, g(w))\}$.

1.5 Método da Resolução de Robinson

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. $C_1 = P(x) \vee Q(x) \qquad C_2 = \neg P(a) \vee R(x)$

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.

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

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

Sumário 7

- O algoritmo de resolução: resolução de exercícios.
- Princípio da Gaiola de Pombos e princípio de Dirichlet.
- Generalização do Princípio da Gaiola de Pombos.

Método de Resolução

Recordemos que verificar $\Gamma \vDash \psi$, é o mesmo que mostrar que $\Gamma \cup \{\neg\psi\}$ é inconsistente.

- transformar todas as fórmulas na FNS
- «ignorar» os quantificadores $\forall$
- renomear as variáveis em cada cláusula por forma a torná-las distintas
- aplicar sucessivamente as duas regras

$$\frac{\neg\psi \vee \theta \qquad \varphi \vee \gamma}{(\theta \vee \gamma)\ \text{u.m.g.}(\varphi, \psi)}\ (\text{BR})$$

$$\frac{\varphi \vee \psi \vee \theta}{(\varphi \vee \theta)\ \text{u.m.g.}(\varphi, \psi)}\ (\text{Fator})$$

Exemplo 1.5.8

- Ninguém que realmente aprecia Beethoven falha de manter o silêncio durante a sonata *Mondschein* (ao Luar);
- Os porquinhos-da-índia são completamente ignorantes no que diz respeito à música;
- Ninguém que é completamente ignorante no que diz respeito à música consegue manter silêncio durante a sonata *Mondschein* (ao Luar);
- Portanto, os porquinhos-da-índia nunca realmente apreciam Beethoven.

Folha 1

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

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

F2: $\exists x\, G(x)$

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

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

Capítulo 2

Princípios de Enumeração Combinatória

2.2 O Princípio da Gaiola dos Pombos

O princípio da gaiola dos pombos

se tivermos n pombos para distribuir por m gaiolas, com $n > m$, haverá pelo menos uma gaiola com dois pombos.

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 distinta), 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 $f : A \to B$ uma função; se $|A| > |B|$, então f não poderá ser injectiva (neste caso, a contraposição é mais óbvia: se $f : A \to B$ é injectiva, então $|A| \leq |B|$).

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 $1.5m$.

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.

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* $q \in \{1, \ldots, n\}$ *tal que* $|q\alpha - p| < \frac{1}{n}$.

Exemplo 2.2.5. Vamos agora mostrar que, dado um subconjunto de $\{1, \ldots, 2n\}$ com $n + 1$ elementos, existirão pelo menos dois elementos distintos x, y nesse subconjunto tais que $x \mid y$ («x divide y») ou $y \mid x$ («y divide x»).

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.

Sumário 8

- Generalização do Princípio da Gaiola de Pombos.
- O princípio da bijecção.
- O príncipio da adição e o princípio da multiplicação.
- O príncipio da multiplicação generalizada.

Generalização

se temos mais do que mk pombos e m gaiolas, então haverá uma gaiola a ter, no mínimo, $k+1$ pombos

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 famĺia 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 $1 \leq i \leq m$.

Folha 2

1. A familia 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?

3. Mostre que escolhendo cinco números inteiros (distintos) entre 1 e 8, dois deles têm soma igual a 9.

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.

2.3 O Princípio da Bijecção

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 $f\colon A \to B$, 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 $A = \{1, 2, \ldots, 9\}$ e o conjunto A^4. De facto, se pensarmos na função $f\colon A^4 \to C$ 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

$$
\begin{aligned}
f \colon \mathcal{P}(X) &\longrightarrow \mathbb{B}^n \\
A &\longmapsto f(A) = x_1 \dots x_n, \quad \text{onde} \quad x_i = \begin{cases} 1, & i \in A, \\ 0, & i \notin A. \end{cases}
\end{aligned}
$$

é uma bijecção.

Exemplo 2.3.3. Consideremos $k, n \in \mathbb{N}$, com $k \leq n$. Vamos tentar determinar quantos são os números inferiores a 10^n de tal forma que a soma dos seus algarismos seja igual a k.

2.4 Os Princípios da Adição e Multiplicação

O **princípio da adição** diz-nos que, para $A_1, \ldots, A_n$ conjuntos finitos dois-a-dois disjuntos (i.e., tais que $A_i \cap A_j = \varnothing$, 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 $A_1, \ldots, A_n$ conjuntos finitos, a cadinalidade do produto entre estes é igual ao produto das cardinalidades de todos, i.e.,

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

Exemplo 2.4.2.

- Qual é o número de números naturais com 4 algarismos que se pode escrever com os dígitos $1, \ldots, 9$?

- Qual é o número de números naturais com 4 algarismos que se podem escrever com os dígitos $0, \ldots, 9$ e que são divisíveis por 5?

Exemplo 2.4.4. Vamos calcular quantos números existem com 4 algarismos distintos.

Exemplo 2.4.5. Vamos calcular quantos números existem com 4 algarismos distintos em 1, ..., 9, um deles igual a 5.

23. São conhecidos os seguintes factos:

- Todo e qualquer cavalo é mais rápido do que todo e qualquer galgo;

Folha 1

- 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

- Cavalo(x) representa «x é um cavalo»;
- Galgo(x) representa «x é um galgo»;
- Coelho(x) representa «x é um coelho»;
- 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.

Sumário 9

- O príncipio da adição e o princípio da multiplicação.
- O príncipio da multiplicação generalizada.
- O princípio de inclusão-exclusão

- MT1

Folha 2

8. Sejam A e B conjuntos tais que $|A| = 2$ e $|B| = 3$.

   a) Quantas funções podemos definir com conjunto de partida A e conjunto de chegada B? Se $|A|=3$ e $|B| = 2$, qual seria a resposta à pergunta anterior? Indique o princípio combinatório utilizado.

   a) Quantas funções injectivas podemos definir com conjunto de partida A e conjunto de chegada B?

13. Qual é o número de palavras com k carateres que se podem formar considerando um alfabeto de n letras,

a) sem qualquer restrição.

b) não podendo existir duas letras consecutivas repetidas.

c) e que sejam palíndromos (i.e., palavras cujos elementos equidistantes dos extremos são iguais; por exemplo: ana, rever, ertutre).

14. Quantos números entre 1000 e 9999 se podem formar:

a) contendo o dígito 1.

b) com todos os dígitos distintos e contendo os dígitos 1 e 2 em posições adjacentes com o 1 a preceder o 2.

c) com dígitos ímpares a ocupar as posições ímpares (onde a primeira posição corresponde às unidades) e dígitos pares a ocupar posições pares.

o princípio da inclusão-exclusão

Teorema 2.4.6 (Inclusão-Exclusão). *Dados conjuntos finitos arbitrários* $A_1, \ldots, A_n$ *(não necessariamente dois-a-dois disjuntos) temos que*

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{k=1}^{n}(-1)^{k+1}\left(\sum_{1\leq i_1\leq\cdots\leq i_k\leq n} |A_{i_1}\cap\cdots\cap A_{i_k}|\right).$$

Exemplo 2.4.7. Vamos determinar o número de números entre 1 e 1000 que são divisíveis por 3 ou por 5.

Folha 2

10. Qual o número de números naturais não superiores a 1000 que não são divisíveis por 4, nem por 6, nem por 9?

12. Num universo de 200 estudantes, 50 estudam Matemática, 140 estudam Economia e 24 estudam ambos os cursos. Dos 200 estudantes, 60 são mulheres, das quais 20 estudam Matemática, 45 estudam Economia e 16 delas estudam ambos os cursos. Determine, para o universo de estudantes considerado, quantos homens é que não estudam nem Matemática nem Economia.