



Departamento de Matemática, Universidade de Aveiro

Matemática Discreta (47166)

Ano Letivo 2023/24

Texto de Apoio

Versão: 13 de maio de 2024

Conteúdo

1	Lógica de Primeira Ordem e Demonstração Automática	1
1.1	Elementos da Lógica Proposicional	1
1.2	Sintaxe e Semântica de lógica de primeira ordem	18
1.3	Formas Normais	27
1.4	Unificação	31
1.5	Método da Resolução de Robinson	38
2	Princípios de Enumeração Combinatória	43
2.1	Introdução	43
2.2	O Princípio da Gaiola dos Pombos	44
2.3	O Princípio da Bijecção	48
2.4	Os Princípios da Adição e Multiplicação	50
3	Agrupamentos e Identidades Combinatórias	55
3.1	Permutações e Arranjos	55
3.2	Combinações	57
3.3	Permutações e Multinómios	77
3.4	Identidades Combinatórias	82
4	Recorrência e Funções Geradoras	89
4.1	Equações de Recorrência	91
4.2	Equações de Recorrência Lineares Homogéneas	94
4.3	Equações de Recorrência Lineares Gerais	104
4.4	Equações de Recorrência Não Lineares	107
4.5	Séries e Funções Geradoras	110
4.5.1	Séries Formais de Potências	111
4.5.2	Álgebra das Séries Formais	112
4.5.3	Somas infinitas de séries de potências	116
4.5.4	Interpretação Combinatorial	122
4.5.5	Séries <i>vs.</i> Funções	128
4.5.6	Derivadas e Integrais	131
4.5.7	Revisitar as Equações de Recorrência	135

5	Elementos da Teoria dos Grafos	139
5.1	Conceitos Fundamentais	140
5.2	Vizinhanças e Graus	143
5.3	Homomorfismos, Isomorfismos e Sub-Grafos	147
5.4	Alguns conceitos métricos	151
5.5	Conexidade	154
5.6	Grafos particulares	158
5.7	Problemas de caminho de custo mínimo em grafos	160
5.8	Árvores e florestas	165
5.9	Árvores abrangentes de custo mínimo	173

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 hipótese de Riemann é falsa ou está a chover.
- Se o S. L. Benfica é campeão, então o F. C. Porto não é campeão.

Vejamos que algumas das proposições acima são verdadeiras e outras são falsas; no entanto, todas elas têm um valor de verdade bem definido (mesmo que não saibamos qual é). Por outro lado, algo como « n é um número par» não poderá ser uma proposição, uma vez que não temos valor de verdade até escolher um n particular.

Os **conectivos** combinam as afirmações lógicas de forma a torná-las mais complexas, i.e., utilizamo-os para construir proposições mais complexas a partir de proposições mais simples. Podemos observar que existem certos conectivos que ocorrem com alguma frequência nas proposições:

- «... e ...»;
- «... não ...»;
- «... ou ...»;
- «Se ... então ...»;

- « ... se e só se ... ».

No entanto, num discurso corrente, ocorrem também com alguma frequência

« ... mas ... », « ... só se ... », « ... excepto se ... » ...

Neste caso:

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

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.

Nota 1.1.1. Existem ainda dois símbolos especiais que serão tidos como proposições atómicas: \perp e \top . Mais à frente veremos o que estes representam.

Porque queremos falar de forma abstracta sobre como raciocinar (e argumentar), não será suposto limitar-mo-nos a proposições em particular, mas explorar o que pode ser dito de forma geral sobre estas. Desta forma, vamos introduzir as **variáveis proposicionais**: símbolos que representam uma proposição atómica. Tradicionalmente, estas serão representadas por letras minúsculas (eventualmente com índices): $p, q, r, \dots, p_1, p_2, p_3, \dots$.

Assim como no caso das variáveis, será útil identificar os conectivos apresentados mais acima de forma simbólica. Desta forma,

- \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 ... »).

Nota 1.1.2. A curiosidade poderá levar-nos a perguntar se, para além dos já apresentados, existem conectivos um pouco mais «exóticos» (que nos permitam construir novos tipos de afirmações). De facto, existem: é o caso do «ou exclusivo» (representado simbolicamente por $\dot{\vee}$ ou \oplus) e da «negação conjunta» (representada simbolicamente por \downarrow).

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, \dots . 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.

Nota 1.1.3. Para tornar a notação menos pesada, vamos suprimir os parêntesis externos. A título de exemplo, escreveremos $\varphi \vee (\psi \rightarrow \xi)$ em vez de $(\varphi \vee (\psi \rightarrow \xi))$. Adicionalmente, entenderemos que \neg tem uma «ligação mais forte» (ou seja, aplica-se primeiro) do que os outros conectivos, ou seja, escreveremos $\neg\varphi \vee \psi$ em vez de $(\neg\varphi) \vee \psi$.

Alternativamente, podemos utilizar a BNF (Forma de Backus-Naur):

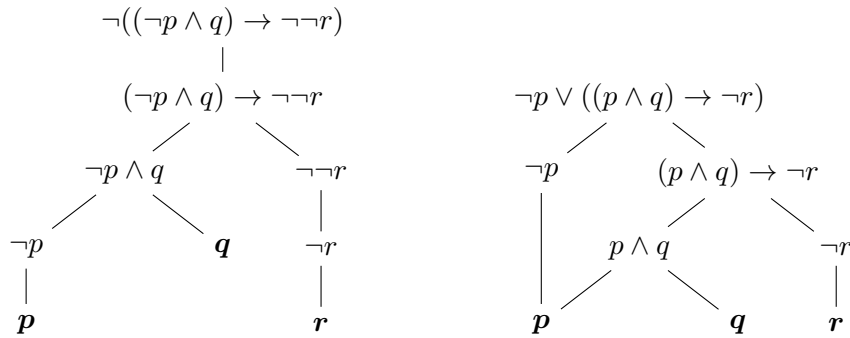
```
<formula> ::= variavel |  $\perp$  |  $\top$ 
           | ( $\neg$  <formula>)
           | (<formula>  $\wedge$  <formula>)
           | (<formula>  $\vee$  <formula>)
           | (<formula>  $\rightarrow$  <formula>)
           | (<formula>  $\leftrightarrow$  <formula>)
```

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

- $\perp, \top, p, q, r, \dots$
- $p \vee q, p \rightarrow \perp, \neg\perp, \dots$
- $(p \wedge q) \leftrightarrow q, (p \rightarrow q) \rightarrow (p \vee q), \dots$
- $(p \wedge q) \rightarrow ((p \vee q) \rightarrow q), \dots$

No entanto, se considerarmos o mesmo conjunto de variáveis, as sequências $(\perp\top)$, (pqr) , $p\neg$, $p \leftrightarrow \vee$, $(\top \rightarrow)$, $(p \wedge q) \rightarrow r$ ou $(p \wedge \rightarrow q)$ 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 construção ilustradas abaixo.



Semântica, Validade e Equivalência

É importante lembrarmos que as fórmulas bem formadas introduzidas anteriormente não são verdadeiras ou falsas por si só: tudo depende da veracidade ou falsidade das afirmações representadas pelas variáveis proposicionais que a compõem. O nosso objetivo agora será perceber de que forma podemos interpretar uma fórmula, uma vez decidido se as suas variáveis proposicionais são verdadeiras ou falsas.

De facto, a maneira mais simples de o fazer é através do preenchimento de uma tabela de verdade para cada conectivo presente na fórmula. Se tomarmos os conectivos como as ideias lógicas informais que estes representam, tudo se torna mais fácil: por exemplo, sabemos que \wedge deve representar «... e ...», pelo que podemos definir (intuitivamente) $\varphi \wedge \psi$ como verdadeira se e só se ambas as componentes forem verdadeiras. Ao proceder da mesma forma para os restantes conectivos, podemos determinar o valor de verdade de qualquer fórmula bem formada ao observar apenas as suas componentes mais simples e os seus valores de verdade.

Definição 1.1.6. 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 1.1.7. Como visto anteriormente, os símbolos \perp e \top representam proposições atómicas especiais. Para qualquer valoração v , vamos convencionar $v(\top) = 1$ e $v(\perp) = 0$.

Exemplo 1.1.8. Se p e q forem variáveis proposicionais, então uma valoração do conjunto $V = \{p, q\}$ poderá ser a função $v: V \rightarrow \{0, 1\}$ tal que $v(p) = 1$ e $v(q) = 0$.

Efectivamente, a valoração apresentada é uma das quatro possíveis atribuições de verdade para um conjunto V com duas variáveis proposicionais.

Nota 1.1.9. Em geral, se estivermos perante n variáveis proposicionais, teremos 2^n valorações distintas para o conjunto destas (uma vez que variável apenas pode receber um de dois valores de verdade).

Uma vez definida a valoração de variáveis proposicionais, o próximo passo será estender estas funções, por forma a obter o valor de verdade de quaisquer fórmulas que utilizem as variáveis em questão (tendo em consideração o significado dos conectivos lógicos presentes). Este nosso problema torna-se relativamente complicado para fórmulas muito complexas. A título de exemplo, se tivermos uma valoração $v: V \rightarrow \{0, 1\}$, onde $V = \{p, q, r\}$, tal que $p, r \mapsto 1$ e $q \mapsto 0$, qual será o valor de verdade da seguinte fórmula?

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

Suponhamos então que, de alguma forma, já sabemos o valor de verdade que vamos atribuir a duas fórmulas φ e ψ . Que valor de verdade devemos dar a $\varphi \vee \psi$?

É claro que temos liberdade de escolha, mas como \vee representa o mesmo que « ... ou ... », será sensato atribuir a $\varphi \vee \psi$ o valor 1 se pelo menos uma fórmula de $\{\varphi, \psi\}$ for verdadeira, e o valor 0 caso contrário.

O escrito imediatamente acima pode ser então resumido na seguinte tabela de verdade.

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

Podemos pensar na tabela de verdade anterior como uma maneira de combinar dois valores de verdade para obter outro, assim como $+$ combina dois números noutro. Neste caso: $1 \vee 1 = 1$, $1 \vee 0 = 1$, $0 \vee 1 = 1$ e $0 \vee 0 = 0$. A vantagem de pensarmos desta forma prende-se com o facto de conseguirmos reduzir o escrito a uma única expressão: $v(\varphi \vee \psi) = v(\varphi) \vee v(\psi)$. Apresentamos agora as tabelas de verdade para os restantes conectivos introduzidos.

φ	$\neg\varphi$	φ	ψ	$\varphi \wedge \psi$	φ	ψ	$\varphi \rightarrow \psi$	φ	ψ	$\varphi \leftrightarrow \psi$
0	1	0	0	0	0	0	1	0	0	1
0	1	0	1	0	0	1	1	0	1	0
1	0	1	0	0	1	0	0	1	0	0
1	0	1	1	1	1	1	1	1	1	1

Suponhamos agora que temos uma valoração de um conjunto de variáveis proposicionais V , $v: V \rightarrow \{0, 1\}$. Existe apenas uma maneira de estender v de forma a que consigamos obter a interpretação de qualquer fórmula que utilize as variáveis proposicionais em V e tal que, se tomarmos φ e ψ duas fórmulas, sejam satisfeitas as seguintes igualdades:

$$v(\perp) = 0$$

$$\begin{aligned}
v(\top) &= 1 \\
v(\varphi \wedge \psi) &= v(\varphi) \wedge v(\psi) \\
v(\varphi \vee \psi) &= v(\varphi) \vee v(\psi) \\
v(\varphi \rightarrow \psi) &= v(\varphi) \rightarrow v(\psi) \\
v(\varphi \leftrightarrow \psi) &= v(\varphi) \leftrightarrow v(\psi) \\
v(\neg \varphi) &= \neg v(\varphi)
\end{aligned}$$

Devemos recordar que utilizamos aqui os símbolos « \wedge , \vee , \neg , ...» com dois significados diferentes: como partes da fórmula, mas também como elementos de combinação dos valores de verdade.

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

$$\begin{aligned}
v(\neg p \rightarrow (p \vee q)) &= v(\neg p) \rightarrow v(p \vee q) \\
&= \neg v(p) \rightarrow (v(p) \vee v(q)) \\
&= \neg 1 \rightarrow (1 \vee 0) \\
&= 0 \rightarrow 1 \\
&= 1
\end{aligned}$$

Uma maneira análoga de obter a interpretação pedida no exemplo anterior seria através do preenchimento da tabela de verdade relativa à fórmula em causa, retirando a informação da linha onde $v(p) = 1$ e $v(q) = 0$. Veremos uma tal situação no próximo exemplo.

Exemplo 1.1.11. Vamos começar por obter todas as possíveis interpretações da fórmula $(p \vee q) \rightarrow q$, de acordo com as tabelas de verdade dos conectivos lógicos nela presentes (\vee , \rightarrow).

p	q	$p \vee q$	$(p \vee q) \rightarrow q$
0	0	0	1
0	1	1	1
1	0	1	0
1	1	1	1

Suponhamos agora que estamos na presença de uma valoração $v: V \rightarrow \{0, 1\}$, onde $V = \{p, q\}$, e tal que $p \mapsto 1$ e $q \mapsto 0$. Se quisermos obter a interpretação da fórmula acima indicada (para a valoração em causa), basta encontrar a linha da tabela onde $v(p) = 1$ e $v(q) = 0$ e retirar a informação na coluna $(p \vee q) \rightarrow q$. Neste caso, $v((p \vee q) \rightarrow q) = 0$.

Definição 1.1.12. Uma fórmula diz-se:

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

Para a verificação das tautologias, contingências e contradições, a técnica mais intuitiva a utilizar será o preenchimento da tabela de verdade associada à fórmula em questão (resume o estudo particular de cada valoração que se possa fazer nas variáveis proposicionais). Vejamos agora alguns exemplos de aplicação.

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

p	q	$p \wedge q$	$(p \wedge q) \rightarrow q$
0	0	0	1
0	1	0	1
1	0	0	1
1	1	1	1

p	q	$p \wedge q$	$(p \wedge q) \rightarrow p$
0	0	0	1
0	1	0	1
1	0	0	1
1	1	1	1

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 $(\neg p \vee q) \equiv (p \rightarrow q) \equiv (\neg q \rightarrow \neg p)$. Efectivamente,

p	q	$p \rightarrow q$	$\neg p$	$\neg p \vee q$	$(\neg p \vee q) \leftrightarrow (p \rightarrow q)$
0	0	1	1	1	1
0	1	1	1	1	1
1	0	0	0	0	1
1	1	1	0	1	1

p	q	$p \rightarrow q$	$\neg q$	$\neg p$	$\neg q \rightarrow \neg p$	$(p \rightarrow q) \leftrightarrow (\neg q \rightarrow \neg p)$
0	0	1	1	1	1	1
0	1	1	0	1	1	1
1	0	0	1	0	0	1
1	1	1	0	0	1	1

Podemos ainda confirmar que se verificam as seguintes equivalências:

$$\begin{array}{ll}
 (p \wedge q) \equiv (q \wedge p), & (p \vee q) \equiv (q \vee p), \\
 ((p \wedge q) \wedge r) \equiv (p \wedge (q \wedge r)), & ((p \vee q) \vee r) \equiv (p \vee (q \vee r)). \\
 (p \wedge p) \equiv p, & (p \vee p) \equiv p, \\
 (p \wedge \top) \equiv p, & (p \vee \perp) \equiv p, \\
 (p \wedge \perp) \equiv \perp, & (p \vee \top) \equiv \top
 \end{array}$$

bem como as leis de distributividade,

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

as leis de De Morgan,

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

e a lei de dupla negação, $\neg\neg p \equiv p$.

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 $\varphi \not\equiv \psi$.

A última questão que vamos explorar nesta sub-secção é a passagem das tabelas de verdade às fórmulas. Para tal, imaginemos uma tabela de verdade do tipo

p	q	r	φ
0	0	0	1
0	0	1	0
0	1	0	0
0	1	1	1
\vdots	\vdots	\vdots	\vdots

onde desconhecemos φ na sua forma explícita. Uma pergunta legítima que podemos fazer neste momento é se existe forma de obter φ explicitamente.

Vejamos que, neste caso, φ será uma fórmula verdadeira quando $p = q = r = 0$ ou quando $p = 0$ e $q = r = 1$ (de entre outras possíveis combinações). De facto, só é necessário traduzir este raciocínio para uma forma lógica. . . « φ é verdadeira quando p e q e r forem falsas ou quando p for falsa e q e r forem verdadeiras» traduz-se então em $\varphi = (\neg p \wedge \neg q \wedge \neg r) \vee (\neg p \wedge q \wedge r)$.

Em termos práticos, só é necessário observar cada linha da tabela onde φ é verdadeira, escrever as condições das variáveis da linha em causa, e fazer a disjunção de todas as condições obtidas.

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

A partir daqui, e de acordo com o escrito anteriormente, é fácil chegarmos à forma explícita de φ . Neste caso, sabemos que apenas temos $\varphi = 1$ na 1ª, 4ª, 5ª, 6ª e 8ª linhas. Assim, vamos escrever as condições relativas às variáveis:

$$\begin{aligned}\varphi_1 &= \neg p \wedge \neg q \wedge \neg r, \\ \varphi_4 &= \neg p \wedge q \wedge r, \\ \varphi_5 &= p \wedge \neg q \wedge \neg r, \\ \varphi_6 &= p \wedge \neg q \wedge r, \\ \varphi_8 &= p \wedge q \wedge r.\end{aligned}$$

Por último, resta-nos fazer a disjunção entre estas condições, obtendo

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

No entanto, podemos ainda imaginar situações onde a fórmula φ é mais vezes verdadeira do que falsa. Neste caso, é conveniente adoptar outra estratégia quanto à obtenção de φ . O método passa por olhar para as linhas da tabela onde φ toma valor 0 e fazer a conjunção da negação de cada uma das condições relativas às variáveis. De acordo com o último exemplo apresentado, teríamos:

$$\varphi_2 = p \vee q \vee \neg r, \quad \varphi_3 = p \vee \neg q \vee r, \quad \varphi_7 = \neg p \vee \neg q \vee r.$$

Desta forma, e como último passo, resta-nos apenas fazer a conjunção das negações das condições prévias, ou seja,

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

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

Demonstração. Se tivermos $L_{j_1} = \neg L_{j_2}$ para dois elementos distintos $j_1, j_2 \in J$, então certamente teremos que $\bigvee_{j \in J} L_j$ é uma tautologia e que $\bigwedge_{j \in J} L_j$ é uma contradição. Se, por outro lado, não houver índices distintos $j_1, j_2 \in J$ tais que $L_{j_1} = \neg L_{j_2}$, então sabemos que existirão valorações v, w para as quais $v(L_{j_1}) = 1$ e $w(L_{j_1}) = 0$. Desta forma, $v(\bigwedge_{j \in J} L_j) = 1$ e $w(\bigvee_{j \in J} L_j) = 0$, ou seja, $\bigwedge_{j \in J} L_j$ não é uma tautologia e $\bigvee_{j \in J} L_j$ é uma contingência. ♦

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.

Nota 1.1.24. A disjunção «vazia» (ou seja, $I = \emptyset$) será a fórmula \perp . De maneira análoga, a conjunção «vazia» será a fórmula \top .

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

A ideia por trás do resultado acima apresentado passa pela aplicação sucessiva das equivalências lógicas ligadas aos conectivos de implicação e equivalência, assim como das leis de De Morgan e das leis de distributividade:

$$\begin{aligned}\varphi \rightarrow \psi &\equiv \neg\varphi \vee \psi, & \varphi \leftrightarrow \psi &\equiv (\varphi \rightarrow \psi) \wedge (\psi \rightarrow \varphi) \\ \neg(p \vee q) &\equiv (\neg p \wedge \neg q), & \neg(p \wedge q) &\equiv (\neg p \vee \neg q), \\ (p \wedge (q \vee r)) &\equiv (p \wedge q) \vee (p \wedge r), \\ (p \vee (q \wedge r)) &\equiv (p \vee q) \wedge (p \vee r)\end{aligned}$$

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

Demonstração. Consideremos uma fórmula $\varphi = \bigwedge_{i \in I} \varphi_i$ na FNC, onde cada φ_i é uma \vee -cláusula. Se cada uma das φ_i for uma tautologia, então para qualquer valoração v teremos $v(\varphi_i) = 1$ (com $i \in I$); portanto $v(\varphi) = v(\bigwedge_{i \in I} \varphi_i) = \bigwedge_{i \in I} v(\varphi_i) = 1$, i.e., φ é uma tautologia. Por outro lado, se existir algum φ_i que não é uma tautologia, existirá certamente uma valoração w para a qual $w(\varphi_i) = 0$; portanto $w(\varphi) = 0$, ou seja, φ não será uma tautologia.

A demonstração para o caso das FND pode ser feita com recurso à mesma linha de pensamento, tendo em conta a dualidade dos conceitos. \blacklozenge

Exemplo 1.1.27. Considerando quatro variáveis proposicionais p, q, r, s , e a fórmula

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

vamos colocar φ na FNC:

1. Substituímos as equivalências (\leftrightarrow) por implicações (\rightarrow):

$$(((p \rightarrow q) \wedge (q \rightarrow p)) \rightarrow (r \rightarrow s)) \wedge (q \rightarrow \neg(p \wedge r)).$$

2. Convertemos todas as implicações em disjunções ($p \rightarrow q \equiv \neg p \vee q$):

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

3. Movemos as negações para o interior das componentes:

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

4. Aplicamos as negações às componentes:

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

Nota 1.1.28. Podemos ainda observar, de forma rápida, que o método utilizado para encontrar uma fórmula φ explicitamente (a partir da sua tabela de verdade) faz com que φ esteja na FND.

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 que avalia todas as fórmulas de $\{\varphi_1, \dots, \varphi_n\}$ em 1.

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 $q \mapsto 1$.

O seguinte exemplo mostra que a lógica proposicional pode ser utilizada como uma linguagem para espessar «restrições».

Exemplo 1.1.31 (<http://www.cs.ox.ac.uk/people/james.worrell/lectures.html>). Vamos analisar o sudoku do ponto de vista lógico. Para todos os $i, j, k \in \{1, 2, \dots, 9\}$, a proposição atômica P_{ijk} representará a afirmação «a posição (i, j) contém o número k ».

Desta forma, e de acordo com o quadro representado abaixo, temos que as fórmulas

$$P_{122}, P_{136}, P_{271}, \dots, P_{984}$$

devem ser válidas.

	2	6						
							1	7
		3	1	6				
	6			5		8		3
		9	2	6	1	7		
5		4		8			6	
			8		4	3		
	4	8						
						9	4	

Além disso, é possível expressarmos logicamente as regras que nos permitem preencher o quadro:

- cada número aparece em cada linha:

$$F_1 = (P_{111} \vee P_{121} \vee \dots \vee P_{191}) \wedge (P_{112} \vee P_{122} \vee \dots) \wedge \dots = \bigwedge_{i=1}^9 \bigwedge_{k=1}^9 \bigvee_{j=1}^9 P_{ijk},$$

- cada número aparece em cada coluna:

$$F_2 = (P_{111} \vee P_{211} \vee \cdots \vee P_{911}) \wedge (P_{112} \vee P_{212} \vee \cdots) \wedge \cdots = \bigwedge_{j=1}^9 \bigwedge_{k=1}^9 \bigvee_{i=1}^9 P_{ijk},$$

- cada número aparece em cada bloco 3×3 :

$$F_3 = \bigwedge_{k=1}^9 \bigwedge_{u=0}^2 \bigwedge_{v=0}^2 \bigvee_{i=1}^3 \bigvee_{j=1}^3 P_{3u+i, 3v+j, k},$$

- nenhuma posição pode ter dois números:

$$F_4 = \neg(P_{111} \wedge P_{112}) \wedge \neg(P_{111} \wedge P_{113}) \wedge \cdots = \bigwedge_{i=1}^9 \bigwedge_{j=1}^9 \bigwedge_{1 \leq k < k' \leq 9} \neg(P_{ijk} \wedge P_{ijk'}).$$

Desta forma, resolver o jogo é o mesmo que verificar que o conjunto de fórmulas

$$\Gamma = \{P_{122}, P_{136}, P_{271}, \dots, P_{984}, F_1, F_2, F_3, F_4\}$$

é consistente. Adicionalmente, podemos ver que o número de variáveis a considerar é $9^3 = 729$, portanto, a correspondente tabela de verdade terá $2^{729} > 10^{200}$ linhas.

Consequência Semântica e Demonstrações

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 $p \rightarrow q$, ou seja, que $p \vee q, p \rightarrow q \models q \vee \neg p$.

p	q	$p \vee q$	$p \rightarrow q$	$\neg p$	$q \vee \neg p$	
0	0	0	1	1	1	
0	1	①	①	1	①	←
1	0	1	0	0	0	
1	1	①	①	0	①	←

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

Demonstração. (\Rightarrow) Suponhamos que ψ é consequência semântica de $\varphi_1, \dots, \varphi_n$ e seja v uma valoração. Se $v(\varphi_1 \wedge \cdots \wedge \varphi_n) = 1$, então, para cada $i = 1, \dots, n$, $v(\varphi_i) = 1$. Portanto,

por definição de consequência semântica, $v(\psi) = 1$. Logo, $v((\varphi_1 \wedge \cdots \wedge \varphi_n) \rightarrow \psi) = 1$.

Por outro lado, se $v(\varphi_1 \wedge \cdots \wedge \varphi_n) = 0$, então $v((\varphi_1 \wedge \cdots \wedge \varphi_n) \rightarrow \psi) = 1$.

(\Leftarrow) Suponhamos que $((\varphi_1 \wedge \cdots \wedge \varphi_n) \rightarrow \psi)$ é válida e seja v uma valoração. Se $v(\varphi_i) = 1$ para cada $i = 1, \dots, n$, então $v(\varphi_1 \wedge \cdots \wedge \varphi_n) = 1$ e por isso $v(\psi) = 1$. Logo, ψ é consequência semântica de $\varphi_1, \dots, \varphi_n$. \blacklozenge

Nota 1.1.35. Dadas fórmulas $\varphi_1, \varphi_2, \psi$, teremos $\dots, \varphi_1 \wedge \varphi_2 \models \psi$ se e só se $\dots, \varphi_1, \varphi_2 \models \psi$.

Uma das formas de validar as consequências semânticas é fazer a verificação de todas as possíveis valorações (ou seja, preencher a tabela de verdade). No entanto, e como veremos mais à frente, na lógica de primeira ordem tal não será muito útil (em geral, existe uma infinidade de interpretações possíveis...). Em alternativa, podemos fazer uma prova (dedução ou argumentação), ou seja, escrever uma sequência de fórmulas

$$\varphi \rightarrow \psi, \psi \rightarrow \theta, \boxed{\dots}, \varphi \rightarrow \theta,$$

onde $\boxed{\dots}$ representa uma sequência de fórmulas justificadas por $\varphi \rightarrow \psi$ e $\psi \rightarrow \theta$ através das seguintes **regras de inferência** da lógica proposicional:

$$\begin{array}{c} \frac{\varphi \quad \psi}{\varphi \wedge \psi} (\wedge \mathcal{I}) \qquad \frac{\varphi \wedge \psi}{\varphi} (\wedge \mathcal{E}_1) \qquad \frac{\varphi \wedge \psi}{\psi} (\wedge \mathcal{E}_2) \\[20pt] \frac{\varphi}{\varphi \vee \psi} (\vee \mathcal{I}_1) \qquad \frac{\psi}{\varphi \vee \psi} (\vee \mathcal{I}_2) \qquad \frac{\varphi \vee \psi \quad \begin{array}{|c|} \hline \varphi \\ \vdots \\ \theta \end{array} \quad \begin{array}{|c|} \hline \psi \\ \vdots \\ \theta \end{array}}{\theta} (\vee \mathcal{E}) \\[20pt] \frac{\begin{array}{|c|} \hline \varphi \\ \vdots \\ \psi \end{array}}{\varphi \rightarrow \psi} (\rightarrow \mathcal{I}) \qquad \frac{\varphi \quad \varphi \rightarrow \psi}{\psi} (\rightarrow \mathcal{E}) \\[20pt] \frac{}{\bot} (\bot \mathcal{E}) \qquad \frac{}{\varphi \vee \neg \varphi} (\text{EM}) \end{array}$$

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

Exemplo 1.1.37. Vamos verificar que $\varphi \rightarrow \psi, \psi \rightarrow \theta \vdash \varphi \rightarrow \theta$.

1	$\varphi \rightarrow \psi$		• por hipótese, $\varphi \rightarrow \psi$ e $\psi \rightarrow \theta$;
2	$\psi \rightarrow \theta$		
3	φ	H	• com o objectivo de provar $\varphi \rightarrow \theta$, suponhamos φ (temporariamente). Como sabemos $\varphi \rightarrow \psi$, temos ψ ; por outro lado, como sabemos $\psi \rightarrow \theta$, temos θ ;
4	ψ	$\rightarrow E, 1, 3$	
5	θ	$\rightarrow E, 2, 4$	
6	$\varphi \rightarrow \theta$	$\rightarrow I, 3, 5$	• assim, concluímos $\varphi \rightarrow \theta$ (e retiramos φ).

Exemplo 1.1.38. Vamos verificar que $\varphi \rightarrow \psi \vdash \varphi \rightarrow (\varphi \wedge \psi)$.

			• por hipótese, $\varphi \rightarrow \psi$;
1	$\varphi \rightarrow \psi$		
2	φ	H	• com o objectivo de provar $\varphi \rightarrow (\varphi \wedge \psi)$, suponhamos φ (temporariamente). Como sabemos $\varphi \rightarrow \psi$, temos ψ , ou seja, podemos ter $\varphi \wedge \psi$;
3	ψ	$\rightarrow E, 1, 2$	
4	$\varphi \wedge \psi$	$\wedge I, 2, 3$	
5	$\varphi \rightarrow (\varphi \wedge \psi)$	$\rightarrow I, 2, 4$	• assim, concluímos $\varphi \rightarrow (\varphi \wedge \psi)$ (e ultimamente retiramos φ).

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

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

Nota 1.1.41. Os enunciados dos últimos resultados podem tomar uma forma mais simples. Para tal, consideremos ψ uma fórmula e $\Gamma = \{\varphi_1, \dots, \varphi_n\}$ um conjunto de fórmulas. O Teorema da Correção 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 Completeness diz-nos que «tudo o que é válido se consegue provar», ou seja, que se $\Gamma \models \psi$, então $\Gamma \vdash \psi$.

O último tópico que vamos abordar nesta sub-secção será motivado pelo resultado que apresentamos a seguir.

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

Demonstração. Por definição, $\Gamma \models \psi$ se e só se, para cada valoração v , se $v(\varphi) = 1$ para cada $\varphi \in \Gamma$, então $v(\psi) = 1$. Por outro lado, $\Gamma \cup \{\neg\psi\}$ é inconsistente se e só se, para cada valoração v , se $v(\varphi) = 1$ para cada $\varphi \in \Gamma$, então $v(\neg\psi) = 0$. ♦

Portanto, a questão principal prende-se com a forma de verificar a inconsistência de um conjunto $\{\theta_1, \dots, \theta_n\}$ de fórmulas. Sem perda de generalidade, podemos supor que cada fórmula θ_i está na forma normal conjuntiva. Ainda mais, como o conjunto $\{\dots, \psi_1 \wedge \psi_2\}$ é consistente se e só se $\{\dots, \psi_1, \psi_2\}$ é consistente, podemos supor que $\{\theta_1, \dots, \theta_n\}$ é um conjunto de cláusulas. No que se segue, é conveniente identificar uma cláusula com o conjunto de literais que ocorrem na cláusula (por causa da associatividade, comutatividade e idempotência da disjunção). Assim, não distinguimos entre

$$p \vee \neg q \vee p, \quad \neg q \vee p \vee p, \quad \neg q \vee p,$$

e a fórmula \perp corresponde ao conjunto vazio de literais.

De facto, o problema resolve-se se conseguirmos deduzir uma contradição, ou seja, se conseguirmos obter uma sequência de fórmulas

$$\vartheta_1 \quad \vartheta_2 \quad \dots \quad \perp,$$

onde $\vartheta_i \in \Gamma \cup \{\neg\psi\}$ ou ϑ_i é consequência de $\Gamma \cup \{\neg\psi\}$. Nesta fase, vamos apenas considerar a **regra de resolução**:

$$\frac{\neg\psi \vee \theta \quad \psi \vee \varphi}{\theta \vee \varphi} \text{ (Res) }, \quad \text{para fórmulas } \varphi, \psi, \theta.$$

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

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

Escrevemos $\Gamma \vdash \perp$ quando existe uma dedução de \perp a partir de $\Gamma = \{\varphi_1, \dots, \varphi_n\}$.

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

Demonstração. (\Leftarrow) Aqui basta de observar que, se

- um conjunto Γ de cláusulas é consistente, e
- ψ é uma resolvente de cláusulas de Γ ,

então $\Gamma \cup \{\psi\}$ é consistente.

(\Rightarrow) Provamos a implicação por indução sobre o número de variáveis em $\Gamma = \{\varphi_1, \dots, \varphi_k\}$. Se Γ tem zero variáveis, então Γ é vazio ou $\Gamma = \{\perp\}$. Se Γ é inconsistente, então $\Gamma = \{\perp\}$ e neste caso deduzimos \perp numa linha.

Seja agora $n \in \mathbb{N}$ com $n \geq 1$, e suponhamos agora que a implicação é verdadeira para cada conjunto de fórmulas com menos do que n variáveis. Suponhamos que Γ contém precisamente as variáveis p_1, \dots, p_n . Consideremos os conjuntos

$$\Gamma_0 = \Gamma[p_n \mapsto \perp] \quad \text{e} \quad \Gamma_1 = \Gamma[p_n \mapsto \top]$$

onde substituímos p_n por \perp e por \top , respetivamente. Isto significa que Γ_1 obtém-se apagando em Γ todas as cláusulas que contêm p_n , e apagar todas as ocorrências de $\neg p_n$ nas cláusulas de Γ . De forma semelhante, Γ_0 obtém-se apagando em Γ todas as cláusulas que contêm $\neg p_n$, e apagar todas as ocorrências de p_n .

Suponhamos que Γ é inconsistente, então Γ_0 e Γ_1 também são inconsistentes. Como Γ_0 tem menos do que n variáveis, por hipótese da indução existe uma dedução $\varphi_0, \varphi_1, \dots, \varphi_m = \perp$ a partir de Γ_0 . «Re-acrescentando» nas fórmulas acima outra vez p_n (também nas resolventes), obtém-se a partir de Γ uma das deduções

$$\varphi'_0, \varphi'_1, \dots, \varphi'_m = \perp \quad \text{ou} \quad \varphi'_0, \varphi'_1, \dots, \varphi'_m = \{p_n\}.$$

No primeiro caso temos que $\Gamma \vdash \perp$. No segundo caso aplicamos o mesmo raciocínio ao Γ_1 o que produz ou $\Gamma \vdash \perp$ ou uma dedução de $\neg p_n$ a partir de Γ . No segundo caso temos então uma dedução de p_n e uma dedução de $\neg p_n$ a partir de Γ , com mais um passo obtém-se \perp . ♦

Nota 1.1.44. Para um conjunto $\Gamma = \{\varphi_1, \dots, \varphi_k\}$ de cláusulas, consideremos o conjunto

$$\text{Res}(\Gamma) = \Gamma \cup \{\psi \mid \psi \text{ é resolvente de cláusulas em } \Gamma\}.$$

Além disso, definimos recursivamente os conjuntos

$$\begin{aligned} \text{Res}^0(\Gamma) &= \Gamma, \\ \text{Res}^{n+1}(\Gamma) &= \text{Res}(\text{Res}^n(\Gamma)) \quad (n \in \mathbb{N}), \\ \text{Res}^* &= \bigcup_{n \in \mathbb{N}} \text{Res}^n. \end{aligned}$$

Por definição,

$$\Gamma_0 \subseteq \Gamma_1 \subseteq \dots \subseteq \Gamma_n \subseteq \dots \subseteq \Gamma^*$$

e Γ é inconsistente se e somente se $\perp \in \Gamma^*$. Recordamos que identificamos as cláusulas com conjuntos de literais, assim, cada $\text{Res}^n(\Gamma)$ é um conjunto de conjuntos de literais. Como Γ é finito, só há um número finito de literais e por isso só há um número finito de resolventes. Portanto, existe $n \in \mathbb{N}$ tal que

$$\Gamma_n = \Gamma_{n+1} = \dots = \Gamma^*.$$

Consequentemente, se calculamos a partir de Γ sucessivamente todas as resolventes, ou num número finito de passos obtemos \perp e concluímos que Γ é inconsistente, ou a partir de um certo passo não há mais resolventes e concluímos que Γ é consistente.

Nota 1.1.45. 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).

Exemplo 1.1.46. Vamos verificar $p \rightarrow q, q \rightarrow r \models p \rightarrow r$. Começamos por considerar as fórmulas $p \rightarrow q$, $q \rightarrow r$ e $\neg(p \rightarrow r)$, ou seja, $\neg p \vee q$, $\neg q \vee r$ e $\neg(\neg p \vee r) \equiv p \wedge \neg r$. A partir daqui, obtemos as cláusulas $\neg p \vee q$, $\neg q \vee r$, p e $\neg r$.

Nesta fase, conseguimos (finalmente) obter a sequência de fórmulas pretendida:

1.	$\neg p \vee q$	Hip.
2.	$\neg q \vee r$	Hip.
3.	p	Hip.
4.	$\neg r$	Hip.
5.	q	Res (1,3)
6.	r	Res (2,5)
7.	\perp	Res (4,6)

Exemplo 1.1.47. Será que $p, p \rightarrow q, \neg(r \wedge \neg q) \models r$? Para responder, consideremos as cláusulas p , $\neg p \vee q$, $\neg r \vee q$, $\neg r$. Obtemos a cláusula q como a resolvente de p e de $\neg p \vee q$, mas não há outras resolventes. Logo, a afirmação

$$p, p \rightarrow q, \neg(r \wedge \neg q) \models r$$

é falsa.

1.2 Sintaxe e Semântica de lógica de primeira ordem

Vimos anteriormente que na lógica proposicional podemos expressar, por exemplo, a fórmula $(p \wedge q) \rightarrow r$. Agora, na lógica de primeira ordem, poderemos ser um pouco mais específicos sobre a estrutura dos átomos e, inclusivamente, quantificar as fórmulas:

$$\forall x \forall y ((\text{par}(x) \wedge \text{par}(y)) \rightarrow \text{par}(x + y)).$$

A título de exemplo, podemos expressar o pensamento «todos os gatos têm garras»:

$$\forall x (\text{gato}(x) \rightarrow \text{garras}(x)).$$

Definição 1.2.1. Um alfabeto de 1ª 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 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);

Exemplo 1.2.2. O alfabeto da teoria dos espaços vectoriais reais consiste (além dos símbolos da lógica e das variáveis):

- de um símbolo constante «0»;
- para cada $\alpha \in \mathbb{R}$, de um símbolo de função « $\alpha \cdot -$ » de uma variável;
- um símbolo de função «+» de duas variáveis.

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.

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

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

- $P(t_1, \dots, t_n)$ 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.

Exemplo 1.2.6.

$$\underbrace{\forall x, y, z \underbrace{\underbrace{(x < y)}_{\text{fórmula}} \rightarrow \underbrace{(x + z < y + z)}_{\text{fórmula}}}_{\text{fórmula}}}$$

termo termo

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.

Atentemos nas seguintes fórmulas...

- $\forall x (\text{gato}(x) \rightarrow \text{garras}(x))$: o alcance de « \forall » é « $(\text{gato}(x) \rightarrow \text{garras}(x))$ ».
- $(\forall x \exists y x < y) \wedge (a < x)$: o alcance de « \forall » é « $\exists y x < y$ », enquanto que o alcance de « \exists » é « $x < y$ ».
- $\forall x \exists y (x < y \wedge a < x)$: o alcance de « \forall » é « $\exists y (x < y \wedge a < x)$ », enquanto que o alcance de « \exists » é « $x < y \wedge a < x$ ».

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 1.2.11.

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

- $\forall x (\text{gato}(x) \rightarrow \text{garras}(x))$: a variável x ocorre ligada. Neste caso, a fórmula é fechada.

- $(\forall x \exists y x < y) \wedge (a < x)$: a variável y ocorre ligada e a variável x ocorre livre e ligada. Neste caso, a fórmula não é fechada.
- $\forall x \exists y (x < y \wedge a < x)$: as variáveis x e y ocorrem ligadas. Neste caso, a fórmula é fechada.

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** $f^{\mathcal{M}}: D^n \rightarrow D$;
- 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**.

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:

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

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

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

temos:

- $v(f(a, x)) = |0| - |-2| = -2$.
- $v(f(f(x, y), a)) = |(|-2| - |1|)| - |0| = 1$.
- $v(f(f(x, a), f(y, f(x, a)))) = |(|-2| - |0|)| - |(|1| - |(|-2| - |0|)|)| = 1$.

Antes de passarmos ao conceito de validade, e por forma a integrarmos fórmulas com quantificadores, vamos introduzir uma ligeira modificação nas valorações.

Definição 1.2.15. Dada uma valoração v , variáveis x, y e um elemento $a \in D$, $v^{\frac{x}{a}}$ denotará a valoração definida por

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

Agora sim, temos todas as ferramentas necessárias para definir a validade numa estrutura \mathcal{M} , consoante uma dada valoração.

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:

- $(\mathcal{M}, v) \models t_1 = t_2$ 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 $a \in D$, $(\mathcal{M}, v \frac{x}{a}) \models \varphi$;
- $(\mathcal{M}, v) \models \forall x \varphi$ 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 $(\mathcal{M}, v) \models \varphi$.

Nota 1.2.18. Se uma fórmula φ não tiver variáveis livres, a interpretação destas será inútil na interpretação de φ .

Nota 1.2.19. Nesta nota explicaremos com alguns exemplos o conceito de interpretação de fórmulas na lógica de 1ª ordem.

Para começar, consideremos uma linguagem com apenas um símbolo de constante c . O que significa, por exemplo, a fórmula

$$x = c?$$

É válida? Ora, para poder responder, precisamos de saber o significado de cada uma das componentes da fórmula. Seguramente não temos grandes dúvidas sobre o significado do símbolo « $=$ ». Além disso, o símbolo c deve representar algum «valor», mas de que tipo? Para começar, especificamos um «universo de discurso», ou seja, um conjunto. Neste exemplo escolhemos o conjunto $D = \{1, 2, 3\}$, e associamos ao símbolo de constante c o valor $2 \in D$. Assim está explicado o significado de cada símbolo da nossa linguagem, com a exceção das variáveis, e chamamos esta parte da interpretação *estrutura*, denotada por \mathcal{M} . Mas ainda não podemos avaliar a fórmula $x = c$, pois falta de saber a interpretação da variável x . Aqui entra o conceito de *valoração*: uma valoração v associa a cada variável um elemento de D . Formalmente trata-se de uma função

$$v: \{\text{os variáveis}\} \longrightarrow D.$$

No caso do nosso exemplo basta de saber a imagem da variável x . Por exemplo, se consideramos $v(x) = 2$, então a fórmula $x = c$ é válida na interpretação (\mathcal{M}, v) porque $2 = 2$ em D , e escrevemos

$$(\mathcal{M}, v) \models x = c.$$

Claro, se consideramos uma função v com $v(x) = 1$, então a fórmula $x = c$ não é válida nesta interpretação porque $1 \neq 2$ em D , neste caso escrevemos

$$(\mathcal{M}, v) \not\models x = c.$$

Continuamos com uma valoração v com $v(x) = 1$, mas consideremos a seguir a fórmula

$$\exists x x = c.$$

A fórmula é válida? Intuitivamente sim, claramente um tal x «existe», embora este x «não é 1». De facto, neste caso não precisamos de saber *a priori* a interpretação do x porque o quantificador « \exists » altera o estado da variável. Assim, $\exists x x = c$ é válida quando $x = c$ é válida para alguma «modificação» de v em x . Para expressar esta ideia, consideremos a valoração v_a^x que interpreta x como a , isto é, $v_a^x(x) = a$, e v_a^x não altera a interpretação dos outros variáveis. Agora podemos expressar a nossa intuição da forma rigorosa:

$$(\mathcal{M}, v) \models \exists x x = c$$

quando, para algum $a \in D$,

$$(\mathcal{M}, v_a^x) \models x = c.$$

Neste caso consideremos $a = 2$, portanto, $v^{\frac{x}{2}}(x) = 2$, logo

$$(\mathcal{M}, v^{\frac{x}{2}}) \models x = c$$

e por isso

$$(\mathcal{M}, v) \models \exists x x = c.$$

Para ter um exemplo mais complexo, consideremos a seguir uma linguagem com um símbolo de predicado R de dois argumentos e um símbolo de predicado S de um argumento. Portanto, para poder interpretar fórmulas nesta linguagem, precisamos de indicar o significado destes símbolos, e neste exemplo escolhemos a seguinte estrutura \mathcal{M} :

- o «universo de discurso» é o conjunto $D = \{1, 2, 3\}$,
- a interpretação do símbolo R é o conjunto $R = \{(1, 1), (1, 2), (1, 3), (2, 2), (3, 3), (3, 2)\} \subseteq D^2$,
- a interpretação do símbolo S é o conjunto $S = \{1, 3\} \subseteq D$.

Para não sobrecarregar a notação, utilizamos aqui a mesma designação para os símbolos de predicado e a sua interpretação. Além disso, consideremos uma valoração v com $v(x) = 3$ e $v(y) = 2$. Começamos com dois exemplos simples:

1. a fórmula $R(x, y)$ é válida nesta interpretação porque $(3, 2) \in R$; em símbolos: $(\mathcal{M}, v) \models R(x, y)$.

2. a fórmula $S(y)$ não é válida nesta interpretação porque $v(y) = 2 \notin S$.

Analisamos agora a fórmula

$$\forall y (S(x) \wedge R(x, y)).$$

Por definição, uma fórmula « $\forall y (\dots \text{algo} \dots)$ » é válida nesta interpretação quando « $(\dots \text{algo} \dots)$ » é válida para todas as interpretações de y , não apenas para $v(y) = 2$. Portanto, tendo em conta que $D = \{1, 2, 3\}$, temos de verificar se

$$(\mathcal{M}, v^{\frac{y}{1}}) \models (S(x) \wedge R(x, y)), \quad (\mathcal{M}, v^{\frac{y}{2}}) \models (S(x) \wedge R(x, y)), \quad \text{e} \quad (\mathcal{M}, v^{\frac{y}{3}}) \models (S(x) \wedge R(x, y)).$$

Seguindo a definição, $(\mathcal{M}, v^{\frac{y}{1}}) \models (S(x) \wedge R(x, y))$ precisamente se

$$(\mathcal{M}, v^{\frac{y}{1}}) \models S(x) \quad \text{e} \quad (\mathcal{M}, v^{\frac{y}{1}}) \models R(x, y).$$

De facto, $(\mathcal{M}, v^{\frac{y}{1}}) \models S(x)$ porque $v^{\frac{y}{1}}(x) = v(x) = 3 \in S$; no entanto, $(\mathcal{M}, v^{\frac{y}{1}}) \not\models R(x, y)$ porque $(3, 1) \notin R$. Como logo o primeiro caso falha, já não precisamos de verificar os outros dois e podemos afirmar que $\forall y (S(x) \wedge R(x, y))$ não é válida em (\mathcal{M}, v) .

Finalmente, analisamos a fórmula

$$\exists x \forall y (S(x) \wedge R(x, y))$$

na mesma interpretação (\mathcal{M}, v) . Tal como no primeiro exemplo, esta fórmula é válida nesta interpretação se encontramos um $a \in D$ com

$$(\mathcal{M}, v^{\frac{x}{a}}) \models \forall y (S(x) \wedge R(x, y)).$$

Olhando para a interpretação do S , não parece muito promissor considerar $a = 2$, e olhando para a interpretação de R , parece sensato considerar $a = 1$. Sendo assim, perguntamos se

$$(\mathcal{M}, v^{\frac{x}{1}}) \models \forall y (S(x) \wedge R(x, y));$$

para responder, temos de analisar se

$$(\mathcal{M}, v^{\frac{x}{1} \frac{y}{1}}) \models (S(x) \wedge R(x, y)), \quad (\mathcal{M}, v^{\frac{x}{1} \frac{y}{2}}) \models (S(x) \wedge R(x, y)), \quad \text{e} \quad (\mathcal{M}, v^{\frac{x}{1} \frac{y}{3}}) \models (S(x) \wedge R(x, y)).$$

Mas isto é o caso porque $1 \in S$ e $(1, 1) \in R$, $(1, 2) \in R$ e $(1, 3) \in R$. Tudo dito,

$$(\mathcal{M}, v) \models \exists x \forall y (S(x) \wedge R(x, y)).$$

Como último ponto, observamos que a interpretação de fórmulas é definida *recursivamente*: a validade de uma fórmula depende da validade das suas subfórmulas.

Exemplo 1.2.20. Vamos interpretar os seguintes termos e fórmulas em $D = \mathbb{R}$ (onde os símbolos «comuns» têm o significado usual):

Expressão	Interpretação
$\cos(\pi) + 3$	$2 \in \mathbb{R}$
$3 < 4$	válida
$x < 4$	depende da interpretação de x
$\forall x \ x < 4$	não válida
$\forall y \ y > 4$	não válida
$\forall y \ \exists y \ y < 4$	válida
$\forall x \ ((x < 4) \rightarrow (1 = 0))$	não válida
$\forall x \ \exists y \ x < y$	válida
$\exists x \ \forall y \ x \leq y$	não válida

Exemplo 1.2.21. Um espaço vectorial pode ser considerado como um modelo para as seguintes fórmulas (no alfabeto da teoria dos espaços vectoriais):

1. $\forall u \ \forall v \ u + v = v + u;$
2. $\forall u \ \forall v \ \forall w \ u + (v + w) = (u + v) + w;$
3. $\forall u \ u + 0 = u;$
4. $\forall u \ 0 \cdot u = 0;$
5. $\forall u \ 1 \cdot u = u;$
6. $\forall u \ \alpha \cdot (\beta \cdot u) = (\alpha\beta) \cdot u;$
7. $\forall u \ (\alpha + \beta) \cdot u = (\alpha \cdot u) + (\beta \cdot u);$
8. $\forall u \ \forall v \ \alpha \cdot (u + v) = (\alpha \cdot u) + (\alpha \cdot v).$

À semelhança do que foi feito para a lógica proposicional, vamos agora introduzir os conceitos de tautologia, contingência, equivalência e consequência semântica das fórmulas de 1ª ordem.

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.

Nota 1.2.23. Dizer que uma fórmula φ é inconsistente é o mesmo que dizer que $\neg\varphi$ é uma tautologia (fórmula válida). Ainda relativamente à validade, é usual escrevermos apenas $\models \psi$ quando ψ é uma tautologia.

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

Nota 1.2.26. As regras de dedução «natural» da lógica proposicional admitem uma certa extensão para a lógica de primeira ordem. Tal como na lógica proposicional, e tendo como base estas regras de dedução, conseguimos agora definir $\varphi_1, \dots, \varphi_n \vdash \psi$ e obter

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

No entanto, nesta secção, vamos ainda considerar o método de resolução, conforme o próximo exemplo.

Exemplo 1.2.27. O nosso objectivo será fazer a dedução de

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

Para tal, devemos começar por expressar tal pensamento numa linguagem de 1ª ordem:

$$\forall x (\text{gato}(x) \rightarrow \text{garras}(x)), \text{gato}(\text{Tom}) \models \text{garras}(\text{Tom}).$$

Aqui, convém termos em atenção que «gato» e «garras» são símbolos de predicado de um argumento e que «Tom» é um símbolo constante.

De acordo com as ideias anteriormente exploradas, vamos preparar as fórmulas para a dedução (converter os antecedentes na FNC e negar o consequente):

$$\begin{aligned} &\forall x (\text{gato}(x) \rightarrow \text{garras}(x)), \text{gato}(\text{Tom}), \text{garras}(\text{Tom}) \\ &\quad \downarrow \\ &\neg\text{gato}(x) \vee \text{garras}(x), \text{gato}(\text{Tom}), \neg\text{garras}(\text{Tom}). \end{aligned}$$

Nesta passagem não escrevemos os quantificadores, mas não os esquecemos.

Por último, começamos a dedução:

$$\text{gato}(\text{Tom}) \quad \neg\text{gato}(x) \vee \text{garras}(x) \quad \dots$$

Nesta passagem, e para prosseguirmos com a dedução, é intuitivo especializar a variável, substituindo « x » por «Tom» (uma vez que a fórmula é válida «para todos»). Assim,

$$\text{gato}(\text{Tom}) \quad \neg\text{gato}(\text{Tom}) \vee \text{garras}(\text{Tom}) \quad \text{garras}(\text{Tom}) \quad \neg\text{garras}(\text{Tom}) \quad \perp.$$

1.3 Formas Normais

■ A partir de agora suponhamos que o domínio da interpretação não é vazio.

Vamos começar por adaptar ligeiramente a definição das fórmulas normais introduzidas no âmbito da lógica proposicional.

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.

Relativamente às formas normais conjuntiva e disjuntiva (FNC e FND), a definição anteriormente dada (Definição 1.1.21) mantém-se, ou seja:

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

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.

É agora absolutamente legítimo perguntarmos de que forma podemos obter/transformar uma dada fórmula na sua FNP. Essencialmente, devemos aplicar os seguintes pontos:

- 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 :

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

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

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

prenex.

$$\begin{aligned}\forall x P(x) \rightarrow \exists x Q(x) &\equiv \neg(\forall x P(x)) \vee (\exists x Q(x)) \\ &\equiv \exists x \neg P(x) \vee \exists x Q(x) \\ &\equiv \exists x \neg P(x) \vee Q(x).\end{aligned}$$

Exemplo 1.3.5. Vamos transformar a fórmula

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

para a forma normal prenex.

$$\begin{aligned}\forall x \forall y (\exists x (P(x, z) \wedge P(y, z))) \rightarrow (\exists u Q(x, y, u)) \\ &\equiv \forall x \forall y (\neg(\exists x (P(x, z) \wedge P(y, z))) \vee (\exists u Q(x, y, u))) \\ &\equiv \forall x \forall y (\forall z (\neg P(x, z) \vee \neg P(y, z)) \vee (\exists u Q(x, y, u))) \\ &\equiv \forall x \forall y \forall z \exists u (\neg P(x, z) \vee \neg P(y, z) \vee Q(x, y, u)).\end{aligned}$$

No entanto, e embora não pareça, a forma de transformar uma dada fórmula na FNP não é única (devido às possíveis trocas de quantificadores). De facto, o processo pode tomar mais (ou menos) passos consoante a abordagem feita. Veremos tal questão em detalhe no próximo exemplo.

Exemplo 1.3.6. Vamos transformar $(\varphi \vee \exists x \psi) \rightarrow \forall z \rho$ na FNP.

$$\begin{aligned}(\varphi \vee \exists x \psi) \rightarrow \forall z \rho &\equiv (\exists x (\varphi \vee \psi)) \rightarrow \forall z \rho \\ &\equiv \neg(\exists x (\varphi \vee \psi)) \vee \forall z \rho \\ &\equiv (\forall x \neg(\varphi \vee \psi)) \vee \forall z \rho \\ &\equiv \forall x (\neg(\varphi \vee \psi) \vee \forall z \rho) \\ &\equiv \forall x ((\varphi \vee \psi) \rightarrow \forall z \rho) \\ &\equiv \forall x (\forall z ((\varphi \vee \psi) \rightarrow \rho)) \\ &\equiv \forall x \forall z ((\varphi \vee \psi) \rightarrow \rho).\end{aligned}$$

No entanto, esta não é a única FNP equivalente à fórmula original. Se começarmos por lidar com o consequente, ao invés do antecedente, podemos obter

$$\begin{aligned}(\varphi \vee \exists x \psi) \rightarrow \forall z \rho &\equiv \forall z ((\varphi \vee \exists x \psi) \rightarrow \rho) \\ &\equiv \forall z ((\exists x (\varphi \vee \psi)) \rightarrow \rho) \\ &\equiv \forall z (\forall x ((\varphi \vee \psi) \rightarrow \rho)) \\ &\equiv \forall z \forall x ((\varphi \vee \psi) \rightarrow \rho).\end{aligned}$$

Tal acontece dado que a ordem dos dois quantificadores universais com o mesmo alcance não altera o significado/valor de verdade da fórmula em questão.

Forma Normal de Skolem e Eliminação dos Quantificadores « \exists »

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 »).

Nota 1.3.8. Como $\forall x_1 \forall x_2 \cdots \forall x_n (\varphi \wedge \psi) \equiv (\forall x_1 \forall x_2 \cdots \forall x_n \varphi) \wedge (\forall x_1 \forall x_2 \cdots \forall x_n \psi)$, qualquer fórmula na FNS pode escrever-se como uma conjunção de fórmulas na FNS $\forall x_1 \cdots \forall x_n \varphi_i$, onde φ_i é uma \forall -cláusula $L_1 \vee \cdots \vee L_n$.

À primeira vista, a obtenção de uma fórmula na FNS pode parecer um processo excepcionalmente complicado. No entanto, existe um procedimento de transformação relativamente simples... só é necessário que a fórmula esteja inicialmente na FNP:

- 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. substituímos 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. substituímos 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.

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

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

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

Começamos por ver que não existem quantificadores universais à esquerda de $\exists x$; que $\exists u$ sucede a dois quantificadores universais ($\forall y$ e $\forall z$); e que $\exists w$ sucede a três quantificadores universais ($\forall y$, $\forall z$ e $\forall v$). Desta forma, vamos substituir a variável x por uma constante c ; a variável u por uma função binária $f(y, z)$; e a variável w por uma função ternária $g(y, z, v)$. Desta forma, obtemos

$$\forall y \forall z \forall v P(c, y, z, f(y, z), v, g(y, z, v)).$$

Exemplo 1.3.11. Vamos obter a FNS da fórmula

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

O primeiro passo será colocar a matriz na FNC:

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

Agora, e dado que $\exists y$ e $\exists z$ sucedem a $\forall x$, resta-nos apenas substituir as variáveis existenciais y e z por funções unárias $f(x)$ e $g(x)$. Desta forma, obtemos

$$\forall x ((\neg P(x, f(x)) \vee R(x, f(x), g(x))) \wedge (Q(x, g(x)) \vee R(x, f(x), g(x)))).$$

Um conjunto de \vee -cláusulas Σ pode ser visto como a conjunção de todos os elementos de Σ , onde qualquer variável é considerada como sendo «governada» por um quantificador universal. Dada esta situação, qualquer FNS pode ser simplesmente vista como um conjunto de cláusulas. A FNS do Exemplo 1.3.11 pode ser representada pelo conjunto

$$\Sigma = \{\neg P(x, f(x)) \vee R(x, f(x), g(x)), Q(x, g(x)) \vee R(x, f(x), g(x))\}.$$

Tendo o acima em conta, podemos eliminar quantificadores existenciais das fórmulas na FNP, sem afectar a propriedade de inconsistência. Tal será evidenciado no próximo resultado.

Teorema 1.3.12. *Seja Σ o conjunto das cláusulas que representam a FNS da fórmula ξ . Então, ξ é inconsistente se e só se Σ é inconsistente.*

Demonstração. Sem perda de generalidade, podemos assumir que ξ está na FNP, i.e., que $\xi = Qx_1 \cdots Qx_n \varphi[x_1, \dots, x_n]$ (utilizamos esta notação para vincar que a matriz de ξ contém as variáveis x_1, \dots, x_n). Vamos considerar Q_r o primeiro quantificador existencial presente em ξ e, além disso, vamos tomar a fórmula

$$\xi_* = \forall x_1 \cdots \forall x_{r-1} Q_{r+1}x_{r+1} \cdots Q_n x_n \varphi[x_1, \dots, x_{r-1}, f(x_1, \dots, x_{r-1}), x_{r+1}, \dots, x_n],$$

onde f é uma função de Skolem correspondente a x_r (para $1 \leq r \leq n$). O nosso objectivo será mostrar que ξ é inconsistente se e só se ξ_* for inconsistente.

(\Rightarrow) Suponhamos que ξ é inconsistente. Se ξ_* for consistente, sabemos que existe uma interpretação (\mathcal{M}, v) tal que $(\mathcal{M}, v) \models \xi_*$. Tal diz-nos que, para todos os x_1, \dots, x_{r-1} , existirá pelo menos um elemento (que será $f(x_1, \dots, x_{r-1})$) de tal forma que

$$Q_{r+1}x_{r+1} \cdots Q_n x_n \varphi[x_1, \dots, x_{r-1}, f(x_1, \dots, x_{r-1}), x_{r+1}, \dots, x_n]$$

seja válida em (\mathcal{M}, v) . Assim, ξ será válida em (\mathcal{M}, v) , o que contradiz o assumido previamente. Desta forma, garantimos a inconsistência de ξ_* .

(\Leftarrow) Suponhamos agora que ξ_* é inconsistente. Se ξ for consistente, então haverá uma interpretação (\mathcal{M}, v) , sobre um domínio D , de tal forma que $(\mathcal{M}, v) \models \xi$. Tal diz-nos que, para todos os x_1, \dots, x_{r-1} , existirá um elemento x_r de forma a que

$$Q_{r+1}x_{r+1} \cdots Q_n x_n \varphi[x_1, \dots, x_{r-1}, x_r, x_{r+1}, \dots, x_n]$$

seja válida em (\mathcal{M}, v) . Podemos agora estender a interpretação de forma a incluir uma função f tal que $f(x_1, \dots, x_{r-1}) = x_r$, para todos os $x_1, \dots, x_{r-1} \in D$. Denotemos essa extensão por (\mathcal{M}, v') . Claramente,

$$(\mathcal{M}, v') \models Q_{r+1}x_{r+1} \cdots Q_n x_n \varphi[x_1, \dots, x_{r-1}, f(x_1, \dots, x_{r-1}), x_{r+1}, \dots, x_n],$$

ou seja, $(\mathcal{M}, v') \models \xi_1$, o que contradiz o assumido previamente. Desta forma, ξ terá de ser inconsistente.

Assumamos agora que existem, inicialmente, m quantificadores existenciais em ξ , e façamos $\xi_0 = \xi$. Vamos obter ξ_k a partir de ξ_{k-1} ao substituir o primeiro quantificador existencial de ξ_{k-1} por uma função de Skolem, para $k = 1, \dots, m$. Claramente, $\Sigma = \xi_m$ e, pelos mesmos argumentos, conseguimos mostrar que ξ_{k-1} é inconsistente se e só se ξ_k for inconsistente. Assim, concluímos o pretendido. \blacklozenge

1.4 Unificação

Para facilitar a compreensão do que se segue, denotamos o conjunto das variáveis por Vars e o conjunto dos termos da lógica de 1ª ordem por Term . Por definição, $\text{Vars} \subseteq \text{Term}$, assim temos a função de inclusão $\text{Vars} \hookrightarrow \text{Term}$.

Substituições

Definição 1.4.1. Uma **substituição** é uma função $\sigma: \text{Vars} \rightarrow \text{Term}$.

Nota 1.4.2. Se o conjunto $\{p \in \text{Vars} \mid \sigma(p) \neq p\} = \{p_1, \dots, p_n\}$ dos pontos não fixos relativos a uma substituição σ for finito, podemos descrever σ indicando apenas as substituições «relevantes»: $\{t_1/p_1, \dots, t_n/p_n\}$, sendo $t_i = \sigma(p_i)$.

Nota 1.4.3. Em particular, a inclusão $\text{Vars} \rightarrow \text{Term}$ dos variáveis nos termos é uma substituição, denotado por ε . Tendo em conta que $\varepsilon(p) = p$ para cada variável, tem-se

$$\{p \in \text{Vars} \mid \varepsilon(p) \neq p\} = \emptyset.$$

Por estas razões designamos esta substituição por **substituição vazia** (ε «não altere nada») ou **substituição identidade** (ε substitui os variáveis «identicamente»).

Exemplo 1.4.4. Consideremos a substituição $\sigma = \{f(z)/x, A/y\}$. Explicitamente, a substituição

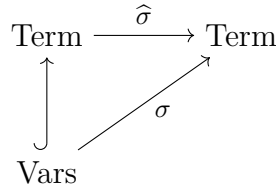
$$\sigma: \text{Vars} \longrightarrow \text{Term}$$

$$p \longmapsto \begin{cases} f(z), & \text{se a variável } p \text{ é } x, \\ A, & \text{se a variável } p \text{ é } y, \\ p, & \text{noutros casos.} \end{cases}$$

No entanto, é possível estendermos as substituições em geral para funções entre termos. Em particular, a substituição $\sigma: \text{Vars} \rightarrow \text{Term}$ induz a função $\hat{\sigma}: \text{Term} \rightarrow \text{Term}$, definida de forma recursiva:

- $\hat{\sigma}(p) = \sigma(p)$, para cada variável p ;
- $\hat{\sigma}(c) = c$, para cada símbolo de constante c ;
- $\hat{\sigma}(f(t_1, \dots, t_n)) = f(\hat{\sigma}(t_1), \dots, \hat{\sigma}(t_n))$, para cada símbolo de função f com aridade n e termos t_1, \dots, t_n .

Desta forma, obtemos o seguinte diagrama:



Nota 1.4.5. Consideremos a substituição vazia ε . Observamos logo que $\hat{\varepsilon}: \text{Term} \rightarrow \text{Term}$ é a função identidade em Term . Além disso, para cada substituição σ , $\hat{\sigma} \circ \varepsilon = \sigma$ e, sendo θ também uma substituição,

$$\sigma = \theta \iff \hat{\sigma} = \hat{\theta}.$$

Felizmente, as extensões não se ficam por aqui! Dada $\sigma: \text{Vars} \rightarrow \text{Term}$ e uma fórmula E (sem quantificadores), denotaremos por $E\sigma$ a fórmula obtida por aplicação de $\hat{\sigma}$ a todos os termos de E . Assim sendo, para um conjunto $\mathcal{E} = \{E_1, \dots, E_n\}$ de fórmulas (sem quantificadores), conseguimos definir $\mathcal{E}\sigma = \{E\sigma \mid E \in \mathcal{E}\}$.

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

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

Se aplicarmos $\hat{\theta}$ a t , obtemos:

$$\begin{aligned} \hat{\theta}(t) &= \hat{\theta}(s(x, f(y, u), h(x, z))) \\ &= s(\hat{\theta}(x), \hat{\theta}(f(y, u)), \hat{\theta}(h(x, z))) \\ &= s(\theta(x), f(\theta(y), \theta(u)), h(\theta(x), \theta(z))) \\ &= s(f(x, z), f(g(y, f(x, y)), v), h(f(x, z), h(x, y))). \end{aligned}$$

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

$$\begin{aligned} E_1\theta &= F(\hat{\theta}(x), \hat{\theta}(y), \hat{\theta}(g(z))) = F(\theta(x), \theta(y), g(\theta(z))) \\ &= F(a, f(b), g(c)). \end{aligned}$$

$$\begin{aligned} E_2\theta &= P(\hat{\theta}(h(x)), \hat{\theta}(y), \hat{\theta}(f(z))) = P(h(\theta(x)), \theta(z), f(\theta(y))) \\ &= P(h(a), c, f(f(b))). \end{aligned}$$

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

De acordo com esta definição, e dadas $\sigma, \theta: \text{Vars} \rightarrow \text{Term}$, a sua composição pode descrever-se pelo seguinte diagrama.

$$\begin{array}{ccccc} \text{Vars} & \xrightarrow{\sigma} & \text{Term} & \xleftarrow{\theta} & \text{Vars} \\ & \searrow & \downarrow \hat{\sigma} & \downarrow \hat{\theta} & \swarrow \\ & \theta_{\Delta}\sigma & \text{Term} & \sigma_{\Delta}\theta & \end{array}$$

Nota 1.4.9. Para cada expressão (termo ou fórmula) E , $E(\theta_{\Delta}\sigma) = (E\sigma)\theta$.

Sejam $\theta = \{\theta(p_1)/p_1, \dots, \theta(p_k)/p_k\}$ e $\sigma = \{\sigma(q_1)/q_1, \dots, \sigma(q_j)/q_j\}$ substituições. Sendo

$$\{p_1, \dots, p_k\} \cup \{q_1, \dots, q_j\} = \{x_1, \dots, x_n\},$$

a composta $\theta_{\Delta}\sigma$ de θ com σ é a substituição dada por

$$\{\hat{\theta}(\sigma(x_1))/x_1, \dots, \hat{\theta}(\sigma(x_n))/x_n\},$$

tendo em conta que, para cada $i = 1, \dots, n$, se $x_i \notin \{q_1, \dots, q_j\}$, então $\sigma(x_i) = x_i$.

Exemplo 1.4.10. Sejam $\theta = \{f(y)/x, z/y, x/u\}$ e $\sigma = \{a/x, g(x)/y, y/z\}$. Então,

$$\begin{aligned} \theta_{\Delta}\sigma &= \hat{\theta} \circ \sigma = \{\hat{\theta}(\sigma(x))/x, \hat{\theta}(\sigma(y))/y, \hat{\theta}(\sigma(z))/z, \hat{\theta}(\sigma(u))/u\} \\ &= \{\hat{\theta}(a)/x, \hat{\theta}(g(x))/y, \hat{\theta}(y)/z, \hat{\theta}(u)/u\} \\ &= \{a/x, g(\theta(x))/y, \theta(y)/z, x/u\} \\ &= \{a/x, g(f(y))/y, z/z, x/u\} \\ &= \{a/x, g(f(y))/y, x/u\}. \end{aligned}$$

Apenas para comparação, vamos ainda calcular $\sigma_{\Delta}\theta$.

$$\begin{aligned} \sigma_{\Delta}\theta &= \hat{\sigma} \circ \theta = \{\hat{\sigma}(\theta(x))/x, \hat{\sigma}(\theta(y))/y, \hat{\sigma}(\theta(z))/z, \hat{\sigma}(\theta(u))/u\} \\ &= \{\hat{\sigma}(f(y))/x, \hat{\sigma}(z)/y, \hat{\sigma}(z)/z, \hat{\sigma}(x)/u\} \\ &= \{f(\sigma(y))/x, \sigma(z)/y, \sigma(z)/z, \sigma(x)/u\} \\ &= \{f(g(x))/x, y/y, y/z, a/u\} \\ &= \{f(g(x))/x, y/z, a/u\}. \end{aligned}$$

Exemplo 1.4.11. No que se segue, queremos *unificar* expressões (termos, fórmulas). Por exemplo, considerando as expressões $E_1 = x$ e $E_2 = y$, as seguintes substituições unificam estes termos:

Substituição	x	y
$\{y/x\}$	y	y
$\{x/y\}$	x	x
$\{f(f(a))/x, f(f(a))/y\}$	$f(f(a))$	$f(f(a))$

Rapidamente podemos ver que

$$\begin{aligned} \{f(f(a))/x, f(f(a))/y\} &= \{f(f(a))/y\} \triangle \{y/x\} \\ &= \{f(f(a))/x\} \triangle \{x/y\}. \end{aligned}$$

Lema 1.4.12. Dada substituições $\theta, \sigma: \text{Vars} \rightarrow \text{Term}$, então

$$\widehat{\theta \triangle \sigma} = \widehat{\theta} \circ \widehat{\sigma}$$

Demonstração. Consideremos a substituição $\tau = \theta \triangle \sigma$ e um termo arbitrário t .

1. Se $t = c$ é um símbolo de constante, então, de acordo com a definição de extensão de uma substituição, $\widehat{\tau}(c) = c$ e $(\widehat{\theta} \circ \widehat{\sigma})(c) = \widehat{\theta}(\widehat{\sigma}(c)) = \widehat{\theta}(c) = c$;
2. Se $t = x$ é uma variável, segue que $\widehat{\tau}(x) = \tau(x) = (\theta \triangle \sigma)(x) = (\widehat{\theta} \circ \sigma)(x) = \widehat{\theta}(\sigma(x))$ e que $(\widehat{\theta} \circ \widehat{\sigma})(x) = \widehat{\theta}(\widehat{\sigma}(x)) = \widehat{\theta}(\sigma(x))$ (notemos que sendo $t \in \text{Vars}$, $\tau(t) = \widehat{\tau}(t)$);
3. Suponhamos que $t = f(t_1, \dots, t_n)$. Então, $\widehat{\tau}(f(t_1, \dots, t_n)) = f(\widehat{\tau}(t_1), \dots, \widehat{\tau}(t_n))$. Nestas condições, para todo o $i \in \{1, \dots, n\}$, se t_i é um símbolo de constante ou uma variável, então, por 1 e 2, $\widehat{\tau}(t_i) = (\widehat{\theta} \circ \widehat{\sigma})(t_i)$, caso contrário, t_i volta a ser da forma $t_i = f_i(t_{i_1}, \dots, t_{i_n})$ e o processo repete-se (ou seja, $\widehat{\tau}(t_i) = f_i(\widehat{\tau}(t_{i_1}), \dots, \widehat{\tau}(t_{i_n}))$) até que se obtenham símbolos de constantes ou variáveis. Em qualquer dos casos vem que $\widehat{\tau}(t) = (\widehat{\theta} \circ \widehat{\sigma})(t)$. \blacklozenge

Teorema 1.4.13. Consideremos S como o conjunto de todas as substituições. Então, a estrutura $\langle S, \triangle, \varepsilon \rangle$ é um monóide, isto é, a composição de substituições é associativa e a substituição vazia ε é neutro para esta operação.

Demonstração. Relativamente à associatividade de \triangle , admitamos três substituições arbitrárias θ, σ, λ . Tendo em conta a Nota 1.4.5 e o Lema 1.4.12:

$$\begin{aligned} \widehat{(\theta \triangle \sigma) \triangle \lambda} &= \widehat{(\theta \triangle \sigma)} \circ \widehat{\lambda} \\ &= (\widehat{\theta} \circ \widehat{\sigma}) \circ \widehat{\lambda} \\ &= \widehat{\theta} \circ (\widehat{\sigma} \circ \widehat{\lambda}) \\ &= \widehat{\theta} \circ \widehat{(\sigma \triangle \lambda)} \end{aligned}$$

$$= \widehat{\theta_{\Delta}(\sigma_{\Delta}\lambda)}.$$

Além disso,

$$\theta_{\Delta}\varepsilon = \widehat{\theta} \circ \varepsilon = \theta \quad \text{e} \quad \varepsilon_{\Delta}\theta = \widehat{\varepsilon} \circ \theta = \theta.$$



Unificadores

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.

Começamos por indicar alguns exemplos simples.

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

$$\theta = \lambda_{\Delta}\sigma,$$

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

Encontrar o u.m.g para um conjunto de expressões \mathcal{E} relativamente reduzido não é tarefa complicada. No entanto, quando \mathcal{E} é suficientemente grande (finito), podemos ter um grande problema em mãos. É em tais situações que devemos aplicar o algoritmo de Robinson (1965). A ideia base consiste em, dado um conjunto de expressões, detectar se estas são ou não idênticas e, no caso de não serem, determinar aquilo em que diferem para posteriormente se tentar a unificação.

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. Consideremos o seguinte conjunto de expressões não idênticas $\mathcal{E} = \{P(a), P(x)\}$, com a um símbolo de constante e x uma variável. Facilmente reconhecemos que estas diferem no facto de a ocorrer na primeira expressão e x ocorrer na segunda. De modo a procedermos à respectiva unificação, teremos de encontrar o conjunto das diferenças; neste caso $\mathcal{D} = \{a, x\}$. No entanto, porque $x \in \text{Vars}$, esta poderá ser substituída por a e, conseqüentemente, as diferenças acabam. Neste caso, o u.m.g. de \mathcal{E} será $\{a/x\}$.

Apresentamos então, de forma altamente resumida, o algoritmo de unificação para um conjunto de expressões \mathcal{E} .

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

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} .

0. $\mathcal{D}_0 = \{y, x, a\}$, portanto $\sigma_1 = (x/y) \triangle \varepsilon = \{x/y\}$, e ficamos com

$$\mathcal{E}_1 = \mathcal{E}\sigma_1 = \{P(x, z), P(x, h(x)), P(a, h(a))\}.$$

1. $\mathcal{D}_1 = \{x, a\}$, portanto $\sigma_2 = \{a/x\} \triangle \sigma_1 = \{a/x, a/y\}$, obtendo posteriormente

$$\mathcal{E}_2 = \mathcal{E}_1\sigma_2 = \{P(a, z), P(a, h(a)), P(a, h(a))\}.$$

2. $\mathcal{D}_2 = \{z, h(a)\}$, portanto $\sigma_3 = \{h(a)/z\} \triangle \sigma_2 = \{h(a)/z, a/x, a/y\}$, chegando entretanto a

$$\mathcal{E}_3 = \mathcal{E}_2 \sigma_3 = \{P(a, h(a)), P(a, h(a)), P(a, h(a))\} = \{P(a, h(a))\}.$$

Na próxima iteração, o algoritmo terminará ($|\mathcal{E}_3| = 1$).

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} .

0. $\mathcal{D}_0 = \{h(x), x, a\}$, portanto $\sigma_1 = \{a/x\}$ e ficamos com

$$\mathcal{E}_1 = \mathcal{E} \sigma_1 = \{P(h(a), z), P(a, h(y)), P(a, h(a))\}.$$

1. $\mathcal{D}_1 = \{h(x), a\}$. Como não existem variáveis em \mathcal{D}_1 , o algoritmo termina no passo 12 ao retorna « \mathcal{E} não é unificável».

Exemplo 1.4.21. Consideremos $\mathcal{E} = \{P(h(x), z), P(x, h(y)), P(x, h(a))\}$, 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} .

0. $\mathcal{D}_0 = \{h(x), x, x\} = \{h(x), x\}$. Como a única variável em \mathcal{D}_0 é x e esta ocorre em $h(x)$, o algoritmo termina no passo 12 ao retorna « \mathcal{E} não é unificável».

Teorema 1.4.22 (Unificação). *Seja \mathcal{E} um conjunto finito de expressões unificáveis. Então, o algoritmo de determinação terminará no passo 4, sendo σ_k o u.m.g. de \mathcal{E} .*

Demonstração. Uma vez que \mathcal{E} é unificável, consideremos um seu qualquer unificador θ . O nosso objectivo será fazer indução em k para mostrar que existe uma substituição λ_k tal que $\theta = \lambda_k \triangle \sigma_k$.

Como passo de base ($k = 0$) temos que $\theta = \lambda_0 \triangle \sigma_0 = \lambda_0$ (uma vez que $\sigma_0 = \varepsilon$).

Admitamos agora como hipótese de indução que $\theta = \lambda_k \triangle \sigma_k$, para $0 \leq k \leq n$:

- se $|\mathcal{E} \sigma_k| = 1$, então o algoritmo termina no passo 4 e, dado que $\theta = \lambda_n \triangle \sigma_n$, σ_n será um u.m.g. para \mathcal{E} ;
- caso $|\mathcal{E} \sigma_n| \neq 1$, o algoritmo encontrará o conjunto das diferenças \mathcal{D}_n de $\mathcal{E} \sigma_n$. Porque $\theta = \lambda_n \triangle \sigma_n$ é um unificador de \mathcal{E} , λ_n deverá unificar \mathcal{D}_n . Contudo, como \mathcal{D}_n é o conjunto das diferenças, deverá ter uma variável, digamos, p_n . Seja então t_n um qualquer outro elemento em \mathcal{D}_n diferente de p_n . Como λ_n unifica \mathcal{D}_n , $\lambda_n(p_n) = \lambda_n(t_n)$. Agora, se p_n ocorrer em t_n , então $\lambda_n(p_n)$ ocorre em $\lambda_n(t_n)$. No entanto,

esta situação é impossível, uma vez que p_n e t_n são distintos e $\lambda_n(p_n) = \lambda_n(t_n)$. Desta forma, p_n não ocorre em t_n . Por consequência, o algoritmo de unificação não chegará passo 12, mas seguirá os passos 7 – 10 para redefinir $\sigma_{n+1} = (t_n/p_n) \Delta \sigma_n$. Seja agora $\lambda_{n+1} = \lambda_n \setminus \{\lambda_n(t_n)/p_n\}$. Então, como p_n não ocorre em t_n , $\lambda_{n+1}(t_n) = \lambda_n \setminus \{\lambda_n(t_n)/p_n\}(t_n) = \lambda_n(t_n)$. Portanto, teremos

$$\begin{aligned}\lambda_{n+1} \Delta \{t_n/p_n\} &= \lambda_{n+1} \cup \{\lambda_{n+1}(t_n)/p_n\} \\ &= \lambda_{n+1} \cup \{\lambda_n(t_n)/p_n\} \\ &= (\lambda_n \setminus \{\lambda_n(t_n)/p_n\}) \cup \{\lambda_n(t_n)/p_n\} \\ &= \lambda_n.\end{aligned}$$

Desta forma, $\lambda_n = \lambda_{n+1} \Delta \{t_n/p_n\}$, pelo que

$$\theta = \lambda_n \Delta \sigma_n = \lambda_{n+1} \Delta \{t_n/p_n\} \Delta \sigma_n = \lambda_{n+1} \Delta \sigma_{n+1},$$

e podemos concluir que, para todo o $k \geq 0$, existirá uma substituição λ_k tal que $\theta = \lambda_k \Delta \sigma_k$.

Uma vez que o algoritmo de unificação deverá terminar (dado que o conjunto \mathcal{E} é finito), e que tal não acontecerá no passo 12, terá de acontecer no passo 4 (retornando σ_k , o u.m.g. de \mathcal{E}). ♦

1.5 Método da Resolução de Robinson

Tendo introduzido o algoritmo de unificação na última secção, podemos agora considerar o Princípio da Resolução para a Lógica de 1ª Ordem.

Daqui em diante (e até ao final desta secção), vamos apenas considerar linguagens sem o símbolo «=». Além disso, continuamos de assumir que o domínio de interpretação em causa é não vazio.

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. Consideremos a cláusula $C = P(x) \vee P(f(y)) \vee \neg Q(x)$, onde x, y são variáveis, f é um símbolo de função unária e P, Q são símbolos de predicado unários. Rapidamente conseguimos ver que existe u.m.g. para $\mathcal{E} = \{P(x), P(f(y))\}$, dada por $\sigma = \{f(y)/x\}$. Desta forma, $(P(f(y)) \vee \neg Q(x))\sigma = P(f(y)) \vee \neg Q(f(y))$ é um factor de C .

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. Consideremos $C_1 = P(x) \vee Q(x)$ e $C_2 = \neg P(a) \vee R(x)$, onde x é uma variável, a um símbolo de constante e P, Q, R são símbolos de predicado unários. Dado que x aparece em C_1 e C_2 , vamos renomeá-la em C_2 , ficando com $C_2 = \neg P(a) \vee R(y)$. De facto, $P(x)$ e $P(a)$ admitirão um u.m.g. $\sigma = \{a/x\}$, logo,

$$(Q(x) \vee R(y))\sigma = Q(a) \vee R(y)$$

será a resolvente binária de C_1 e C_2 .

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. Consideremos duas cláusulas $C_1 = P(x) \vee P(f(y)) \vee R(g(y))$ e $C_2 = \neg P(f(g(a))) \vee Q(b)$, onde x, y são variáveis, a é um símbolo de constante, f e g são símbolos de função unárias e P, Q, R são símbolos de predicado unários.

- $P(f(y)) \vee R(g(y))$ é um factor de C_1 ;
- $R(g(g(a))) \vee Q(b)$ é uma resolvente binária de um factor de C_1 e C_2 ;
- $R(g(g(a))) \vee Q(b)$ é uma resolvente de C_1 e C_2 .

Simbolicamente, as regras que vamos utilizar são dadas consoante os seguintes esquemas dedutivos:

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

Na regra (BR) suponha-se que $\neg\psi \vee \theta$ e $\varphi \vee \gamma$ não têm variáveis em comum.

Nota 1.5.7. Recordemos que verificar $\Gamma \models \psi$, é o mesmo que mostrar que $\Gamma \cup \{\neg\psi\}$ é inconsistente. Uma vez mais, este processo passa por: transformar todas as fórmulas na FNS, «ignorar» os quantificadores \forall (já que não existem outros e todas as variáveis são quantificadas), renomear as variáveis em cada cláusula por forma a torná-las distintas e aplicar sucessivamente as duas regras acima (BR e Fator), até obtermos uma contradição (se for possível).

Exemplo 1.5.8 (Caroll (1896)). Vamos considerar o seguinte conjunto de constatações e tentar justificar a consequência, por aplicação do Método de Resolução.

- 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.

O primeiro passo será tentar traduzir estas ideias (na língua portuguesa) para uma linguagem de 1ª ordem. Vamos então denotar

$$\begin{aligned}
 B(x) : & \quad x \text{ aprecia Beethoven,} \\
 S(x) : & \quad x \text{ mantém o silêncio durante a sonata } \textit{Mondschein}, \\
 I(x) : & \quad x \text{ é completamente ignorante no que diz respeito à música,} \\
 P(x) : & \quad x \text{ é um porquinho-da-índia.}
 \end{aligned}$$

A partir daqui, conseguimos obter:

- $\neg \exists x (B(x) \wedge \neg S(x))$;
- $\forall x (P(x) \rightarrow I(x))$;
- $\neg \exists x (I(x) \wedge S(x))$;
- $\forall x (P(x) \rightarrow \neg B(x)) \rightsquigarrow \exists x (P(x) \wedge B(x))$ (negação).

O nosso próximo passo passará por transformar cada uma das fórmulas acima na sua FNS. Desta forma,

- $\neg \exists x (B(x) \wedge \neg S(x)) \equiv \forall x (\neg B(x) \vee S(x))$;
- $\forall x (P(x) \rightarrow I(x)) \equiv \forall x (\neg P(x) \vee I(x))$;
- $\neg \exists x (I(x) \wedge S(x)) \equiv \forall x (\neg I(x) \vee \neg S(x))$;
- $\exists x (P(x) \wedge B(x)) \rightsquigarrow P(c) \wedge B(c)$

Desta feita, vamos considerar as seguintes fórmulas

$$\neg B(x) \vee S(x), \quad \neg P(y) \vee I(y), \quad \neg I(z) \vee \neg S(z), \quad P(c), \quad B(c),$$

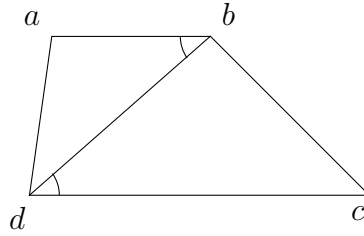
e tentar, a partir delas, a dedução de $\perp \dots$

$$\begin{array}{cccccccccc}
 & & \text{BR}(1,2) & & \text{BR}(3,4) & & \text{BR}(5,6) & & & \\
 & & \downarrow & & \downarrow & & \downarrow & & & \\
 P(c) & \neg P(y) \vee I(y) & I(c) & \neg I(z) \vee \neg S(z) & \neg S(c) & \neg B(x) \vee S(x) & \neg B(c) & B(c) & \perp & \\
 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 &
 \end{array}$$

Exemplo 1.5.9 (Chang e Lee (1973)). Embora pareça uma questão geométrica muito simples de comprovar, vamos mostrar que os ângulos internos formados pela diagonal de um trapézio são iguais. O primeiro passo será axiomatizar o resultado de forma conveniente.

Seja $T(x, y, z, w)$ um trapézio cujo vértice superior esquerdo é x , o vértice superior direito é y , o vértice inferior direito é z e o vértice inferior esquerdo é w ; seja $P(x, y, z, w)$ o predicado que nos diz que a linha que une o segmento xy é paralela à linha que une o segmento zw ; e $E(x, y, u, z, w, v)$ o predicado que nos diz que o ângulo xyu é igual ao ângulo zwv . Conseguimos então encontrar os seguintes axiomas:

$$\begin{aligned} A_1 &= \forall x \forall y \forall z \forall w (T(x, y, z, w) \rightarrow P(x, y, z, w)), \\ A_2 &= \forall x \forall y \forall z \forall w (P(x, y, z, w) \rightarrow E(x, y, u, z, w, v)), \\ A_3 &= T(a, b, c, d). \end{aligned}$$



A partir destes axiomas, deveremos estar em condições de concluir que $E(x, y, u, z, w, v)$ é verdadeiro, ou seja, que $A_1 \wedge A_2 \wedge A_3 \rightarrow E(a, b, d, c, d, b)$. Uma vez que pretendemos utilizar um algoritmo de refutação, o objectivo será mostrar que

$$A_1 \wedge A_2 \wedge A_3 \wedge \neg E(a, b, d, c, d, b)$$

é inconsistente. Para o fazer, vamos transformar o conjunto constituído por esta fórmula e pelos axiomas no conjunto de cláusulas

$$\{\neg T(x, y, z, w) \vee P(x, y, z, w), \neg P(x, y, z, w) \vee E(x, y, u, z, w, v), T(a, b, c, d), \neg E(a, b, d, c, d, b)\}.$$

Estamos então prontos para a começar a dedução.

1. $\neg P(x, y, z, w) \vee E(x, y, u, z, w, v)$
2. $\neg E(a, b, d, c, d, b)$
3. $\neg P(a, b, c, d)$ BR(1, 2)
4. $\neg T(x, y, z, w) \vee P(x, y, z, w)$
5. $\neg T(a, b, c, d)$ BR(3, 4)
6. $T(a, b, c, d)$
7. \perp

Como se verificou, o conjunto de cláusulas proposto é inconsistente, o que nos leva à conclusão de que o resultado inicial é válido.

Princípios de Enumeração Combinatória

2.1 Introdução

Neste novo capítulo, deixamos a lógica (proposicional e de 1ª ordem) de lado e partimos ao estudo da combinatória (ramo da matemática que estuda a contagem, tanto como meio quanto como fim, na obtenção de resultados e certas propriedades de colecções finitas de elementos). Este será, de facto, o tema de estudo para os próximos dois capítulos. Numa primeira parte, estaremos maioritariamente interessados em analisar e tentar responder ao tipo de perguntas que se segue:

- Quantas sequências binárias de comprimento n existem?
- Quantos números de 4 algarismos (divisíveis por 5) se podem escrever com os dígitos $1, \dots, 9$?
- Quantas maneiras existem de colocar k bolas em n caixas?
- Quantas sequências binárias com k uns e $n - 1$ zeros existem?
- Sejam $k, n \in \mathbb{N}$. Quantas soluções tem a equação $x_1 + \dots + x_n = k$, com $x_i \in \mathbb{N}$?
- Considerem-se 50 pessoas numa sala quadrada com $7m$ de lado. Será que existem pelo menos duas pessoas a uma distância inferior a $1.5m$?

No entanto, e antes de nos debruçarmos afincadamente sobre este novo tópico, vamos fazer uma ligeira revisão de alguns conceitos relacionados com funções.

Definição 2.1.1. Seja $f: A \rightarrow B$ uma função. Então, f diz-se:

- **injectiva** quando, para todos os $x, y \in A$, $f(x) = f(y) \implies x = y$;
- **sobrejectiva** quando todo o $y \in B$ é imagem de algum $x \in A$; i.e., quando para todo o $y \in B$ existe um $x \in A$ tal que $f(x) = y$;
- **bijectiva** quando f for injectiva e sobrejectiva.

Definição 2.1.2. Uma função $f: A \rightarrow B$ diz-se **invertível** quando existir uma função $g: B \rightarrow A$ tal que $g \circ f = \text{id}_A$ e $f \circ g = \text{id}_B$.

Teorema 2.1.3. Uma função $f: A \rightarrow B$ é invertível se e só se é bijectiva.

Demonstração. (\Rightarrow) Dado que f é invertível, vamos considerar a inversa $f^{-1}: B \rightarrow A$. O primeiro passo será mostrar que f^{-1} é sobrejectiva. Para tal, suponhamos $y \in B$ e $x = f^{-1}(y)$. Então,

$$f(x) = f(f^{-1}(y)) = (f \circ f^{-1})(y) = \text{id}_B(y) = y.$$

Desta forma, resta-nos mostrar a injectividade de f^{-1} . Suponhamos, para tal, $x_1, x_2 \in A$ tais que $f(x_1) = f(x_2)$ (o objectivo será concluirmos $x_1 = x_2$). Consideremos ainda $y = f(x_1)$ e $x = f^{-1}(y)$. Então,

$$x_2 = \text{id}_A(x_2) = (f^{-1} \circ f)(x_2) = f^{-1}(f(x_2)) = f^{-1}(y) = x.$$

Contudo, temos ainda que

$$x_1 = \text{id}_A(x_1) = (f^{-1} \circ f)(x_1) = f^{-1}(f(x_1)) = f^{-1}(f(x_2)) = f^{-1}(y) = x,$$

concluindo assim a primeira parte da prova.

(\Leftarrow) Suponhamos agora que f é bijectiva. Pela sobrejetividade de f , para cada $y \in B$ sabemos que existe um $x \in A$ tal que $f(x) = y$; pela injectividade de f , este x será único. Portanto, vamos definir

$$\begin{aligned} f^{-1}: B &\longrightarrow A. \\ y &\longmapsto \text{o único } x \in A \text{ com } f(x) = y \end{aligned}$$

Agora, resta-nos mostrar que f^{-1} é, de facto, a inversa de f . Consideremos $x \in A$ e $y = f(x)$. Então, por definição, $f^{-1}(y) = x$, pelo que $(f^{-1} \circ f)(x) = f^{-1}(f(x)) = f^{-1}(y) = x$, ou seja, $f^{-1} \circ f = \text{id}_A$. Por outro lado, se considerarmos $y \in B$ e $x = f^{-1}(y)$, então, por definição, $f(x) = y$ e temos que $(f \circ f^{-1})(y) = f(f^{-1}(y)) = f(x) = y$, i.e., que $f \circ f^{-1} = \text{id}_B$. \blacklozenge

Nota 2.1.4. Para um conjunto finito A , denotamos por $|A|$ o número de elementos (= cardinalidade) de A .

2.2 O Princípio da Gaiola dos Pombos

O **princípio da gaiola dos pombos** é uma importante ferramenta matemática, muitas vezes utilizada despecebidamente no decorrer das demonstrações. Na sua forma mais simples, constata que se tivermos n pombos para distribuir por m gaiolas, com $n > m$, haverá pelo menos uma gaiola com dois pombos.

Este princípio surgiu pela primeira vez em 1624, pela mão de Leurechon, mas tornou-se

conhecido como o **princípio das gavetas de Dirichlet** (quando este o apresentou em 1834, com o nome *Schubfachprinzip*).

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 $f: A \rightarrow B$ 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 $|A| \leq |B|$).

Nota 2.2.1. Será a partir desta última formulação que iremos fazer a extensão deste princípio aos conjuntos infinitos (contáveis e não contáveis).

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

Consideremos a função

$$f: \{\text{pessoas na sala}\} \longrightarrow \{\text{Janeiro}, \dots, \text{Dezembro}\}$$

de tal forma que a cada pessoa seja atribuído o seu mês de aniversário. Dado que

$$|\{\text{Janeiro}, \dots, \text{Dezembro}\}| = 12 \text{ e } |\{\text{pessoas na sala}\}| > 12,$$

podemos imediatamente verificar que f não é injectiva (ou seja, que existem, 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 $1.5m$.

Se dividirmos a sala em quadrados unitários e considerarmos a função

$$\begin{aligned} f: \{\text{pessoas na sala}\} &\longrightarrow \{\text{quadrados}\} \\ p &\longmapsto \text{quadrado onde está } p, \end{aligned}$$

podemos ver que esta não será injectiva. Dado que $|\{\text{pessoas na sala}\}| = 50$ e $|\{\text{quadrados}\}| = 49$, existirá pelo menos um quadrado com duas pessoas. Como a maior distância num qualquer destes quadrados é $\sqrt{2} \approx 1.4142m$, temos que as duas pessoas em questão estarão a uma distância inferior a $1.5m$.

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 $|q\alpha - p| < \frac{1}{n}$.

Demonstração. A prova deste resultado passa por, para cada $k \in \{0, \dots, n\}$, considerar $r_k = k\alpha - \lfloor k\alpha \rfloor \in [0, 1[$. De seguida, consideramos ainda a função

$$f: \{0, \dots, n\} \longrightarrow \left\{ \left[0, \frac{1}{n}\right[, \left[\frac{1}{n}, \frac{2}{n}\right[, \dots, \left[\frac{n-1}{n}, 1\right[\right\}$$

$$k \longmapsto \text{intervalo } \mathcal{I} \text{ com } r_k \in \mathcal{I}$$

Então, pelo princípio da gaiola dos pombos, existirão inteiros ℓ e k em $\{0, \dots, n\}$ (com $\ell < k$, sem perda de generalidade) tal que $|r_\ell - r_k| < \frac{1}{n}$. Assim,

$$\frac{1}{n} > |k\alpha - \lfloor k\alpha \rfloor - \ell\alpha + \lfloor \ell\alpha \rfloor| = |(k - \ell)\alpha - (\lfloor k\alpha \rfloor - \lfloor \ell\alpha \rfloor)|.$$

Por último, basta escolhermos $q = k - \ell \in \{1, \dots, n\}$ e $p = \lfloor k\alpha \rfloor - \lfloor \ell\alpha \rfloor$. ♦

Exemplo 2.2.5. Vamos agora mostrar que, dado um subconjunto de $\{1, \dots, 2n\}$ 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 »).

Sabemos que é possível escrever $\{1, \dots, 2n\}$ como união disjunta de dois seus subconjuntos: o subconjunto $E = \{2, 4, \dots, 2n\}$ dos elementos pares e o subconjunto $O = \{1, 3, \dots, 2n-1\}$ dos elementos ímpares, sendo $|E| = |O| = n$. Consideremos então um elemento $z \in \{1, \dots, 2n\}$. Pelo facto de cada número natural é de maneira única um produto de números primos, podemos escrever $z = 2^a b$ (de maneira única), onde b é ímpar. A partir daqui podemos definir a função

$$f: \{1, \dots, 2n\} \longrightarrow O.$$

$$z \longmapsto \text{aquele único } b$$

Além disso, e porque $|O| = n$, $|f(C)| \leq n$, para qualquer subconjunto $C \subseteq \{1, \dots, 2n\}$. Desta forma, se $C \subseteq \{1, \dots, 2n\}$ tiver eventualmente $n + 1$ elementos, deverão existir $y_1, y_2 \in C$ tais que $f(y_1) = f(y_2)$. Por outras palavras, $y_1 = 2^{x_1} b$ e $y_2 = 2^{x_2} b$, pelo que se $x_1 < x_2$ temos $y_1 \mid y_2$ (e análogamente para o caso contrário).

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.

Comecemos por fixar a jornada e por considerar

$$N: \{\text{equipas}\} \longrightarrow \{0, \dots, n-1\}$$

$$e \longmapsto \text{total de jogos de } e.$$

- **Caso 1:** Cada equipa realizou pelo menos um jogo. Então, podemos considerar acima o conjunto de chegada $\{1, \dots, n-1\}$; pelo princípio da gaiola dos pombos, N não é injectiva;

- **Caso 2:** Pelo menos uma equipa não realizou nenhum jogo. Logo, nenhuma equipa realizou $n - 1$ jogos e, por isso podemos considerar acima o conjunto de chegada $\{1, \dots, n - 2\}$; pelo princípio da gaiola dos pombos, N também não será injectiva.

Generalização

A ideia da generalização do princípio da gaiola dos pombos é tão compreensível como o enunciado original: suponhamos que temos m gaiolas; se em cada caixa houver, no máximo, k pombos, então teremos (no máximo) mk pombos (a contraposição é, novamente, mais óbvia - 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 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 $1 \leq i \leq m$.

Podemos ainda ter uma formulação alternativa relacionada com a injectividade de funções: sejam A, B conjuntos e $f: A \rightarrow B$ uma função; se $k|B| < |A|$, então existirá um $y \in B$ tal que $|f^{-1}(y)| = |\{x \in A \mid f(x) = y\}| > k$.

Exemplo 2.2.7. Na área metropolitana de Lisboa há, pelo menos, 15 pessoas com o mesmo número de fios de cabelo na cabeça. (vamos assumir que cada pessoa tem, no máximo, 200000 fios de cabelo na cabeça e que na área metropolitana de Lisboa, residem 2,870,208 pessoas).

Para aplicar o princípio da gaiola dos pombos, vamos considerar a função $f: \{\text{Lisboetas}\} \rightarrow \{0, \dots, 200000\}$ que a cada lisboeta faz corresponder o número de fios de cabelo na cabeça. Como $14 \times 200001 < 2870208$, existirá um $n \in \{0, \dots, 200000\}$ tal que $|f^{-1}(n)| > 14$, ou seja, que existirão, pelo menos, 15 pessoas com n fios de cabelo na cabeça.

Extensão ao Infinito

A matéria desta subsecção é complementar e não foi dada na aula. Portanto, não faz parte da avaliação.

O princípio, tal como introduzido anteriormente, pode não funcionar se considerarmos conjuntos infinitos (contáveis ou não contáveis). De facto, tal é verificado pelo paradoxo do grande hotel de Hilbert, que enunciamos a seguir.

Paradoxo do Grande Hotel (Hilbert): «Consideremos um hotel imaginário com quartos infinitos, numerados por $1, 2, 3, \dots$. Numa noite, com o hotel completamente cheio, um hóspede solitário chega em busca de um quarto. O engenhoso gerente do hotel move cada hóspede um quarto acima, de modo que o habitante do quarto 1 se mova para o quarto 2, o

do quarto 2 para o 3, e assim por diante. . . Com todos os hóspedes realocados, o quarto 1 fica novamente livre para o hóspede que acabou de chegar! No dia seguinte chega um autocarro com um número infinito de passageiros à procura de quarto. Desta vez, o gerente move o hóspede do quarto 1 para o quarto 2, o do quarto 2 para o 4, o do quarto 3 para o 6, . . . , o do quarto n para o $2n$. Isso libertará todos os quartos ímpares, de modo que o passageiro 1 do autocarro possa ir para o quarto 1, o passageiro 2 para o quarto 3, o passageiro 3 para o quarto 5 e, em geral, o passageiro n para o quarto $2n + 1$.»

Neste caso, conseguimos claramente ver que, para $n = |\mathbb{N}|$, será possível distribuir $n + 1$ (ou mesmo $2n$) pessoas por n quartos, sem que cada quarto tenha mais que uma pessoa.

Definição 2.2.8. Um conjunto A é dito **infinito contável** se existir uma bijecção $f: \mathbb{N} \rightarrow A$. Além disso, A será dito **contável** se for finito ou se for infinito contável. Adicionalmente, e caso A seja infinito, mas não infinito contável, será dito **não contável**.

Há que ter algum cuidado quando começamos a considerar conjuntos infinitos (tanto contáveis, como não contáveis). A ideia presente na Nota 2.2.1 é, de facto, o que nos permite fazer a extensão necessária. Contudo, nessa forma, o princípio é tautológico (i.e., a condição antecedente « se A, B são conjuntos tais que $|A| > |B|$ » é equivalente à consequente « então não existem funções injectivas de A em B »).

Uma outra forma de expressar o princípio da gaiola dos pombos para conjuntos finitos é equivalente ao princípio de que todos os conjuntos finitos são Dedekind-finitos¹: sejam A e B conjuntos finitos; se houver uma função sobrejectiva de A para B que não é injectiva, então nenhuma função sobrejectiva de A para B será injectiva.

Existem então dois princípios semelhantes para os conjuntos infinitos:

Versão Infinita: Seja A um conjunto infinito e B um conjunto finito. Então, se $f: A \rightarrow B$ for uma função, existirá um $y \in B$ de tal forma que $f^{-1}(y)$ seja um conjunto infinito.

Versão Não Contável: Seja A um conjunto infinito não contável e B um conjunto infinito contável. Então, se $f: A \rightarrow B$ for uma função, existirá um $y \in B$ de tal forma que $f^{-1}(y)$ seja um conjunto infinito não contável.

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 $f: A \rightarrow B$, então $|A| = |B|$. Tipicamente utilizamos este princípio quando é mais fácil contar os elementos de um destes conjuntos.

¹Um conjunto A diz-se **Dedekind-infinito** se existir algum seu subconjunto próprio $B \subsetneq A$ tal que $|B| = |A|$. Quando um conjunto não for Dedekind-infinito, será dito **Dedekind-finito**.

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 seqüências 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.

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 .

O primeiro passo será ver que todo o número inferior a 10^n terá, no máximo, n algarismos. Assim, podemos expressá-los por uma seqüência $(x_1, \dots, x_n) \in \{0, \dots, 9\}^n$ e traduzir o problema na questão de encontrar os n -tuplos (x_1, \dots, x_n) que satisfazem a equação

$$x_1 + x_2 + \dots + x_n = k.$$

Acontece que o número de n -tuplos nestas condições coincide exactamente com o número de maneiras de colocar k bolas indistinguíveis em n caixas numeradas. Este último, por sua vez, coincide com o número de seqüências binárias com k uns e $n - 1$ zeros (para $n > 0$).

$$\begin{array}{ccccccc} \boxed{\bullet \bullet \bullet} & \boxed{\bullet} & \boxed{} & \boxed{\bullet \bullet \bullet \bullet} \\ 111 & 0 & 1 & 0 & 0 & 1111 \end{array}$$

Por outro lado, o número de seqüências binárias com k uns e $n - 1$ zeros coincide com o número de subconjuntos de k elementos de um conjunto com $k + n - 1$ elementos. Veremos no próximo capítulo como calcular este número.

Exemplo 2.3.4. Todos conhecemos o conjunto dos números naturais ($\mathbb{N} = \{0, 1, 2, \dots\}$) e o conjunto dos números inteiros ($\mathbb{Z} = \{\dots, -2, -1, 0, 1, \dots\}$). No entanto, o que muitas das vezes pode fazer alguma confusão é o facto destes conjuntos terem o mesmo número de

elementos. Se examinarmos com alguma cautela, conseguimos verificar que a função

$$f: \mathbb{N} \longrightarrow \mathbb{Z}$$

$$n \longmapsto f(n) = \begin{cases} \frac{n}{2}, & n \text{ é par,} \\ -\frac{n+1}{2}, & n \text{ é ímpar.} \end{cases}$$

é uma bijecção. Desta forma, concluímos que $|\mathbb{N}| = |\mathbb{Z}|$.

Outro exemplo de equipotência «estranha» de conjuntos faz-se entre o intervalo $]0, 1[$ e o conjunto dos números reais (\mathbb{R}) . Neste caso, a propriedade será verificada com recurso à função tangente (definida no seu período fundamental: $]-\frac{\pi}{2}, \frac{\pi}{2}[$). De facto, se aplicarmos algumas transformações à função original, é possível verificar que

$$g:]0, 1[\longrightarrow \mathbb{R}$$

$$x \longmapsto \tan\left(\pi\left(x - \frac{1}{2}\right)\right)$$

é uma bijecção entre os referidos conjuntos. Por conseguinte, $]0, 1[= |\mathbb{R}|$.

2.4 Os Princípios da Adição e Multiplicação

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

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

Nota 2.4.1. O princípio da adição é muitas vezes utilizado para «dividir o problema em casos».

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.,

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

Exemplo 2.4.2. • O número de sequências binárias de comprimento n é 2^n . Para chegar a tal resultado, contamos os elementos de $\{0, 1\}^n$. Pelo Exemplo 2.3.2, para um conjunto X , com $|X| = n$, $|\mathcal{P}(X)| = 2^n$.

- Qual é o número de números naturais com 4 algarismos que se pode escrever com os dígitos $1, \dots, 9$? Pelo Exemplo 2.3.1, basta determinarmos o tamanho do conjunto $\{1, \dots, 9\}^4$. Neste caso, existirão $9^4 = 6561$ elementos.
- Qual é o número de números naturais com 4 algarismos que se podem escrever com os dígitos $0, \dots, 9$ e que são divisíveis por 5? O conjunto

$$\{1, \dots, 9\} \times \{0, 1, \dots, 9\}^2 \times \{0, 5\}$$

tem cardinalidade 1800.

Exemplo 2.4.3. Vamos determinar o número de palavras de comprimento 5 que podemos escrever com os símbolos «a», «b», «c», «(», «)» de modo a que:

- o número de «(» é igual ao número de «)»;
- em cada parte inicial da palavra, o número de «(» é maior ou igual ao número de «)»;
- entre os símbolos «(» e «)» está pelo menos um dos símbolos «a, b, c».

Tomemos então S como o conjunto destas palavras e consideremos: S_0 como o subconjunto das palavras sem parêntesis; S_1 como o subconjunto das palavras onde há uma ocorrência única de «(»; e S_2 como o subconjunto das palavras onde ocorre duas vezes o símbolo «(». Logo, $S = S_0 \cup S_1 \cup S_2$ (dois-a-dois disjunto) e, por isso,

$$|S| = |S_0| + |S_1| + |S_2|.$$

Em termos de cardinalidades dos subconjuntos, temos:

- $|S_0| = 3^5 = 243$;
- $S_1 = S_1^{1,3} \cup S_1^{1,4} \cup S_1^{1,5} \cup S_1^{2,4} \cup S_1^{2,5} \cup S_1^{3,5}$ (dois a dois disjuntos), onde o primeiro número do índice superior representa a posição de «(» e o segundo representa a posição de «)»;
- $S_2 = \{«((a))», «((b))», «((c))»\}$, logo $|S_2| = 3$.

Concluindo, $|S| = 243 + 162 + 3 = 408$.

Generalizações

Vamos agora tomar uma generalização do princípio da multiplicação: suponhamos que temos um procedimento com n escolhas onde temos:

- r_1 possibilidades para a primeira escolha;
- r_2 possibilidades para a segunda escolha (independentemente da primeira escolha);
- ...
- r_n possibilidades para a última escolha (independentemente das $n - 1$ escolhas feitas anteriormente).

Então, existirão $r_1 \cdot r_2 \cdot \dots \cdot r_n$ maneiras de realizar o procedimento.

Exemplo 2.4.4. Vamos calcular quantos números existem com 4 algarismos distintos. De facto, se o número tem 4 algarismos, para primeira escolha podemos tomar qualquer ele-

mento em $\{1, \dots, 9\}$. De seguida, podemos tomar qualquer número diferente do escolhido anteriormente, e assim sucessivamente. Desta forma,

$$|\{\text{números com 4 algarismos distintos}\}| = 9 \times 9 \times 8 \times 7 = 4536.$$

Exemplo 2.4.5. Vamos calcular quantos números existem com 4 algarismos distintos em $1, \dots, 9$, um deles igual a 5. Neste caso, para primeira escolha podemos tomar a posição do algarismo 5, há quatro possibilidades. Depois podemos sucessivamente escolher os outros algarismos, portanto, existem

$$4 \times 8 \times 7 \times 6 = 1344$$

tais números.

Como vimos anteriormente, o princípio da adição só é válido quando os conjuntos A_1, \dots, A_n são dois-a-dois disjuntos. No entanto, quando temos problemas em que tal não acontece, podemos utilizar outra ferramenta: o **princípio da inclusão-exclusão**.

Só para ficarmos com uma ligeira ideia do que aí vem, vamos apresentar o princípio para alguns casos:

- $n = 2$. Para conjuntos A_1 e A_2 , a soma $|A_1| + |A_2|$ conta os elementos comuns de A_1 e A_2 duas vezes; portanto,

$$|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|.$$

- $n = 3$. Baseado no caso anterior, para conjuntos A_1, A_2 e A_3 calculamos

$$\begin{aligned} |A_1 \cup (A_2 \cup A_3)| &= |A_1| + |A_2 \cup A_3| - |A_1 \cap (A_2 \cup A_3)| \\ &= |A_1| + |A_2 \cup A_3| - |(A_1 \cap A_2) \cup (A_1 \cap A_3)| \\ &= |A_1| + |A_2| + |A_3| - |A_2 \cap A_3| \\ &\quad - (|A_1 \cap A_2| + |A_1 \cap A_3| + |A_1 \cap A_2 \cap A_3|) \\ &= |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_1 \cap A_3| \\ &\quad - |A_2 \cap A_3| + |A_1 \cap A_2 \cap A_3|. \end{aligned}$$

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

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

Demonstração. Vamos fazer a prova deste resultado por indução no número n de conjuntos considerados. Como base da indução, conseguimos rapidamente ver que, para $n = 1$, $|A_1| = |A_1|$ e, para $n = 2$, $|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$. Como hipótese de indução,

vamos supor que o resultado é verdadeiro para n conjuntos com $n \geq 2$. Desta forma,

$$\begin{aligned}
\left| \bigcup_{i=1}^{n+1} A_i \right| &= \left| \bigcup_{i=1}^n A_i \right| + |A_{n+1}| - \left| \bigcup_{i=1}^n A_i \cap A_{n+1} \right| \\
&= \sum_{k=1}^n (-1)^{k+1} \left(\sum_{1 \leq i_1 \leq \dots \leq i_k \leq n} |A_{i_1} \cap \dots \cap A_{i_k}| \right) + |A_{n+1}| \\
&\quad - \sum_{k=1}^n (-1)^{k+1} \left(\sum_{1 \leq i_1 \leq \dots \leq i_k \leq n} |A_{i_1} \cap \dots \cap A_{i_k} \cap A_{n+1}| \right) \\
&= |A_1| + \dots + |A_n| + |A_{n+1}| \\
&\quad + \sum_{k=2}^n (-1)^{k+1} \left(\sum_{1 \leq i_1 \leq \dots \leq i_k \leq n} |A_{i_1} \cap \dots \cap A_{i_k}| \right) \\
&\quad + \sum_{k=1}^{n-1} (-1)^{k+2} \left(\sum_{1 \leq i_1 \leq \dots \leq i_k \leq n} |A_{i_1} \cap \dots \cap A_{i_k} \cap A_{n+1}| \right) \\
&\quad + (-1)^{n+2} |A_1 \cap \dots \cap A_n \cap A_{n+1}| \\
&= |A_1| + \dots + |A_n| + |A_{n+1}| \\
&\quad + \sum_{k=2}^n (-1)^{k+1} \left(\sum_{1 \leq i_1 \leq \dots \leq i_k \leq n} |A_{i_1} \cap \dots \cap A_{i_k}| \right) \\
&\quad + \sum_{k=2}^n (-1)^{k+1} \left(\sum_{1 \leq i_1 \leq \dots \leq i_k \leq n+1} |A_{i_1} \cap \dots \cap A_{i_k}| \right) \\
&\quad + (-1)^{n+2} |A_1 \cap \dots \cap A_n \cap A_{n+1}| \\
&= |A_1| + \dots + |A_n| + |A_{n+1}| \\
&\quad + \sum_{k=2}^n (-1)^{k+1} \left(\sum_{1 \leq i_1 \leq \dots \leq i_k \leq n+1} |A_{i_1} \cap \dots \cap A_{i_k}| \right) \\
&\quad + (-1)^{n+2} |A_1 \cap \dots \cap A_n \cap A_{n+1}| \\
&= \sum_{k=1}^{n+1} (-1)^{k+1} \left(\sum_{1 \leq i_1 \leq \dots \leq i_k \leq n+1} |A_{i_1} \cap \dots \cap A_{i_k}| \right). \quad \blacklozenge
\end{aligned}$$

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

Começemos por considerar os conjuntos $A_k = \{n \in \{1, \dots, 1000\} \mid k \text{ divide } n\}$, para $k = 1, \dots, 1000$. Desta forma,

$$\begin{aligned}
|A_3 \cup A_5| &= |A_3| + |A_5| - |A_3 \cap A_5| \\
&= \left\lfloor \frac{1000}{3} \right\rfloor + \left\lfloor \frac{1000}{5} \right\rfloor - \left\lfloor \frac{1000}{15} \right\rfloor \\
&= 333 + 200 - 66 = 467.
\end{aligned}$$

Exemplo 2.4.8. Quantas palavras de comprimento 10 com letras em $\{a, \dots, z\}$ (23 letras) existem que não contêm todas as vogais («a, e, i, o, u»)?

Sejam A_a, \dots, A_u os conjuntos das palavras de comprimento 10 sem «a», \dots , «u», respectivamente. Então, aquilo que procuramos é, justamente, $|A_a \cup \dots \cup A_u|$.

- $|A_a| = \dots = |A_u| = 22^{10}$;
- $|A_a \cap A_e| = \dots = |A_o \cap A_u| = 21^{10}$;
- $|A_a \cap A_e \cap A_i| = \dots = |A_i \cap A_o \cap A_u| = 20^{10}$;
- $|A_a \cap A_e \cap A_i \cap A_o| = \dots = |A_e \cap A_i \cap A_o \cap A_u| = 19^{10}$;
- $|A_a \cap A_e \cap A_i \cap A_o \cap A_u| = 18^{10}$.

No total, existirão 10 intersecções de 2 conjuntos, 10 intersecções de 3 conjuntos e 5 intersecções de 4 conjuntos. Logo,

$$|A_a \cup A_e \cup A_i \cup A_o \cup A_u| = 5 \cdot 22^{10} - 10 \cdot 21^{10} + 10 \cdot 20^{10} - 5 \cdot 19^{10} + 18^{10}.$$

Exemplo 2.4.9. Sejam X um conjunto finito e p_1, \dots, p_n , propriedades aplicáveis aos elementos de X e $N(i_1, i_2, \dots, i_k)$ o número de elementos de X que têm, pelo menos, as propriedades p_{i_1}, \dots, p_{i_k} .

Designando o conjunto dos elementos de X que tem a propriedade p_i por A_i , sabemos que o número de elementos de X que têm, pelo menos, uma das propriedades p_1, \dots, p_n é dado pela expressão

$$\begin{aligned} |A| = |A_1 \cup \dots \cup A_n| &= N(1) + \dots + N(n) \\ &\quad - N(1, 2) - \dots - N(n-1, n) \\ &\quad + N(1, 2, 3) + \dots + N(n-2, n-1, n) \\ &\quad \vdots \\ &\quad + (-1)^{n+1} N(1, \dots, n). \end{aligned}$$

De forma semelhante, o número de elementos de X que não tem qualquer propriedade p_1, \dots, p_n é dado pela expressão

$$\begin{aligned} |X \setminus A| &= |X| - N(1) + \dots - N(n) \\ &\quad + N(1, 2) - \dots - N(n-1, n) \\ &\quad - N(1, 2, 3) + \dots + N(n-2, n-1, n) \\ &\quad \vdots \\ &\quad + (-1)^n N(1, \dots, n). \end{aligned}$$

Agrupamentos e Identidades

Combinatórias

Neste capítulo, veremos situações em que faremos escolha de mais do que um item de entre uma população finita, na qual cada item é unicamente identificado. De facto, estaremos interessados em responder ao tipo de pergunta que se segue:

De quantas maneiras podemos escolher k elementos de uma colecção de n elementos?

Tal dependerá, de forma óbvia, do que consideramos «diferente»... Podemos repetir elementos? A ordem destes elementos interessa?

Em termos de nomenclatura, falaremos de **arranjos** quando a ordem dos elementos interessar e de **combinações** quando a ordem não interessar.

3.1 Permutações e Arranjos

Definição 3.1.1. Um **arranjo com repetição** de n elementos k a k é uma «maneira» de escolher k elementos entre n com repetição e dependente da ordem, ou seja, uma função do tipo

$$f: \{1, \dots, k\} \longrightarrow \{1, \dots, n\}.$$

É usual denotarmos o número de arranjos com repetição de n elementos k a k por $A^r(n, k)$.

De acordo com a definição imediatamente acima, $f(1)$ será a primeira escolha, $f(2)$ será a segunda escolha, e assim por diante ...

No entanto, devemos ver que existem n possibilidades de escolha para $f(1)$, da mesma forma que existirão n possibilidades para $f(2)$ (uma vez que estamos a considerar as repetições).

O mesmo se passará até $f(k)$. Desta forma, e por aplicação do Princípio da Multiplicação (visto anteriormente),

$$A^r(n, k) = \underbrace{n \times \cdots \times n}_{k \text{ vezes}} = n^k.$$

Nota 3.1.2. Para cada $n \in \mathbb{N}$, $A^r(n, 0) = n^0 = 1$. Em particular, $A^r(0, 0) = 0^0 = 1$.

Exemplo 3.1.3. Suponhamos que fazemos a pergunta «Qual é o dia da semana do seu aniversário» a 6 pessoas. O número de respostas possível, de acordo com o conceito que acabámos de definir, é dado por $A^r(7, 6) = 7^6 = 117649$.

Exemplo 3.1.4. Suponhamos que se encontra ao nosso dispor um número ilimitado de bolas vermelhas, azuis e verdes. Sabendo que as bolas da mesma cor são indistinguíveis, de qual será o número de sequências que podemos formar com 5?

De facto, o problema pode simplesmente traduzir-se na contagem das possibilidades de formar $k = 5$ escolhas em $\{\bullet, \bullet, \bullet\}$. Desta forma, será possível formar $A^r(3, 5) = 3^5 = 243$ sequências.

Definição 3.1.5. Um **arranjo sem repetição** (ou **arranjo simples**) de n elementos k a k é uma «maneira» de escolher k elementos entre n sem repetição e dependendo da ordem, ou seja, é uma função injectiva do tipo

$$f: \{1, \dots, k\} \longrightarrow \{1, \dots, n\}.$$

Aqui, denotaremos o número de arranjos sem repetição de n elementos k a k por $A^s(n, k)$.

Neste caso, e contrariamente aos arranjos com repetição, existirão n possibilidades de escolha para $f(1)$, mas apenas $n - 1$ possibilidades para $f(2)$ (uma vez que $f(2) \neq f(1)$). Assim, e por aplicação do Princípio da Multiplicação Generalizado, temos que

$$A^s(n, k) = n \cdot (n - 1) \cdot (n - 2) \cdots (n - k + 1) = \frac{n!}{(n - k)!}.$$

Nota 3.1.6. Existem certos casos dos arranjos sem repetição a que devemos prestar alguma atenção, nomeadamente:

- ($n \in \mathbb{N}$ e $k = 0$): $A^s(n, 0) = \frac{n!}{n!} = 1$;
- ($n \in \mathbb{N}$ e $k > n$): $A^s(n, k) = 0$;
- ($n \in \mathbb{N}$ e $k = n$): $A^s(n, n) = \frac{n!}{(n-n)!} = \frac{n!}{0!} = n!$.

O último caso apresentado merece um certo «destaque adicional». De facto, os arranjos simples $A^s(n, n)$ designam-se por **permutações simples** (e podem ser interpretadas como funções bijectivas $\{1, \dots, n\} \rightarrow \{1, \dots, n\}$).

Exemplo 3.1.7. De acordo com o conceito agora introduzido, torna-se extremamente fácil calcular o número de formas distintas de sentar k pessoas retiradas de um grupo de n pessoas num banco corrido. De facto, a resposta será $A^s(n, k)$.

No entanto, se ao invés de um banco corrido tivermos uma mesa redonda, devemos ter em conta que as rotações de uma mesma configuração não geram formas distintas. Neste caso, o número de maneiras diferentes de sentar as tais k pessoas é dado por $\frac{A^s(n, k)}{k}$.

Exemplo 3.1.8. Vamos calcular o número de alinhamentos possíveis de 12 escuteiros de tal forma que dois deles (fixos) sejam sempre vizinhos um do outro.

Consideremos A e B como os escuteiros fixos e retiremos A do grupo. O número de alinhamentos possíveis dos restantes 11 será dado por $11! = 39916800$. No entanto, em cada um destes alinhamentos, podemos inserir A ou à esquerda de B , ou à direita de B ; portanto, o número total de alinhamentos será dado por $2 \times 11! = 79833600$.

Exemplo 3.1.9. Vamos calcular a soma de todos os números obtidos por permutações dos dígitos 23456789.

Sabemos que, no total, existirão $A^s(8, 8) = 8! = 40320$ parcelas na soma. Se considerarmos agora uma qualquer posição fixa dessas parcelas, sabemos que exactamente $\frac{1}{8}$ delas têm cada um dos 8 dígitos dados nessa posição; i.e., $\frac{A^s(8, 8)}{8} = 7! = 5040$ parcelas. Desta forma, a soma dos dígitos nesta posição é

$$5040(2 + 3 + 4 + 5 + 6 + 7 + 8 + 9) = 221760.$$

Assim sendo, a soma total será dada por

$$221760(1 + 10 + 10^2 + 10^3 + 10^4 + 10^5 + 10^6 + 10^7) = 221760(11111111) = 2463999975360.$$

3.2 Combinações

Definição 3.2.1. Uma **combinação sem repetição** (ou **combinação simples**) de n elementos k a k é um subconjunto de k elementos de um conjunto de n elementos. Denotarmos o número de combinações simples de n elementos k a k por $\binom{n}{k}$.

Em termos de cálculo, é possível vermos que existe uma certa relação entre as combinações e os arranjos (ambos sem repetição):

$$\binom{n}{k} = \frac{A^s(n, k)}{k!} = \frac{n \cdot (n-1) \cdot \dots \cdot (n-k+1)}{k!} = \frac{n!}{(n-k)!k!}$$

Nota 3.2.2. Apenas faz sentido calcular $\binom{n}{k}$ com a formula acima quando temos $0 \leq k \leq n$. Caso tal não aconteça, temos que $\binom{n}{k} = 0$.

Exemplo 3.2.3. Vamos regressar ao Exemplo 2.3.3 e denotar agora por $\mathbb{B}_{k,m}^{k+m}$ o conjunto das sequências binárias com k uns e m zeros. Então, $|\mathbb{B}_{k,m}^{k+m}|$ coincide com o número de subconjuntos de k elementos de um conjunto de $k+m$ elementos, ou seja, $|\mathbb{B}_{k,m}^{k+m}| = \binom{k+m}{k} = \binom{k+m}{m}$.

De facto, fazendo $X = \{1, \dots, k+m\}$, a função

$$f: \{A \subseteq X \mid |A| = k\} \longrightarrow \mathbb{B}_{k,m}^{k+m}$$

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

tem inversa

$$f^{-1}: \mathbb{B}_{k,m}^{k+m} \longrightarrow \{A \subseteq X \mid |A| = k\}$$

$$x_1 \dots x_{k+m} \longmapsto \{i \in X \mid a_i = 1\}.$$

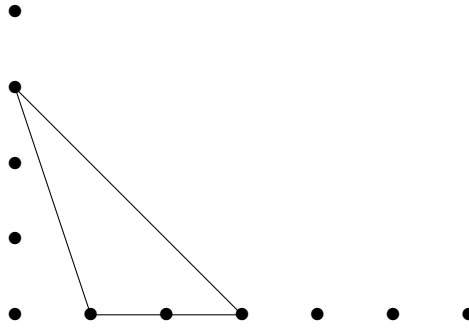
Exemplo 3.2.4. Sabendo que existem apenas 6 tipos diferentes de bilhetes da lotaria, podemos pensar em quantas maneiras existem de comprar 3 bilhetes diferentes. De facto, existirão $\binom{6}{3} = 20$ possibilidades.

Exemplo 3.2.5. Num grupo de 16 raparigas e 15 rapazes, quantos grupos de 5 pessoas conseguimos formar com, pelo menos, 3 rapazes? Temos três hipóteses em cima da mesa:

- o grupo tem 3 rapazes: $\binom{15}{3}\binom{16}{2} = 54600$;
- o grupo tem 4 rapazes: $\binom{15}{4}\binom{16}{1} = 21840$;
- o grupo tem 5 rapazes: $\binom{15}{5} = 3003$.

Para obtermos o total dos grupos, basta somarmos todas as possibilidades: $54600 + 21840 + 3003 = 79443$.

Exemplo 3.2.6. Vamos considerar o conjunto dos triângulos (com ângulos não nulos) cujos vértices são os pontos mostrados na figura abaixo.



Podemos perguntar qual será o tamanho de um tal conjunto de triângulos? A resposta não é muito complicada; basta pensarmos um pouco no problema.

Sabemos que não podemos ter três vértices colineares (uma vez que tal levará a triângulos com ângulos nulos). No entanto, há que ter (também) algum cuidado com o vértice que pertence à intersecção dos eixos. Temos então 3 casos a considerar:

- dois dos vértices pertencem ao eixo horizontal (sem intersecção) e o restante pertence ao eixo vertical (também sem intersecção): $\binom{6}{2}\binom{4}{1} = 60$;
- dois dos vértices pertencem ao eixo vertical (sem intersecção) e o restante pertence ao eixo horizontal (também sem intersecção): $\binom{4}{2}\binom{6}{1} = 36$;
- um vértice é a intersecção dos dois eixos, outro pertence ao eixo horizontal, e o restante ao eixo vertical: $\binom{6}{1}\binom{4}{1} = 24$.

Por último, resta-nos somar as possibilidades: $60 + 36 + 24 = 120$.

Exemplo 3.2.7. Para um truque de magia, pedimos a um colega que tire três cartas de um baralho clássico com 52 cartas. Como sabemos, o número de maneiras distintas que de obter essas três cartas é dado por $\binom{52}{3}$.

Alterando ligeiramente o truque, pedimos agora que o colega retire 3 cartas, mas que a primeira não seja do naipe \spadesuit (caso tal não aconteça, o colega repõe a carta ao fundo do baralho e torna a retirar). As restantes 2 cartas poderão ser de qualquer naipe ($\spadesuit, \clubsuit, \diamond$ ou \heartsuit). Quantos conjuntos distintos de 3 cartas podemos agora ter?

Atenção: Neste caso, ter $\{4\diamond, 6\spadesuit, 10\clubsuit\}$ não é diferente de ter $\{6\spadesuit, 10\clubsuit, 4\diamond\}$.

A resolução do problema passa por perceber que as únicas escolhas que não podem ocorrer prendem-se à possibilidade do conjunto ser formado apenas por cartas do naipe \spadesuit . Desta forma, haverá $\binom{52}{3} - \binom{13}{3} = 21814$ conjuntos distintos.

Exemplo 3.2.8. Suponhamos um conjunto X de tal forma que $|X| = x$. Se adicionarmos 8 elementos a X , as possibilidades de escolha de 2 elementos de X aumentam em 11 vezes. Quantos elementos tem X ?

Bem, o primeiro passo para a resolução será traduzir o enunciado do problema em linguagem matemática. Desta forma, obtemos

$$\binom{x+8}{2} = 11 \binom{x}{2}.$$

Resta-nos então resolver esta expressão:

$$\begin{aligned} \binom{x+8}{2} = 11 \binom{x}{2} &\iff \frac{(x+8)!}{(x+6)!2!} = 11 \frac{x!}{(x-2)!2!} \\ &\iff (x+8)(x+7) = 11x(x+1) \\ &\iff x^2 + 15x + 56 = 11x^2 - 11x \\ &\iff 10x^2 - 26x - 56 = 0 \\ &\iff x = 4 \vee x = -\frac{7}{5}. \end{aligned}$$

Desta forma, concluímos que $|X| = 4$.

Teorema 3.2.9. *Sejam $n, k \in \mathbb{N}$, com $k \leq n$. Então:*

1. $\binom{n}{k} = \binom{n}{n-k}$;
2. $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$ (supondo $n, k > 0$);
3. $\sum_{i=0}^n \binom{n}{i} = 2^n$.

Demonstração. Consideremos o conjunto $X = \{1, \dots, n\}$. Para o primeiro ponto do resultado, basta verificarmos que a função

$$\begin{aligned} f: \{A \subseteq X \mid |A| = k\} &\longrightarrow \{B \subseteq X \mid |B| = n - k\} \\ A &\longmapsto A^c = X \setminus A \end{aligned}$$

é invertível e, por isso, bijectiva.

Para o segundo ponto, vamos considerar X e um conjunto $Y = X \setminus \{n\} = \{1, \dots, n-1\}$. Temos então que

$$\begin{aligned} \{A \subseteq X \mid |A| = k\} &= \{A \subseteq X \mid |A| = k, n \notin A\} \cup \{A \subseteq X \mid |A| = k, n \in A\} \\ &= \{A \subseteq Y \mid |A| = k\} \cup \{B \cup \{n\} \mid B \subseteq Y, |B| = k-1\}. \end{aligned}$$

Por último, vejamos ainda que (considerando X),

$$\mathcal{P}(X) = \bigcup_{i=0}^n \{A \subseteq X \mid |A| = i\}$$

Demonstração. O primeiro ponto é de relativamente fácil demonstração se tivermos em conta os argumentos combinatórios certos. Sabemos que

$$\begin{aligned}
 (1+x)^n &= \overbrace{(1+x)(1+x)\dots(1+x)}^{n \text{ vezes}} \\
 &= 1 \cdot 1 \dots 1 \\
 &\quad + \underbrace{x \cdot 1 \dots 1}_{x \text{ do primeiro factor}} + \underbrace{1 \cdot x \cdot 1 \dots 1}_{x \text{ do segundo factor}} + \dots + \underbrace{1 \dots 1 \cdot x}_{x \text{ do último factor}} \\
 &\quad + x \cdot x \cdot 1 \dots 1 + x \cdot 1 \cdot x \cdot 1 \dots 1 + \dots + 1 \dots 1 \cdot x \cdot x \\
 &\quad \vdots \\
 &\quad + x \dots x.
 \end{aligned}$$

Desta forma, existirão $\binom{n}{1} = n$ factores com apenas um x , $\binom{n}{2}$ factores com dois x 's, e assim por diante. Pela comutatividade da multiplicação e pela neutralidade do elemento 1 para esta operação, podemos concluir que

$$(1+x)^n = \sum_{k=0}^n \binom{n}{k} x^k.$$

Relativamente ao segundo ponto do resultado, era possível fazermos uma prova semelhante à previamente apresentada, ou se pode deduzir a segunda fórmula a partir da primeira considerando $(a+b)^n = a^n(1+\frac{b}{a})^n$ se $a \neq 0$. No entanto, vamos seguir um caminho diferente (indução matemática). A primeira coisa a fazer será verificar a base da indução ($n = 1, 2$):

$$(a+b)^1 = a+b = \binom{1}{0} a^1 b^0 + \binom{1}{1} a^0 b^1 = \sum_{k=0}^1 \binom{1}{k} a^{1-k} b^k.$$

$$(a+b)^2 = a^2 + 2ab + b^2 = \binom{2}{0} a^2 b^0 + \binom{2}{1} a^1 b^1 + \binom{2}{2} a^0 b^2 = \sum_{k=0}^2 \binom{2}{k} a^{2-k} b^k.$$

Como hipótese de indução, vamos admitir que a fórmula é válida para todos os números naturais até n (inclusive). O objectivo será agora mostrar que esta ainda será válida para $n+1$. Então, fazendo o passo de indução,

$$\begin{aligned}
 (a+b)^{n+1} &= (a+b)(a+b)^n \\
 &= (a+b) \left[a^n + \binom{n}{1} a^{n-1} b + \binom{n}{2} a^{n-2} b^2 + \dots + \binom{n}{n-1} a b^{n-1} + b^n \right] \\
 &= a^{n+1} + \left[1 + \binom{n}{1} \right] a^n b + \left[\binom{n}{1} + \binom{n}{2} \right] a^{n-1} b^2 + \dots \\
 &\quad \dots + \left[\binom{n}{r-1} + \binom{n}{r} \right] a^{n-r+1} b^r + \dots + \left[\binom{n}{n-1} + 1 \right] a b^n + b^{n+1}.
 \end{aligned}$$



Nota 3.2.12. Se fizermos $x = 1$ na primeira fórmula do resultado acima, conseguimos obter uma segunda demonstração (puramente algébrica) para o ponto 3. do Teorema 3.2.9 ($\sum_{i=0}^n \binom{n}{i} = 2^n$).

Exemplo 3.2.13. O segundo, terceiro e quarto termos de uma expansão binomial $(a + b)^n$ são, respectivamente, 240, 720 e 1080. Vamos encontrar os valores de a, b e n .

Vejamos que

$$\begin{cases} \binom{n}{1}a^{n-1}b = 240 \\ \binom{n}{2}a^{n-2}b^2 = 720 \\ \binom{n}{3}a^{n-3}b^3 = 1080 \end{cases}$$

Ao dividir a 2ª equação pela 1ª, e a 3ª equação pela 2ª, obtemos $\frac{b}{a} = \frac{6}{n-1}$ e $\frac{b}{a} = \frac{9}{2(n-2)}$, o que nos leva a

$$\frac{6}{n-1} = \frac{9}{2(n-2)} \iff n = 5.$$

Ora,

$$\frac{\binom{5}{1}a^{5-1}b}{\frac{b}{a}} = \frac{240}{\frac{6}{4}} \iff 5a^5 = 160 \iff a = 2,$$

e, por substituição em $\frac{b}{a} = \frac{6}{n-1}$, atingimos $b = 3$.

Exemplo 3.2.14. Utilizando o Teorema Binomial, vamos mostrar que, se $n \in \mathbb{N}$, então $6^n - 5n \equiv 1 \pmod{25}$, ou seja, $6^n - 5n = 1 + 25k$ para algum $k \in \mathbb{N}$.

Consideremos a expansão que figura no enunciado do Teorema Binomial,

$$(1 + x)^n = \sum_{k=0}^n \binom{n}{k} x^k.$$

Tomando $x = 5$, obtemos

$$6^n = (1 + 5)^n = \sum_{k=0}^n \binom{n}{k} 5^k = 1 + 5n + 25 \left[\binom{n}{2} + 5 \binom{n}{3} + \dots + \binom{n}{n} 5^{n-2} \right]$$

se e somente se

$$6^n - 5n = 1 + 25k, \text{ onde } k = \binom{n}{2} + 5 \binom{n}{3} + \dots + \binom{n}{n} 5^{n-2}.$$

Exemplo 3.2.15. Vamos encontrar os últimos dois dígitos do número 7^{400} .

Temos que

$$7^{400} = (7^2)^{200} = (50 - 1)^{200}$$

$$\begin{aligned}
&= \binom{200}{0} 50^{200} - \binom{200}{1} 50^{199} + \cdots + \binom{200}{198} 50^2 - \binom{200}{199} 50 + \binom{200}{200} \\
&= 50^2 \left[\binom{200}{0} 50^{198} - \binom{200}{1} 50^{197} + \cdots + \binom{200}{198} \right] - 200 \cdot 50 + 1.
\end{aligned}$$

Porque 50^2 e 200 são divisíveis por 100, os últimos dois dígitos de 7^{400} serão «01».

Exemplo 3.2.16. Uma das muitas aplicações do Teorema Binomial na Análise Complexa (e Real) é relativa à obtenção de fórmulas para os senos e co-senos de ângulos múltiplos. De acordo com a fórmula de De Moivre,

$$\cos(n\theta) + i \sin(n\theta) = (\cos(\theta) + i \sin(\theta))^n.$$

Ao expandir o membro direito da equação acima, obtemos

$$\cos(n\theta) + i \sin(n\theta) = \sum_{k=0}^n \left[\binom{n}{k} \cos^{n-k}(\theta) i^k \sin^k(\theta) \right].$$

No entanto, porque $i^{4k} = 1$, $i^{4k+1} = i$, $i^{4k+2} = -1$ e $i^{4k+3} = -i$ (para qualquer $k \in \mathbb{N}$), devemos separar a soma em «duas partes» e tratar o caso par e ímpar de k separadamente.

$$\begin{aligned}
\sum_{k=0}^n \left[\binom{n}{k} \cos^{n-k}(\theta) i^k \sin^k(\theta) \right] &= \sum_{j \in 2\mathbb{N}} \binom{n}{j} \left[(-1)^{\frac{j}{2}} \cos^{n-j}(\theta) \sin^j(\theta) \right] \\
&\quad + i \sum_{j \in 2\mathbb{N}+1} \binom{n}{j} \left[(-1)^{\frac{j-1}{2}} \cos^{n-j}(\theta) \sin^j(\theta) \right]
\end{aligned}$$

A partir daqui, chegamos a

$$\begin{aligned}
\cos(n\theta) &= \sum_{j \in 2\mathbb{N}} \binom{n}{j} \left[(-1)^{\frac{j}{2}} \cos^{n-j}(\theta) \sin^j(\theta) \right], \\
\sin(n\theta) &= \sum_{j \in 2\mathbb{N}+1} \binom{n}{j} \left[(-1)^{\frac{j-1}{2}} \cos^{n-j}(\theta) \sin^j(\theta) \right].
\end{aligned}$$

Exemplo 3.2.17. O número de Neper (ou número de Euler) é, muitas vezes, tomado como

$$e = \lim_{n \rightarrow \infty} \left(1 + \frac{1}{n} \right)^n.$$

Ao aplicar o Teorema Binomial e expandir a fórmula interior ao limite, obtemos

$$\lim_{n \rightarrow \infty} \left(1 + \frac{1}{n} \right)^n = \lim_{n \rightarrow \infty} \sum_{k=0}^n \binom{n}{k} \frac{1}{n^k}$$

No entanto, não é directa a troca entre o operador limite e operador soma. Em verdade,

tal só será possível devido a um «corolário» do Teorema da Convergência Dominada de Lebesgue, dito Teorema de Tannery, que passamos a enunciar:

Teorema 3.2.18 (Tannery). *Dado um $k \in \mathbb{N}$, seja $f_k(n)$ uma função de variável natural. Suponhamos que existem sucessões $(L_k)_{k \in \mathbb{N}}$ e $(M_k)_{k \in \mathbb{N}}$, onde cada M_k é independente de n , tais que $\lim_{n \rightarrow \infty} f_k(n) = L_k$ e $|f_k(n)| \leq M_k$, para todos os k, n . Se $\sum_{k=0}^{\infty} M_k$ for convergente, então*

$$\lim_{n \rightarrow \infty} \sum_{k=0}^n f_k(n) = \sum_{k=0}^{\infty} \lim_{n \rightarrow \infty} f_k(n) = \sum_{k=0}^{\infty} L_k.$$

Tomando então $f_k(n) = \binom{n}{k} \frac{1}{n^k}$ e $L_k = \frac{1}{k!} = M_k$, podemos aplicar o resultado auxiliar acima apresentado e concluir que

$$e = \lim_{n \rightarrow \infty} \left(1 + \frac{1}{n}\right)^n = \lim_{n \rightarrow \infty} \sum_{k=0}^n \binom{n}{k} \frac{1}{n^k} = \sum_{k=0}^{\infty} \lim_{n \rightarrow \infty} \binom{n}{k} \frac{1}{n^k} = \sum_{k=0}^{\infty} \frac{1}{k!} = 1 + 1 + \frac{1}{2!} + \frac{1}{3!} + \dots$$

Exemplo 3.2.19. A generalização da Regra de Leibniz (regra para a derivada do produto de duas funções) toma forma semelhante à do Teorema Binomial. De facto, para duas funções n -diferenciáveis f, g , temos que

$$(fg)^{(n)} = \sum_{k=0}^n \binom{n}{k} f^{(n-k)} g^{(k)}.$$

É possível mostrarmos que tal fórmula é válida ao aplicar indução matemática.

Como base da indução teremos o caso $n = 1$:

$$(fg)^{(1)} = \sum_{k=0}^1 \binom{1}{k} f^{(1-k)} g^{(k)} = f^{(1-0)} g^{(0)} + f^{(1-1)} g^{(1)} = f'g + fg' = (fg)'$$

Como hipótese de indução, vamos admitir que a igualdade acima é válida para qualquer natural até n (inclusive). Então,

$$\begin{aligned} (fg)^{(n+1)} &= \left[\sum_{k=0}^n \binom{n}{k} f^{(n-k)} g^{(k)} \right]' = \sum_{k=0}^n \binom{n}{k} f^{(n+1-k)} g^{(k)} + \sum_{k=0}^n \binom{n}{k} f^{(n-k)} g^{(k+1)} \\ &= \sum_{k=0}^n \binom{n}{k} f^{(n+1-k)} g^{(k)} + \sum_{k=1}^{n+1} \binom{n}{k-1} f^{(n+1-k)} g^{(k)} \\ &= \binom{n}{0} f^{(n+1)} g + \sum_{k=1}^n \binom{n}{k} f^{(n+1-k)} g^{(k)} + \sum_{k=1}^n \binom{n}{k-1} f^{(n+1-k)} g^{(k)} + \binom{n}{n} f g^{(n+1)} \\ &= \binom{n+1}{0} f^{(n+1)} g + \left(\sum_{k=1}^n \left[\binom{n}{k-1} + \binom{n}{k} \right] f^{(n+1-k)} g^{(k)} \right) + \binom{n+1}{n+1} f g^{(n+1)} \end{aligned}$$

$$\begin{aligned}
&= \binom{n+1}{0} f^{(n+1)} g + \sum_{k=1}^n \binom{n+1}{k} f^{(n+1-k)} g^{(k)} + \binom{n+1}{n+1} f g^{(n+1)} \\
&= \sum_{k=0}^{n+1} \binom{n+1}{k} f^{(n+1-k)} g^{(k)}.
\end{aligned}$$

Exemplo 3.2.20. Utilizando o Teorema Binomial, vamos mostrar que, para quaisquer elementos distintos $a, b \in \mathbb{N}$, $a^n - b^n \equiv 0 \pmod{a-b}$, ou seja, $a^n - b^n = (a-b)k$ para algum $k \in \mathbb{N}$.

Vejamos que

$$\begin{aligned}
a^n &= (b + (a-b))^n = \sum_{k=0}^n \binom{n}{k} b^{n-k} (a-b)^k \\
&= \binom{n}{0} b^n + \binom{n}{1} b^{n-1} (a-b) + \binom{n}{2} b^{n-2} (a-b)^2 + \cdots + \binom{n}{n} (a-b)^n,
\end{aligned}$$

que é equivalente a escrever

$$a^n - b^n = \sum_{k=1}^n \binom{n}{k} b^{n-k} (a-b)^k = (a-b) \left[\sum_{k=1}^n \binom{n}{k} b^{n-k} (a-b)^{k-1} \right],$$

ou seja,

$$a^n - b^n = (a-b)k, \text{ onde } k = \sum_{k=1}^n \binom{n}{k} b^{n-k} (a-b)^{k-1}.$$

Exemplo 3.2.21. O nosso objectivo agora será encontrar uma fórmula fechada para a soma $\sum_{k=1}^n k^2$.

Comecemos por mostrar que

$$\sum_{k=1}^n \binom{k}{1} = \frac{n(n+1)}{2}.$$

Prosseguindo por indução matemática, admitimos como base da indução teremos o caso $n = 1$: $\sum_{k=1}^1 \binom{k}{1} = \binom{1}{1} = 1 = \frac{1(1+1)}{2}$. Como hipótese de indução, vamos admitir que a igualdade é válida para qualquer natural até $m-1$ (inclusive). Então,

$$\begin{aligned}
\sum_{k=1}^m \binom{k}{1} &= \left[\sum_{k=1}^{m-1} \binom{k}{1} \right] + \binom{m}{1} \\
&= \frac{(m-1)m}{2} + \frac{m!}{(m-1)!1!} \\
&= \frac{(m-1)m}{2} + m = \frac{m(m+1)}{2}.
\end{aligned}$$

O próximo passo será ver que

$$\sum_{k=1}^n \binom{k}{2} = \frac{n(n+1)(n-1)}{3!}.$$

Prosseguindo novamente por indução matemática, admitimos como base da indução teremos o caso $n = 1$: $\sum_{k=1}^1 \binom{k}{2} = \binom{1}{2} = 0 = \frac{1(1+1)(1-1)}{6}$. Como hipótese de indução, vamos admitir que a igualdade é válida para qualquer natural até $m - 1$ (inclusive). Então,

$$\begin{aligned} \sum_{k=1}^m \binom{k}{2} &= \left[\sum_{k=1}^{m-1} \binom{k}{2} \right] + \binom{m}{2} \\ &= \frac{m(m-1)(m-2)}{6} + \frac{m!}{(m-2)!2!} \\ &= \frac{m(m-1)(m-2)}{6} + \frac{m(m-1)}{2} = \frac{m(m-1)(m+1)}{6}. \end{aligned}$$

É ainda possível verificar que existem $a, b \in \mathbb{Z}$ tais que $k^2 = a\binom{k}{2} + b\binom{k}{1}$. De facto,

$$\begin{aligned} k^2 = a \frac{k!}{(k-2)!2!} + b \frac{k!}{(k-1)!1!} &\iff k^2 = \frac{k![a(k-1) + 2b]}{(k-1)!2!} \\ &\iff k^2 = \frac{k[a(k-1) + 2b]}{2} = \frac{ak^2 - ak + 2bk}{2} \\ &\iff \begin{cases} \frac{a}{2} = 1 \\ \frac{2b-a}{2} = 0 \end{cases} \Rightarrow \begin{cases} a = 2 \\ b = 1 \end{cases} \end{aligned}$$

Desta forma,

$$\begin{aligned} \sum_{k=1}^n k^2 &= 2 \sum_{k=1}^n \binom{k}{2} + \sum_{k=1}^n \binom{k}{1} = \frac{2n(n+1)(n-1)}{6} + \frac{n(n+1)}{2} \\ &= \frac{2n(n+1)(n-1)}{6} + \frac{3n(n+1)}{6} = \frac{n(n+1)(2n+1)}{6}. \end{aligned}$$

A seguir vamos considerar *combinações com repetição*; intuitivamente, «maneiras» de escolher k elementos de $\{1, \dots, n\}$ sem considerar a ordem mas agora admitimos repetições. Para formular esta ideia formalmente, introduzimos o conceito de «conjunto com elementos repetidos».

Definição 3.2.22. Seja X um conjunto finito. Um **multiconjunto** M em X é um par (X, ν) onde $\nu: X \rightarrow \mathbb{N}$.

Aqui interpretamos $\nu(x)$ como «o número de repetições» de x ou «a multiplicidade» de x . O número $\sum_{x \in X} \nu(x)$ designa-se por **tamanho de M** ou **número de elementos de M** ou **cardinalidade de M** .

Nota 3.2.23. Seja $M = (X, \nu)$ um multiconjunto com $X = \{x_1, \dots, x_n\}$. Com $a_i = \nu(x_i)$, representamos o multiconjunto M da forma mais intuitiva por

$$M = \{x_1^{a_1}, \dots, x_n^{a_n}\} \quad \text{ou} \quad M = \{\underbrace{x_1, \dots, x_1}_{a_1 \text{ vezes}}, \dots, \underbrace{x_n, \dots, x_n}_{a_n \text{ vezes}}\}.$$

Definição 3.2.24. Uma **combinação com repetição** de n elementos k a k é um multiconjunto de k elementos num conjunto de n elementos. O número de combinações com repetição de n elementos k a k denota-se por $\binom{n}{k}$.

Um multiconjunto de k elementos em $X = \{x_1, \dots, x_n\}$ podemos interpretar como a solução $(\nu(x_1), \dots, \nu(x_n))$ da equação $x_1 + \dots + x_n = k$ nas incógnitas x_1, \dots, x_n ; *vice versa*, cada solução em \mathbb{N} desta equação define um multiconjunto de k elementos. Tendo em conta os Exemplos 2.3.3 e 3.2.3, obtém-se

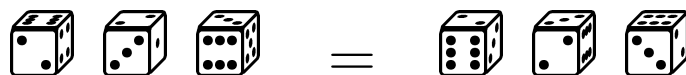
Teorema 3.2.25. O número de combinações com repetição de n elementos k a k é igual ao número de soluções em \mathbb{N} da equação $x_1 + \dots + x_n = k$. Portanto, se $n > 0$,

$$\binom{n}{k} = \binom{k+n-1}{k} = \binom{k+n-1}{n-1}$$

Exemplo 3.2.26. Existem 56 possibilidades de combinar com repetição 5 elementos de $\{1, 2, 3, 4\}$. Neste caso, cada combinação « $n_1 n_2 n_3 n_4 n_5$ » $\in \{1, 2, 3, 4\}^5$ corresponderá a um quádruplo (s_1, \dots, s_4) , onde s_i denota o número de vezes que $i \in \{1, 2, 3, 4\}$ é escolhido.

A título de exemplo, «11431» = «13141» \neq «13443». Aqui, «11431» e «13141» corresponderão à sequência $(3, 0, 1, 1)$, enquanto que «13443» corresponderá a $(1, 0, 2, 2)$.

Exemplo 3.2.27. Consideremos a contagem de alguns lançamentos de três dados cúbicos (regulares). Aqui, dois resultados serão ditos iguais se, independentemente da ordem, os dados mostrarem as mesmas faces, i.e.,



Quantos resultados diferentes existem?

De facto, existirão $\binom{6}{3} = \binom{6+3-1}{3} = \binom{8}{3} = 56$ resultados diferentes.

Exemplo 3.2.28. Vamos determinar o número de possibilidades de colocação de 20 bolas indistinguíveis em 5 caixas numeradas, com pelo menos duas bolas em cada caixa.

Começamos por colocar duas bolas em cada caixa. Depois, para cada uma das restantes bolas, escolhemos uma das 5 caixas; i.e., fazemos uma sequência de 10 escolhas entre 5 elementos. No entanto, o resultado final é independente da ordem das escolhas (no fim, apenas podemos observar quantas bolas estão em cada caixa).

Portanto, temos uma combinação com repetição de 5 elementos 10 a 10:

$$\binom{5}{10} = \binom{5+10-1}{10} = \binom{14}{10} = \binom{14}{4} = \frac{14 \cdot 13 \cdot 12 \cdot 11}{4 \cdot 3 \cdot 2} = 7 \cdot 13 \cdot 11 = 1001.$$

Exemplo 3.2.29. Suponhamos que $n + k$ pessoas querem comprar gelados que custam 1\$, e que, entre elas, n pessoas têm uma moeda de 1\$ e k pessoas têm uma moeda de 2\$. Qual o número de maneiras de ordenar as pessoas na fila de tal forma que o vendedor de gelados arranje sempre uma moeda para dar de troco quando tal é necessário (assumindo-se que, inicialmente, o vendedor não tem qualquer moeda)?

Começamos por notar que o vendedor deverá iniciar as vendas sem qualquer moeda na caixa, o que implica que o primeiro cliente a comprar gelados terá de pagar com 1\$. Seja então $v = (v_1, \dots, v_{n+k})$ a sequência das $n + k$ pessoas que aparecem (por ordem) no estabelecimento. Pelo anterior, temos $v_1 = 1\$$.

Após um qualquer número de vendas, chega-se à conclusão de que, desde o início, nunca poderemos ter mais pessoas a pagar com 2\$ do que com 1\$, i.e., que a sequência v é «totalmente equilibrada» ($k \leq n$). O nosso objectivo será então calcular o número de sequências totalmente equilibradas de comprimento $n + k$. Vemos, com alguma rapidez, que o número de sequências de $n + k$ elementos que se poderá construir com n «uns» e k «dois» é dado por $\binom{n+k}{n} = \binom{n+k}{k}$.

No entanto, é mais prático calcularmos o número de sequências nestas condições que são não totalmente equilibradas. Assim, se (u_1, \dots, u_{n+k}) for uma sequência complementar, existirá um índice i relativamente ao qual, na subsequência (u_1, \dots, u_i) , o número de «uns» é inferior ao número de «dois». Sendo j o menor destes índices i , sabemos que será ímpar e que $1 \leq j \leq n + k - 1$. Considere-se então uma função ψ definida no conjunto das sequências complementares, tal que

$$\psi(u_1, \dots, u_{n+k}) = (3 - u_1, \dots, 3 - u_j, u_{j+1}, \dots, u_{n+k}).$$

Vamos então mostrar que ψ é uma bijecção entre o conjunto I_{n+k} das sequências complementares e as sequências de $n + k$ elementos com $n + 1$ «uns» e $k - 1$ «dois»:

- ψ está bem definida: Seja $u = (u_1, \dots, u_{n+k})$ uma sequência complementar e $j = 2r - 1$, $r \in \mathbb{N}$, fazendo com que nos primeiros j dígitos de u existam r «dois» e $r - 1$ «uns». Então, nos primeiros j dígitos de $\psi(u)$ teremos $r - 1$ «dois» e r «uns». Como consequência, na imagem por ψ de qualquer sequência complementar, o número de

«uns» cresce uma unidade, enquanto que o número de «dois» decresce uma unidade; o que faz com que $\psi(u) \in I_{n+k}$.

- ψ é injectiva: Sejam $x = (x_1, \dots, x_{n+k})$ e $y = (y_1, \dots, y_{n+k})$ duas sequências complementares distintas e sejam j_x e j_y os valores de j , respectivamente, para x e y . Sem perda de generalidade, podemos assumir que $j_x \leq j_y$. Dado que $x \neq y$, existirá um índice s tal que $x_s \neq y_s$ e, adicionalmente
 - Se $j_x = j_y$, então $\psi(x)_s \neq \psi(y)_s$,
 - Se $j_x < j_y$, então admitimos que $s \leq j_x$ e, consequentemente, $\psi(x)_s \neq \psi(y)_s$.

Em ambos os casos se conclui que $x \neq y \Rightarrow \psi(x) \neq \psi(y)$

- ψ é sobrejectiva: Seja $u = (u_1, \dots, u_{n+k}) \in I_{n+k}$, ou seja, u é uma sequência com $n+1$ «uns» e $k-1$ «dois». Seja t o menor índice para o qual, nos w primeiros dígitos de u , temos menor número de «uns» relativamente ao número de «dois». Então,

$$\psi(2 - u_1, \dots, 2 - u_t, u_{t+1}, \dots, u_{n+k})$$

é uma sequência complementar e chegamos ao resultado pretendido,

$$\psi(2 - u_1, \dots, 2 - u_t, u_{t+1}, \dots, u_{n+k}) = (u_1, \dots, u_{n+k}).$$

Desta forma, o número de sequências complementares é igual a $|I_{n+k}|$. Finalmente, e uma vez que o número de sequências de comprimento $n+k$ com k «dois» é $\binom{n+k}{k} = \binom{n+k}{n}$ e $|I_{n+k}| = \binom{n+k}{k-1} = \binom{n+k}{n+1}$, o número de sequências totalmente equilibradas será dado por

$$\begin{aligned} \binom{n+k}{n} - \binom{n+k}{n+1} &= \frac{(n+k)!}{n!k!} - \frac{(n+k)!}{(n+1)!(k-1)!} \\ &= \frac{(n+k)!}{n!k!} - \frac{(n+k)!k}{(n+1)n!k!} \\ &= \left(\frac{(n+k)!}{n!k!} \right) \left(1 - \frac{k}{n+1} \right) = \binom{n+k}{n} \left(\frac{n+1-k}{n+1} \right), \end{aligned}$$

onde, no caso $n = k$, atingimos $\binom{2n}{n} \frac{1}{n+1} = C_n$.

Mencionamos ainda algumas propriedades dos números $\binom{n}{k}$.

Teorema 3.2.30. *Sejam $n, k \in \mathbb{N}$. Então:*

1. $\binom{n}{0} = 1$.
2. Para $k > 1$, $\binom{0}{k} = 0$.
3. Para $n > 0$ e $k > 0$, $\binom{n}{k} = \binom{n}{k-1} + \binom{n-1}{k}$.

Demonstração. Seguramente há um único multiconjunto em X com zero elementos (escolher $\nu(x) = 0$, para cada $x \in X$) e não existe $\nu: \emptyset \rightarrow \mathbb{N}$ com $\sum_{x \in \emptyset} \nu(x) > 0$. A justificação da última propriedade é muito parecida da prova do Teorema 3.2.9: para $X = \{x_1, \dots, x_n\}$, basta observar que

$$\begin{aligned} \{k\text{-multiconjuntos em } X\} &= \{k\text{-multiconjuntos em } X \text{ com } \nu(x_n) > 0\} \\ &\cup \{k\text{-multiconjuntos em } X \text{ com } \nu(x_n) = 0\}. \end{aligned}$$



Extensão do Teorema Binomial

Depois de abordarmos o Teorema Binomial (Teorema 3.2.11), é natural questionarmos o que acontece quando, ao invés de considerarmos um parâmetro $n \in \mathbb{N}$, consideramos um parâmetro $\alpha \in \mathbb{R}$, ou $\alpha \in \mathbb{C}$. A resposta ao problema é relativamente simples... ao invés de considerarmos uma soma finita, consideramos uma soma infinita (em particular, uma série de potências).

Numa primeira instância, e antes ainda de chegarmos às séries, devemos começar por generalizar o conceito de coeficiente binomial.

Definição 3.2.31. Tomemos um $\alpha \in \mathbb{C}$ e $k \in \mathbb{N}$. Através da fórmula multiplicativa utilizada para os coeficientes binomiais, conseguimos obter o **coeficiente binomial generalizado** $\binom{\alpha}{k}$,

$$\binom{\alpha}{k} = \frac{(\alpha)_k}{k!} = \frac{\alpha(\alpha-1)(\alpha-2)\dots(\alpha-k+1)}{k!}.$$

Teorema 3.2.32. *A convergência da série binomial*

$$(1+x)^\alpha = \sum_{k=0}^{\infty} \binom{\alpha}{k} x^k y^{\alpha-k}$$

depende apenas dos valores que α e x tomam, nomeadamente:

1. Se $|x| < 1$, a série converge de forma absoluta para qualquer $\alpha \in \mathbb{C}$.
2. Caso $|x| = 1$:
 - Se $\operatorname{Re}(\alpha) > 0$, a série converge de forma absoluta.
 - Se $-1 < \operatorname{Re}(\alpha) \leq 0$, então a série converge (de forma simples) para $x \neq -1$ e diverge para $x = -1$.
 - Se $\operatorname{Re}(\alpha) \leq -1$, a série diverge.
3. Se $|x| > 1$, a série diverge, a não ser que $\alpha \in \mathbb{N}$ (neste caso, a soma é finita).

Nota 3.2.33. Devemos ter em conta que, a não ser quando $\alpha \in \mathbb{N}$ (caso em que o coeficiente «desaparece» se $\alpha < k$), existe uma relação assintótica deveras útil relacionada com os coeficientes binomiais generalizados. Se considerarmos a notação de Bachmann-Landau,

$$\binom{\alpha}{k} = \frac{(-1)^k}{\Gamma(-\alpha)k^{1+\alpha}}(1 + o(1))$$

quando $k \rightarrow \infty$, o que é praticamente equivalente à definição que Euler deu para a função Gama,

$$\Gamma(z) = \lim_{k \rightarrow \infty} \frac{k!k^z}{z(z+1)\dots(z+k)},$$

e implica (de forma quase imediata) as desigualdades

$$\frac{m}{k^{1+\operatorname{Re}(\alpha)}} \leq \left| \binom{\alpha}{k} \right| \leq \frac{M}{k^{1+\operatorname{Re}(\alpha)}},$$

para certas constantes positivas m e M .

Demonstração. Vamos começar por demonstrar o ponto 1.. O objectivo passa por aplicar o Teste do Quociente de D'Alembert e utilizar a identidade $\binom{\alpha}{k+1} = \binom{\alpha}{k} \frac{\alpha-k}{k+1}$, com vista a mostrar que sempre que $\alpha \notin \mathbb{N}$, o raio de convergência de $(1+x)^\alpha$ é exactamente 1.

$$\ell = \lim_{k \rightarrow \infty} \left| \frac{\binom{\alpha}{k+1}}{\binom{\alpha}{k}} \right| = \lim_{k \rightarrow \infty} \left| \frac{\binom{\alpha}{k} \frac{\alpha-k}{k+1}}{\binom{\alpha}{k}} \right| = \lim_{k \rightarrow \infty} \left| \frac{\alpha-k}{k+1} \right| = 1.$$

Tendo o imediatamente acima em conta, segue também a demonstração do ponto 3..

Para obter a demonstração do primeiro item do ponto 2., basta compararmos a desigualdade da Nota 3.2.33 com a série geométrica de ordem p ,

$$\sum_{k=1}^{\infty} \frac{1}{k^p} = \sum_{k=1}^{\infty} k^{-p}.$$

Neste caso, sabemos que $\sum_{k=1}^{\infty} \frac{1}{k^{1+\operatorname{Re}(\alpha)}}$ irá convergir se e só se o expoente $p = 1 + \operatorname{Re}(\alpha) > 1$, ou seja, se e só se $\operatorname{Re}(\alpha) > 0$.

Para o segundo item do ponto 2., devemos começar por ver que, através da identidade de Pascal, é possível obter

$$(1+x) \sum_{k=0}^n \binom{\alpha}{k} x^k = \sum_{k=0}^n \binom{\alpha+1}{k} x^k + \binom{\alpha}{n} x^{n+1}.$$

Agora, e através do primeiro item do ponto 2. e da desigualdade da Nota 3.2.33, conseguimos chegar à convergência do membro direito da equação acima (para $\operatorname{Re}(\alpha) > -1$). Por outro lado, e novamente pela desigualdade anteriormente referida, sabemos que a série não irá convergir se $|x| = 1$ e $\operatorname{Re}(\alpha) \leq -1$. Alternativamente, podemos observar que, para todo o j ,

$$\left| \frac{\alpha+1}{j} - 1 \right| \geq 1 - \frac{\operatorname{Re}(\alpha+1)}{j} \geq 1.$$

Assim, pelo desenvolvimento de $\binom{\alpha}{k}$ como produto, temos que, para todo o k , $\left| \binom{\alpha}{k} \right| \geq 1$.

Relativamente ao último item do ponto 2., devemos utilizar a identidade acima com $x = -1$ e $\alpha - 1$ em lugar de α , juntamente com a relação assintótica dos coeficientes binomiais generalizados. Desta forma, conseguimos obter

$$\sum_{k=0}^n \binom{\alpha}{k} (-1)^k = \binom{\alpha-1}{n} (-1)^n = \frac{1}{\Gamma(-\alpha+1)n^\alpha} (1 + o(1))$$

quando $n \rightarrow \infty$. A asserção segue agora do comportamento assintótico da sucessão $(n^{-\alpha})_{n \in \mathbb{N}} = (e^{-\alpha \log(n)})_{n \in \mathbb{N}}$ (mais precisamente, $|e^{-\alpha \log(n)}| = e^{-\operatorname{Re}(\alpha) \log(n)}$ certamente converge para 0 quando $\operatorname{Re}(\alpha) > 0$ e diverge se $\operatorname{Re}(\alpha) < 0$. Se $\operatorname{Re}(\alpha) = 0$, então $n^{-\alpha} = e^{-i \cdot \operatorname{Im}(\alpha) \log(n)}$ converge se e só se a sucessão $\operatorname{Im}(\alpha) \log(n)$ convergir (mod 2π), o que certamente será verdadeiro se $\alpha = 0$, mas falso se $\operatorname{Im}(\alpha) \neq 0$: neste último caso, a sucessão será densa (mod 2π), devido ao facto de $\log(n)$ divergir e de $\log(n+1) - \log(n)$ convergir para 0). \blacklozenge

Nota 3.2.34. Embora tenhamos apresentado a expansão do Teorema Binomial para o caso $(1+x)^\alpha$, devemos ter sempre presente que podemos transformar $(1+x)^\alpha$ em $(a \pm b)^\alpha$ ao tomar $x = \pm \frac{b}{a}$, com $|b| < |a|$.

Exemplo 3.2.35. Ao particularizar o parâmetro α , conseguimos obter os seguintes casos da expansão do Teorema Binomial:

- $\alpha = -1$:

$$\begin{aligned} \frac{1}{1+x} &= (1+x)^{-1} = \sum_{k=0}^{\infty} \binom{-1}{k} x^k 1^{-(1+k)} = \sum_{k=0}^{\infty} \frac{(-1)_k}{k!} x^k \\ &= \sum_{k=0}^{\infty} \frac{(-1)^k k!}{k!} x^k = \sum_{k=0}^{\infty} (-1)^k x^k \\ &= 1 - x + x^2 - x^3 + x^4 - x^5 + \dots \end{aligned}$$

- $\alpha = \frac{1}{2}$

$$\begin{aligned} \sqrt{1+x} &= (1+x)^{\frac{1}{2}} = \sum_{k=0}^{\infty} \binom{\frac{1}{2}}{k} x^k 1^{\frac{1}{2}-k} = \sum_{k=0}^{\infty} \frac{\frac{1}{2}(-\frac{1}{2}) \cdots (\frac{3-2k}{2})}{k!} x^k \\ &= \sum_{k=0}^{\infty} \frac{(\frac{1}{2})^k (-1)^{k-1} (2k-3)!!}{k!} x^k = \sum_{k=0}^{\infty} \frac{(-1)^{k-1} (2k-3)!!}{2^k k!} x^k \\ &= 1 - \frac{x}{2} + \frac{x^2}{8} - \frac{x^3}{16} + \frac{5x^4}{128} + \dots \end{aligned}$$

Paridade dos Coeficientes Binomiais

Além do básico abordado sobre os coeficientes binomiais, existem ainda imensas curiosidades que podemos analisar. A título de exemplo, podemos perguntar se é possível determinar a paridade de um determinado coeficiente binomial sem efectuar uma imensidão de cálculos. Ao analisar o Triângulo de Pascal, conseguimos responder rapidamente à questão. Começemos por observar que todas as entradas das linhas 1, 3 e 7 (e, em particular, de naturais da forma $2^n - 1$) são ímpares. Além disso, o número de números ímpares que figura em cada linha parece ser uma potência de base 2. Em termos históricos, a determinação da paridade dos coeficientes binomiais foi inicialmente estudada (de forma sistematica) por James Glaisher.

Teorema 3.2.36. *Consideremos $n, k \in \mathbb{N}$. Então,*

$$\binom{n}{k} \equiv \begin{cases} 0 \pmod{2}, & n \text{ par e } k \text{ ímpar,} \\ \binom{\lfloor n/2 \rfloor}{\lfloor k/2 \rfloor} \pmod{2}, & \text{caso contrário.} \end{cases}$$

Demonstração. A prova deste resultado divide-se em 4 casos:

- **n par e k ímpar:** Dado que n é par, fica claro que, para este caso, o valor do lado direito da propriedade de absorção

$$k \binom{n}{k} = n \binom{n-1}{k-1}$$

é par. Sabendo que o produto $k \binom{n}{k}$ também será par, e que k é ímpar, segue de forma automática que $\binom{n}{k}$ é par, ou seja, que $\binom{n}{k} \equiv 0 \pmod{2}$.

- **n, k pares:** Vamos começar por expandir o coeficiente binomial

$$\begin{aligned} \binom{n}{k} &= \frac{n!}{(n-k)!k!} \\ &= \frac{n(n-1) \dots (n-k+1)}{k!} \\ &= \frac{(n-1)(n-3) \dots (n-k+1)}{1 \cdot 3 \cdot 5 \dots (k-1)} \cdot \frac{n(n-2)(n-4) \dots (n-k+2)}{2 \cdot 4 \cdot 6 \dots k} \\ &= \frac{(n-1)(n-3) \dots (n-k+1)}{1 \cdot 3 \cdot 5 \dots (k-1)} \cdot \frac{n(n-2)(n-4) \dots (n-k+2)}{2^{k/2}(1 \cdot 2 \dots k/2)} \\ &= \frac{(n-1)(n-3) \dots (n-k+1)}{1 \cdot 3 \cdot 5 \dots (k-1)} \cdot \frac{2^{k/2} \cdot \frac{n}{2}(\frac{n}{2}-1)(\frac{n}{2}-2) \dots (\frac{n-k}{2}+1)}{2^{k/2}(1 \cdot 2 \dots k/2)} \\ &= \frac{(n-1)(n-3) \dots (n-k+1)}{1 \cdot 3 \cdot 5 \dots (k-1)} \binom{n/2}{k/2}. \end{aligned}$$

Desta forma,

$$1 \cdot 3 \cdot 5 \dots (k-1) \binom{n}{k} = (n-1)(n-3) \dots (n-k+1) \binom{n/2}{k/2},$$

pelo que se obtém, se n, k forem pares,

$$\binom{n}{k} \equiv \binom{n/2}{k/2} \equiv \binom{\lfloor n/2 \rfloor}{\lfloor k/2 \rfloor} \pmod{2}.$$

Vejamos que a primeira equivalência na fórmula acima deve-se ao facto de que cada um dos factores que precede os coeficientes binomiais é ímpar, além do facto de que a multiplicação por um número ímpar não alterar as paridades. Por outro lado, a segunda equivalência deve-se às igualdades $n/2 = \lfloor n/2 \rfloor$ e $k/2 = \lfloor k/2 \rfloor$ quando n, k são pares.

- **n, k ímpares:** Assim como no primeiro ponto, vamos começar por considerar a propriedade de absorção

$$k \binom{n}{k} = n \binom{n-1}{k-1}.$$

Dado que n, k são ambos ímpares e que a multiplicação por ímpares não altera a paridade, conseguimos concluir que

$$\binom{n}{k} \equiv \binom{n-1}{k-1} \pmod{2}.$$

Além disso, e porque $n-1$ e $k-1$ são ambos pares, segue pelo segundo ponto da demonstração que

$$\binom{n}{k} \equiv \binom{n-1}{k-1} \equiv \binom{\lfloor n/2 \rfloor}{\lfloor k/2 \rfloor} \pmod{2}.$$

- **n ímpar e k par:** A simetria dos coeficientes binomiais implica que

$$(n-k) \binom{n}{k} = (n-k) \binom{n}{n-k} \quad \text{e} \quad n \binom{n-1}{n-k-1} = n \binom{n-1}{k}.$$

Segue então, por aplicação da propriedade de absorção em $(n-k) \binom{n}{n-k} = n \binom{n-1}{n-k-1}$, que

$$(n-k) \binom{n}{k} = n \binom{n-1}{k}.$$

Dado que $n-k$ e n são ambos ímpares, temos que

$$\binom{n}{k} \equiv \binom{n-1}{k} \pmod{2},$$

e, por aplicação do segundo ponto, que

$$\binom{n}{k} \equiv \binom{n-1}{k} \equiv \binom{\lfloor (n-1)/2 \rfloor}{\lfloor k/2 \rfloor} \pmod{2}.$$

Por último, resta-nos apenas ver que, porque n é ímpar, $\lfloor (n-1)/2 \rfloor = \lfloor n/2 \rfloor$.



Um «procedimento» simples para o cálculo da paridade de um coeficiente binomial é a aplicação sucessiva do Teorema 3.2.36, ou até que o índice superior seja par e o índice

inferior ímpar, ou até que o índice inferior seja 0.

Exemplo 3.2.37. São aqui apresentados os dois tipos possíveis de finalização do «procedimento» acima descrito.

$$\binom{165}{93} \equiv \binom{82}{46} \equiv \binom{41}{23} \equiv \binom{20}{11} \equiv 0 \pmod{2}$$

$$\binom{75}{11} \equiv \binom{37}{5} \equiv \binom{18}{2} \equiv \binom{9}{1} \equiv \binom{4}{0} \equiv 1 \pmod{2}.$$

Para vermos que o número de coeficientes binários ímpares numa linha do triângulo de Pascal é uma potência de base 2, basta observarmos que, em base binária, a operação inteira

$$n \mapsto \lfloor n/2 \rfloor$$

corresponde ao apagar do *bit* mais à direita. Vejamos também que o primeiro ponto do Teorema 3.2.36, (onde n é par e k é ímpar) é discernível por um *bit* 0 na extremidade direita da representação binário de n (e um *bit* 1 na extremidade direita para k). Se o «procedimento» utilizar representações binárias, então o «apagar» de *bits* mais à direita é desnecessário. Nesse caso, será possível alinhar as representações (n e k) à direita e corrê-las (para a esquerda), de maneira a verificar se existe algum *bit* 0 em n imediatamente acima de um *bit* 1 de k .

Vamos tornar as questões mais práticas e considerar os números

$$n = 165_{10} = 10100101_2,$$

$$k = 93_{10} = 01011101_2.$$

Ao percorrer os números da direita para a esquerda, vemos que a primeira ocorrência de um 0 na representação de n acontece no 2^1 -*bit*. Como existe também um *bit* 0 imediatamente abaixo (na representação de k), o «procedimento» continua. O próximo 0 de n situa-se no 2^3 -*bit*, sendo que neste caso, haverá um *bit* 1 abaixo deste (na representação de k). Aqui, o «procedimento» termina e chegamos à conclusão de que $\binom{163}{73} \equiv 0 \pmod{2}$.

Ao analisar ainda os binários alinhados

$$n = 75_{10} = 1001011_2,$$

$$k = 11_{10} = 0001011_2.$$

observamos que apenas existem *bits* 0 (na representação de 11) abaixo de cada *bit* 0 na representação de n . Desta forma, concluímos que $\binom{75}{11} \equiv 1 \pmod{2}$.

Proposição 3.2.38. *O número de coeficientes binários ímpares na n -ésima linha do Triângulo de Pascal é 2^w , onde w é o número de uns que figuram na representação binária de n .*

Demonstração. Para que o coeficiente binomial $\binom{n}{k}$ ser ímpar, sabemos que deverão existir *bits* 0 na representação de n que estão na mesma posição da representação de k . Contudo, se existir um *bit* 1 na representação de n , é indiferente o que poderá aparecer em k . Se existem w *bits* 1 na representação de n , então existirão 2^w valores para que k satisfaça a regra dos *bits* 0. ♦

Corolário 3.2.39. *Se um natural n for da forma $2^k - 1$, então todos os coeficientes binomiais da n -ésima linha do Triângulo de Pascal são ímpares.*

Demonstração. Não existem zeros na representação binária de um natural da forma $2^k - 1$. ♦

3.3 Permutações e Multinómios

Embora tenhamos introduzido anteriormente as permutações e as combinações simples, falta ainda atingir o mesmo conceito tendo agora em conta a (possível) repetição de elementos. Para termos uma noção do que nos espera, pensemos no seguinte problema...

«Quantos números de telefone da rede fixa podem ser atribuídos com dois 2 (incluindo já o 2 inicial), quatro 3, dois 6 e um 9?»

Devemos começar por ver que os números terão a forma 2 — — — — — — — —; ou seja, que teremos 8 lugares para «permutar 2, 3, 6 e 9 com repetição». Para obtermos o número de tais «permutações», aplicamos o seguinte raciocínio:

- entre os 8 lugares, escolhemos o lugar do 2;
- de entre os restantes $8 - 1 = 7$ lugares, escolhemos os 4 lugares onde deve estar o 3;
- de entre os restantes $7 - 4 = 3$ lugares, escolhemos os 2 lugares onde deve estar o 6;
- por último, restam $3 - 2 = 1$ lugares para o 9.

Desta forma, o número total de possibilidades é dado por:

$$\binom{8}{1} \binom{7}{4} \binom{3}{2} \binom{1}{1} = \frac{8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1}{1! \cdot 4! \cdot 2! \cdot 1!} = \frac{8!}{1! \cdot 4! \cdot 2! \cdot 1!} = 840.$$

Definição 3.3.1. Seja $M = (X, \nu)$ um multiconjunto de tamanho n . Uma **permutação de M** (ou **permutação com repetição**) é uma sequência $s = (x_1, \dots, x_n)$ de elementos de X tal que cada $x \in X$ ocorre $\nu(x)$ vezes em s .

Com um argumento semelhante ao argumento do exemplo acima, obtém-se logo:

Teorema 3.3.2. O número de permutações do multiconjunto $\{x_1^{n_1}, \dots, x_k^{n_k}\}$ de tamanho n é

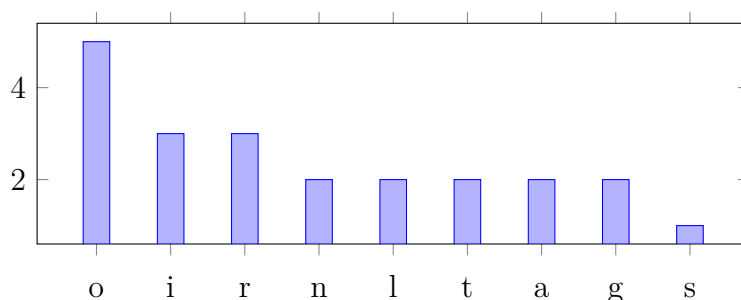
$$\frac{n!}{n_1! \cdot \dots \cdot n_k!}.$$

Exemplo 3.3.3. Pelo nosso exemplo acima, o número de permutações do multiconjunto $\{2, 3, 3, 3, 3, 6, 6, 9\}$ de 8 elementos é

$$\frac{8!}{1! \cdot 4! \cdot 2! \cdot 1!} = 840.$$

Exemplo 3.3.4. Pensemos numa palavra com 22 letras ... «otorrinolaringologista». Ao fazer uma análise da frequência das letras que ocorrem nesta palavra, conseguimos obter o histograma abaixo indicado. Assim, sabemos que existem 5 ocorrências da letra «o», 3 da letra «i», 3 da letra «r», 2 da letra «n», 2 da letra «l», 2 da letra «t», 2 da letra «a», 2 da letra «g», e que a restante letra («s») apenas ocorre uma vez. Desta forma, o número de palavras que podemos formar com as letras de «otorrinolaringologista» (contando o número de repetições) é dado por

$$\binom{22}{5 \ 3 \ 3 \ 2 \ 2 \ 2 \ 2 \ 2 \ 1}.$$



O coeficiente binomial $\binom{n}{k}$ pode-se interpretar como o número de maneiras de dividir o conjunto $\{x_1, \dots, x_n\}$ de n elementos em duas categorias C_1 e C_2 com k elementos na categoria C_1 (e consequentemente $n - k$ elementos na categoria C_2). Generalizamos agora esta ideia para um número arbitrário de categorias.

Definição 3.3.5. Seja X um conjunto de n elementos e sejam n_1, n_2, \dots, n_k números naturais com $n_1 + n_2 + \dots + n_k = n$. O número de sequências (A_1, A_2, \dots, A_k) de k subconjuntos de X dois a dois disjuntos e com $|A_i| = n_i$, $i = 1, \dots, k$, designa-se por **coeficiente multinomial** e denota-se por

$$\binom{n}{n_1 \ n_2 \ \dots \ n_k}.$$

Teorema 3.3.6. *Seja X um conjunto de n elementos e sejam n_1, n_2, \dots, n_k números naturais, com $n_1 + n_2 + \dots + n_k = n$. Então,*

$$\binom{n}{n_1 \ n_2 \ \dots \ n_k} = \frac{n!}{n_1! \cdot \dots \cdot n_k!}.$$

Demonstração. Sem perda de generalidade, comecemos por escolher os n_1 elementos que vão compor A_1 . Neste caso, sabemos que temos $\binom{n}{n_1}$ possibilidades. Seguidamente, fazemos a escolha dos n_2 elementos de A_2 (não esquecendo que esta terá de ser feita dentro dos $n - n_1$ elementos que restam). Desta forma, existirão $\binom{n-n_1}{n_2}$ possibilidades para escolher os elementos de A_2 . Se procedermos do mesmo modo até atingirmos o subconjunto A_k , e através do Princípio da Multiplicação Generalizado, obtemos

$$\begin{aligned} \binom{n}{n_1} \binom{n-n_1}{n_2} \dots \binom{n-n_1-n_2-\dots-n_{k-1}}{n_k} &= \\ \frac{n(n-1) \dots (n-n_1-1) \dots 1}{n_1! \dots n_k!} &= \frac{n!}{n_1! \cdot \dots \cdot n_k!} \end{aligned}$$

◆

Nota 3.3.7. Existem alguns casos particulares dos coeficientes multinomiais que merecem destaque:

- Se $n_1 = \dots = n_k = 1$, então $\binom{n}{n_1 \ n_2 \ \dots \ n_k} = n!$;
- Se $k = 2$, então o coeficiente multinomial $\binom{n}{n_1 \ n - n_1}$ torna-se no coeficiente binomial $\binom{n}{n_1}$.

Teorema 3.3.8. *Consideremos $a_1, \dots, a_k \in \mathbb{R}$ e $n \in \mathbb{N}$. Então,*

$$\begin{aligned} (a_1 + a_2 + \dots + a_k)^n &= \sum_{n_1 + \dots + n_k = n} \binom{n}{n_1 \ \dots \ n_k} a_1^{n_1} a_2^{n_2} \dots a_k^{n_k} \\ &= \sum_{n_1 + \dots + n_k = n} \binom{n}{n_1 \ \dots \ n_k} \prod_{1 \leq i \leq k} a_i^{n_i}. \end{aligned}$$

Demonstração. A ideia por trás desta demonstração passa por desenvolver o produto apresentado, $(a_1 + \dots + a_k)^n$, nos n factores do tipo $(a_1 + \dots + a_k)$. Ao proceder de tal forma, obteremos termos da forma $a_1^{n_1} \dots a_k^{n_k}$, com $n_1 + \dots + n_k = n$, que correspondem à escolha de a_1 em n_1 dos factores, de a_2 em n_2 factores, e assim por diante. Nestas condições, e por definição de coeficiente multinomial, conseguimos concluir que existirão $\binom{n}{n_1 \ \dots \ n_k}$ termos da forma $a_1^{n_1} \dots a_k^{n_k}$. ◆

Exemplo 3.3.9.

$$\begin{aligned}(a+b+c)^3 &= \binom{3}{3\ 0\ 0}a^3 + \binom{3}{0\ 3\ 0}b^3 + \binom{3}{0\ 0\ 3}c^3 \\ &+ \binom{3}{2\ 1\ 0}a^2b + \binom{3}{2\ 0\ 1}a^2c + \binom{3}{1\ 2\ 0}ab^2 + \binom{3}{0\ 2\ 1}b^2c + \binom{3}{1\ 0\ 2}ac^2 + \binom{3}{0\ 1\ 2}bc^2 \\ &+ \binom{3}{1\ 1\ 1}abc\end{aligned}$$

Exemplo 3.3.10. A generalização da Regra de Leibniz vista no Exemplo 3.2.19 pode ser ainda estendida ao produto de m funções. De facto, para funções n -diferenciáveis f_1, \dots, f_m , temos que

$$(f_1 f_2 \dots f_m)^{(n)} = \sum_{n_1 + \dots + n_m = n} \binom{n}{n_1 \dots n_m} \prod_{1 \leq i \leq m} f_i^{(k_i)}.$$

Exemplo 3.3.11. Vamos determinar o coeficiente de $a^2 b^4 d$ na expansão de $(3a + 5b - 2c + d)^7$.

Comecemos por ver que um termo geral da expansão de $(3a + 5b - 2c + d)^7$ será da forma

$$\binom{7}{n_1 \ n_2 \ n_3 \ n_4} (3a)^{n_1} (5b)^{n_2} (-2c)^{n_3} d^{n_4},$$

com $n_1 + n_2 + n_3 + n_4 = 7$. Para atingirmos o termo $a^2 b^4 d$, deveremos então ter $n_1 = 2$, $n_2 = 4$, $n_3 = 0$ e $n_4 = 1$, o que nos leva até

$$\begin{aligned}\binom{7}{2\ 4\ 0\ 1} (3a)^2 (5b)^4 (-2c)^0 d^1 &= \frac{7!}{2!4!0!1!} (9a^2) (625b^4) d \\ &= 105(5625)a^2 b^4 d \\ &= 590625a^2 b^4 d.\end{aligned}$$

Desta forma, concluímos que o coeficiente pedido é 590625.

Exemplo 3.3.12. Vamos determinar o coeficiente de x^{23} na expansão de $(1 - 2x + 3x^2 - x^4 - x^5)^5$.

Como explorado anteriormente, o termo geral da expansão de $(1 - 2x + 3x^2 - x^4 - x^5)^5$ será

$$\binom{5}{n_1 \ n_2 \ n_3 \ n_4 \ n_5} (1)^{n_1} (-2x)^{n_2} (3x^2)^{n_3} (-x^4)^{n_4} (-x^5)^{n_5}$$

com $n_1 + n_2 + n_3 + n_4 + n_5 = 5$. Para o cálculo do coeficiente de x^{23} , teremos de tomar $n_2 + 2n_3 + 4n_4 + 5n_5 = 23$.

Não será muito difícil verificar que a única solução não negativa para as equações acima é dada pelo tuplo $(n_1, n_2, n_3, n_4, n_5) = (0, 0, 0, 2, 3)$. Desta forma,

$$\binom{5}{0 \ 0 \ 0 \ 2 \ 3} (1)^0 (-2x)^0 (3x^2)^0 (-x^4)^2 (-x^5)^3 = -\binom{5}{2 \ 3} = -10.$$

Exemplo 3.3.13. Vamos tentar determinar o coeficiente de t^{20} na expansão de $(t^3 - 3t^2 + 7t + 1)^{11}$.

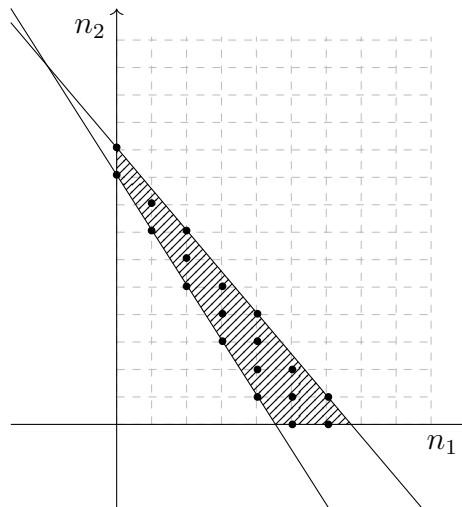
Começamos por ver que um termo geral da expansão de $(t^3 + 3t^2 + 7t + 1)^{11}$ será da forma

$$\binom{11}{n_1 \ n_2 \ n_3 \ n_4} (t^3)^{n_1} (-3t^2)^{n_2} (7t)^{n_3} (1)^{n_4},$$

com $n_1 + n_2 + n_3 + n_4 = 11$. Para o coeficiente de t^{20} , teremos de tomar $3n_1 + 2n_2 + n_3 = 20$. Vejamos que podemos então escrever $n_3 = 20 - 2n_2 - 3n_1$ e $n_4 = 11 - n_1 - n_2 - n_3 = 2n_1 + n_2 - 9$. Desta forma, o coeficiente será dado pela soma

$$\sum_{n_1, n_2 \geq 0} \binom{11}{n_1, n_2, 20 - 2n_2 - 3n_1, 2n_1 + n_2 - 9} (-3)^{n_2} 7^{20 - 2n_2 - 3n_1}$$

de tal forma que $2n_2 + 3n_1 \leq 20$ e $2n_1 + n_2 \geq 9$.



É possível verificar que existirão exactamente 19 possibilidades para formar pares (n_1, n_2) nas condições acima indicadas. As tabelas 3.1 abaixo resumem a informação necessária acerca desses tuplos. Ao efectuar a soma dos produtos entre os elementos das duas últimas colunas, atingimos o resultado pretendido, i.e., que o coeficiente do termo t^{20} nesta expansão é -7643472342 .

Tabela 3.1:

n_1	n_2	$20 - 2n_2 - 3n_1$	$\binom{11}{n_1, n_2, 20-2n_2-3n_1, 2n_1+n_2-9}$	$(-3)^{n_2} 7^{20-2n_2-3n_1}$
0	10	0	11	59049
0	9	2	55	-964467
1	8	1	990	45927
1	7	3	1320	-750141
2	7	0	1980	-2187
2	6	2	13860	35721
2	5	4	6930	-583443
3	5	1	27720	-1701
3	4	3	46200	27783
3	3	5	9240	-453789
4	4	0	11550	81
4	3	2	69300	-1323
4	2	4	34650	21609
4	1	6	2310	-352947
5	2	1	27720	63
5	1	3	27720	-1029
5	0	5	2772	16807
6	1	0	2310	-3
6	0	2	4620	49

3.4 Identidades Combinatórias

Nesta próxima secção vamos explorar, como o próprio nome indica, algumas identidades combinatórias que podem ser obtidas pelos coeficientes binomiais (e até multinomiais). Ao invés de as formularmos como teoremas, vamos apresentá-las (de forma mais simples) como exemplos.

Exemplo 3.4.1. Para todos os $n, m \in \mathbb{N}$, temos que

$$\sum_{k=0}^m \binom{k}{n} = \binom{m+1}{n+1}.$$

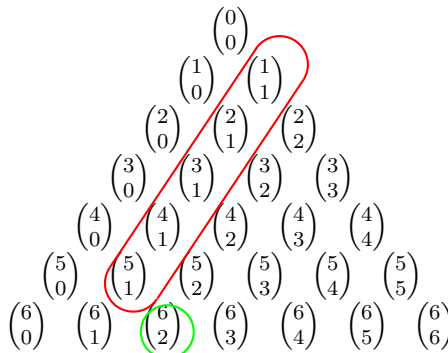
Prova Algébrica: Vamos proceder por indução sobre m . Como base da indução teremos o caso $n = 0$: $\sum_{k=0}^0 \binom{0}{k} = \binom{0}{0} = 1 = \binom{1}{1}$. Como hipótese de indução, vamos admitir que a

igualdade é válida para qualquer natural até $m - 1$ (inclusive). Então,

$$\begin{aligned}\sum_{k=0}^m \binom{k}{n} &= \sum_{k=0}^{m-1} \binom{k}{n} + \binom{m}{n} \\ &= \binom{m}{n+1} + \binom{m}{n} \\ &= \binom{m+1}{n+1}.\end{aligned}$$

Prova Combinatória: Começemos por ver que o coeficiente binomial $\binom{m+1}{n+1}$ é igual ao tamanho do conjunto $Y = \{A \subseteq \{1, \dots, m+1\} \mid |A| = n+1\}$, i.e., que o membro direito da igualdade corresponde à cardinalidade de Y . Agora, e para cada $k \in \{n, \dots, m\}$, vamos considerar os subconjuntos de Y da forma $Y_k = \{A \subseteq Y \mid \max(A) = k+1\}$. É relativamente fácil ver que $Y = \bigcup_{i=n}^m Y_i$ e que $|Y_k| = \binom{k}{n}$, uma vez que para obtermos os subconjuntos de Y_k , basta fixarmos $k+1$ e determinar todas as combinações de n elementos de $\{1, \dots, k\}$. Tendo ainda em conta que $k < n$ implica $\binom{k}{n} = 0$, concluímos o pretendido.

Como exemplo, temos abaixo representado o caso para $m = 5$ e $n = 1$:



$$\sum_{k=0}^5 \binom{k}{1} = \underbrace{\binom{0}{1}}_{=0} + \binom{1}{1} + \binom{2}{1} + \binom{3}{1} + \binom{4}{1} + \binom{5}{1} = \binom{6}{2}$$

Exemplo 3.4.2. Consideremos $n, m, \ell \in \mathbb{N}$. Vamos demonstrar a **identidade (convolução) de Vandermonde**:

$$\sum_{k=0}^{\ell} \binom{n}{k} \binom{m}{\ell-k} = \binom{n+m}{\ell}.$$

Prova Algébrica: Se tivermos alguma atenção, a soma presente no membro esquerdo na identidade é igual ao coeficiente de x^{ℓ} no membro esquerdo da equação $(1+x)^n(1+x)^m = (1+x)^{m+n}$. De forma semelhante, o coeficiente presente no membro direito da identidade é igual ao coeficiente de x^{ℓ} no membro direito da equação $(1+x)^n(1+x)^m = (1+x)^{m+n}$.

Prova Combinatória: Suponhamos que existem $n + m$ objectos num conjunto, n deles azuis e m deles vermelhos, e que vamos escolher ℓ objectos. Este número de escolhas é representado no membro direito da igualdade.

O número de maneiras de seleccionar k objectos azuis e $\ell - k$ objectos vermelhos é dado pelo produto $\binom{n}{k} \binom{m}{\ell-k}$; desta forma, a soma de todos estes produtos, que figura no membro esquerdo da identidade, deverá ser igual à expressão do membro direito.

Nota 3.4.3. Se atentarmos na identidade (convolução) de Vandermonde e particularizarmos $n = m = k$, conseguimos obter outra identidade binomial conhecida:

$$\binom{2n}{n} = \sum_{k=0}^n \binom{n}{k} \binom{n}{n-k} = \sum_{k=0}^n \binom{n}{k} \binom{n}{k} = \sum_{k=0}^n \binom{n}{k}^2.$$

Exemplo 3.4.4. Vamos verificar mais uma propriedade das somas diagonais do triângulo de Pascal:

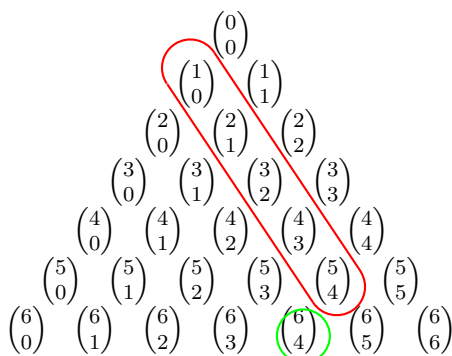
$$\sum_{k=0}^r \binom{n+k}{k} = \binom{n+r+1}{r}.$$

Prova Algébrica:

$$\sum_{k=0}^r \binom{n+k}{k} = \sum_{k=0}^r \binom{n+k}{n} = \binom{n+r+1}{n+1} = \binom{n+r+1}{r}$$

Prova Combinatória:

Como exemplo, temos abaixo representado o caso para $r = 4$ e $n = 1$:



Exemplo 3.4.5. Vamos demonstrar a propriedade de **absorção** ligada aos coeficientes binomiais, i.e., que para $0 \leq k \leq n$ se tem

$$k \binom{n}{k} = n \binom{n-1}{k-1}.$$

Prova Algébrica: Basta seguirmos por definição dos coeficientes binomiais,

$$\begin{aligned}
 k \binom{n}{k} &= k \frac{n!}{(n-k)!k!} \\
 &= \frac{n \cdot (n-1) \cdots (n-k+1)}{(k-1)!} \\
 &= n \frac{(n-1) \cdots (n-k+1)}{(k-1)!} \\
 &= n \frac{(n-1)!}{(n-1-(k-1))!(k-1)!} \\
 &= n \binom{n-1}{k-1}.
 \end{aligned}$$

Prova Combinatória: É apenas necessário observar que $k \binom{n}{k}$ pode ser dado como o número de maneiras de escolher k pessoas entre n e, posteriormente, dessas k , escolher 1. Claramente, tal processo é equivalente a escolher primeiro 1 pessoa entre as n e, unicamente após, escolher $k-1$ pessoas de entre as $n-1$ que restam, i.e., $n \binom{n-1}{k-1}$.

Nota 3.4.6. A partir da propriedade de absorção, conseguirmos provar uma outra relação entre os coeficientes binomiais. De facto, $\sum_{k=0}^n k \binom{n}{k} = n2^{n-1}$, uma vez que

$$\sum_{k=0}^n k \binom{n}{k} = \sum_{k=1}^n k \binom{n}{k} = \sum_{k=1}^n n \binom{n-1}{k-1} = n \sum_{k=1}^n \binom{n-1}{k-1} = n \sum_{j=0}^{n-1} \binom{n-1}{j} = n2^{n-1}.$$

Exemplo 3.4.7. Vamos demonstrar a **identidade dos subconjuntos** para os coeficientes binomiais, ou seja, que para quaisquer $0 \leq k \leq m \leq n$ se tem

$$\binom{n}{m} \binom{m}{k} = \binom{n}{k} \binom{n-k}{m-k}.$$

Prova Algébrica: Basta seguirmos por definição dos coeficientes binomiais,

$$\begin{aligned}
 \binom{n}{m} \binom{m}{k} &= \frac{n!}{(n-m)!m!} \cdot \frac{m!}{(m-k)!k!} \\
 &= \frac{n!}{(n-m)!(m-k)!k!} \\
 &= \frac{n!}{(n-k)!k!} \cdot \frac{(n-k)!}{(n-m)!(m-k)!} \\
 &= \binom{n}{k} \binom{n-k}{m-k}.
 \end{aligned}$$

Prova Combinatória: É apenas necessário observar que $\binom{n}{m} \binom{m}{k}$ pode ser dado como o número de maneiras de escolher m pessoas entre n , e posteriormente k dentro das m

previamente escolhidas. Claramente, tal processo é equivalente a escolher primeiro as k tais pessoas e, só depois de tal ser feito, escolher as restantes $m - k$ pessoas entre as $n - k$ que restam, ou seja, $\binom{n}{k} \binom{n-k}{m-k}$.

Exemplo 3.4.8. Para cada $n, n_1, \dots, n_k \in \mathbb{N}$ de tal forma que $n_1 + \dots + n_k = n$, é válida a seguinte igualdade:

$$\binom{n}{n_1 \dots n_k} = \sum_{i=1}^k \binom{n-1}{n_1 \dots (n_i-1) \dots n_k}.$$

Prova Algébrica:

$$\begin{aligned} & \binom{n-1}{(n_1-1) n_2 \dots n_k} + \binom{n-1}{n_1 (n_2-1) \dots n_k} + \dots + \binom{n-1}{n_1 n_2 \dots (n_k-1)} \\ &= \\ & \frac{(n-1)!}{(n_1-1)! n_2! \dots n_k!} + \frac{(n-1)!}{n_1! (n_2-1)! \dots n_k!} + \dots + \frac{(n-1)!}{n_1! n_2! \dots (n_k-1)!} \\ &= \\ & \frac{(n-1)! n_1}{n_1! n_2! \dots n_k!} + \frac{(n-1)! n_2}{n_1! n_2! \dots n_k!} + \dots + \frac{(n-1)! n_k}{n_1! n_2! \dots n_k!} \\ &= \\ & \frac{(n-1)! (n_1 + n_2 + \dots + n_k)}{n_1! n_2! \dots n_k!} = \frac{n!}{n_1! n_2! \dots n_k!} = \binom{n}{n_1 \dots n_k}. \end{aligned}$$

Prova Combinatória: No que se segue, chamamos uma sequência (A_1, \dots, A_k) de subconjuntos de um conjunto finito $X = \{1, 2, \dots, n\}$ dois a dois disjuntos e com $|A_i| = n_i$ ($i \in \{1, \dots, k\}$) partição de X do tipo (n_1, \dots, n_k) .

Por definição, $\binom{n}{n_1 \dots n_k}$ é o número de elementos do conjunto

$$\{\text{partições } (A_1, \dots, A_k) \text{ de } X \text{ do tipo } (n_1, \dots, n_k)\}.$$

Podemos representar este conjunto como a união (dois a dois disjunta) dos seguintes conjuntos:

- O conjunto das sequências $(B_1 \cup \{n\}, B_2, \dots, B_k)$ onde (B_1, B_2, \dots, B_k) é uma partição de $\{1, \dots, n-1\}$ do tipo (n_1-1, n_2, \dots, n_k) ;
- O conjunto das sequências $(B_1, B_2 \cup \{n\}, \dots, B_k)$ onde (B_1, B_2, \dots, B_k) é uma partição de $\{1, \dots, n-1\}$ do tipo (n_1, n_2-1, \dots, n_k) ;
- \vdots
- O conjunto das sequências $(B_1, B_2, \dots, B_k \cup \{n\})$ onde (B_1, B_2, \dots, B_k) é uma partição de $\{1, \dots, n-1\}$ do tipo (n_1, n_2, \dots, n_k-1) .

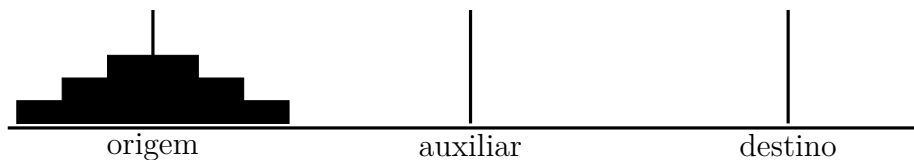
Logo,

$$\binom{n-1}{n_1-1 \ n_2 \ \dots \ n_k} + \binom{n-1}{n_1 \ n_2-1 \ \dots \ n_k} + \dots + \binom{n-1}{n_1 \ n_2 \ \dots \ n_k-1} = \binom{n}{n_1 \ \dots \ n_k}.$$

Recorrência e Funções Geradoras

São muitos os exemplos de recorrência nas definições de funções e expressões combinatórias. É caso para dizer que o desenvolvimento dos próprios sistemas numéricos estabelece as bases para o surgimento das recorrências na Matemática. Neste capítulo, vamos apresentar um tratamento mais sistemático destas questões, onde o objectivo final será o de encontrar expressões fechadas para funções definidas recursivamente - sempre que possível. Vamos começar por nos concentrar nas equações de recorrência lineares, passando depois ao caso não linear. Numa última secção, vamos abordar as funções (e séries) geradoras e as formas como estas podem ser utilizadas para resolver recorrências.

Torres de Hanoi



O problema em mãos prende-se com o mover n discos de um pino «origem» para um pino «destino», com a ajuda de um pino «auxiliar», de modo a que:

- apenas um disco possa ser movido a cada passo (iteração)
- um disco maior nunca possa ficar sobre um disco menor.

Reza a lenda que, no templo hindu de Kashi Vishwanath, havia uma sala com uma torre de 64 discos de ouro (assentes sobre um pino «origem») e mais duas estacas (pinos «auxiliar» e «destino») equilibradas sobre uma plataforma. Os monges desse templo haviam sido ordenados, pelo deus Brama, a mover todos os discos até à última estaca. Segundo a lenda, quando todos os discos fossem transferidos, o mundo desapareceria. Temos de nos preocupar com tal situação?

Se, para n discos (digamos, com $n \in \mathbb{N}$), denotamos por a_n o menor número de passos necessários para mover esses n discos até ao pino «destino», qual será o valor de a_{64} ?

Neste caso, é mais fácil pensar de forma recursiva:

- se $n = 1$, basta mover o disco directamente do pino «origem» para o pino «destino».
- se $n > 1$, então:
 - movemos os $n - 1$ primeiros discos para o pino «auxiliar» (utilizando o pino «destino»)
 - movemos o último disco para o pino «destino»
 - movemos os $n - 1$ discos do pino «auxiliar» para o pino «destino» (utilizando o pino «origem»).

Logo, podemos concluir que $a_n = a_{n-1} + 1 + a_{n-1} = 2a_{n-1} + 1$.

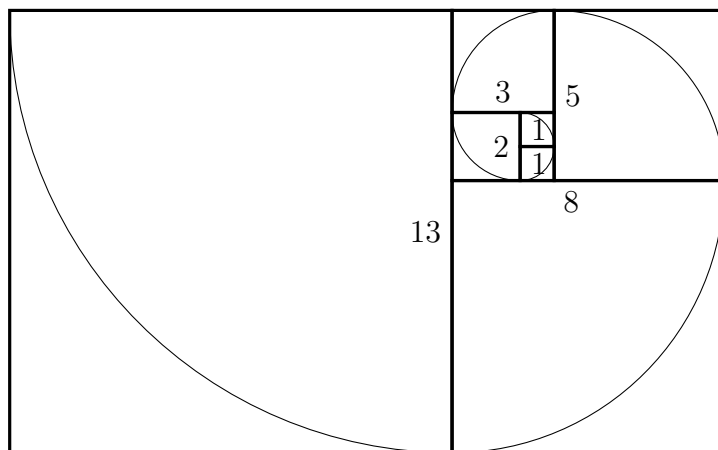
Como veremos mais à frente, caso a lenda fosse verdadeira e os monges fossem capazes de mover um disco por segundo, usando o menor número de movimentos, seriam precisos $2^{64} - 1$ segundos (aproximadamente 585 biliões de anos) para o mundo desaparecer (cerca de 42 vezes mais comparativamente à idade estimada actual).

Números de Fibonacci

Os famosos números de Fibonacci

$$1, 1, 2, 3, 5, 8, 13, 21, \dots$$

são os termos da sucessão $(F_n)_{n \in \mathbb{N}}$ que tem condições iniciais $F_0 = 0$ e $F_1 = 1$ e satisfaz a regra $F_{n+2} = F_{n+1} + F_n$, para todo o $n \in \mathbb{N}$.



Embora os números de Fibonacci sejam completamente determinados pelos primeiros dois termos (F_0 e F_1), não será de fácil cálculo, por exemplo, $F_{312493741}$, dado que, por definição, é necessário calcular primeiro $F_{312493740}$ e $F_{312493739}$, e para isso precisamos de $F_{312493738}$ e $F_{312493737}$, ... e assim sucessivamente até $F_2 = F_1 + F_0$.

Estes números aparecem nos mais variados contextos, mas uma das primeiras aparições, presente no «*Liber Abaci*» de Fibonacci (publicado em 1202), prende-se, de forma muito interessante, com o estudo do crescimento de populações de coelhos:

Exemplo 4.0.1. Numa população coelhos existem animais adultos (que podem ter descendentes) e animais jovens (que ainda não podem ter descendentes). Suponhamos que

- cada par de coelhos adultos tem um par de descendentes (necessariamente jovem) no final do mês,
- depois de um mês, um coelho jovem passa a ser um coelho adulto,
- sendo vegetarianos, os coelhos vivem «eternamente».

No que se segue, a_n denota o número de pares de coelhos adultos e b_n o número de pares de coelhos jovens no final do mês n . Começando com um par de coelhos jovens, qual é o número $c_n = a_n + b_n$ de pares de coelhos? Por hipótese, $a_0 = 0$, $b_0 = 1$, $a_1 = 1$, $b_1 = 0$ e, para $n \geq 1$,

$$a_n = a_{n-1} + b_{n-1} \quad \text{e} \quad b_n = a_{n-1}.$$

Portanto, para $n \geq 2$, $a_n = a_{n-1} + a_{n-2}$; e $c_n = a_n + b_n$ satisfaz

$$c_0 = 1, \quad c_1 = 1, \quad c_n = c_{n-1} + c_{n-2} \quad (n \geq 2).$$

A título de exemplo, vamos determinar a soma dos n primeiros números de Fibonacci. Utilizando o facto de $F_n = F_{n+1} - F_{n-1}$ (para $n \geq 1$), podemos calcular

$$\sum_{k=0}^{n-1} F_k = F_0 + (F_2 - F_0) + (F_3 - F_1) + \cdots = F_0 + \sum_{k=2}^n F_k - \sum_{k=0}^{n-2} F_k = F_n + F_{n-1} - 1 = F_{n+1} - 1.$$

4.1 Equações de Recorrência

Definição 4.1.1. • Uma **equação de recorrência** (ou **relação de recorrência**) é uma equação da forma

$$x_n = f(n, x_{n-1}, x_{n-2}, \dots, x_{n-k}), \quad (4.1.i)$$

com $n \in \mathbb{N}$, para $n \geq k$.

- A equação de recorrência anterior diz-se de **ordem** k ou que tem **profundidade** k (supondo que f depende da última variável).
- Uma sucessão $(a_n)_{n \in \mathbb{N}}$ diz-se **solução** de (4.1.i) quando os seus termos satisfazem a equação (4.1.i), para todo o $n \geq k$.

Nota 4.1.2. Resolver uma relação de recorrência é o mesmo que determinar todas as suas soluções. Em particular, estaremos interessados em descrever as soluções com fórmulas

fechadas; i.e., numa forma

$$a_n = \text{«uma expressão que apenas envolve a variável } n\text{»}.$$

No que se segue consideremos em particular as *equações de recorrência lineares*.

Definição 4.1.3. Uma **equação de recorrência linear** (de coeficientes constantes e) **de ordem** k é uma equação da forma

$$x_n = c_1x_{n-1} + c_2x_{n-2} + \cdots + c_kx_{n-k} + d_n, \quad (4.1.ii)$$

(para $n \geq k$), onde c_1, c_2, \dots, c_k (com $c_k \neq 0$) são constantes e $(d_n)_{n \in \mathbb{N}}$ é uma sucessão. A equação (4.1.ii) diz-se **homogénea** quando $(d_n)_{n \in \mathbb{N}}$ é a sucessão nula.

A equação homogénea **associada** a (4.1.ii) é a equação

$$x_n = c_1x_{n-1} + c_2x_{n-2} + \cdots + c_kx_{n-k}.$$

Exemplo 4.1.4. • $x_n = 3x_{n-1} + 2x_{n-2} + 3n$ é uma equação de recorrência linear (não homogénea) da ordem 2.

- $x_n = 3x_{n-1} + 2x_{n-2}$ é a equação homogénea associada.

Exemplo 4.1.5. • A equação da recorrência $x_{n+1} = (n+1)x_n$ é linear e homogénea, mas **não tem coeficientes constantes**.

- A equação $x_n = 2x_{n-1} - x_{n-2}$ ($n \geq 2$) é uma equação de recorrência linear homogénea (de coeficientes constantes).

Verificamos que a sucessão $(a_n)_{n \in \mathbb{N}}$ definida por

$$a_n = 3n \quad (n \in \mathbb{N})$$

é solução desta equação. De facto, para cada $n \geq 2$,

$$2a_{n-1} - a_{n-2} = 2(3(n-1)) - 3(n-2) = 3(2(n-1) - (n-2)) = 3n = a_n.$$

Um cálculo semelhante revela que as sucessões

$$(0)_{n \in \mathbb{N}}, \quad (n)_{n \in \mathbb{N}}, \quad (1)_{n \in \mathbb{N}}, \quad (5n+2)_{n \in \mathbb{N}}$$

são soluções da equação acima.

Explicaremos mais adiante que uma equação de recorrência linear pode-se descrever utilizando uma função linear; nesta perspetiva, o seguinte resultado já é conhecida da Álgebra Linear.

Teorema 4.1.6. *O conjunto de todas as soluções da equação de recorrência linear*

$$x_n = c_1x_{n-1} + c_2x_{n-2} + \cdots + c_kx_{n-k} + d_n \quad (4.1.iii)$$

obtem-se como

uma solução particular
de (4.1.iii)

+

todas as soluções da equação homogé-
nea associada à equação (4.1.iii)

Demonstração. Consideremos $(a_n^{(h)})_{n \in \mathbb{N}}$ como uma solução geral da equação homogénea associada a (4.1.iii) e $(a_n^{(p)})_{n \in \mathbb{N}}$ como solução particular de (4.1.iii). Ora, tomando $(a_n)_{n \in \mathbb{N}} = (a_n^{(h)} + a_n^{(p)})_{n \in \mathbb{N}}$, podemos ver que

$$\begin{aligned} a_n - c_1a_{n-1} - c_2a_{n-2} - \cdots - c_ka_{n-k} &= a_n - \sum_{i=1}^k c_i a_{n-i} \\ &= (a_n^{(h)} + a_n^{(p)}) - \sum_{i=1}^k c_i (a_{n-i}^{(h)} + a_{n-i}^{(p)}) \\ &= a_n^{(h)} + a_n^{(p)} - \sum_{i=1}^k c_i a_{n-i}^{(h)} - \sum_{i=1}^k c_i a_{n-i}^{(p)} \\ &= \left(a_n^{(h)} - \sum_{i=1}^k c_i a_{n-i}^{(h)} \right) + \left(a_n^{(p)} - \sum_{i=1}^k c_i a_{n-i}^{(p)} \right) \\ &= 0 + d_n = d_n \end{aligned}$$

De semelhante forma é ainda possível ver que, dadas duas soluções particulares $(a_n^{(p1)})_{n \in \mathbb{N}}$ e $(a_n^{(p2)})_{n \in \mathbb{N}}$ de (4.1.iii), então $(a_n)_{n \in \mathbb{N}} = (a_n^{(p1)} - a_n^{(p2)})_{n \in \mathbb{N}}$ será uma solução da equação homogénea associada a (4.1.iii). De facto,

$$\begin{aligned} a_n - c_1a_{n-1} - c_2a_{n-2} - \cdots - c_ka_{n-k} &= a_n - \sum_{i=1}^k c_i a_{n-i} \\ &= (a_n^{(p1)} - a_n^{(p2)}) - \sum_{i=1}^k c_i (a_{n-i}^{(p1)} - a_{n-i}^{(p2)}) \\ &= a_n^{(p1)} - a_n^{(p2)} - \sum_{i=1}^k c_i a_{n-i}^{(p1)} + \sum_{i=1}^k c_i a_{n-i}^{(p2)} \\ &= \left(a_n^{(p1)} - \sum_{i=1}^k c_i a_{n-i}^{(p1)} \right) - \left(a_n^{(p2)} - \sum_{i=1}^k c_i a_{n-i}^{(p2)} \right) \\ &= d_n - d_n = 0 \end{aligned}$$

◆

Resta-nos então saber como atingir as soluções particulares e a solução geral das equações homogéneas associadas.

4.2 Equações de Recorrência Lineares Homogêneas

Vamos começar por fazer algumas considerações iniciais relativamente a este sub-tópico. Consideremos

$$x_n = c_1 x_{n-1} + c_2 x_{n-2} + \cdots + c_k x_{n-k} \quad (4.2.i)$$

($c_k \neq 0$) uma equação de recorrência linear homogênea de ordem k .

- O conjunto das soluções de (4.2.i) é um sub-espço do espaço vectorial de todas as sucessões (reais ou complexos).
- Cada solução $(a_n)_{n \in \mathbb{N}}$ de (4.2.i) é completamente determinada pelos seus primeiros k termos. De facto,

$$\begin{aligned} \mathbb{C}^k \text{ ou } \mathbb{R}^k &\longrightarrow \{\text{as soluções de (4.2.i)}\} \\ (a_0, \dots, a_{k-1}) &\longmapsto (a_0, \dots, a_{k-1}, c_1 a_{k-1} + \cdots + c_k a_0, \dots) \end{aligned}$$

é um isomorfismo; logo: $\dim\{\text{as soluções de (4.2.i)}\} = k$.

Concluindo ... para descrever todas as soluções de (4.2.i), é apenas necessário encontrar k soluções de (4.2.i) linearmente independentes. Uma forma (mais ou menos) «inteligente» de o fazer é proceder da seguinte maneira: consideremos a equação de recorrência linear homogênea

$$0 = x_n - c_1 x_{n-1} - c_2 x_{n-2} - \cdots - c_k x_{n-k} \quad (k \geq 1, c_k \neq 0). \quad (4.2.i)$$

Para uma sucessão da forma $(q^n)_{n \in \mathbb{N}}$, para quais valores de q obtemos uma solução? Seguramente não para $q = 0$, e para $q \neq 0$ temos

$$\begin{aligned} 0 &= q^n - c_1 q^{n-1} - c_2 q^{n-2} - \cdots - c_k q^{n-k} \\ &= q^{n-k} (q^k - c_1 q^{k-1} - c_2 q^{k-2} - \cdots - c_k), \end{aligned}$$

portanto, $(q^n)_{n \in \mathbb{N}}$ é solução de (4.2.i) se e somente se

$$0 = \underbrace{q^k - c_1 q^{k-1} - c_2 q^{k-2} - \cdots - c_k}_{\text{polinómio em } q \text{ de grau } k}.$$

A equação acima diz-se **equação caraterística** de (4.2.i). e o polinómio $q^k - c_1 q^{k-1} - c_2 q^{k-2} - \cdots - c_k$ **polinómio caraterístico** de (4.2.i).

Teorema 4.2.1. *Consideremos a equação de recorrência linear homogênea*

$$x_n = c_1 x_{n-1} + c_2 x_{n-2} + \cdots + c_k x_{n-k} \quad (k \geq 1, c_k \neq 0). \quad (4.2.ii)$$

Se a equação caraterística

$$0 = q^k - c_1 q^{k-1} - c_2 q^{k-2} - \cdots - c_k$$

de (4.2.ii) têm as k soluções (diferentes) q_1, q_2, \dots, q_k , então as soluções de (4.2.ii) são precisamente as combinações lineares das sucessões (linearmente independentes) $(q_i^n)_{n \in \mathbb{N}}$,

$\dots, (q_k^n)_{n \in \mathbb{N}}$; ou seja, as sucessões da forma

$$(C_1 q_1^n + C_2 q_2^n + \dots + C_k q_k^n)_{n \in \mathbb{N}},$$

com constantes C_1, C_2, \dots, C_k .

Demonstração. Mais tarde veremos que as sucessões $(q_1^n)_{n \in \mathbb{N}}, \dots, (q_k^n)_{n \in \mathbb{N}}$ serão vetores próprios associados a valores próprios distintos, portanto, são linearmente independentes. Como o espaço das soluções de (4.2.ii) tem a dimensão k , cada solução de (4.2.ii) é uma combinação linear destas sucessões. \blacklozenge

Exemplo 4.2.2. Vamos tentar encontrar a solução da equação de recorrência linear homogênea

$$0 = x_n - x_{n-1} - 2x_{n-2} \quad (n \geq 2).$$

que satisfaz as condições iniciais $x_0 = 5$ e $x_1 = 4$.

O primeiro passo será descobrir a forma da solução geral da equação dada. Pelo que vimos no procedimento anterior, será (mais ou menos) claro obter $0 = q^2 - q - 2 = (q - 2)(q + 1)$, polinómio este que tem soluções $q_0 = 2$ e $q_1 = -1$. Verifica-se então que as sucessões $(2^n)_{n \in \mathbb{N}}$ e $((-1)^n)_{n \in \mathbb{N}}$ são linearmente independentes; portanto, todas as soluções (reais) da equação dada serão da forma

$$(\alpha 2^n + \beta (-1)^n)_{n \in \mathbb{N}} \quad \alpha, \beta \in \mathbb{R}.$$

No entanto, a resolução não fica por aqui. Tendo em conta as condições iniciais ($x_0 = 5$ e $x_1 = 4$), é possível atingirmos

$$\alpha + \beta = 5 \quad (\text{para o caso } n = 0) \quad \text{e} \quad 2\alpha - \beta = 4 \quad (\text{para o caso } n = 1).$$

Resolvendo o sistema de equações lineares, obtemos $\alpha = 3$ e $\beta = 2$, o que nos leva a concluir que a solução para o problema em mãos é a sucessão $(a_n)_{n \in \mathbb{N}}$, onde $a_n = 3 \cdot 2^n + 2 \cdot (-1)^n$.

Exemplo 4.2.3. Vamos agora tentar encontrar aproximações racionais para $\sqrt{5}$ a partir de recorrências. Para tal, o primeiro passo será encontrar uma relação de recorrência com forma fechada

$$a_n = (2 + \sqrt{5})^n + (2 - \sqrt{5})^n.$$

Claramente, e invertendo o processo até agora explorado, é possível ver que o polinómio característico ligado à recorrência em causa é $(x - (2 + \sqrt{5}))(x - (2 - \sqrt{5})) = x^2 - 4x - 1$, o que nos leva a $a_n = 4a_{n-1} + a_{n-2}$, com $a_0 = 2$ e $a_1 = 4$.

Seguidamente, devemos perceber o que acontece ao termo $(2 - \sqrt{5})^n$ quando $n \rightarrow \infty$. De facto, porque $\sqrt{5} \approx 2,23606$, temos $|2 - \sqrt{5}| < 1$, o que implica que $(2 - \sqrt{5})^n \xrightarrow{n \rightarrow \infty} 0$. Tal permite-nos concluir que $\frac{a_n}{a_{n-1}} \xrightarrow{n \rightarrow \infty} 2 + \sqrt{5}$, ou seja, que $\frac{a_n}{a_{n-1}} - 2$ nos dá uma boa aproximação racional de $\sqrt{5}$.

n	0	1	2	3	4	5	6	7
a_n	2	4	18	76	322	1364	5778	24476
$\frac{a_n}{a_{n-1}} - 2$	—	0	2,5	2,22222...	2,23684...	2,23602...	2,23607...	2,23606...

Exemplo 4.2.4. Seja p_n o número de formas distintas de construir um tubo de comprimento n , utilizando segmentos de plástico ou metal de comprimentos 1 ou 2.

Podemos ver que $p_1 = 2$, dado que podemos usar um segmento de comprimento 1 de plástico ou metal; e $p_2 = 6$, pois podemos usar qualquer segmento de comprimento 2 (de plástico ou metal) ou qualquer um das 2^2 possibilidades (escolhas de comprimento 1).

Tomando $p_0 = 1$, não será muito difícil verificar que a relação de recorrência para p_n é dada por $2p_{n-1} + 2p_{n-2}$. De facto, para um tubo de comprimento n , podemos considerar um tubo de comprimento $n - 1$ (p_{n-1}) e acrescentar-lhe um tubo de comprimento 1 (de plástico ou metal); ou ter um tubo de comprimento $n - 2$ (p_{n-2}) e acrescentar-lhe um tubo de comprimento 2 (de plástico ou metal). Assim,

$$\begin{array}{c}
 \text{Diagram of a tube of length } p_n \\
 \hline
 = \\
 \text{Diagram of a tube of length } p_{n-1} \text{ followed by a segment of length 1 (metal or plastic)} \\
 + \\
 \text{Diagram of a tube of length } p_{n-2} \text{ followed by a segment of length 2 (metal or plastic)} \\
 \hline
 \boxed{p_n = 2p_{n-1} + 2p_{n-2}}
 \end{array}$$

O primeiro passo será descobrir a forma da solução geral da equação dada. O polinómio característico, $x^2 - 2x - 2$, admite raízes $x_1 = 1 + \sqrt{3}$ e $x_2 = 1 - \sqrt{3}$. Verificamos que as sucessões $((1 + \sqrt{3})^n)_{n \in \mathbb{N}}$ e $((1 - \sqrt{3})^n)_{n \in \mathbb{N}}$ são linearmente independentes; portanto, todas as soluções (reais) da equação dada serão da forma

$$(\alpha(1 + \sqrt{3})^n + \beta(1 - \sqrt{3})^n)_{n \in \mathbb{N}} \quad \alpha, \beta \in \mathbb{R}.$$

Tendo em conta as condições iniciais ($p_0 = 1$ e $p_1 = 2$), é possível atingirmos

$$\alpha + \beta = 1, \quad \alpha(1 + \sqrt{3}) + \beta(1 - \sqrt{3}) = 2.$$

Resolvendo o sistema de equações lineares, obtemos $\alpha = \frac{(1+\sqrt{3})}{2\sqrt{3}}$ e $\beta = \frac{-(1-\sqrt{3})}{2\sqrt{3}}$, o que nos leva a concluir que a solução para o problema em mãos é a sucessão $(p_n)_{n \in \mathbb{N}}$, onde

$$p_n = \frac{(1 + \sqrt{3})^{n+1} - (1 - \sqrt{3})^{n+1}}{2\sqrt{3}}.$$

Teorema 4.2.5. *Consideremos a equação de recorrência linear homogênea*

$$0 = x_n - c_1x_{n-1} - c_2x_{n-2} - \cdots - c_kx_{n-k} \quad (k \geq 1, c_k \neq 0) \quad (4.2.iii)$$

com a equação característica

$$0 = q^k - c_1q^{k-1} - c_2q^{k-2} - \cdots - c_k = (q - q_1)^{n_1} \cdots (q - q_l)^{n_l}$$

com $n_1 + \cdots + n_l = k$ e $n_i > 0$. Então, as soluções da equação (4.2.iii) são precisamente as combinações lineares das k sucessões

$$\begin{array}{cccccc} (q_1^n)_{n \in \mathbb{N}}, & (n \cdot q_1^n)_{n \in \mathbb{N}}, & (n^2 \cdot q_1^n)_{n \in \mathbb{N}}, & \cdots & (n^{n_1-1} \cdot q_1^n)_{n \in \mathbb{N}}, \\ (q_2^n)_{n \in \mathbb{N}}, & (n \cdot q_2^n)_{n \in \mathbb{N}}, & (n^2 \cdot q_2^n)_{n \in \mathbb{N}}, & \cdots & (n^{n_2-1} \cdot q_2^n)_{n \in \mathbb{N}}, \\ \vdots & & & & \\ (q_l^n)_{n \in \mathbb{N}}, & (n \cdot q_l^n)_{n \in \mathbb{N}}, & (n^2 \cdot q_l^n)_{n \in \mathbb{N}}, & \cdots & (n^{n_l-1} \cdot q_l^n)_{n \in \mathbb{N}}. \end{array}$$

Demonstração. (Ideia) Consideremos a função linear S «esquecer o primeiro termo» definida por

$$S((x_n)_{n \in \mathbb{N}}) = (x_{n+1})_{n \in \mathbb{N}}.$$

Então, uma sucessão $a = (a_n)_{n \in \mathbb{N}}$ é solução da equação de recorrência (4.2.iii) se e só se

$$\begin{aligned} \text{sucessão nula} &= S^n(a) - c_1S^{n-1}(a) - \cdots - c_kS^{n-k}(a) \\ &= (S^n - c_1S^{n-1} - \cdots - c_kS^{n-k})(a) \\ &= S^{n-k} \circ (S^k - c_1S^{k-1} - \cdots - c_k\text{id})(a), \end{aligned}$$

para cada $n \geq k$. Veremos agora quais sucessões a função linear

$$S^k - c_1S^{k-1} - \cdots - c_k\text{id}$$

anula.

Seja (com $n_1 + \cdots + n_l = k$, $n_i > 0$)

$$0 = q^k - c_1q^{k-1} - c_2q^{k-2} - \cdots - c_k = (q - q_1)^{n_1} \cdots (q - q_l)^{n_l}$$

a equação característica, então

$$S^k - c_1S^{k-1} - \cdots - c_k\text{id} = (S - q_1\text{id})^{n_1} \circ \cdots \circ (S - q_l\text{id})^{n_l}.$$

«A chave» da demonstração reside no resultado auxiliar que apresentamos de seguida. \blacklozenge

Lema 4.2.6. *Para $q \in \mathbb{R}$ e $m \in \mathbb{N}$, $m \geq 1$, a função linear $(S - q\text{id})^m$ anula as sucessões*

$$(q^n)_{n \in \mathbb{N}}, \quad (n \cdot q^n)_{n \in \mathbb{N}}, \quad (n^2 \cdot q^n)_{n \in \mathbb{N}}, \quad \cdots \quad (n^{m-1} \cdot q^n)_{n \in \mathbb{N}}.$$

Demonstração. Para $m = 1$: $S((q^n)_{n \in \mathbb{N}}) = (q^{n+1})_{n \in \mathbb{N}} = q(q^n)_{n \in \mathbb{N}}$; ou seja

$$(S - q\text{id})(s_1) = \text{a sucessão nula.}$$

Nota: Portanto, $(q^n)_{n \in \mathbb{N}}$ é um vetor próprio de S com valor próprio q .

Seja agora $m > 1$ e suponhamos que $(S - q\text{id})^{m-1}$ anula s_1, \dots, s_{m-1} . Logo, $(S - q\text{id})^m$ também anula s_1, \dots, s_{m-1} . Calculamos primeiro, para cada $n \in \mathbb{N}$, o termo n de $(S - q\text{id})(s_m)$:

$$\begin{aligned} (n+1)^{m-1} \cdot q^{n+1} - n^{m-1} q^{n+1} &= \left(\sum_{i=0}^{m-1} \binom{m-1}{i} \cdot n^i \cdot q^{n+1} \right) - n^{m-1} q^{n+1} \\ &= \underbrace{\left(\sum_{i=0}^{m-2} q \cdot \binom{m-1}{i} \cdot n^i \cdot q^n \right)}_{\text{combinação linear do termo } n \text{ de } s_1, \dots, s_{m-1}} \end{aligned}$$

Logo, $(S - q\text{id})(s_m) = \alpha_1 s_1 + \dots + \alpha_{m-1} s_{m-1}$ e por isso

$$(S - q\text{id})^m(s_m) = \text{a sucessão nula.} \quad \blacklozenge$$

Exemplo 4.2.7. Consideremos a equação de recorrência linear homogênea

$$x_n = 5x_{n-1} - 8x_{n-2} + 4x_{n-3}, \quad (n \geq 3)$$

com valores iniciais $x_0 = 0$, $x_1 = 4$ e $x_2 = 18$. A equação caraterística associada será

$$0 = q^3 - 5q^2 + 8q - 4 = (q-1)(q-2)(q-2) = (q-1)(q-2)^2$$

portanto, as soluções da equação de recorrência serão as sucessões da forma (com $\alpha, \beta, \gamma \in \mathbb{R}$)

$$(\alpha 1^n + \beta 2^n + \gamma n 2^n)_{n \in \mathbb{N}}.$$

Considerando os valores iniciais, procuramos $\alpha, \beta, \gamma \in \mathbb{R}$ de tal forma que

$$\alpha + \beta = 0, \quad \alpha + 2\beta + 2\gamma = 4, \quad \alpha + 4\beta + 8\gamma = 18.$$

Ora,

$$\begin{cases} \alpha + \beta = 0, \\ \alpha + 2\beta + 2\gamma = 4, \\ \alpha + 4\beta + 8\gamma = 18 \end{cases} \Leftrightarrow \begin{cases} - - - - - \\ \beta + 2\gamma = 4 \\ 3\beta + 8\gamma = 18 \end{cases} \Leftrightarrow \begin{cases} \alpha = 2 \\ \beta = -2 \\ \gamma = 3 \end{cases},$$

pelo que a solução da equação de recorrência com os dados valores iniciais é a sucessão

$$(2 - 2^{n+1} + 3n2^n)_{n \in \mathbb{N}}.$$

Suponhamos que o polinómio caraterístico de uma equação de recorrência linear homogênea

tem as raízes complexas

$$z = a + ib \quad \text{e} \quad \bar{z} = a - ib.$$

Portanto, obtemos as duas soluções (da equação de recorrência):

$$\begin{aligned} a &= (z^n)_{n \in \mathbb{N}} = (r^n(\cos(\theta) + i \sin(\theta))^n)_{n \in \mathbb{N}} = (r^n(\cos(n\theta) + i \sin(n\theta)))_{n \in \mathbb{N}}, \\ b &= (\bar{z}^n)_{n \in \mathbb{N}} = (r^n(\cos(\theta) - i \sin(\theta))^n)_{n \in \mathbb{N}} = (r^n(\cos(n\theta) - i \sin(n\theta)))_{n \in \mathbb{N}}. \end{aligned}$$

Assim, obtemos as soluções (linearmente independentes)

$$\frac{a+b}{2} = (r^n \cos(n\theta))_{n \in \mathbb{N}} \quad \text{e} \quad \frac{a-b}{2i} = (r^n \sin(n\theta))_{n \in \mathbb{N}}.$$

Por último, se z e \bar{z} são raízes múltiplas, consideremos

$$\dots, (r^n n^i \cos(n\theta))_{n \in \mathbb{N}}, \dots, (r^n n^i \sin(n\theta))_{n \in \mathbb{N}}, \dots$$

Exemplo 4.2.8. Consideremos a equação de recorrência

$$a_{n+2} = a_{n+1} - a_n, \quad n \geq 0, \quad \text{com} \quad a_0 = 0, a_1 = 1.$$

A correspondente equação característica será $0 = q^2 - q + 1$, com soluções

$$z = \frac{1}{2} + i\frac{\sqrt{3}}{2} \quad \text{e} \quad \bar{z} = \frac{1}{2} - i\frac{\sqrt{3}}{2}.$$

Portanto, $r = 1$ e $\tan(\theta) = \sqrt{3}$, logo $\theta = \frac{\pi}{3}$; e a solução geral será dada por

$$\left(\alpha \cos\left(\frac{n\pi}{3}\right) + \beta \sin\left(\frac{n\pi}{3}\right) \right)_{n \in \mathbb{N}} \quad (\alpha, \beta \in \mathbb{R}).$$

Com a condição inicial $a_0 = 0$ obtemos $\alpha = 0$, e com $a_1 = 1$ obtemos

$$1 = \beta \sin\left(\frac{\pi}{3}\right) = \beta \frac{\sqrt{3}}{2}.$$

Portanto, a solução será a sucessão

$$\left(\frac{2}{\sqrt{3}} \sin\left(\frac{n\pi}{3}\right) \right)_{n \in \mathbb{N}}.$$

Números de Fibonacci (Revisitados) e o Número de Ouro

Recordamos que os números de Fibonacci $(F_n)_{n \in \mathbb{N}}$ satisfazem as equações

$$F_n = F_{n-1} + F_{n-2}, \quad \text{com} \quad F_0 = 1 \text{ e } F_1 = 1.$$

Para resolver a equação de recorrência linear homogênea $F_n = F_{n-1} + F_{n-2}$, consideremos a equação de segundo grau $q^2 - q - 1 = 0$ (que tem as duas soluções):

$$\phi = \frac{1 + \sqrt{5}}{2} \quad \text{e} \quad \psi = \frac{1 - \sqrt{5}}{2}.$$

Portanto, todas as soluções da equação homogênea são combinações lineares das sucessões $(\phi^n)_{n \in \mathbb{N}}$ e $(\psi^n)_{n \in \mathbb{N}}$. Em particular,

$$(F_n)_{n \in \mathbb{N}} = \alpha(\phi^n)_{n \in \mathbb{N}} + \beta(\psi^n)_{n \in \mathbb{N}}$$

Vejamos que $\phi\psi = -1$, $\phi + \psi = 1$ e $\phi - \psi = \sqrt{5}$, portanto, para $n = 0$ e $n = 1$ obtemos

$$1 = \alpha + \beta, \quad 1 = \alpha \overbrace{\left(\frac{1 + \sqrt{5}}{2}\right)}^{\phi} + \beta \overbrace{\left(\frac{1 - \sqrt{5}}{2}\right)}^{\psi}.$$

Fazendo redução com a correspondente matriz

$$\begin{bmatrix} 1 & 1 & 1 \\ \psi & \phi & 1 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 1 & 1 & 1 \\ 0 & \phi - \psi & (1 - \psi) \end{bmatrix}$$

obtemos $\beta = \frac{1-\psi}{\phi-\psi} = \frac{\phi}{\sqrt{5}}$ e $\alpha = 1 - \beta = -\frac{\psi}{\sqrt{5}}$. Portanto, obtém-se a **fórmula de Binet**:

$$F_n = \frac{\phi^{n+1} - \psi^{n+1}}{\sqrt{5}}.$$

Apresentamos agora a definição clássica da **proporção áurea**. Dois números $x, y \in \mathbb{R}^+$, com $x > y$, são ditos na proporção áurea se o quociente entre o maior número (x) e o menor número (y) for igual ao quociente entre a soma de ambos e o maior número, ou seja,

$$\overbrace{\hspace{1.5cm}}^x \quad \overbrace{\hspace{1.5cm}}^y \quad \frac{x}{y} = \frac{x+y}{x}.$$

Denotando $\frac{x}{y}$ por ϕ (como a proporção áurea), a relação anterior transforma-se em

$$\phi = 1 + \frac{1}{\phi},$$

ou, equivalentemente, ϕ é a única raiz positiva da equação $x^2 - x - 1$.

Dividindo por a relação de recorrência por F_{n-1} , obtemos

$$\frac{F_n}{F_{n-1}} = 1 + \frac{F_{n-2}}{F_{n-1}}. \quad (4.2.iv)$$

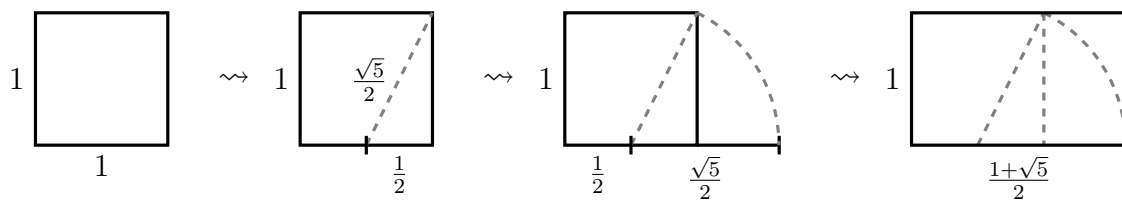
Aqui, assumimos que a razão entre dois números de Fibonacci consecutivos se aproxima de um dado número real α , ou seja, $\lim_{n \rightarrow \infty} \frac{F_n}{F_{n-1}} = \alpha$. Desta forma, temos ainda que $\lim_{n \rightarrow \infty} \frac{F_{n-1}}{F_n} = \frac{1}{\alpha}$. Tomando agora o limite de (4.2.iv), temos que $\alpha = 1 + \frac{1}{\alpha}$, a mesma identidade satisfeita pela proporção áurea. Assim, se o limite existir, a razão entre dois números de Fibonacci consecutivos deve aproximar-se de ϕ para n suficientemente grande, ou seja,

$$\lim_{n \rightarrow \infty} \frac{F_n}{F_{n-1}} = \phi.$$

Apresentamos na tabela que se segue alguns quocientes de números de Fibonacci consecutivos.

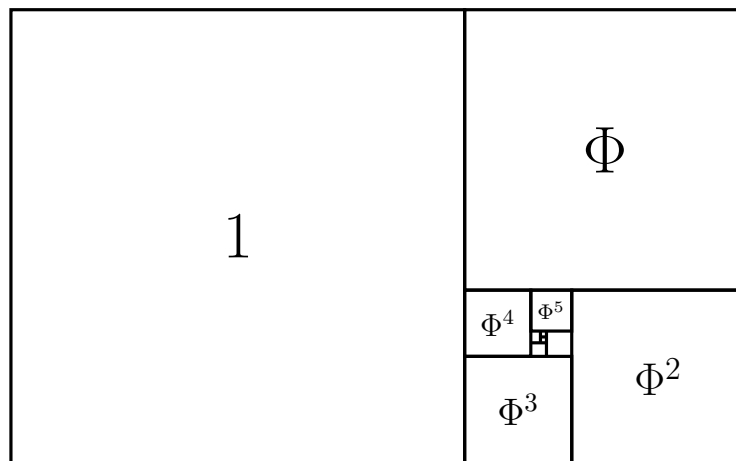
n	0	1	2	3	4	5	6	7	8	9	10
F_n	0	1	1	2	3	5	8	13	21	34	55
$\frac{F_n}{F_{n-1}}$	—	—	1	2	1,5	1,6666...	1,6	1,6250	1,6153...	1,6190...	1,6176...

Exemplo 4.2.9. Um rectângulo áureo é um retângulo cujos comprimentos dos lados estão na proporção áurea. Numa construção clássica, o primeiro passo é desenhar um quadrado de lado unitário. De seguida, devemos traçar uma linha que parte do ponto médio de um dos lados e termina num canto do lado oposto. Depois, desenhemos um arco desde o canto até uma extensão do lado com o ponto médio e, por último, completamos o rectângulo. O procedimento pode ser ilustrado pela figura seguinte.



Para construir um rectângulo de ouro de comprimento ϕ e largura unitária, anexámos um rectângulo menor (de comprimento 1 e largura $\Phi = \frac{1}{\phi} = \phi - 1$, i.e., áureo). Este rectângulo menor pode ser novamente sub-dividido num quadrado ainda menor noutro rectângulo áureo. O processo pode continuar *ad infinitum*.

Em cada sub-divisão, o comprimento do quadrado será reduzido por um fator Φ . Observemos ainda que cada rectângulo áureo é uma cópia em escala reduzida da figura total (são ditas figuras auto-selhantes).



Relativamente a estas construções, é ainda possível mostrar que $x = \sum_{i=0}^{\infty} \Phi^{2i} = \phi$. De facto,

$$x = 1 + \Phi^2 + \Phi^4 + \Phi^6 + \dots,$$

$$\Phi^2 x = \Phi^2 + \Phi^4 + \Phi^6 + \Phi^8 + \dots,$$

o que nos leva a $(1 - \Phi^2)x = 1$, ou seja,

$$x = \frac{1}{1 - \Phi^2} = \frac{\phi^2}{\phi^2 - 1} = \frac{\phi^2}{\phi} = \phi.$$

Voltando ao problema da população de coelhos, podemos traduzir a informação do sistema de relações de recorrência dado numa forma matricial

$$\begin{cases} a_{n+1} &= a_n + b_n, \\ b_{n+1} &= a_n, \end{cases} \Leftrightarrow \begin{bmatrix} a_{n+1} \\ b_{n+1} \end{bmatrix} = \underbrace{\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}}_Q \begin{bmatrix} a_n \\ b_n \end{bmatrix},$$

onde a matriz de coeficientes presente na expressão anterior é a dita **matriz Q de Fibonacci**. A multiplicação repetida de $[a_n; b_n]$ por Q faz avançar a população de coelhos para os meses seguintes. De facto, o avançar k meses na população é alcançado através de

$$\begin{bmatrix} a_{n+k} \\ b_{n+k} \end{bmatrix} = Q^k \begin{bmatrix} a_n \\ b_n \end{bmatrix}.$$

Como veremos, estas potências da matriz Q estão intimamente relacionadas com a sucessão de Fibonacci. Se multiplicarmos uma matriz 2×2 arbitrária por Q , podemos observar que

$$\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a + c & b + d \\ a & b \end{bmatrix},$$

ou seja, a multiplicação da matriz por Q substitui a primeira linha pela soma da primeira e segunda linhas, e a segunda linha pela primeira linha. Ao re-escrever Q em termos de números de Fibonacci e fazer uso da relação de recorrência que os define, conseguimos atingir

$$\begin{aligned} Q &= \begin{bmatrix} F_2 & F_1 \\ F_1 & F_0 \end{bmatrix}, \\ Q^2 &= \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} F_2 & F_1 \\ F_1 & F_0 \end{bmatrix} = \begin{bmatrix} F_3 & F_2 \\ F_2 & F_1 \end{bmatrix}, \\ Q^3 &= \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} F_3 & F_2 \\ F_2 & F_1 \end{bmatrix} = \begin{bmatrix} F_4 & F_3 \\ F_3 & F_2 \end{bmatrix}, \end{aligned}$$

e assim sucessivamente... sendo evidente o padrão que se gera e que nos leva a concluir

$$Q^n = \begin{bmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{bmatrix}.$$

Através destes desenvolvimentos matriciais e do facto de $Q^n Q^m = Q^{n+m}$, é possível mostrar ainda que, para $n \geq 1$ e $m \geq 0$, são válidas as seguintes igualdades:

$$F_{n+m} = F_m F_{n-1} + F_n F_{m+1}, \quad (4.2.v)$$

$$F_{2n-1} = F_{n-1}^2 + F_n^2, \quad (4.2.vi)$$

$$F_{2n} = F_n(F_{n-1} + F_{n+1}). \quad (4.2.vii)$$

Da Teoria de Matrizes e Determinantes sabemos que $\det(AB) = \det(A)\det(B)$. A aplicação repetida deste resultado produz $\det(Q^n) = \det(Q)^n$, que culmina na **identidade de Cassini**,

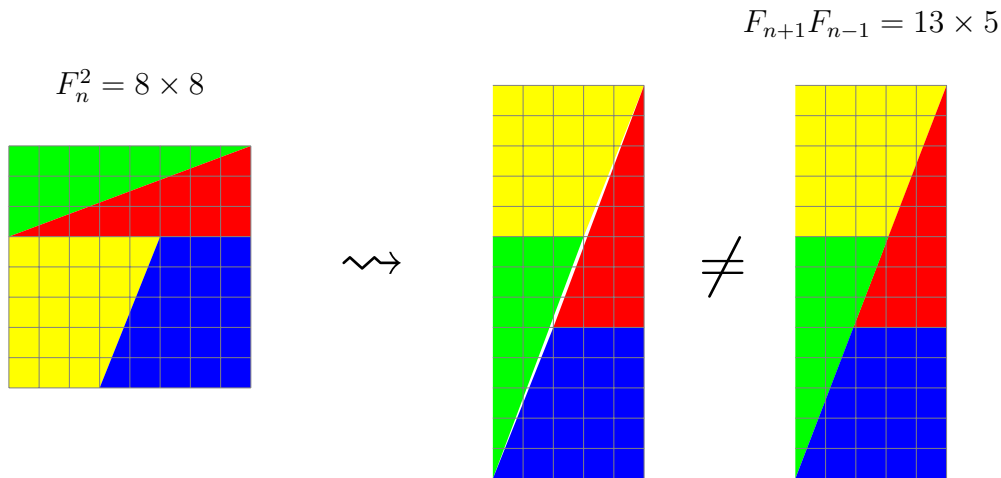
$$F_{n+1}F_{n-1} - F_n^2 = (-1)^n.$$

Adicionalmente, e tendo em conta (4.2.v), conseguimos deduzir a **identidade de Catalan**,

$$F_n^2 - F_{n-r}F_{n+r} = (-1)^{n-r}F_r^2.$$

A identidade de Cassini pode ser interpretada geometricamente. De facto, a parcela $F_{n+1}F_{n-1}$ pode ser tida como a área de um rectângulo de comprimento F_{n+1} e largura F_{n-1} , da mesma forma que F_n^2 pode ser a área de um quadrado de lateral F_n .

Neste caso, a identidade afirma que a diferença absoluta e entre as áreas é de apenas uma unidade de área. À medida que n se torna arbitrariamente grande, esta unidade de diferença torna-se tão pequena em relação às áreas que é facilmente cometida uma falácia, a “ilusão de Fibonacci”.



Para realizar a “ilusão de Fibonacci”, dissecamos um quadrado com lado F_n de tal forma a que, rearranjando as peças resultantes, pareça ser possível construir um rectângulo com comprimentos F_{n+1} e largura F_{n-1} , com uma unidade de área maior ou menor que o original quadrado.

É normal perguntarmo-nos sobre o porquê da unidade de área ausente (ou extra) ser distribuída ao longo da diagonal do rectângulo? Na figura acima é possível ver que a inclinação lateral dos trapézios é dada por $\frac{F_5}{F_3} = \frac{5}{2} = 2.5$, enquanto que a inclinação da hipotenusa do triângulo é dada por $\frac{F_6}{F_4} = \frac{8}{3} = 2.(6)$. Esta ligeira incompatibilidade de declives resulta num constante aumento ou redução da distância entre o trapézio e o triângulo (quando alinhados). A lacuna entre estes objectos pode ser facilmente escondida se dividirmos a diferença pelas peças alinhadas, como feito no rectângulo construído de forma «desonesta».

4.3 Equações de Recorrência Lineares Gerais

Relativamente ao problema em mãos, já sabemos resolver a primeira questão (equações de recorrência lineares homogêneas). Agora, vamos estudar alguns métodos para obter uma solução particular de uma equação de recorrência linear geral.

Consideremos então uma equação de recorrência linear

$$x_n = c_1 x_{n-1} + c_2 x_{n-2} + \cdots + c_k x_{n-k} + d_n.$$

- Se $d_n = c \cdot p^n$: Procuramos uma solução da forma

$$b_n = A \cdot p^n \quad \text{resp.} \quad b_n = A \cdot n^m \cdot p^n$$

(com $A \in \mathbb{R}$ a determinar) se p não é solução da equação caraterística (mais geral, se p é solução da equação caraterística de multiplicidade m).

- Se $d_n = \sum_{i=0}^j Z_i n^i$: Procuramos uma solução da forma:

* $b_n = A_0 + A_1 n + \cdots + A_j n^j$ (com $A_i \in \mathbb{R}$ a determinar) caso 1 não seja solução da equação caraterística.

* $b_n = (A_0 + A_1 n + \cdots + A_j n^j) \cdot n^m$ (com $A_i \in \mathbb{R}$ a determinar) caso 1 seja solução da equação caraterística de multiplicidade m .

Os valores dos parâmetros A, A_i obtém-se substituindo b_n na equação de recorrência dada.

Exemplo 4.3.1. Vamos determinar a solução da equação de recorrência

$$x_n = 3x_{n-1} - 2x_{n-2} + 2^n, \quad n = 2, 3, \dots$$

com $x_0 = 0$ e $x_1 = -2$. Procuramos primeiro a solução geral da equação homogênea associada, cuja equação caraterística é $0 = q^2 - 3q + 2 = (q - 2)(q - 1)$. Portanto, a solução geral da equação de recorrência homogênea é a sucessão $(a_n)_{n \in \mathbb{N}}$ dada por

$$a_n = \alpha \cdot 1^n + \beta \cdot 2^n = \alpha + \beta \cdot 2^n \quad (n \in \mathbb{N}).$$

Agora procuramos uma solução de

$$x_n - 3x_{n-1} + 2x_{n-2} = 2^n, \quad n = 2, 3, \dots$$

que seja da forma $b_n = n \cdot A \cdot 2^n$, com $n \in \mathbb{N}$. Tendo em conta que 2 é uma raiz simples de $q^2 - 3q + 2$, ao substituir na equação acima, obtemos

$$An2^n - 3A(n-1)2^{n-1} + 2A(n-2)2^{n-2} = 2^n,$$

que é equivalente a

$$2 = 2An - 3A(n-1) + A(n-2) = A.$$

Logo, uma solução da equação de recorrência acima é $(n2^{n+1})_{n \in \mathbb{N}}$. Assim, sabemos que a solução geral da equação

$$x_n = 3x_{n-1} - 2x_{n-2} + 2^n, \quad n = 2, 3, \dots$$

é dada por $(\alpha + \beta 2^n + n2^{n+1})_{n \in \mathbb{N}}$. Finalmente, procuramos aquele solução que satisfaz as condições iniciais $x_0 = 0$ e $x_1 = -2$. Portanto, para $n = 0$ e $n = 1$ obtemos as equações

$$\begin{array}{rcl} 0 & = & \alpha + \beta \\ -2 & = & \alpha + 2\beta + 4 \end{array} \quad \rightsquigarrow \quad \begin{array}{rcl} 0 & = & \alpha + \beta \\ -6 & = & \alpha + 2\beta \end{array}.$$

Subtraindo a primeira linha à segunda dá $\beta = -6$ e por isso $\alpha = 6$. Portanto, a solução é

$$(6 + (n - 3)2^{n+1})_{n \in \mathbb{N}}.$$

Exemplo 4.3.2. Vamos determinar a solução da equação de recorrência

$$x_n = x_{n-1} + n^2$$

com $x_0 = 0$. Procuramos primeiro a solução geral da equação homogênea associada, cuja equação característica é $0 = q - 1$. Portanto, a solução geral da equação de recorrência homogênea é a sucessão $(a_n)_{n \in \mathbb{N}}$ dada por

$$a_n = \alpha \cdot 1^n = \alpha \quad (n \in \mathbb{N}).$$

Agora procuramos uma solução de

$$x_n - x_{n-1} = n^2,$$

que seja da forma $b_n = (A_0 + A_1 n + A_2 n^2) \cdot n$, com $n \in \mathbb{N}$. Tendo em conta que 1 é uma raiz simples de $q - 1$, ao substituir na equação acima, obtemos

$$n(A_0 + A_1 n + A_2 n^2) - (n - 1)(A_0 + A_1(n - 1) + A_2(n - 1)^2) = n^2,$$

que é equivalente a

$$\begin{cases} A_0 - A_1 + A_2 = 0 \\ 2A_1 - 3A_2 = 0 \\ 3A_2 = 1 \end{cases} \quad \Leftrightarrow \quad \begin{cases} A_0 = \frac{1}{6} \\ A_1 = \frac{1}{2} \\ A_2 = \frac{1}{3} \end{cases}.$$

Logo, uma solução da equação de recorrência acima é $(\frac{n}{6} + \frac{n^2}{2} + \frac{n^3}{3})_{n \in \mathbb{N}}$. Assim, sabemos que a solução geral da equação

$$x_n = x_{n-1} + n^2$$

é dada por $(\alpha + \frac{n}{6} + \frac{n^2}{2} + \frac{n^3}{3})_{n \in \mathbb{N}}$. Finalmente, procuramos a solução que satisfaz a condição inicial $x_0 = 0$. Portanto, para $n = 0$, obtemos a equação

$$\alpha + 0 = 0 \quad \rightsquigarrow \quad \alpha = 0.$$

Desta forma, a solução será da forma

$$\left(\frac{n}{6} + \frac{n^2}{2} + \frac{n^3}{3} \right)_{n \in \mathbb{N}} = \left(\frac{n(n+1)(2n+1)}{6} \right)_{n \in \mathbb{N}}.$$

Teorema 4.3.3. *Seja*

$$x_n = c_1 x_{n-1} + c_2 x_{n-2} + \cdots + c_k x_{n-k} + d_n^{(1)} + \cdots + d_n^{(m)} \quad (4.3.i)$$

uma equação de recorrência linear e suponhamos que as sucessões $b^{(1)}, b^{(2)}, \dots, b^{(m)}$ são soluções de

$$\begin{aligned} x_n &= c_1 x_{n-1} + c_2 x_{n-2} + \cdots + c_k x_{n-k} + d_n^{(1)}, \\ x_n &= c_1 x_{n-1} + c_2 x_{n-2} + \cdots + c_k x_{n-k} + d_n^{(2)}, \\ &\vdots \\ x_n &= c_1 x_{n-1} + c_2 x_{n-2} + \cdots + c_k x_{n-k} + d_n^{(m)}, \end{aligned}$$

respectivamente. Então, a sucessão $b^{(1)} + \cdots + b^{(m)}$ é uma solução de (4.3.i).

Demonstração. Dado que $b^{(1)}, b^{(2)}, \dots, b^{(m)}$ são soluções das equações respectivas, sabemos que

$$\begin{aligned} b_n^{(1)} &= c_1 b_{n-1}^{(1)} + c_2 b_{n-2}^{(1)} + \cdots + c_k b_{n-k}^{(1)} + d_n^{(1)}, \\ b_n^{(2)} &= c_1 b_{n-1}^{(2)} + c_2 b_{n-2}^{(2)} + \cdots + c_k b_{n-k}^{(2)} + d_n^{(2)}, \\ &\vdots \\ b_n^{(m)} &= c_1 b_{n-1}^{(m)} + c_2 b_{n-2}^{(m)} + \cdots + c_k b_{n-k}^{(m)} + d_n^{(m)}. \end{aligned}$$

Ora, ao somar todas as equações anteriores e re-arranjar convenientemente os seus termos, obtemos o pretendido

$$\begin{aligned} b_n^{(1)} + b_n^{(2)} + \cdots + b_n^{(m)} &= c_1 (b_{n-1}^{(1)} + b_{n-1}^{(2)} + \cdots + b_{n-1}^{(m)}) + c_2 (b_{n-2}^{(1)} + b_{n-2}^{(2)} + \cdots + b_{n-2}^{(m)}) \\ &\quad + \cdots + c_k (b_{n-k}^{(1)} + b_{n-k}^{(2)} + \cdots + b_{n-k}^{(m)}) + (d_n^{(1)} + d_n^{(2)} + \cdots + d_n^{(m)}) \end{aligned}$$

◆

Exemplo 4.3.4. Vamos agora determinar a solução da equação de recorrência

$$x_n = 3x_{n-1} - 2x_{n-2} + 2^n + (1+n), \quad n = 2, 3, \dots$$

com $x_0 = 0$ e $x_1 = -2$. A solução geral desta equação (ignorando as condições iniciais) é da forma $(a_n + b_n^{(1)} + b_n^{(2)})_{n \in \mathbb{N}}$, onde $(a_n)_{n \in \mathbb{N}}$ denota a solução geral da equação homogênea associada, $(b_n^{(1)})_{n \in \mathbb{N}}$ é uma solução da equação de recorrência

$$x_n = 3x_{n-1} - 2x_{n-2} + 2^n, \quad n = 2, 3, \dots$$

e $(b_n^{(2)})_{n \in \mathbb{N}}$ é uma solução da equação de recorrência

$$x_n = 3x_{n-1} - 2x_{n-2} + (1 + n), \quad n = 2, 3, \dots$$

Falta-nos então determinar uma solução da equação de recorrência

$$x_n - 3x_{n-1} + 2x_{n-2} = 1 + n, \quad n = 2, 3, \dots$$

Uma vez que $1 + n$ é um polinómio de grau 1 e 1 é raiz de multiplicidade 1 da equação característica $0 = q^2 - 3q + 2 = (q - 2)(q - 1)$, consideramos $b_n^{(2)} = (A_0 + A_1 n)n^1 = A_0 n + A_1 n^2$. Substituindo na equação acima, obtemos $b_n^{(2)} = -\frac{7}{2}n - \frac{1}{2}n^2$. Assim, a solução geral da equação de recorrência

$$x_n = 3x_{n-1} - 2x_{n-2} + 2^n + (1 + n), \quad n = 2, 3, \dots$$

é dada por

$$(\alpha + \beta 2^n + n2^{n+1} - \frac{7}{2}n - \frac{1}{2}n^2)_{n \in \mathbb{N}} \quad (\alpha, \beta \in \mathbb{R}).$$

Finalmente, procuramos aquela solução que satisfaz as condições iniciais $x_0 = 0$ e $x_1 = -2$. Portanto, para $n = 0$ e $n = 1$ em

$$(\alpha + \beta 2^n + n2^{n+1} - \frac{7}{2}n - \frac{1}{2}n^2)_{n \in \mathbb{N}}$$

obtemos as equações

$$\begin{array}{rcl} 0 & = & \alpha + \beta \\ -2 & = & \alpha + 2\beta + 4 - \frac{7+1}{2} \end{array} \rightsquigarrow \begin{array}{rcl} 0 & = & \alpha + \beta \\ -2 & = & \alpha + 2\beta \end{array}$$

logo $\beta = -2$ e $\alpha = 2$. Logo, a solução da equação de recorrência dada com as condições iniciais $x_0 = 0$ e $x_1 = -2$ é

$$(2 + (n - 1)2^{n+1} - \frac{7}{2}n - \frac{1}{2}n^2)_{n \in \mathbb{N}}.$$

4.4 Equações de Recorrência Não Lineares

Nesta parte vamos considerar equações de recorrência onde x_n não depende de forma linear dos termos x_{n-1}, \dots, x_{n-k} . Em muitos casos poderemos «linearizar» a equação utilizando uma substituição adequada.

Exemplo 4.4.1. Consideremos a equação de recorrência não linear

$$x_n^2 = 2x_{n-1}^2 + 1 \quad (n \geq 1),$$

com a condição inicial $x_0 = 2$; aqui suponhamos $x_n \geq 0$, para todo o $n \in \mathbb{N}$. Ao escrever $y_n = x_n^2$, a equação de recorrência não linear transforma-se na equação de recorrência linear

$$y_n = 2y_{n-1} + 1 \quad (n \geq 1),$$

com a condição inicial $y_0 = x_0^2 = 4$.

$$y_n = 2y_{n-1} + 1 \quad (n \geq 1), \quad y_0 = 4.$$

- A solução geral da equação homogênea associada $y_n = 2y_{n-1}$ é dada por $c \cdot (2^n)_{n \in \mathbb{N}}$, $c \in \mathbb{R}$.
- Como o termo «não homogêneo» é um polinómio 1 de grau zero, e como 1 não é raiz do polinómio característico $q - 2$, sabemos que existe uma solução particular $(b_n)_{n \in \mathbb{N}}$ onde $b_n = A$, para todo o $n \in \mathbb{N}$. Substituindo na equação produz $A = 2A + 1$, ou seja, $A = -1$.
- Consequentemente, as soluções desta equação de recorrência são precisamente as sucessões $(c \cdot 2^n - 1)_{n \in \mathbb{N}}$, com $c \in \mathbb{R}$.

Tendo em conta a condição inicial $y_0 = 4$, obtemos $c = 5$; assim, a solução da equação $x_n^2 = 2x_{n-1}^2 + 1$ com $x_0 = 2$ é a sucessão

$$(\sqrt{5 \cdot 2^n - 1})_{n \in \mathbb{N}}.$$

Nota 4.4.2. Devemos recordar que, para cada $a \in \mathbb{R}^+$, com $a \neq 1$, a função $\log_a: \mathbb{R}^+ \rightarrow \mathbb{R}$ é bijectiva e satisfaz

$$\log_a(x \cdot y) = \log_a(x) + \log_a(y), \quad \log_a(1) = 0.$$

Logo, em muitos casos podemos «linearizar» equações utilizando o logaritmo.

Exemplo 4.4.3. Consideremos a equação de recorrência não linear

$$x_n = x_{n-1} \cdot x_{n-2} \quad (n \geq 2), \quad x_0 = x_1 = 2.$$

Esta equação é equivalente à equação (para $n \geq 2$)

$$\log_2(x_n) = \log_2(x_{n-1}) + \log_2(x_{n-2}), \quad \log_2(x_0) = \log_2(x_1) = 1.$$

Tomando então $y_n = \log_2(x_n)$ para cada $n \in \mathbb{N}$, obtemos a equação de recorrência linear

$$y_n = y_{n-1} + y_{n-2} \quad (n \geq 2), \quad y_0 = y_1 = 1;$$

cuja solução é a sucessão $(F_n)_{n \in \mathbb{N}}$ dos números de Fibonacci. Desta forma, a solução da equação acima com as dadas condições iniciais é

$$(2^{F_n})_{n \in \mathbb{N}}.$$

Exemplo 4.4.4. Consideremos agora a equação de recorrência não linear

$$x_n = \sqrt{x_{n-1} + \underbrace{\sqrt{x_{n-2} + \sqrt{x_{n-3} + \sqrt{\dots \sqrt{x_0}}}}_{x_{n-1}}}$$

com a condição inicial $x_0 = 4$. Portanto, $x_1 = \sqrt{x_0} = 2$, e para $n \geq 2$ temos

$$x_n = \sqrt{x_{n-1} + x_{n-1}} > 0;$$

ou seja $x_n^2 = 2x_{n-1}$ ($n \geq 2$); o que é equivalente a

$$2 \log_2(x_n) = 1 + \log_2(x_{n-1}) \quad (n \geq 2).$$

Fazendo $y_n = \log_2(x_n)$, obtemos a equação de recorrência linear

$$y_n = \frac{1}{2}y_{n-1} + \frac{1}{2} \quad (n \geq 2)$$

com a condição inicial $y_1 = 1$. A solução geral da equação de recorrência (ignorando a condição inicial) é dado por

$$\left(c \left(\frac{1}{2} \right)^n + 1 \right)_{n \geq 1} \quad (c \in \mathbb{R}).$$

Utilizando a condição inicial $y_1 = 1$ obtemos

$$1 = \frac{c}{2} + 1;$$

logo, $c = 0$. Portanto, para todo o $n \geq 1$,

$$x_n = 2^{y_n} = 2.$$

Exemplo 4.4.5. Finalmente, consideremos a equação de recorrência (linear mas não com coeficientes constantes)

$$x_n = n \cdot x_{n-1} \quad (n \geq 1).$$

Com $x_n = n! \cdot y_n$, a equação acima é equivalente a

$$n! \cdot y_n = n \cdot (n-1)! \cdot y_{n-1} = n! \cdot y_{n-1},$$

o que é equivalente a $y_n = y_{n-1}$, para todo o $n \geq 1$. Portanto, a solução geral da equação

acima é dada por

$$(n! \cdot c)_{n \in \mathbb{N}} \quad (c \in \mathbb{R}).$$

4.5 Séries e Funções Geradoras

Em problemas de contagem, queremos tipicamente descobrir uma sucessão $(a_n)_{n \in \mathbb{N}}$ onde a_n é tido como «o número de maneiras de fazer algo - ordenar, permutar, pintar, formar equipas de futebol - com n objectos» (distinguíveis ou indistinguíveis).

Alguns exemplos de «fazer algo com n objetos»:

- «sequências binárias» $\rightsquigarrow a_n = 2^n$.
- «sequências binárias com três uns» $\rightsquigarrow a_n = \binom{n}{3}$.
- «colocar bolas indistinguíveis nas caixas C_1, C_2, C_3 » $\rightsquigarrow a_n = \binom{3}{n}$.
- «colocar bolas indistinguíveis em três caixas tal que a primeira caixa não é vazia e a terceira tem um número par de bolas» $\rightsquigarrow a_n = ??$.
- «Partições de $\{1, 2, \dots, n\}$ » $\rightsquigarrow a_n = ??$.

Por norma, para descobrirmos $(a_n)_{n \in \mathbb{N}}$, é útil:

- decompor o problema em sub-problemas mais simples
- saber como calcular as sucessões associadas a cada um dos sub-problemas
- conseguir «compor» as soluções dos sub-problemas na solução do problema inicial.

Exemplo 4.5.1. Determinamos o número c_n de maneiras de escolher um sub-conjunto de dois ou três elementos em $[n] = \{1, 2, \dots, n\}$, ou seja, o número de elementos do conjunto

$$C_n = A_n \cup B_n \quad (\text{união disjunta})$$

com $A_n = \{S \subseteq [n] : |S| = 2\}$ e $B_n = \{S \subseteq [n] : |S| = 3\}$. Sabemos que

$$a_n = |A_n| = \binom{n}{2} \quad \text{e} \quad b_n = |B_n| = \binom{n}{3},$$

logo,

$$c_n = |A_n \cup B_n| = |A_n| + |B_n| = a_n + b_n = \binom{n}{2} + \binom{n}{3} = \binom{n+1}{3}.$$

O cálculo com estas sucessões é uma espécie de generalização do cálculo com polinómios, pelo que será conveniente escrever $(a_n)_{n \in \mathbb{N}}$ como uma **série formal de potências**:

$$a_0 + a_1x + a_2x^2 + \cdots = \sum_{n=0}^{\infty} a_n x^n$$

ou como uma série na forma **exponencial**:

$$a_0 + a_1x + \frac{a_2}{2!}x^2 + \frac{a_3}{3!}x^3 + \cdots = \sum_{n=0}^{\infty} \frac{a_n}{n!} x^n.$$

Além disso veremos ainda de que forma este cálculo é útil na resolução das equações de recorrência (anteriormente abordadas).

4.5.1 Séries Formais de Potências

Definição 4.5.2. Uma **série formal de potências** é uma série passível de manipulação algébrica (por adição, multiplicação, somas parciais, ...) dada por uma sucessão $(a_n)_{n \in \mathbb{N}}$ de números (em \mathbb{N} , \mathbb{Z} , \mathbb{Q} , ... ou até \mathbb{C}), que escrevemos, de forma mais intuitiva, numa indeterminada - variável ou símbolo - x ,

$$\mathcal{A} = a_0 + a_1x + a_2x^2 + \cdots = \sum_{n=0}^{\infty} a_n x^n.$$

Nota 4.5.3. • Uma série formal de potências pode ser interpretada como um algo semelhante a um polinómio (com infinitos termos).

- Alternativamente, e para os mais familiarizados com séries de potências, podemos pensar numa série formal (de potências) como uma série de potências na qual ignoramos quaisquer questões de convergência ao assumir que x não denota qualquer valor numérico.
- Duas séries de potências $\mathcal{A} = \sum_{n=0}^{\infty} a_n x^n$ e $\mathcal{B} = \sum_{n=0}^{\infty} b_n x^n$ dizem-se iguais se e só se $a_n = b_n$, para todo o $n \in \mathbb{N}$.

Exemplo 4.5.4. Vamos determinar a série formal de potências correspondente ao problema de contar as formas de «colocar bolas indistinguíveis em caixas (estas últimas em número suficientemente grande)». Veremos mais tarde que muitos problemas podem ser vistos como combinações destas questões simples.

- «distribuir n bolas em três caixas numeradas»:

$$1 + 3x + \cdots + \binom{3}{n} x^n + \cdots$$

- «colocar n bolas numa única caixa»:

$$1 + x + x^2 + x^3 + \cdots = \sum_{n=0}^{\infty} x^n.$$

- «colocar n bolas numa única caixa com, no máximo, 4 lugares»:

$$1 + x + x^2 + x^3 + x^4 + 0x^5 + \dots = 1 + x + x^2 + x^3 + x^4.$$

- «colocar n bolas numa única caixa com exactamente 4 lugares»:

$$0 + 0x + 0x^2 + 0x^3 + 1x^4 + 0x^5 + \dots = x^4.$$

Exemplo 4.5.5. Mencionamos agora algumas séries que consideremos ao longo do texto.

- A série exponencial: $\exp = \sum_{n=0}^{\infty} \frac{x^n}{n!} = 1 + x + \frac{x^2}{2} + \frac{x^3}{6} + \dots$
- A série uniforme: $U = \sum_{n=0}^{\infty} x^n = 1 + x + x^2 + \dots$
- A série dos números de Fibonacci: $\text{fib} = 1 + x + 2x^2 + 3x^3 + 5x^4 + \dots$

4.5.2 Álgebra das Séries Formais

Definição 4.5.6. O conjunto de todas as séries formais de potências numa indeterminada x com coeficientes no corpo \mathbb{C} , que denotaremos daqui em diante por $\mathbb{C}[[x]]$, quando munido da adição e multiplicação escalar usuais,

$$\mathcal{A} + \mathcal{B} = \left(\sum_{n=0}^{\infty} a_n x^n \right) + \left(\sum_{n=0}^{\infty} b_n x^n \right) = \sum_{n=0}^{\infty} (a_n + b_n) x^n, \quad \lambda \mathcal{A} = \lambda \left(\sum_{n=0}^{\infty} a_n x^n \right) = \sum_{n=0}^{\infty} (\lambda a_n) x^n,$$

toma a estrutura de um espaço vectorial sobre \mathbb{C} .

Nesta estrutura, identificamos cada elemento $z \in \mathbb{C}$ com a **série de potências constante** dada pela sucessão $(a_n)_{n \in \mathbb{N}}$ onde

$$a_n = \begin{cases} z, & n = 0 \\ 0, & n \geq 1 \end{cases}.$$

Um caso particular a ter em especial conta será o **elemento neutro** (da adição) do espaço vectorial, 0, identificado com a **série nula**, $\sum_{n=0}^{\infty} 0x^n$.

É ainda possível construir um produto entre elementos de $\mathbb{C}[[x]]$, o chamado **produto de Cauchy** (ou **convolução discreta**). De facto, dadas duas séries formais $\mathcal{A}, \mathcal{B} \in \mathbb{C}[[x]]$, definimos o seu produto $\mathcal{A} \cdot \mathcal{B}$ como

$$\mathcal{A} \cdot \mathcal{B} = \left(\sum_{n=0}^{\infty} a_n x^n \right) \cdot \left(\sum_{n=0}^{\infty} b_n x^n \right) = \sum_{n=0}^{\infty} \left(\sum_{k=0}^n a_k b_{n-k} \right) x^n.$$

Para este produto, convém notarmos que o elemento neutro será a série formal dada pela sucessão $(a_n)_{n \in \mathbb{N}}$ onde $a_0 = 1$ e $a_i = 0$, para $i \geq 1$. Denotaremos esta série (convenientemente) por 1.

Nota 4.5.7. • Para os polinômios (vistos como séries formais de potências), o produto definido imediatamente acima coincide com o produto usual de polinômios.

- No cálculo com séries formais de potências, verificam-se as leis de comutatividade, associatividade, distributividade, etc... (provenientes da axiomática dos espaços vectoriais).

Definição 4.5.8. Uma série formal $\mathcal{A} \in \mathbb{C}[[x]]$ diz-se **invertível** se existir uma série $\mathcal{B} \in \mathbb{C}[[x]]$ de tal forma que $\mathcal{A} \cdot \mathcal{B} = 1$.

Nota 4.5.9.

- Quando uma tal série \mathcal{B} existir, será unicamente determinada e dita **inversa** de \mathcal{A} . Em termos de notação, escreveremos \mathcal{A}^{-1} ou $1/\mathcal{A}$ em lugar de \mathcal{B} .
- Para três séries formais $\mathcal{A}, \mathcal{B}, \mathcal{C} \in \mathbb{C}[[x]]$, é usual escrevermos $\mathcal{A} = \frac{\mathcal{B}}{\mathcal{C}}$ se $\mathcal{A}\mathcal{C} = \mathcal{B}$ (independentemente da invertibilidade de \mathcal{C}). Adicionalmente, para $n \in \mathbb{N}$, denotaremos o produto $\underbrace{\mathcal{A} \cdot \mathcal{A} \cdots \mathcal{A}}_{n \text{ factores}}$ por \mathcal{A}^n .

Lema 4.5.10. *Seja $\mathcal{A} = \sum_{n=0}^{\infty} a_n x^n \in \mathbb{C}[[x]]$. Então, \mathcal{A} é invertível se e só se $a_0 \neq 0$.*

Demonstração. (\Rightarrow) Seja $\mathcal{B} = \sum_{n=0}^{\infty} b_n x^n \in \mathbb{C}[[x]]$ uma série formal tal que $\mathcal{A} \cdot \mathcal{B} = 1$. Então, $a_0 b_0 = 1$ e $a_0 \neq 0$.

(\Leftarrow) Suponhamos que $a_0 \neq 0$. Então, definimos b_0, b_1, \dots em \mathbb{C} recursivamente por $b_0 := 1/a_0$ e

$$b_k := -\frac{1}{a_0} \sum_{i=1}^k a_i b_{k-i} \in \mathbb{C},$$

para $k \geq 1$. Então,

$$\sum_{i=0}^k a_i b_{k-i} = \begin{cases} 1, & k = 0, \\ 0, & k > 0. \end{cases}$$

Desta forma, $\mathcal{A} \cdot \mathcal{B} = 1$, onde $\mathcal{B} = \sum_{n=0}^{\infty} b_n x^n$. ♦

Exemplo 4.5.11. A série de potências fib da sucessão dos números de Fibonacci $(F_n)_{n \in \mathbb{N}}$ (definida por $F_0 = 0$ e $F_1 = 1$ e $F_n = F_{n-1} + F_{n-2}$, $n \geq 2$) é dada por

$$\text{fib} = \sum_{n=0}^{\infty} F_n x^n = \frac{x}{1 - x - x^2}.$$

De facto, temos

$$\begin{aligned}
 \sum_{n=0}^{\infty} F_n x^n &= x + \sum_{n=2}^{\infty} (F_{n-1} + F_{n-2}) x^n \\
 &= x + \sum_{n=2}^{\infty} F_{n-1} x^n + \sum_{n=2}^{\infty} F_{n-2} x^n \\
 &= x + x \sum_{n=2}^{\infty} F_{n-1} x^{n-1} + x^2 \sum_{n=2}^{\infty} F_{n-2} x^{n-2} \\
 &= x + x \sum_{n=1}^{\infty} F_n x^n + x^2 \sum_{n=0}^{\infty} F_n x^n \\
 &= x + x \sum_{n=0}^{\infty} F_n x^n + x^2 \sum_{n=0}^{\infty} F_n x^n \\
 &= x + (x + x^2) \sum_{n=0}^{\infty} F_n x^n.
 \end{aligned}$$

Exemplo 4.5.12. Consideremos $\mathcal{A} = 1 - x$ e $\mathcal{B} = \sum_{n=0}^{\infty} x^n$. Então,

$$\begin{aligned}
 (1 - x) \sum_{n=0}^{\infty} x^n &= (1 + x + x^2 + x^3 + x^4 + \dots) \\
 &\quad - (x + x^2 + x^3 + x^4 + \dots) \\
 &= 1
 \end{aligned}$$

ou seja, $\mathcal{B} = \sum_{n=0}^{\infty} x^n$ é a série inversa da série $\mathcal{A} = 1 - x$:

$$\sum_{n=0}^{\infty} x^n = (1 - x)^{-1}, \quad \text{escrevendo também} \quad \sum_{n=0}^{\infty} x^n = \frac{1}{1 - x}.$$

Exemplo 4.5.13. Para cada $\alpha \in \mathbb{R}$,

$$\sum_{n=0}^{\infty} \alpha^n x^n = \frac{1}{1 - \alpha x}.$$

De facto, tomando $\mathcal{A} = \sum_{n=0}^{\infty} \alpha^n x^n$, segue que:

$$\begin{aligned}
 \mathcal{A} &= 1 + (\alpha x + \alpha^2 x^2 + \alpha^3 x^3 + \dots) \\
 &= 1 + (\alpha x) (1 + \alpha x + \alpha^2 x^2 + \dots) \\
 &= 1 + (\alpha x) \mathcal{A},
 \end{aligned}$$

portanto, $\mathcal{A}(1 - \alpha x) = 1$.

Exemplo 4.5.14. Utilizando a indução matemática é possível mostrar que, para cada $m \geq 1$ e $\alpha \in \mathbb{R}$,

$$\frac{1}{(1 - \alpha x)^m} = \sum_{n=0}^{\infty} \binom{m+n-1}{m-1} \alpha^n x^n = \sum_{n=0}^{\infty} \binom{m+n-1}{n} \alpha^n x^n.$$

De facto, para $m = 1$ (passo base), temos

$$\frac{1}{1 - \alpha x} = \sum_{n=0}^{\infty} \binom{n}{0} \alpha^n x^n = \sum_{n=0}^{\infty} \alpha^n x^n.$$

Como hipótese de indução, admitimos que tal fórmula é válida para $m = k - 1$. Tentamos agora mostrar a validade para k :

$$\begin{aligned} \frac{1}{(1 - \alpha x)^k} &= \left(\frac{1}{(1 - \alpha x)^{k-1}} \right) \cdot \left(\frac{1}{1 - \alpha x} \right) = \left(\sum_{n=0}^{\infty} \binom{k+n-2}{k-2} \alpha^n x^n \right) \cdot \left(\sum_{n=0}^{\infty} \alpha^n x^n \right) \\ &= \sum_{n=0}^{\infty} \left(\sum_{j=0}^n \binom{k+j-2}{k-2} \alpha^j \alpha^{n-j} \right) x^n \\ &= \sum_{n=0}^{\infty} \left(\sum_{j=0}^n \binom{k+j-2}{k-2} \right) \alpha^n x^n \\ &= \sum_{n=0}^{\infty} \binom{k+n-1}{n-1} \alpha^n x^n. \end{aligned}$$

Como caso particular, tomando $m = 2$ e $\alpha = 1$, obtemos:

$$\frac{1}{(1 - x)^2} = \sum_{n=0}^{\infty} \binom{n+1}{1} x^n = \sum_{n=0}^{\infty} (n+1) x^n, \quad \text{ou seja, } 1 + 2x + 3x^2 + 4x^3 + \cdots = \frac{1}{(1 - x)^2}.$$

Mais tarde (Exemplo 4.5.36) veremos um argumento de combinatória para justificar esta igualdade.

Introduzimos ainda mais uma operação com séries:

Definição 4.5.15. Dadas duas séries formais $\mathcal{A} = \sum_{n=0}^{\infty} a_n x^n$, $\mathcal{B} = \sum_{n=0}^{\infty} b_n x^n \in \mathbb{C}[[x]]$, com $b_0 = 0$, definimos a série obtida por **substituição** de \mathcal{B} em \mathcal{A} como

$$\mathcal{A} \circ \mathcal{B} = \mathcal{A}(\mathcal{B}) = \sum_{n=0}^{\infty} a_n \mathcal{B}^n = a_0 + a_1 \mathcal{B} + a_2 \mathcal{B}^2 + \cdots$$

Nota 4.5.16. • Como o termo constante b_0 de \mathcal{B} é igual a 0, todos os termos em \mathcal{B}^m de grau $0, 1, \dots, m-1$ são iguais a 0. Portanto, para calcular o m -ésimo termo de $\mathcal{A}(\mathcal{B})$, basta considerar $a_0 + a_1 \mathcal{B} + \cdots + a_m \mathcal{B}^m$.

- O termo c_n de ordem n de $\mathcal{A} \circ \mathcal{B} = \sum_{n=0}^{\infty} c_n x^n$ é dado por

$$c_n = \sum_{\substack{0 \leq k \leq n \\ j_1 + \cdots + j_k = n}} a_k b_{j_1} \cdots b_{j_k}.$$

Notamos que a substituição de séries envolve de facto uma «soma infinita» de séries, uma situação que estudaremos no que se segue.

4.5.3 Somas infinitas de séries de potências

A grande parte da matéria desta subsecção é complementar e não foi dada na aula (com a exceção do Corolário 4.5.28).

Agora começamos a formar somas infinitas de séries de potências. Para justificar este processo vamos introduzir uma norma discreta, que se comporta de forma muito mais simples que a norma euclidiana em \mathbb{C} , por exemplo.

Definição 4.5.17. Dada uma série $\mathcal{A} = \sum_{n=0}^{\infty} a_n x^n \in \mathbb{C}[[x]]$, definimos a sua **norma**

$$\|\mathcal{A}\| := 2^{-\inf(\mathcal{A})} \in \mathbb{R},$$

onde $\inf(\mathcal{A})$ denota o menor índice $n \in \mathbb{N}$ para o qual $a_n \neq 0$.

Nota 4.5.18. • Por convenção, tomamos $\inf(0) = \inf(\emptyset) = \infty$, o que nos leva a concluir que $\|0\| = 2^{-\infty} = 0$.

- De facto, a base 2 presente na definição acima pode ser substituída por qualquer número real superior a 1.
- Nestas condições, uma série formal $\mathcal{A} \in \mathbb{C}[[x]]$ é invertível se e só se $\|\mathcal{A}\| = 1$.

O próximo resultado, transforma $(\mathbb{C}[[x]], \|\cdot\|)$ num espaço ultra-métrico.

Lema 4.5.19. Consideremos $\mathcal{A}, \mathcal{B} \in \mathbb{C}[[x]]$. Então:

1. $\|\mathcal{A}\| \geq 0$, atingindo-se a igualdade se e só se $\mathcal{A} = 0$.
2. $\|\mathcal{A} \cdot \mathcal{B}\| = \|\mathcal{A}\| \cdot \|\mathcal{B}\|$.
3. $\|\mathcal{A} + \mathcal{B}\| \leq \max\{\|\mathcal{A}\|, \|\mathcal{B}\|\}$, atingindo-se a igualdade se $\|\mathcal{A}\| \neq \|\mathcal{B}\|$.

Demonstração. 1. Segue directamente da definição.

2. Sem perda de generalidade, consideremos $\mathcal{A} \neq 0 \neq \mathcal{B}$, com $\inf(\mathcal{A}) = k$ e $\inf(\mathcal{B}) = \ell$. Então, o $k + \ell$ -ésimo coeficiente de $\mathcal{A} \cdot \mathcal{B}$ será

$$\sum_{i=0}^{k+\ell} a_i b_{k+\ell-i} = a_k b_\ell \neq 0.$$

Em particular, temos que $\inf(\mathcal{A} \cdot \mathcal{B}) = \inf(\mathcal{A}) + \inf(\mathcal{B})$, pelo que é possível concluir

$$\|\mathcal{A} \cdot \mathcal{B}\| = 2^{-\inf(\mathcal{A} \cdot \mathcal{B})} = 2^{-(\inf(\mathcal{A}) + \inf(\mathcal{B}))} = 2^{-\inf(\mathcal{A})} \cdot 2^{-\inf(\mathcal{B})} = \|\mathcal{A}\| \cdot \|\mathcal{B}\|.$$

3. A partir de $a_n + b_n \neq 0$ conseguimos obter $a_n \neq 0$ ou $b_n \neq 0$. Segue então que $\inf(\mathcal{A} +$

$\mathcal{B}) \geq \min\{\inf(\mathcal{A}), \inf(\mathcal{B})\}$. Esta última desigualdade transforma-se na desigualdade ultra-métrica $\|\mathcal{A} + \mathcal{B}\| \leq \max\{\|\mathcal{A}\|, \|\mathcal{B}\|\}$. Caso $\inf(\mathcal{A}) > \inf(\mathcal{B})$, então claramente $\inf(\mathcal{A} + \mathcal{B}) = \inf(\mathcal{B})$.

◆

Teorema 4.5.20. *O espaço vectorial $\mathbb{C}[[x]]$, munido da norma anteriormente introduzida, $\|\cdot\|$, é um espaço de Banach (espaço vectorial normado completo).*

Demonstração. Como $\|\mathcal{A} + \mathcal{B}\| \leq \max\{\|\mathcal{A}\|, \|\mathcal{B}\|\} \leq \|\mathcal{A}\| + \|\mathcal{B}\|$ para $\mathcal{A}, \mathcal{B} \in \mathbb{C}[[x]]$, a aplicação $\mathcal{A} \mapsto \|\mathcal{A}\|$ cumpre os requisitos de norma no sentido analítico (de acordo com o Lema 4.5.19).

Consideremos então uma sucessão de Cauchy $(\mathcal{A}_k)_{k \in \mathbb{N}}$ de elementos de $\mathbb{C}[[x]]$, onde

$$\mathcal{A}_m = \sum_{n=0}^{\infty} a_{m,n} x^n, \quad \text{Para } i \geq 1.$$

Ora, para todo $k \geq 0$ existirá uma ordem $N_k \geq 1$ a partir da qual se tem que $\|\mathcal{A}_m - \mathcal{A}_{N_k}\| < 2^{-k}$, para todos os $m \geq N_k$. Tal mostra-nos que $a_{m,n} = a_{N_k,n}$ para todo o $m \geq N_k$ e $n \leq k$. Sem perda de generalidade, podemos assumir que $N_0 \leq N_1 \leq \dots$ e definir

$$a_k := a_{N_k,k} \quad \text{e} \quad \mathcal{A} = \sum_{k=0}^{\infty} a_k x^k.$$

Então, $\|\mathcal{A} - \mathcal{A}_m\| < 2^{-k}$, para todo o $m \geq N_k$, i.e., $\lim_{m \rightarrow \infty} \mathcal{A}_m = \mathcal{A}$. Desta forma, concluimos que $\mathbb{C}[[x]]$ é completo em relação a $\|\cdot\|$.

◆

Vejamos que $\mathbb{C}[[x]]$ é o completamento de $\mathbb{C}[x]$ em relação a $\|\cdot\|$. Por outras palavras, as séries formais de potências podem ser consideradas como sucessões de Cauchy de polinómios. Para sucessões convergentes $(\mathcal{A}_k)_{k \in \mathbb{N}}$ e $(\mathcal{B}_k)_{k \in \mathbb{N}}$ temos (como em qualquer espaço métrico com multiplicação)

$$\lim_{k \rightarrow \infty} (\mathcal{A}_k + \mathcal{B}_k) = \lim_{k \rightarrow \infty} \mathcal{A}_k + \lim_{k \rightarrow \infty} \mathcal{B}_k, \quad \lim_{k \rightarrow \infty} (\mathcal{A}_k \cdot \mathcal{B}_k) = \lim_{k \rightarrow \infty} \mathcal{A}_k \cdot \lim_{k \rightarrow \infty} \mathcal{B}_k.$$

A soma infinita

$$\sum_{k=1}^{\infty} \mathcal{A}_k := \lim_{n \rightarrow \infty} \sum_{k=1}^n \mathcal{A}_k$$

só pode convergir se $(\mathcal{A}_k)_{k \in \mathbb{N}}$ for uma sucessão cujo termo geral tende para a série nula, ou seja, $\lim_{k \rightarrow \infty} \|\mathcal{A}_k\| = 0$. Surpreendentemente, e em total contraste com os espaços euclidianos, o recíproco é ainda verdadeiro, como veremos. Este facto crucial torna a aritmética de séries formais de potências muito mais simples do que a sua contra-parte analítica.

Lema 4.5.21. *Consideremos a sucessão $(\mathcal{A}_k)_{k \in \mathbb{N}}$ de elementos de $\mathbb{C}[[x]]$ que convergem para a série nula. Então, as séries $\sum_{k=1}^{\infty} \mathcal{A}_k$ e $\prod_{k=1}^{\infty} (1 + \mathcal{A}_k)$ convergem (i.e., estão bem definidas em $\mathbb{C}[[x]]$).*

Demonstração. Pelo Teorema 4.5.20, é suficiente mostrar que a sucessão das somas parciais é de Cauchy. Assim, para $\varepsilon > 0$, consideremos uma ordem $N \in \mathbb{N}$ a partir da qual, se $k \geq N_0$, então $\|\mathcal{A}_k\| < \varepsilon$. Por conseguinte, para $k > \ell \geq N_0$, temos

$$\begin{aligned} \left\| \sum_{i=1}^k \mathcal{A}_i - \sum_{i=1}^{\ell} \mathcal{A}_i \right\| &= \left\| \sum_{i=\ell+1}^k \mathcal{A}_i \right\| \leq \max\{\|\mathcal{A}_i\| : i = \ell+1, \dots, k\} < \varepsilon, \\ \left\| \prod_{i=1}^k (1 + \mathcal{A}_i) - \prod_{i=1}^{\ell} (1 + \mathcal{A}_i) \right\| &= \left\| \prod_{i=1}^{\ell} \underbrace{\|1 + \mathcal{A}_i\|}_{\leq 1} \prod_{i=\ell+1}^k (1 + \mathcal{A}_i) - 1 \right\| \leq \left\| \sum_{\emptyset \neq I \subset \{\ell+1, \dots, k\}} \prod_{i \in I} \mathcal{A}_i \right\| \\ &\leq \max\{\|\mathcal{A}_i\| : i = \ell+1, \dots, k\} < \varepsilon. \end{aligned} \quad \blacklozenge$$

Muitas vezes consideramos sequências como sucessões cujos elementos convergem para a série nula. Consideremos uma sucessão de séries de $\mathbb{C}[[x]]$, $(\mathcal{A}_k)_{k \in \mathbb{N}}$, onde $\mathcal{A}_k = \sum_{n=0}^{\infty} a_{k,n} x^n$, para $k \geq 1$. Para cada $n \geq 0$, apenas um número finito de coeficientes $a_{1,n}, a_{2,n}, \dots$ são não nulos. Tal mostra-nos que o coeficiente do termo x^n em

$$\sum_{k=1}^{\infty} \mathcal{A}_k = \sum_{n=0}^{\infty} \left(\sum_{k=1}^{\infty} a_{k,n} \right) x^n$$

depende apenas de um número finito de termos. O mesmo raciocínio se pode aplicar à série $\prod_{k=1}^{\infty} (1 + \mathcal{A}_k)$.

Para $\mathcal{C} \in \mathbb{C}[[x]]$ e sucessões $(\mathcal{A}_k)_{k \in \mathbb{N}}$ e $(\mathcal{B}_k)_{k \in \mathbb{N}}$ é válido que $\sum_k \mathcal{A}_k + \sum_k \mathcal{B}_k = \sum_k \mathcal{A}_k + \mathcal{B}_k$ e $\mathcal{C} \sum_k \mathcal{A}_k = \sum_k \mathcal{C} \cdot \mathcal{A}_k$ (conforme esperado).

Corolário 4.5.22. *Sejam $(\mathcal{A}_k)_{k \in \mathbb{N}}$ uma sucessão de séries formais que converge para a série nula e $\pi : \mathbb{N} \rightarrow \mathbb{N}$ uma bijecção. Então,*

$$\sum_{k=1}^{\infty} \mathcal{A}_k = \sum_{k=1}^{\infty} \mathcal{A}_{\pi(k)}.$$

Demonstração. Para todo o $n \in \mathbb{N}$, sabemos que existirá uma ordem $N_0 \in \mathbb{N}$ de tal forma que $\pi(k) > n$, para todo o $k > N_0$. Desta forma,

$$\left\| \sum_{k=1}^{N_0} \mathcal{A}_k - \sum_{k=1}^{N_0} \mathcal{A}_{\pi(k)} \right\| \leq \max\{\|\mathcal{A}_k\| : k > n\} \rightarrow 0. \quad \blacklozenge$$

Corolário 4.5.23 (Teorema de Fubini - Versão Discreta). *Considere-se uma sucessão de séries formais $(\mathcal{A}_{k,n})$ de tal forma que $\lim_{k+n \rightarrow \infty} \mathcal{A}_{k,n} = 0$. Então,*

$$\sum_{k=1}^{\infty} \sum_{n=1}^{\infty} \mathcal{A}_{k,n} = \sum_{n=1}^{\infty} \sum_{k=1}^{\infty} \mathcal{A}_{k,n}.$$

Demonstração. Segue directamente do facto de

$$\left\| \sum_{k=1}^{\infty} \sum_{n=1}^{\infty} \mathcal{A}_{k,n} - \sum_{n=1}^{N_0} \sum_{k=1}^{\infty} \mathcal{A}_{k,n} \right\| = \left\| \sum_{k=1}^{\infty} \sum_{n=1}^{\infty} \mathcal{A}_{k,n} - \sum_{k=1}^{\infty} \sum_{n=1}^{N_0} \mathcal{A}_{k,n} \right\| = \left\| \sum_{k=1}^{\infty} \sum_{n=N_0+1}^{\infty} \mathcal{A}_{k,n} \right\| \xrightarrow{N_0 \rightarrow \infty} 0. \quad \blacklozenge$$

Nota 4.5.24. Consideremos a substituição $\mathcal{A} \circ \mathcal{B}$ de séries (ver Definição 4.5.15). Se \mathcal{A} for um polinómio (ou seja, uma série formal cujos coeficientes, a partir de uma dada ordem, são nulos), $\mathcal{A}(\mathcal{B})$ será uma série usual de potências, enquanto que se $b_0 = 0$, a convergência de $\mathcal{A}(\mathcal{B})$ é garantida pelo Lema 4.5.21.

Nos próximos vamos admitir (subrepticiamente) que uma das condições do último ponto é válida. Observemos que $\|\mathcal{A}(\mathcal{B})\| \leq \|\mathcal{A}\|$ se $b_0 = 0$.

Exemplo 4.5.25. Consideremos $\exp = \sum_{n=0}^{\infty} \frac{x^n}{n!}$, $\mathcal{A} = \sum_{n=0}^{\infty} a_n x^n$ e $\mathcal{B} = x^2$. Então,

$$\begin{aligned} \mathcal{A}(0) &= \sum_{n=0}^{\infty} a_n 0^n = a_0, \\ \mathcal{A}(\mathcal{B}) &= \mathcal{A}(x^2) = \sum_{n=0}^{\infty} a_n (x^2)^n = \sum_{n=0}^{\infty} a_n x^{2n}, \\ \exp(\mathcal{B}) &= \sum_{n=0}^{\infty} \frac{(x^2)^n}{n!} = \sum_{n=0}^{\infty} \frac{x^{2n}}{n!}. \end{aligned}$$

Teorema 4.5.26. Consideremos três séries formais $\mathcal{A}, \mathcal{B}, \mathcal{C} \in \mathbb{C}[[x]]$ com primeiro coeficiente nulo (ou seja, $a_0 = b_0 = c_0 = 0$) e uma sucessão $(\mathcal{A}_k)_{k \in \mathbb{N}}$ de séries formais convergentes para a série nula. Então, temos que

1. $(\sum_k \mathcal{A}_k)(\mathcal{B}) = \sum_k \mathcal{A}_k(\mathcal{B})$.
2. $(\prod_k (1 + \mathcal{A}_k))(\mathcal{B}) = \prod_k (1 + \mathcal{A}_k(\mathcal{B}))$.
3. $\mathcal{A}(\mathcal{B}(\mathcal{C})) = (\mathcal{A}(\mathcal{B}))(\mathcal{C})$.

Demonstração. 1. Dado que $\|\mathcal{A}_k(\mathcal{B})\| \leq \|\mathcal{A}_k\| \xrightarrow{k \rightarrow \infty} 0$, podemos concluir que todas as séries formais estão bem definidas. Podemos então deduzir

$$\left(\sum_k \mathcal{A}_k \right) (\mathcal{B}) = \sum_{n=0}^{\infty} \left(\sum_k a_{k,n} \right) \mathcal{B}^n = \sum_k \left(\sum_{n=0}^{\infty} a_{k,n} \mathcal{B}^n \right) = \sum_k \mathcal{A}_k(\mathcal{B}).$$

2. Vamos primeiramente demonstrar o resultado considerando dois factores $\mathcal{A}_1 = \sum_{n=0}^{\infty} a_{1,n} x^n$ e $\mathcal{A}_2 = \sum_{n=0}^{\infty} a_{2,n} x^n$:

$$(\mathcal{A}_1 \cdot \mathcal{A}_2)(\mathcal{B}) = \sum_{n=0}^{\infty} \left(\sum_{k=0}^n a_{1,k} a_{2,n-k} \right) \mathcal{B}^n = \sum_{n=0}^{\infty} \sum_{k=0}^n (a_{1,k} \mathcal{B}^k) (a_{2,n-k} \mathcal{B}^{n-k}) = \mathcal{A}_1(\mathcal{B}) \cdot \mathcal{A}_2(\mathcal{B}).$$

Inductivamente, podemos estender o processo a um número finito de séries formais,

pelo que

$$\begin{aligned} \left\| \left(\prod_k (1 + \mathcal{A}_k) \right) (\mathcal{B}) - \prod_{k=1}^n (1 + \mathcal{A}_k(\mathcal{B})) \right\| &= \left\| \left(\prod_{k=1}^{\infty} (1 + \mathcal{A}_k) - \prod_{k=1}^n (1 + \mathcal{A}_k) \right) (\mathcal{B}) \right\| \\ &\leq \left\| \prod_{k=1}^{\infty} (1 + \mathcal{A}_k) - \prod_{k=1}^n (1 + \mathcal{A}_k) \right\| \xrightarrow{n \rightarrow \infty} 0. \end{aligned}$$

3. Tomando $\mathcal{A} = \sum_{n=0}^{\infty} a_n x^n$, e tendo em conta os últimos dois pontos, concluímos que

$$\mathcal{A}(\mathcal{B}(\mathcal{C})) = \sum_{n=0}^{\infty} a_n (\mathcal{B} \circ \mathcal{C})^n = \sum_{n=0}^{\infty} a_n (\mathcal{B}^n \circ \mathcal{C}) = \left(\sum_{n=0}^{\infty} a_n \mathcal{B}^n \right) \circ \mathcal{C} = (\mathcal{A}(\mathcal{B}))(\mathcal{C}). \quad \blacklozenge$$

Nota 4.5.27. Devemos notar que, em geral,

$$\mathcal{A}(\mathcal{B}) \neq \mathcal{B}(\mathcal{A}), \quad \mathcal{A}(\mathcal{B} \cdot \mathcal{C}) \neq \mathcal{A}(\mathcal{B}) \cdot \mathcal{A}(\mathcal{C}), \quad \mathcal{A}(\mathcal{B} + \mathcal{C}) \neq \mathcal{A}(\mathcal{B}) + \mathcal{A}(\mathcal{C}).$$

Corolário 4.5.28. *Consideremos duas séries $\mathcal{A}, \mathcal{B} \in \mathbb{C}[[x]]$, onde o termo constante de \mathcal{B} é nulo e \mathcal{A} é invertível. Então, $\mathcal{A}(\mathcal{B})^{-1} = \mathcal{A}^{-1}(\mathcal{B})$*

Exemplo 4.5.29. Consideremos a série formal de potências $\sum_{n=0}^{\infty} \alpha^n x^n = U(\alpha x)$. Então,

$$U(\alpha x) = \frac{1}{1 - \alpha x}.$$

No que se segue, vamos considerar $\langle x \rangle$ e $\langle x^2 \rangle$ como, respectivamente, o conjunto das séries formais com termo constante nulo e o conjunto das séries formais com termos ímpares nulos.

Teorema 4.5.30. *O conjunto das séries formais $\langle x \rangle \setminus \langle x^2 \rangle \subseteq \mathbb{C}[[x]]$ é um grupo para a operação de substituição.*

Demonstração. Sejam $\mathcal{A}, \mathcal{B} \in \langle x \rangle \setminus \langle x^2 \rangle$. Então, $\mathcal{A}(\mathcal{B}) \in \langle x \rangle \setminus \langle x^2 \rangle$. Pelo Teorema 4.5.26 segue ainda que são válidas as leis de associatividade. Adicionalmente, $x \in \langle x \rangle \setminus \langle x^2 \rangle$ e $x(\mathcal{A}) = \mathcal{A} = \mathcal{A}(x)$.

A construção dos elementos inversos segue da mesma forma que no Lema 4.5.10. Para tal, consideremos $\mathcal{A}^k = \sum_{n=0}^{\infty} a_{k,n} x^n$, para $k \in \mathbb{N}$. Dado que $a_{1,0} = 0$, teremos que $a_{k,n} = 0$, para $n < k$, e $a_{n,n} = a_{1,1}^n \neq 0$. Definimos então $b_0, b_1, \dots \in \mathbb{C}$ recursivamente por $b_0 := 0$ e

$$b_k := -\frac{1}{a_{k,k}} \sum_{i=1}^{k-1} b_i a_{i,k},$$

para $n \geq 2$. Tomando $\mathcal{B} = \sum_{n=0}^{\infty} b_n x^n \in \langle x \rangle \setminus \langle x^2 \rangle$, obtemos

$$\mathcal{B}(\mathcal{A}) = \sum_{k=0}^{\infty} b_k \mathcal{A}^k = \sum_{k=1}^{\infty} \sum_{n=0}^{\infty} b_k a_{k,n} x^n = \sum_{n=0}^{\infty} \left(\sum_{k=1}^n b_k a_{k,n} \right) x^n = x.$$

Substituindo agora \mathcal{A} por \mathcal{B} , é possível encontrar um $\mathcal{C} \in \langle x \rangle \setminus \langle x^2 \rangle$ tal que $\mathcal{C}(\mathcal{B}) = x$.

Desta forma,

$$\mathcal{C} = \mathcal{C}(x) = \mathcal{C}(\mathcal{B}(\mathcal{A})) = (\mathcal{C}(\mathcal{B}))(\mathcal{A}) = x(\mathcal{A}) = \mathcal{A}$$

e concluimos que $\mathcal{A}(\mathcal{B}) = x$. ◆

Definição 4.5.31. Para $\mathcal{A} \in \langle x \rangle \setminus \langle x^2 \rangle$, existirá uma única $\mathcal{B} \in \langle x \rangle \setminus \langle x^2 \rangle$ de tal forma que $\mathcal{A}(\mathcal{B}) = x = \mathcal{B}(\mathcal{A})$. A esta série formal chamaremos **reversa** de \mathcal{A} .

Exemplo 4.5.32. Tomemos \mathcal{A} como a série reversa de $x + x^2 + \cdots = \frac{x}{1-x}$. É possível verificar que

$$x = \frac{\mathcal{A}}{1 - \mathcal{A}}$$

e segue que $\mathcal{A} = \frac{x}{1-x} = x - x^2 + x^3 - \cdots$. Este é um exemplo de uma **transformação de Möbius** (homografias — transformações projectivas — da linha projectiva complexa).

Nota 4.5.33. Em geral, não é muito fácil encontrar a série reversa de uma dada série formal de potências em $\langle x \rangle \setminus \langle x^2 \rangle \subseteq \mathbb{C}[[x]]$. Um último recurso é a utilização da **Fórmula de Inversão de Lagrange-Bürmann**. No entanto, esta envolve alguns conceitos “não muito triviais” da Análise Complexa (em particular, da Teoria de Resíduos e algumas propriedades das Séries de Laurent).

Teorema 4.5.34 (Fórmula de Inversão de Lagrange-Bürmann). *Dada uma série formal $\mathcal{A} \in \langle x \rangle \setminus \langle x^2 \rangle \subseteq \mathbb{C}[[x]]$, a sua série reversa é dada por*

$$\sum_{k=1}^{\infty} \frac{\text{res}(\mathcal{A}^{-k})}{k} x^k,$$

onde $\text{res}(\cdot)$ denota o resíduo da série \mathcal{A}^{-k} , que é definido como o coeficiente do termo de ordem -1 da expansão de \mathcal{A}^{-k} em série de Laurent.

Lema 4.5.35. *Dada uma sucessão $(\mathcal{A}_k)_{k \in \mathbb{N}}$ (de séries formais de $\mathbb{C}[[x]]$ com coeficiente constante nulo) que convirja para a série nula, temos que*

$$\exp\left(\sum_k \mathcal{A}_k\right) = \prod_k \exp(\mathcal{A}_k).$$

Em particular, tem-se que $\exp(kx) = \exp(x)^k$, para $k \in \mathbb{Z}$.

Demonstração. Dado que $\sum_k \mathcal{A}_k$ tem coeficiente constante nulo e $\exp(\mathcal{A}_k) \in \sum_{n=0}^{\infty} \frac{\mathcal{A}_k^n}{n!}$, ambos os membros do enunciado estão bem definidos. Para somas com duas parcelas, \mathcal{A}, \mathcal{B} , calculamos

$$\exp(\mathcal{A} + \mathcal{B}) = \sum_{n=0}^{\infty} \frac{(\mathcal{A} + \mathcal{B})^n}{n!} = \sum_{n=0}^{\infty} \sum_{k=0}^n \binom{n}{k} \frac{\mathcal{A}^k \mathcal{B}^{n-k}}{n!}$$

$$= \sum_{n=0}^{\infty} \sum_{k=0}^n \frac{\mathcal{A}^k \mathcal{B}^{n-k}}{k!(n-k)!} = \left(\sum_{n=0}^{\infty} \frac{\mathcal{A}^n}{n!} \right) \left(\sum_{n=0}^{\infty} \frac{\mathcal{B}^n}{n!} \right) = \exp(\mathcal{A}) \exp(\mathcal{B}).$$

Por indução no número (finito) de parcelas da soma, conseguimos obter

$$\begin{aligned} \left\| \exp \left(\sum_k \mathcal{A}_k \right) - \prod_{k=1}^n \exp(\mathcal{A}_k) \right\| &= \left\| \exp \left(\sum_{k=1}^n \mathcal{A}_k + \sum_{k=n+1}^{\infty} \mathcal{A}_k \right) - \exp \left(\sum_{k=1}^n \mathcal{A}_k \right) \right\| \\ &= \left\| \exp \left(\sum_{k=1}^n \mathcal{A}_k \right) \right\| \cdot \left\| \exp \left(\sum_{k=n+1}^{\infty} \mathcal{A}_k \right) - 1 \right\| \xrightarrow{n \rightarrow \infty} 0. \end{aligned}$$

Para a segunda parte do enunciado, consideremos \mathbb{N} . Então, $\exp(kx) = \exp(x + \cdots + x) = \exp(x)^k$. Dado que

$$\exp(kx) \exp(-kx) = \exp(kx - kx) = \exp(0) = 1,$$

temos também que $\exp(-kx) = \exp(kx)^{-1} = \exp(x)^{-k}$. ◆

Para acabar esta subsecção, colecionamos alguns resultados sobre o cálculo com séries formais que serão úteis no que se segue.

- $\sum_{n=0}^{\infty} \alpha^n x^n = \mathcal{U}(\alpha x) = \frac{1}{1 - \alpha x}$.
- De forma mais geral: $\sum_{n=0}^{\infty} \binom{m+n-1}{n} \alpha^n x^n = \frac{1}{(1 - \alpha x)^m}$.
- Para cada $m \in \mathbb{N}$: $\sum_{n=0}^{\infty} \binom{m}{n} x^n = \sum_{n=0}^m \binom{m}{n} x^n = (1 + x)^m$.

4.5.4 Interpretação Combinatorial

Consideremos um **problema de contagem A** e um **problema de contagem B** (com objectos «indistinguíveis»), com as séries associadas

$$\mathcal{A} = \sum_{n=0}^{\infty} a_n x^n \quad e \quad \mathcal{B} = \sum_{n=0}^{\infty} b_n x^n.$$

O que os coeficientes $c_n = a_0 b_n + a_1 b_{n-1} + \cdots + a_n b_0$ do produto $\mathcal{A} \cdot \mathcal{B}$ estão a contar?

$$\begin{array}{ccc} \mathbf{A} & \mathbf{B} & ?? \\ \downarrow & \downarrow & \downarrow \\ \mathcal{A} & \mathcal{B} & \mathcal{AB} \end{array}$$

De facto, c_n é igual ao número de maneiras (denotado por $\mathbf{A} * \mathbf{B}$) de

- partir uma coleção de n objectos indistinguíveis em duas partes E_1 (de k elementos) e E_2 (de $n - k$ elementos) disjuntas, ou seja, escrever $n = k + (n - k)$.
- aplicar o problema \mathbf{A} a E_1 (existem a_k maneiras), e
- aplicar o problema \mathbf{B} a E_2 (existem b_{n-k} maneiras).

Ou seja, obtém-se $\text{Série}(\mathbf{A} * \mathbf{B}) = \text{Série}(\mathbf{A}) \cdot \text{Série}(\mathbf{B})$.

Exemplo 4.5.36. Consideremos a questão \mathbf{A}

“colocar n bolas indistinguíveis numa única caixa (suficientemente grande)”.

Portanto, a série correspondente a \mathbf{A} é a série formal uniforme $U = \sum_{n=0}^{\infty} x^n$. A questão $\mathbf{A} * \mathbf{A}$ corresponde a:

- partir a coleção de n bolas indistinguíveis em duas partes E_1 (de k elementos) e E_2 (de $n - k$ elementos) disjuntas,
- colocar E_1 numa caixa,
- colocar E_2 numa (outra) caixa.

Ou seja, $\mathbf{A} * \mathbf{A}$ é o problema de distribuir n bolas indistinguíveis em duas caixas, e a série correspondente a $\mathbf{A} * \mathbf{A}$ é

$$U \cdot U = \text{Série}(\mathbf{A} * \mathbf{A}) = \sum_{n=0}^{\infty} \binom{2}{n} x^n = \sum_{n=0}^{\infty} \binom{n+1}{1} x^n = \sum_{n=0}^{\infty} (n+1) x^n.$$

Tendo em conta que $U = \frac{1}{1-x}$, obtém-se

$$\frac{1}{(1-x)^2} = \sum_{n=0}^{\infty} \binom{2}{n} x^n = \sum_{n=0}^{\infty} (n+1) x^n.$$

De mesmo modo, para cada $m \in \mathbb{N}$, obtém-se

$$U^m = \frac{1}{(1-x)^m} = \sum_{n=0}^{\infty} \binom{m}{n} x^n.$$

Seja $\alpha \in \mathbb{R}$ (ou $\alpha \in \mathbb{C}$). Substituir αx nas séries acima, obtém-se

$$\frac{1}{(1-\alpha x)^m} = \sum_{n=0}^{\infty} \binom{m}{n} \alpha^n x^n;$$

portanto, para $m \geq 1$,

$$\frac{1}{(1-\alpha x)^m} = \sum_{n=0}^{\infty} \binom{n+m-1}{m-1} \alpha^n x^n.$$

Esta igualdade já foi provado em Exemplo 4.5.14, utilizando indução matemática.

Tipicamente temos o problema «inverso»: Dada uma questão **C**, encontrar **A** e **B** de tal forma que $\mathbf{C} = \mathbf{A} * \mathbf{B}$.

Exemplo 4.5.37. Determinamos o número de maneiras de distribuir quatro objectos indistinguíveis em duas caixas numeradas de modo que hajam no máximo dois objectos na primeira caixa. Mais geral, se temos n tais objectos, para os distribuir temos de

- dividir a coleção (de facto, o número de elementos) em duas partes disjuntas: E_1 (k elementos) e E_2 ($n - k$ elementos);
- os objectos de E_1 destinam-se à primeira caixa, portanto, «há uma maneira» se $k \leq 2$ e é «impossível» para $k > 2$;
- os objectos de E_2 destinam-se à segunda caixa; portanto «há uma maneira».

Considerando c_n como o número de maneiras de distribuir os quatro objectos nas condições acima indicadas, segue que

$$\sum_{n=0}^{\infty} c_n x^n = (1 + x + x^2)(1 + x + x^2 + x^3 + x^4 + \dots),$$

e, ao desenvolver o produto exposto, atingimos o pretendido, $c_4 = 3$.

Vamos agora alterar ligeiramente o problema inicial, querendo determinar o número de maneiras de distribuir quatro objectos indistinguíveis em cinco caixas numeradas de modo que hajam no máximo um objecto em cada das primeiras três caixas e no máximo dois objectos em cada das últimas duas caixas.

Se considerarmos d_n como o número de maneiras de ... distribuir os quatro objectos nas condições acima indicadas, então:

$$\begin{aligned} \sum_{n=0}^{\infty} d_n x^n &= (1 + x)(1 + x)(1 + x)(1 + x + x^2)(1 + x + x^2) \\ &= (1 + x)^3(1 + x + x^2)^2 \\ &= (1 + 3x + 3x^2 + x^3)(1 + 2x + 3x^2 + 2x^3 + x^4) \\ &= 1 + 5x + 12x^2 + 18x^3 + 18x^4 + 12x^5 + 5x^6 + 1x^7. \end{aligned}$$

Logo, há $d_4 = 18$ tais maneiras.

Apresentamos ainda duas variações desta questão.

Exemplo 4.5.38. Determinamos o número de maneiras de distribuir vinte objetos indistinguíveis em quatro caixas numeradas de modo que hajam no máximo dez objetos em cada uma das primeiras três caixas e pelo menos dois objetos na última caixa caixas.

Sendo c_n o número de maneiras de de distribuir n objetos nas condições acima indicadas,

então

$$\begin{aligned}
 \sum_{n=0}^{\infty} c_n x^n &= (1 + \dots + x^{10})^3 (x^2 + x^3 + \dots) \\
 &= (U - x^{11} U)^3 x^2 U = x^2 (1 - x^{11})^3 U^4 \\
 &= x^2 \left(\sum_{k=0}^3 \binom{3}{k} (-1)^k x^{11k} \right) \left(\sum_{n=0}^{\infty} \binom{4}{n} x^n \right) \\
 &= x^2 (1 - 3x^{11} + 3x^{22} - x^{33}) \left(\sum_{n=0}^{\infty} \binom{4}{n} x^n \right).
 \end{aligned}$$

Logo, há $c_{20} = \binom{4}{18} - 3 \binom{4}{7} = \binom{31}{3} - 3 \binom{10}{3} = 970$ tais maneiras.

Exemplo 4.5.39. Determinamos o número de maneiras de distribuir n objetos indistinguíveis em duas caixas numeradas de modo que haja um número par de objetos na primeira caixa.

Sendo c_n o número de maneiras de ... (ver acima) ..., então

$$\begin{aligned}
 \sum_{n=0}^{\infty} c_n x^n &= (1 + x^2 + x^4 + \dots)(1 + x + x^2 + \dots) \\
 &= U(x^2) U \\
 &= \frac{1}{(1 - x^2)(1 - x)} = \frac{1}{(1 + x)(1 - x)^2} \\
 &= \frac{1}{4} \cdot \frac{1}{1 + x} + \frac{1}{4} \cdot \frac{1}{1 - x} + \frac{1}{2} \cdot \frac{1}{(1 - x)^2} \\
 &= \frac{1}{4} \sum_{n=0}^{\infty} (-1)^n x^n + \frac{1}{4} \sum_{n=0}^{\infty} x^n + \frac{1}{2} \sum_{n=0}^{\infty} \binom{2}{n} x^n.
 \end{aligned}$$

Logo, há $c_n = \frac{1}{4}(1 + (-1)^n) + \frac{1}{2}(n + 1)$ tais maneiras.

No que se segue consideremos problemas de contagem com objetos distinguíveis (por exemplo, bolas numeradas). Sendo a_n o número de maneiras correspondente, veremos que é conveniente considerar a série exponencial

$$\sum_{n=0}^{\infty} \frac{a_n}{n!}.$$

Em geral, notamos que o coeficiente de índice n do produto

$$\left(\sum_{n=0}^{\infty} \frac{a_n}{n!} \right) \cdot \left(\sum_{n=0}^{\infty} \frac{b_n}{n!} \right)$$

é

$$\sum_{k=0}^n \frac{a_k}{k!} \frac{b_{n-k}}{(n-k)!} = \frac{1}{n!} \sum_{k=0}^n \frac{n!}{k!(n-k)!} a_k b_{n-k} = \frac{\sum_{k=0}^n \binom{n}{k} a_k b_{n-k}}{n!}.$$

Consideremos então problemas de contagem **A** e **B** com objectos distinguíveis, onde a_n e b_n denotam, respectivamente, o número de maneiras de aplicar **A** resp. **B** ao conjunto $\{1, \dots, n\}$.

Seja c_n o número de maneiras de

- partir o conjunto $\{1, \dots, n\}$ numa parte E_1 (com k elementos) e numa parte E_2 (com $n - k$ elementos), há $\binom{n}{k}$ maneiras;
- aplicar «A» ao conjunto E_1 , há a_k maneiras;
- aplicar «B» ao conjunto E_2 , há b_{n-k} maneiras.

Logo, $\sum_{n=0}^{\infty} \frac{c_n}{n!} = \left(\sum_{n=0}^{\infty} \frac{a_n}{n!} \right) \cdot \left(\sum_{n=0}^{\infty} \frac{b_n}{n!} \right)$, ou seja,

$$\text{SérieExp}(\mathbf{A} * \mathbf{B}) = \text{SérieExp}(\mathbf{A}) \cdot \text{SérieExp}(\mathbf{B}).$$

Exemplo 4.5.40. Determinamos o número de maneiras de distribuir quatro objectos numerados em duas caixas numeradas de modo que hajam no máximo dois objectos na primeira caixa.

Mais geral, se temos n objectos, para os distribuir temos de

- dividir a coleção em duas partes E_1 e E_2 disjuntas;
- os objectos de E_1 destinam-se à primeira caixa, portanto, «há uma maneira» se $|E_1| \leq 2$ e é «impossível» para $|E_1| > 2$;
- os objectos de E_2 destinam-se à segunda caixa; portanto «há uma maneira».

Sendo c_n o número de maneiras de \dots , então

$$\sum_{n=0}^{\infty} \frac{c_n}{n!} x^n = \left(1 + x + \frac{1}{2}x^2 \right) \left(1 + x + \frac{1}{2}x^2 + \frac{1}{3!}x^3 + \frac{1}{4!}x^4 + \dots \right).$$

Em particular, $c_4 = 11$.

Dado um «problema de contagem» com a correspondente sucessão

$$c_n = \text{o número de maneiras de } \dots \text{ com } n \text{ objectos,}$$

consideremos as seguintes séries associadas a $(c_n)_{n \in \mathbb{N}}$.

A série geradora ordinária:

$$\sum_{n=0}^{\infty} c_n x^n.$$

Utilizamos esta série no caso de «objetos indistinguíveis»: bolas «iguais», votação secreta, \dots

A série geradora exponencial:

$$\sum_{n=0}^{\infty} \frac{c_n}{n!} x^n.$$

Utilizamos esta série no caso de «objetos distinguíveis»: bolas numeradas, votação aberta, \dots

Nota 4.5.41. Também se utiliza a designação **função geradora**, embora neste momento não interpretemos as séries formais como funções (i.e., não consideramos questões de convergência).

Acabamos esta secção com um caso particular da substituição. Consideremos um problema de contagem **A** com objectos distinguíveis, e a_n denota o número de maneiras de aplicar **A** ao conjunto $\{1, 2, \dots, n\}$. Suponhamos que $a_0 = 0$ e seja

$$\mathcal{A} = \sum_{n=0}^{\infty} \frac{a_n}{n!} x^n$$

a correspondente série geradora exponencial. Sendo

$$\sum_{n=0}^{\infty} \frac{c_n}{n!} x^n = \exp(\mathcal{A})$$

a série obtida por substituir \mathcal{A} em \exp , então

c_n é o número de maneiras de

- escolher uma partição P de $\{1, 2, \dots, n\}$, e
- aplicar **A** a cada bloco de P .

Para preparar o Exemplo 4.5.45, introduzimos o seguinte conceito.

Definição 4.5.42. Para cada $n \in \mathbb{N}$, definimos recursivamente o **factorial duplo** de n , $n!!$, da seguinte forma:

$$n!! = \begin{cases} 1, & n = 0 \text{ ou } n = 1, \\ n(n-2)!!, & n \geq 2. \end{cases}$$

Nota 4.5.43. • Para cada $n \in \mathbb{N}$, $n!!$ é o produto de todos os números naturais não superiores a n e com a mesma paridade de n .

- Para cada $n \geq 1$, tem-se que $n!!(n-1)!! = n!$.

Exemplo 4.5.44. Para cada $k \in \mathbb{N}$, $(2k)!! = 2^k k!$. De facto, com $n = 2k$:

$$\begin{aligned} n!! &= 2 \cdot 4 \cdot 6 \cdots (n-2) \cdot n \\ &= (2 \cdot 1) \cdot (2 \cdot 2) \cdot (2 \cdot 3) \cdots (2(k-1)) \cdot 2k \\ &= 2^k k! \end{aligned}$$

Caso $n = 2k + 1$, então $n!! = \frac{(2k+1)!}{(2k)!!} = \frac{(2k+1)!}{2^k k!}$.

Exemplo 4.5.45. Determinarmos o número de partições de $\{1, 2, \dots, n\}$ em blocos de dois elementos.

Intuitivamente, escolhemos uma partição e «aceitamos» se cada bloco tem exatamente dois elementos. Como a série exponencial de «aceitar se tem exatamente dois elementos» é $\frac{x^2}{2}$, o número de tais partições é o coeficiente de $\frac{x^n}{n!}$ na série $\exp(\frac{x^2}{2})$.

Calculamos:

$$\exp\left(\frac{x^2}{2}\right) = \sum_{n=0}^{\infty} \frac{1}{n!} \frac{x^{2n}}{2^n} = \sum_{n=0}^{\infty} \frac{1}{(2n)!!} x^{2n} = 1 + \sum_{n=1}^{\infty} \frac{(2n-1)!!}{(2n)!} x^{2n}.$$

Portanto, $c_0 = 1$ e

$$c_m = \begin{cases} 0 & \text{se } m \text{ for ímpar,} \\ (m-1)!! & \text{se } m \text{ for par, } m \geq 2. \end{cases}$$

4.5.5 Séries vs. Funções

Convém recordarmos agora do Cálculo que

- Interpretando a série formal de potências

$$\mathcal{A} = \sum_{n=0}^{\infty} a_n x^n$$

como uma **série de potências** em \mathbb{R} (ou em \mathbb{C}), então existe um R com $0 \leq R \leq \infty$ (**raio de convergência**) de tal forma que $\sum_{n=0}^{\infty} a_n t^n$ é absolutamente convergente, para cada t com $|t| < R$.

- Se $R > 0$, associamos à série \mathcal{A} a função

$$\mathcal{A}: \{x \mid |x| < R\} \longrightarrow \mathbb{R}, \quad t \longmapsto \sum_{n=0}^{\infty} a_n t^n.$$

A função \mathcal{A} admite derivadas de cada ordem em $\{x \mid |x| < R\}$ e, para cada $n \in \mathbb{N}$,

$$a_n = \frac{\mathcal{A}^{(n)}(0)}{n!}.$$

Exemplo 4.5.46. 1. O polinómio $a_0 + a_1 x + a_2 x^2 + \dots + a_k x^k$ define a função polinomial

$$\mathbb{R} \longrightarrow \mathbb{R}, \quad t \longmapsto a_0 + a_1 t + a_2 t^2 + \dots + a_k t^k.$$

2. A série (formal) $\mathcal{A} = \sum_{n=0}^{\infty} n! x^n$ tem o raio de convergência $R = 0$; por isso nem vale a pena considerar a função correspondente.
3. A série (formal) $\mathcal{A} = \sum_{n=0}^{\infty} 2^n x^n$ tem o raio de convergência $R = \frac{1}{2}$; portanto, a série

\mathcal{A} define a função

$$\mathcal{A}: \left] \frac{-1}{2}, \frac{1}{2} \right[\longrightarrow \mathbb{R}, \quad t \longmapsto \sum_{n=0}^{\infty} 2^n t^n = \frac{1}{1-2t}.$$

4. A série (formal) $\exp = \sum_{n=0}^{\infty} \frac{1}{n!} x^n$ tem o raio de convergência $R = \infty$; de facto, a série \exp define a função

$$\exp: \mathbb{R} \longrightarrow \mathbb{R}, \quad t \longmapsto \sum_{n=0}^{\infty} \frac{t^n}{n!} = e^t.$$

Nota 4.5.47. O cálculo com séries formais corresponde (numa certa forma) ao cálculo com funções (o que, por vezes, é mais conveniente). Mais concretamente:

- A série nula corresponde à função nula, a série «um» corresponde à função definida por $t \longmapsto 1$,
- A soma de séries corresponde à soma de funções,

$$(f + g)(t) = f(t) + g(t).$$

- A multiplicação por escalares de séries corresponde à multiplicação por escalares de funções,

$$(\alpha \cdot g)(t) = \alpha \cdot g(t).$$

- O produto de Cauchy de séries corresponde ao produto de funções.

$$(f \cdot g)(t) = f(t) \cdot g(t).$$

- A substituição de séries corresponde à composição de funções.

Exemplo 4.5.48. • Pelo Exemplo 4.5.11, a função geradora ordinária fib da sucessão dos números de Fibonacci $(F_n)_{n \in \mathbb{N}}$ (definida por $F_0 = 0$ e $F_1 = 1$ e $F_n = F_{n-1} + F_{n-2}$, $n \geq 2$) é dada por

$$\text{fib}(x) = \sum_{n=0}^{\infty} F_n x^n = \frac{x}{1-x-x^2}.$$

Como $\lim_{n \rightarrow \infty} \frac{f_{n+1}}{f_n} = \phi$ (o número de ouro), o raio de convergência é $R = \frac{1}{\phi}$.

- Seja $n \in \mathbb{N}$ e, para cada $k \in \mathbb{N}$, seja c_k o número de arranjos com repetição de n objetos k a k ; ou seja, $c_k = n^k$.

Então, a função geradora exponencial correspondente f é definida por

$$f(x) = \sum_{k=0}^{\infty} n^k \frac{x^k}{k!} = \sum_{k=0}^{\infty} \frac{(nx)^k}{k!} = e^{nx}.$$

Exemplo 4.5.49. Qual o número p_n de partições ordenadas (E_1, E_2) de $\{1, \dots, n\}$ em duas partes não-vazias?

Como se trata de objetos «distinguíveis», consideremos a correspondente série exponencial \mathcal{P} :

$$\mathcal{P} = \sum_{n=0}^{\infty} \frac{p_n}{n!} x^n = \left(\sum_{n=1}^{\infty} \frac{1}{n!} x^n \right) \cdot \left(\sum_{n=1}^{\infty} \frac{1}{n!} x^n \right) = (\exp - 1) \cdot (\exp - 1).$$

Logo,

$$\mathcal{P} = \exp(2x) - 2\exp + 1 = \sum_{n=0}^{\infty} \frac{2^n x^n}{n!} - 2 \sum_{n=0}^{\infty} \frac{x^n}{n!} + 1,$$

e por isso $p_0 = 0$ e, para $n \geq 1$, $p_n = 2^n - 2 = 2(2^{n-1} - 1)$.

Finalmente, o número de partições de $\{1, \dots, n\}$ em duas partes não-vazias é $2^{n-1} - 1$, para $n \geq 1$.

Exemplo 4.5.50. Determinarmos o número $a_{m,n}$ de funções sobrejetivas do tipo $\{1, \dots, m\} \rightarrow \{1, \dots, n\}$.

Fixamos $m \in \mathbb{N}$, e consideremos as seguintes questões sobre um conjunto X de n elementos:

1. **F:** funções $\{1, \dots, m\} \rightarrow X$,
2. **S:** funções sobrejetivas $\{1, \dots, m\} \rightarrow X$,
3. **U:** «fazer nada» (um elemento).

Então,

$$\mathbf{F} = \mathbf{S} * \mathbf{U}, \quad \text{logo} \quad \sum_{n=0}^{\infty} n^m \frac{x^n}{n!} = \left(\sum_{n=0}^{\infty} a_{m,n} \frac{x^n}{n!} \right) \exp$$

e por isso

$$\sum_{n=0}^{\infty} a_{m,n} \frac{x^n}{n!} = \left(\sum_{n=0}^{\infty} n^m \frac{x^n}{n!} \right) \exp(-x) = \left(\sum_{n=0}^{\infty} n^m \frac{x^n}{n!} \right) \left(\sum_{n=0}^{\infty} (-1)^n \frac{x^n}{n!} \right).$$

Consequentemente, para cada $n \in \mathbb{N}$,

$$a_{m,n} = \sum_{k=0}^n \binom{n}{k} (-1)^k (n-k)^m.$$

Nota 4.5.51 (O binomial generalizado). Recordamos que, para cada $m \in \mathbb{N}$:

$$(1+x)^m = \sum_{n=0}^m \binom{m}{n} x^n = (1+x)^m = \sum_{n=0}^{\infty} \binom{m}{n} x^n.$$

Consideremos agora o *coeficiente binomial generalizado*: para $r \in \mathbb{R}$ e $n \in \mathbb{N}$,

$$\binom{r}{n} = \frac{\overbrace{r(r-1)\dots(r-n+1)}^{n \text{ fatores}}}{n!}, \quad \text{em particular} \quad \binom{r}{0} = 1.$$

Pelos resultados do **Cálculo**, a série de Taylor da função f definida por $f(x) = (1+x)^r$ é dado por

$$\sum_{n=0}^{\infty} \binom{r}{n} x^n,$$

e esta série converge absolutamente em $] -1, 1[$ para $f(x)$. Sendo assim, *definimos a série formal de potências* $(1+x)^r$ (com $r \in \mathbb{R}$) por

$$(1+x)^r := \sum_{n=0}^{\infty} \binom{r}{n} x^n.$$

Ainda pelos resultados do **Cálculo**, verifica-se a igualdade

$$(1+x)^r \cdot (1+x)^s = (1+x)^{r+s}$$

para todos os x com $|x| < 1$, portanto, esta igualdade também é válida para as séries formais. Por exemplo, concluímos, para todos os $r, s \in \mathbb{R}$ e todo o $n \in \mathbb{N}$:

$$\binom{r+s}{n} = \sum_{k=0}^n \binom{r}{k} \binom{s}{n-k}.$$

4.5.6 Derivadas e Integrais

Definição 4.5.52. Seja $\mathcal{A} = \sum_{n=0}^{\infty} a_n x^n \in \mathbb{C}[[x]]$. Chamamos **derivada** de \mathcal{A} à série formal

$$\mathcal{A}' = a_1 + 2a_2x + 3a_3x^2 + \cdots = \sum_{n=0}^{\infty} (n+1)a_{n+1}x^n \in \mathbb{C}[[x]].$$

Analogamente, chamamos também **anti-derivada** (ou **integral**) de \mathcal{A} à série formal

$$\int \mathcal{A} = a_0x + \frac{a_1}{2}x^2 + \frac{a_2}{3}x^3 + \cdots = \sum_{n=0}^{\infty} \frac{a_n}{n+1}x^{n+1} \in \mathbb{C}[[x]].$$

Em corpos com característica nula (como é o caso de \mathbb{Q} , \mathbb{R} ou \mathbb{C}), as derivadas dão-nos uma forma altamente conveniente de extrair os coeficientes das séries formais. Para $\mathcal{A} = \sum_{n=0}^{\infty} a_n x^n \in \mathbb{C}[[x]]$, podemos vemos que $\mathcal{A}^{(0)}(0) = \mathcal{A}(0) = a_0$, $\mathcal{A}'(0) = a_1$, $\mathcal{A}''(0) = 2a_2$, ..., $\mathcal{A}^{(n)}(0) = n!a_n$. Desta forma, é ainda válido o Teorema de Taylor (mais precisamente, a série de MacLaurin):

$$\mathcal{A} = \sum_{n=0}^{\infty} \frac{\mathcal{A}^{(n)}(0)}{n!} x^n.$$

Nota 4.5.53. • As séries de potências formais \mathcal{A}' e $\int \mathcal{A}$ têm o mesmo raio de convergência que a série \mathcal{A} .

- Dentro do intervalo de convergência da série \mathcal{A} , a derivada (formal) e o integral (formal) correspondem às operações com as funções definidas pelas séries.

Mais concretamente, a função definida pela série formal \mathcal{A}' é a derivada da função definida pela série \mathcal{A} . Adicionalmente, para cada x dentro do intervalo de conver-

gência,

$$\left(\int \mathcal{A}\right)(x) = \int_0^x \mathcal{A}(t) dt.$$

Proposição 4.5.54. *Dadas $\mathcal{A}, \mathcal{B} \in \mathbb{C}[[x]]$ e uma sucessão $(\mathcal{A}_k)_{k \in \mathbb{N}}$ de séries formais que convergem para a série nula, temos que:*

1. $(\sum_k \mathcal{A}_k)' = \sum_k \mathcal{A}'_k$
2. $(\mathcal{A} \cdot \mathcal{B})' = \mathcal{A}' \cdot \mathcal{B} + \mathcal{A} \cdot \mathcal{B}'$
3. $(\prod_k (1 + \mathcal{A}_k))' = \prod_k (1 + \mathcal{A}_k) \sum_k \frac{\mathcal{A}'_k}{1 + \mathcal{A}_k}$
4. $\left(\frac{\mathcal{A}}{\mathcal{B}}\right)' = \frac{\mathcal{A}' \cdot \mathcal{B} - \mathcal{A} \cdot \mathcal{B}'}{\mathcal{B}^2}$
5. $(\mathcal{A}(\mathcal{B}))' = \mathcal{A}'(\mathcal{B}) \cdot \mathcal{B}'$
6. $\int(\sum_k \mathcal{A}_k) = \sum_k \int \mathcal{A}_k$
7. $(\int \mathcal{A})' = \mathcal{A}$.

Demonstração. 1. Temos que

$$\left(\sum_k \mathcal{A}_k\right)' = \left(\sum_{n=0}^{\infty} \sum_k a_{k,n} x^n\right)' = \sum_{n=0}^{\infty} \sum_k n a_{k,n} x^{n-1} = \sum_k \left(\sum_{n=0}^{\infty} n a_{k,n} x^{n-1}\right) = \sum_k \mathcal{A}'_k.$$

2. Podemos assumir, sem perda de generalidade, que $\mathcal{A} = x^\ell$ e $\mathcal{B} = x^k$. Então, pelo ponto anterior,

$$(\mathcal{A} \cdot \mathcal{B})' = (x^{\ell+k})' = (\ell + k)x^{\ell+k-1} = \ell x^{\ell-1} x^k + k x^{k-1} x^\ell = \mathcal{A}' \cdot \mathcal{B} + \mathcal{A} \cdot \mathcal{B}'.$$

3. Sem perda de generalidade, assumamos que $\mathcal{A}_k \neq -1$ para todo o $k \in \mathbb{N}$ (caso contrário, $1 - \mathcal{A}_k = 0$). Consideremos que, para um algum $N_0 \in \mathbb{N}$, $\|\mathcal{A}_k\| < 2^{-(N_0+1)}$, para todo o $k > n$. Então, o coeficiente de x^{N_0} em ambos os lados da equação depende apenas de $\mathcal{A}_1, \dots, \mathcal{A}_n$. Pelo ponto anterior, verificamos inductivamente que

$$\left(\prod_{k=1}^n (1 + \mathcal{A}_k)\right)' = \prod_{k=1}^n (1 + \mathcal{A}_k) \sum_{\ell=1}^n \frac{\mathcal{A}'_\ell}{1 + \mathcal{A}_\ell}$$

para todo o $n \in \mathbb{N}$. Ao fazer tender $N_0 \rightarrow \infty$, obtemos o pretendido.

4. Pelo ponto 2.,

$$\mathcal{A}' = \left(\frac{\mathcal{A}}{\mathcal{B}} \cdot \mathcal{B}\right)' = \left(\frac{\mathcal{A}}{\mathcal{B}}\right)' \cdot \mathcal{B} + \frac{\mathcal{A} \cdot \mathcal{B}'}{\mathcal{B}}.$$

5. Pelo ponto 3., sabemos é válida a regra de derivação da potência, $(\mathcal{A}^n)' = n\mathcal{A}^{n-1}\mathcal{A}'$ (para $n \in \mathbb{N}$). Desta forma, a derivada da soma implica que

$$(\mathcal{A}(\mathcal{B}))' = \left(\sum_{n=0}^{\infty} a_n \mathcal{B}^n\right)' = \sum_{n=0}^{\infty} a_n (\mathcal{B}^n)' = \sum_{n=1}^{\infty} n a_n \mathcal{B}^{n-1} \mathcal{B}' = \mathcal{A}'(\mathcal{B}) \cdot \mathcal{B}'.$$

6. Vejamos que

$$\begin{aligned} \int \left(\sum_k \mathcal{A}_k \right) &= \int \left(\sum_k \sum_{n=0}^{\infty} a_{k,n} x^n \right) = \int \left(\sum_{n=0}^{\infty} \sum_k a_{k,n} x^n \right) \\ &= \sum_{n=0}^{\infty} \sum_k \frac{a_{k,n}}{n+1} x^{n+1} = \sum_k \sum_{n=0}^{\infty} \frac{a_{k,n}}{n+1} x^{n+1} = \sum_k \left(\int \mathcal{A}_k \right). \end{aligned}$$

$$7. \left(\int \mathcal{A} \right)' = \left(\int \left(\sum_{n=0}^{\infty} a_n x^n \right) \right)' = \left(\sum_{n=0}^{\infty} \frac{a_n}{n+1} x^{n+1} \right)' = \left(\sum_{n=0}^{\infty} \frac{a_n}{n+1} x^{n+1} \right)' = \sum_{n=0}^{\infty} a_n x^n = \mathcal{A}.$$

◆

Nota 4.5.55. A regra de derivação do produto implica ainda a “trivial” derivada da multiplicação escalar, $(\lambda \mathcal{A})' = \lambda \mathcal{A}'$, assim como a conhecida regra de Leibniz

$$(\mathcal{A} \cdot \mathcal{B})^{(n)} = \sum_{k=0}^n \binom{n}{k} \mathcal{A}^{(k)} \cdot \mathcal{B}^{(n-k)},$$

para $\lambda \in \mathbb{C}$ e $\mathcal{A}, \mathcal{B} \in \mathbb{C}[[x]]$.

Exemplo 4.5.56. Vamos agora mostrar que, dadas $\mathcal{A}, \mathcal{B} \in \langle x \rangle$, com $\mathcal{B} \notin \langle x^2 \rangle$, é ainda válida a regra de L'Hôpital:

$$\frac{\mathcal{A}}{\mathcal{B}}(0) = \frac{\mathcal{A}'(0)}{\mathcal{B}'(0)}.$$

Porque $\mathcal{A}, \mathcal{B} \in \langle x \rangle$, é natural questionarmos a não invertibilidade de \mathcal{B} . Para tal, devemos recordar o segundo ponto da Nota 4.5.9:

“Para três séries formais $\mathcal{A}, \mathcal{B}, \mathcal{C} \in \mathbb{C}[[x]]$, é usual escrevermos $\mathcal{A} = \frac{\mathcal{B}}{\mathcal{C}}$ se $\mathcal{A}\mathcal{C} = \mathcal{B}$ (independentemente da invertibilidade de \mathcal{C}).”

Da Análise Real, sabemos então que as condições necessárias à aplicação da referida regra são:

- **Indeterminação na forma:** $\lim_{x \rightarrow a} f(x) = \lim_{x \rightarrow a} g(x) = 0$ ou $\pm\infty$.
- **Diferenciabilidade das funções:** $f(x)$ e $g(x)$ são diferenciáveis num aberto (excepto possivelmente no ponto a - ponto limite)
- **Derivada não nula no denominador:** $g'(x) \neq 0$ para todo o x num aberto (excepto possivelmente no ponto a)
- **Existência do limite do quociente das derivadas:** $\lim_{x \rightarrow a} \frac{f'(x)}{g'(x)}$ existe.

Desta forma, dado que $\mathcal{A}, \mathcal{B} \in \langle x \rangle$, sabemos que $\mathcal{A}(0) = a_0 = 0 = b_0 = \mathcal{B}(0)$ (pelo que existirá uma indeterminação na forma). Adicionalmente, sabemos que tanto \mathcal{A} como \mathcal{B} são

diferenciáveis e, porque $\mathcal{B} \notin \langle x^2 \rangle$, $b_1 \neq 0$ (o que garante derivada não nula no denominador da forma). Por último, conhecemos o limite do quociente das derivadas:

$$\frac{\mathcal{A}'(0)}{\mathcal{B}'(0)} = \frac{(\sum_{n=0}^{\infty} (n+1)a_{n+1}x^n)(0)}{(\sum_{n=0}^{\infty} (n+1)b_{n+1}x^n)(0)} = \frac{a_1}{b_1}.$$

No entanto, é ainda possível ver que

$$\begin{aligned}\mathcal{A} &= \sum_{n=0}^{\infty} a_n x^n = \sum_{n=1}^{\infty} a_n x^n = x \sum_{n=1}^{\infty} a_n x^{n-1} = x(a_1 + a_2 x + a_3 x^2 + \cdots), \\ \mathcal{B} &= \sum_{n=0}^{\infty} b_n x^n = \sum_{n=1}^{\infty} b_n x^n = x \sum_{n=1}^{\infty} b_n x^{n-1} = x(b_1 + b_2 x + b_3 x^2 + \cdots).\end{aligned}$$

Assim, e uma vez que $\mathcal{B} \notin \langle x^2 \rangle$, $b_1 \neq 0$, temos

$$\frac{\mathcal{A}}{\mathcal{B}}(0) = \frac{x \sum_{n=1}^{\infty} a_n x^{n-1}}{x \sum_{n=1}^{\infty} b_n x^{n-1}}(0) = \frac{a_1 + a_2 x + a_3 x^2 + \cdots}{b_1 + b_2 x + b_3 x^2 + \cdots}(0) = \frac{a_1}{b_1}.$$

Exemplo 4.5.57. Definimos o logarítmo formal através da **série de Mercator**

$$\log(1+x) := \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n} x^n = x - \frac{x^2}{2} + \frac{x^3}{3} \pm \cdots \in \mathbb{C}[[x]].$$

Pelo Teorema 4.5.30, $\mathcal{A} := \exp(x) - 1$ possui reversa e $\log(\exp(x)) = \log(1 + \mathcal{A})$. Dado que

$$\log(1+x)' = 1 - x + x^2 \pm \cdots = \sum_{n=0}^{\infty} (-1)x^n = \frac{1}{1+x},$$

a regra da cadeia leva-nos até

$$\log(1+\mathcal{A})' = \frac{\mathcal{A}'}{1+\mathcal{A}} = \frac{\exp(x)}{\exp(1)} = 1.$$

Tal mostra-nos que $\log(\exp(x)) = x$, pelo que se conclui que $\log(1+x)$ é a série reversa de $\mathcal{A} = \exp(x) - 1$ (conforme esperado). Adicionalmente, $\log(1-x) = -\sum_{n=1}^{\infty} \frac{x^n}{n}$.

Lema 4.5.58. Para uma qualquer sucessão $(\mathcal{A}_k)_{k \in \mathbb{N}}$ de séries formais em $\langle x \rangle$ que converge para a série nula, tem-se que

$$\log\left(\prod_k (1 + \mathcal{A}_k)\right) = \sum_k \log(1 + \mathcal{A}_k).$$

Demonstração.

$$\begin{aligned}\log\left(\prod_k (1 + \mathcal{A}_k)\right) &= \log\left(\prod_k \exp(\log(1 + \mathcal{A}_k))\right) \\ &= \log\left(\exp\left(\sum_k \log(1 + \mathcal{A}_k)\right)\right)\end{aligned}$$

$$= \sum_k \log(1 + \mathcal{A}_k).$$

◆

Exemplo 4.5.59. • $\sum_{n=0}^{\infty} nx^n = \sum_{n=1}^{\infty} nx^n = x \sum_{n=0}^{\infty} (n+1)x^n = x \left(\sum_{n=0}^{\infty} x^n \right)' = x \left(\frac{1}{1-x} \right)' = \frac{x}{(1-x)^2}.$

• Consideremos

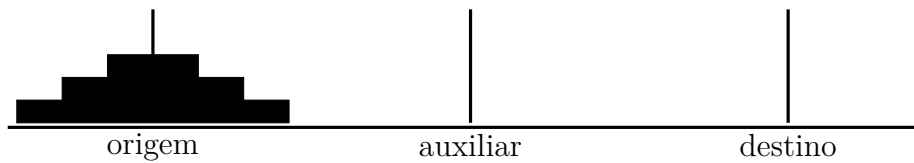
$$\mathcal{A} = \sum_{n=1}^{\infty} \frac{x^n}{n} = \int \left(\sum_{n=1}^{\infty} x^{n-1} \right) = \int \left(\sum_{n=0}^{\infty} x^n \right) = \int (1-x)^{-1}.$$

Portanto, a correspondente função é dada por, para $x \in]-1, 1[$,

$$\mathcal{A}(x) = \int_0^x \frac{1}{1-t} dt = -\ln(1-x).$$

4.5.7 Revisitar as Equações de Recorrência

Como introdução a esta secção, vamos revisitar o primeiro exemplo dado no capítulo (Torres de Hanói).



Recordamos que o número mínimo de passos necessários para transportar n discos do pino origem ao pino destino é dado pela equação

$$a_n = 2a_{n-1} + 1 \quad (\text{para } n \geq 2) \quad \text{e} \quad a_1 = 1. \quad (4.5.i)$$

Utilizando os métodos introduzidos anteriormente, consideremos primeiro a equação homogénea $a_n = 2a_{n-1}$, cuja solução geral é $(c \cdot 2^n)_{n \geq 1}$.

Também é possível verificar que a sucessão «constante» $(-1)_{n \geq 1}$ é uma solução de (4.5.i); desta forma, a solução geral de (4.5.i) é dada por $(c \cdot 2^n - 1)_{n \geq 1}$.

Por último, tendo em conta a condição inicial $a_1 = 1$, obtemos $1 = 2c - 1$, ou seja, $c = 1$. Assim, a solução é $a_n = 2^n - 1$. Agora utilizamos a série geradora ordinária $\mathcal{A} = \sum_{n=1}^{\infty} a_n x^n$.

$$\begin{aligned} \mathcal{A} &= \sum_{n=1}^{\infty} a_n x^n = a_1 x + \sum_{n=2}^{\infty} a_n x^n = x + \sum_{n=2}^{\infty} (2a_{n-1} + 1) x^n \\ &= x + \sum_{n=2}^{\infty} 2a_{n-1} x^n + \sum_{n=2}^{\infty} x^n = x + 2x \sum_{n=1}^{\infty} a_n x^n + x^2 \sum_{n=0}^{\infty} x^n \\ &= x + 2x\mathcal{A} + \frac{x^2}{1-x} = 2x\mathcal{A} + \frac{x}{1-x}. \end{aligned}$$

Portanto,

$$\mathcal{A} = \frac{x}{(1-x)(1-2x)} = \frac{1}{1-2x} - \frac{1}{1-x} = \left(\sum_{n=1}^{\infty} (2x)^n + 1 \right) - \left(\sum_{n=1}^{\infty} x^n + 1 \right) = \sum_{n=1}^{\infty} (2^n - 1)x^n,$$

e obtemos-se $a_n = 2^n - 1$.

Exemplo 4.5.60. Equação de recorrência: $a_n = a_{n-1} + 6a_{n-2}$ ($n \geq 2$), $a_0 = 3$, $a_1 = 4$.

$$\begin{aligned} \mathcal{A} &= \sum_{n=0}^{\infty} a_n x^n = a_0 + a_1 x + \sum_{n=2}^{\infty} a_n x^n \\ &= 3 + 4x + \sum_{n=2}^{\infty} a_{n-1} x^n + 6 \sum_{n=2}^{\infty} a_{n-2} x^n \\ &= 3 + 4x + x \sum_{n=2}^{\infty} a_{n-1} x^{n-1} + 6x^2 \sum_{n=2}^{\infty} a_{n-2} x^{n-2} \\ &= 3 + 4x + x \sum_{n=1}^{\infty} a_n x^n + 6x^2 \sum_{n=0}^{\infty} a_n x^n \\ &= 3 + 4x + x(\mathcal{A} - a_0) + 6x^2 \mathcal{A} \\ &= 3 + 4x + x(\mathcal{A} - 3) + 6x^2 \mathcal{A} \\ &= (6x^2 + x)\mathcal{A} + x + 3 \end{aligned}$$

logo,

$$\mathcal{A} = \frac{x+3}{-6x^2-x+1} = \frac{x+3}{(1-3x)(1+2x)}.$$

Procuramos agora a decomposição em «frações simples». Consideremos

$$\frac{x+3}{(1-3x)(1+2x)} = \frac{A}{1-3x} + \frac{B}{1+2x},$$

multiplicando ambos os lados por $(1-3x)$ obtemos

$$\frac{x+3}{1+2x} = A + \frac{B(1-3x)}{1+2x},$$

com $x = \frac{1}{3}$ obtemos $A = \frac{\frac{1}{3}+3}{1+\frac{2}{3}} = 2$. De forma semelhante obtém-se $B = 1$, por isso

$$\mathcal{A} = \frac{2}{1-3x} + \frac{1}{1+2x}.$$

Consequentemente,

$$\mathcal{A} = 2 \frac{1}{1-3x} + \frac{1}{1+2x} = 2 \sum_{n=0}^{\infty} 3^n x^n + \sum_{n=0}^{\infty} (-2)^n x^n$$

Assim, o coeficiente de x^n é $a_n = 2 \cdot 3^n + (-2)^n$.

Resumindo, para resolver uma equação de recorrência com séries geradoras devemos:

- Desenvolver a série ordinária $\mathcal{A} = \sum_{n=0}^{\infty} a_n x^n$ (ou a série exponencial $\mathcal{A} = \sum_{n=0}^{\infty} \frac{a_n}{n!} x^n$) utilizando a equação de recorrência e as condições iniciais.
- Obter tipicamente

$$\mathcal{A} = \frac{\text{polinómio 1}}{\text{polinómio 2}} = \frac{\text{polinómio 1}}{(1 - \lambda_1 x)^{n_1} \dots (1 - \lambda_k x)^{n_k}}.$$

- Escrever \mathcal{A} na forma

$$\mathcal{A} = \text{polinómio} + \left(\dots + \frac{\text{constante}}{1 - \lambda_i x} + \frac{\text{constante}}{(1 - \lambda_i x)^2} + \dots \right).$$

- Recordar (e utilizar) que

$$\frac{1}{(1 - \lambda x)^m} = \sum_{n=0}^{\infty} \binom{m+n-1}{m-1} \lambda^n x^n.$$

Exemplo 4.5.61. Vamos resolver o sistema de equações de recorrência

$$\left. \begin{aligned} a_n &= 2a_{n-1} + b_{n-1} + 1 \\ b_n &= a_{n-1} + 2b_{n-1} + 2^{n-1} \end{aligned} \right\} \quad (n \geq 1) \quad \text{e} \quad a_0 = b_0 = 0.$$

Com $\mathcal{A} = \sum_{n=0}^{\infty} a_n x^n$ e $\mathcal{B} = \sum_{n=0}^{\infty} b_n x^n$, obtemos:

$$\begin{aligned} \mathcal{A} &= \sum_{n=0}^{\infty} a_n x^n = a_0 + \sum_{n=1}^{\infty} a_n x^n \\ &= 0 + 2 \sum_{n=1}^{\infty} a_{n-1} x^n + \sum_{n=1}^{\infty} b_{n-1} x^n + \sum_{n=1}^{\infty} x^n \\ &= 2x \sum_{n=1}^{\infty} a_{n-1} x^{n-1} + x \sum_{n=1}^{\infty} b_{n-1} x^{n-1} + x \sum_{n=1}^{\infty} x^{n-1} \\ &= 2x\mathcal{A} + x\mathcal{B} + \frac{x}{1-x}. \end{aligned}$$

Portanto, $\mathcal{A} = 2x\mathcal{A} + x\mathcal{B} + \frac{x}{1-x}$.

Utilizando agora a segunda equação, obtém-se $\mathcal{B} = x\mathcal{A} + 2x\mathcal{B} + \frac{x}{1-2x}$. Assim, temos

$$\begin{aligned} (1-2x)\mathcal{A} - x\mathcal{B} &= \frac{x}{1-x}, \\ -x\mathcal{A} + (1-2x)\mathcal{B} &= \frac{x}{1-2x}; \end{aligned}$$

ou seja, na linguagem de matrizes:

$$\begin{bmatrix} (1-2x) & -x \\ -x & (1-2x) \end{bmatrix} \begin{bmatrix} \mathcal{A} \\ \mathcal{B} \end{bmatrix} = \begin{bmatrix} \frac{x}{1-x} \\ \frac{x}{1-2x} \end{bmatrix}.$$

Agora precisamos de alguma paciência ... utilizamos a **regra de Cramer**, por isso precisamos:

$$\begin{vmatrix} (1-2x) & -x \\ -x & (1-2x) \end{vmatrix} = (1-2x)^2 - x^2 = (1-x)(1-3x),$$

$$\begin{vmatrix} \frac{x}{1-x} & -x \\ \frac{x}{1-2x} & (1-2x) \end{vmatrix} = \frac{x(1-2x)}{1-x} + \frac{x^2}{1-2x} = \frac{x-3x^2+3x^3}{(1-x)(1-2x)},$$

$$\begin{vmatrix} (1-2x) & \frac{x}{1-x} \\ -x & \frac{x}{1-2x} \end{vmatrix} = x + \frac{x^2}{1-x} = \frac{x}{1-x}.$$

Portanto:

$$\mathcal{A} = \frac{x-3x^2+3x^3}{(1-x)^2(1-2x)(1-3x)}, \quad \mathcal{B} = \frac{x}{(1-x)^2(1-3x)}.$$

Agora calculamos:

$$\begin{aligned} \mathcal{B} &= \frac{x}{(1-x)^2(1-3x)} \\ &= \frac{A}{1-x} + \frac{B}{(1-x)^2} + \frac{C}{1-3x} \\ &= -\frac{1}{4} \frac{1}{1-x} - \frac{1}{2} \frac{1}{(1-x)^2} + \frac{3}{4} \frac{1}{1-3x} \\ &= -\frac{1}{4} \sum_{n=0}^{\infty} x^n - \frac{1}{2} \sum_{n=0}^{\infty} \binom{n+1}{1} x^n + \frac{3}{4} \sum_{n=0}^{\infty} 3^n x^n. \end{aligned}$$

Conclusão:

$$(b_n)_{n \in \mathbb{N}} = \left(-\frac{1}{4} - \frac{1}{2}(n+1) + \frac{3}{4}3^n \right)_{n \in \mathbb{N}}.$$

Para \mathcal{A} , obtemos semelhantemente:

$$\begin{aligned} \mathcal{A} &= \frac{x-3x^2+3x^3}{(1-x)^2(1-2x)(1-3x)} \\ &= \frac{A}{1-x} + \frac{B}{(1-x)^2} + \frac{C}{1-2x} + \frac{D}{1-3x} \\ &= -\frac{1}{4} \frac{1}{1-x} + \frac{1}{2} \frac{1}{(1-x)^2} - \frac{1}{1-2x} + \frac{3}{4} \frac{1}{1-3x} \\ &= -\frac{1}{4} \sum_{n=0}^{\infty} x^n + \frac{1}{2} \sum_{n=0}^{\infty} \binom{n+1}{1} x^n - \sum_{n=0}^{\infty} (2x)^n + \frac{3}{4} \sum_{n=0}^{\infty} (3x)^n. \end{aligned}$$

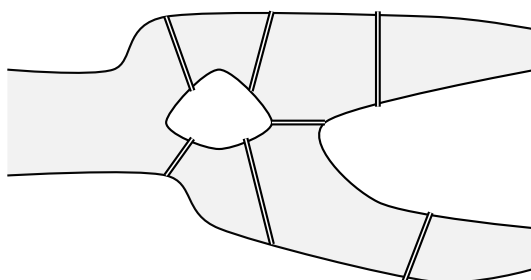
Conclusão:

$$(a_n)_{n \in \mathbb{N}} = \left(-\frac{1}{4} + \frac{1}{2}(n+1) - 2^n + \frac{3}{4}3^n \right)_{n \in \mathbb{N}}.$$

Elementos da Teoria dos Grafos

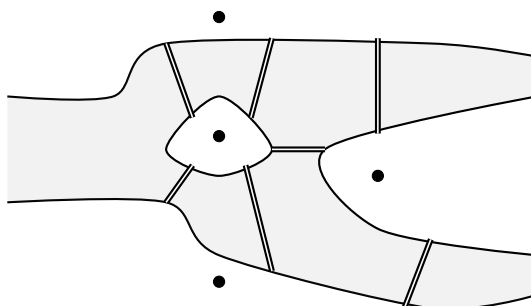
Introdução

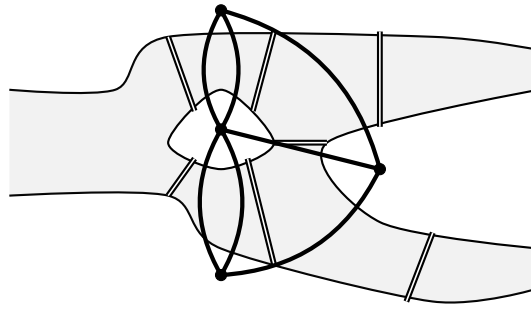
No século XVIII, a cidade de Königsberg (actualmente Kaliningrado), no reino da Prússia, ficava localizada em ambas as margens do rio Pregel e incluía duas grandes ilhas (Kneiphof e Lomse). A conexão a Kneiphof e Lomse - quer entre si, quer às margens do rio - era feita por sete pontes, conforme indicado na figura abaixo.



Em 1736, Euler interrogou-se sobre se seria possível caminhar pela cidade, começando e terminando na mesma margem/ilha, de modo que atravessássemos cada ponte exactamente uma vez.

Do ponto de vista da Teoria dos Grafos, se associarmos a cada margem/ilha um vértice e a cada ponte uma aresta, acabamos por obter um grafo conexo conforme ilustrado seguidamente.





Mais tarde viria a concluir-se que facto do grafo associado a este problema não ser euleriano (i.e., não admitir nenhum circuito de Euler - caminho que começa e termina no mesmo vértice e percorre cada aresta do grafo apenas uma vez) responde à questão posta inicialmente.

Teorema 5.0.1 (Euler). *Um grafo conexo admite um circuito de Euler se e só se os seus vértices tiverem grau par.*

Mal saberia Euler que a Matemática dos séculos seguintes seria altamente influenciada por esta “inocente” situação relativa às pontes de Königsberg. De facto, este pensamento culminou no artigo “*Solutio Problematis ad Geometriam Situs Pertinentis*”, escrito pelo próprio Euler em 1736 e considerado hoje como o primeiro artigo na história da Teoria dos Grafos. Este, em conjunto com o escrito por Vandermonde em 1774, “*Remarques sur les Problèmes de Situation*”, sobre o Problema do Movimento dos Cavalos (relacionado com o movimento destas peças num tabuleiro de xadrez), deram continuação ao *Analysis Situs* de Leibniz.

De notar que o desenvolvimento da Teoria dos Grafos serviu também de base ao surgimento de outros importantes ramos da Matemática. A título de exemplo, a fórmula de Euler para poliedros convexos (que relaciona o número de arestas, vértices e faces) foi estudada e generalizada por Cauchy e L’Huillier, dando início a um dos mais conhecidos ramos da ciência rainha: a Topologia.

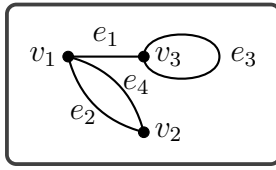
5.1 Conceitos Fundamentais

Definição 5.1.1. Designamos por **grafo (não orientado)** um terno $G = (V, E, \psi)$, onde:

- V é um conjunto (diremos que os elementos de V são **vértices**),
- E é um conjunto (diremos que os elementos de E são **arestas**),
- ψ é uma função (de facto, **função de incidência**)

$$\psi: E \longrightarrow \{A \subseteq V \mid 1 \leq |A| \leq 2\}.$$

Se $\psi(e) = \{u, v\}$, u e v dizem-se os **pontos extremos** da aresta e .

Exemplo 5.1.2.

$$V = \{v_1, v_2, v_3\}, \quad E = \{e_1, e_2, e_3, e_4\},$$

$$\psi(e_1) = \{v_1, v_3\}, \quad \psi(e_2) = \{v_1, v_2\}, \quad \psi(e_3) = \{v_3\},$$

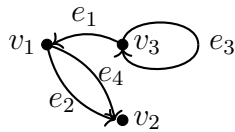
$$\psi(e_4) = \{v_1, v_2\} = \{v_2, v_1\}.$$

Definição 5.1.3. Designa-se por **grafo orientado** (ou **digrafo**) um terno $\vec{G} = (V, E, \psi)$ onde

- V é um conjunto (diremos que os elementos de V são **vértices**),
- E é um conjunto (diremos que os elementos de E são **arcos**),
- ψ é uma função (**função de incidência** do grafo)

$$\psi: E \longrightarrow V \times V.$$

Se $\psi(e) = (u, v)$, u diz-se **cauda** de e e v **cabeça** de e .

Exemplo 5.1.4.

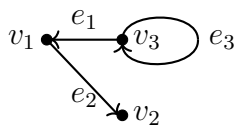
$$V = \{v_1, v_2, v_3\}, \quad E = \{e_1, e_2, e_3, e_4\},$$

$$\psi(e_1) = (3, 1), \quad \psi(e_2) = (1, 2), \quad \psi(e_3) = (3, 3), \quad \psi(e_4) = (2, 3).$$

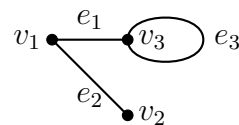
A cada grafo orientado $\vec{G} = (V, E, \psi)$ podemos associar um grafo não orientado $G = (V, E, \hat{\psi})$ onde

$$\hat{\psi}(e) = \{u, v\} \quad \text{precisamente quando} \quad \psi(e) = (u, v) \quad \text{ou} \quad \psi(e) = (v, u)$$

(ou seja, esquecemos a direcção dos arcos). Desde modo, os vários conceitos relativos aos grafos aplicam-se igualmente aos digrafos.

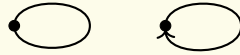
Exemplo 5.1.5.

\mapsto



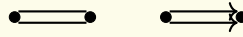
Definição 5.1.6. Consideremos um grafo $G = (V, E, \psi)$, resp., um digrafo $\vec{G} = (V, E, \psi)$.

- Uma aresta (um arco) com os pontos extremos iguais diz-se **lacete**.



- Arestas com os mesmos vértices extremos designam-se por **arestas paralelas**, e arcos com a mesma cauda e a mesma cabeça designam-se por **arcos paralelos**.

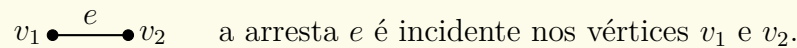
– paralelas:



– não paralelas:



- G (respetivamente \vec{G}) diz-se **simples** quando não contém arestas (arcos) paralelas(os) nem lacetes.
- Uma aresta (um arco) diz-se **incidente** nos seus vértices extremos.



- Os vértices v_1 e v_2 dizem-se **adjacentes** se existir uma aresta (um arco) com pontos extremos v_1 e v_2 .



- Arestas (arcos) incidentes num mesmo vértice dizem-se **adjacentes**.



Definição 5.1.7. Um grafo $G = (V, E, \psi)$ respetivamente digrafo $\vec{G} = (V, E, \psi)$ diz-se **finito** quando os conjuntos V e E são finitos.

Exemplo 5.1.8. Designa-se por **grafo trivial** um grafo simples com um único vértice, ou seja, tal que $|V| = 1$ e $E = \emptyset$.

Nota 5.1.9. No que se segue, consideremos tipicamente grafos finitos.

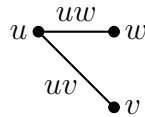
Definição 5.1.10. Seja $G = (V, E, \psi)$ um grafo finito.

- **ordem de G :** $\nu(G) = |V|$ (o número de vértices).
- **dimensão de G :** $\varepsilon(G) = |E|$ (o número de arestas).

(e de igual forma para digrafos.)

Recordemos que um grafo (respectivamente digrafo) diz-se **simples** quando não contém arestas (arcos) paralelas(os) nem lacetes. (Di)Grafos não simples denota-se também por **multi(di)grafo**.

Nota 5.1.11. Num grafo (respectivamente digrafo) simples, cada aresta (arco) a é completamente determinada(o) pelos vértices extremos u e v (cauda u e cabeça v). Neste caso escrevemos da forma mais sugestivo uv em lugar de a .

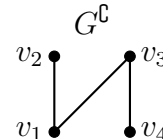
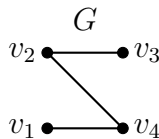


Com esta notação, o (di)grafo (V, E, ψ) é completamente determinado por (V, E) (ou seja, podemos «dispensar» ψ).

Definição 5.1.12. Seja $G = (V, E)$ um grafo simples. O **grafo complementar** de G é o grafo $G^c = (V, E^c)$ com o mesmo conjunto de vértices e com

$$uv \in E^c \iff uv \notin E.$$

Exemplo 5.1.13.



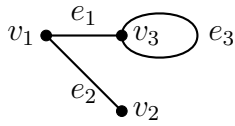
Nota 5.1.14. O operador \bullet^c é involutório (tem ordem 2), i.e., $(\bullet^c)^c = \bullet$. Desta forma, para qualquer grafo G , $(G^c)^c = G$.

5.2 Vizinhanças e Graus

Definição 5.2.1. • Seja $G = (V, E, \psi)$ um grafo e $v \in V$.

O conjunto de todos os vértices adjacentes a v designa-se por **vizinhança** de v e denota-se por $\mathcal{N}_G(v)$ (ou simplesmente $\mathcal{N}(v)$).

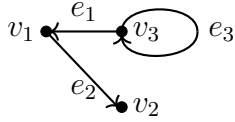
- Seja $\vec{G} = (V, E, \psi)$ um digrafo e $v \in V$. A **vizinhança de entrada** de v é o conjunto $\mathcal{N}^-(v)$ de todos os vértices u tal que existe um $e \in E$ com $\psi(e) = (u, v)$, e a **vizinhança de saída** de v é o conjunto $\mathcal{N}^+(v)$ de todos os vértices u tal que existe um $e \in E$ com $\psi(e) = (v, u)$.

Exemplo 5.2.2.

$$\mathcal{N}(v_1) = \{v_2, v_3\},$$

$$\mathcal{N}(v_2) = \{v_1\},$$

$$\mathcal{N}(v_3) = \{v_1, v_3\}.$$



$$\mathcal{N}^-(v_1) = \{v_3\}, \quad \mathcal{N}^+(v_1) = \{v_2\}, \quad \mathcal{N}(v_1) = \{v_2, v_3\},$$

$$\mathcal{N}^-(v_2) = \{v_1\}, \quad \mathcal{N}^+(v_2) = \emptyset, \quad \mathcal{N}(v_2) = \{v_1\},$$

$$\mathcal{N}^-(v_3) = \{v_3\}, \quad \mathcal{N}^+(v_3) = \{v_1, v_3\}, \quad \mathcal{N}(v_3) = \{v_1, v_3\}.$$

Definição 5.2.3. Seja $G = (V, E, \psi)$ um grafo finito com $V \neq \emptyset$.

- Seja $v \in V$. O **grau** de v é o número $d(v)$ de arestas incidentes em v (onde cada lacete conta duas vezes).
- O **maior grau dos vértices** do grafo G denota-se por $\Delta(G)$:

$$\Delta(G) := \max\{d(v) \mid v \in V\}.$$

- O **menor grau dos vértices** do grafo G denota-se por $\delta(G)$:

$$\delta(G) := \min\{d(v) \mid v \in V\}.$$

Nota 5.2.4. No caso de um digrafo $\vec{G} = (V, E, \psi)$, consideremos ainda

- o **semigrau de entrada**: $d^-(v) = |\{e : \exists u \in V, \psi(e) = (u, v)\}|$.

Ou seja, $d^-(v)$ é o número de arcos com «cabeça em v ».

- o **semigrau de saída**: $d^+(v) = |\{e : \exists u \in V, \psi(e) = (v, u)\}|$.

Ou seja, $d^+(v)$ é o número de arcos com «cauda em v ».

- $d(v) = d^-(v) + d^+(v)$.

Exemplo 5.2.5. O Sr. e a Sra. Silva convidaram quatro casais para jantar em casa. Alguns são amigos do Sr. Silva e outros amigos da Sra. Silva. Em casa do casal Silva os convidados que já se conheciam cumprimentaram-se com um aperto de mão e os restantes apenas se saudaram.

Depois de todos terem chegado o Sr. Silva observou:

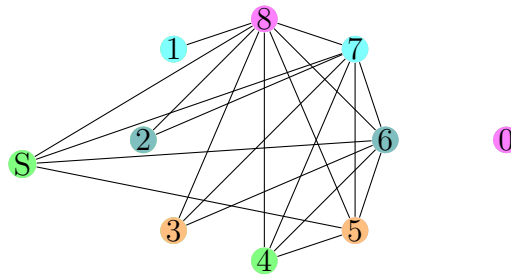
“se me excluir a mim, todos deram um número diferente de apertos de mão”

Quantos apertos de mão deu o Sr. Silva?

É claro que os membros de um mesmo casal não se cumprimentaram um ao outro, pelo que o número de cumprimentos variou entre 0 e 8.

Por outro lado, uma vez que, excluindo o Sr. Silva, todas as restantes 9 pessoas deram um número diferente de apertos de mão, podemos atribuir a cada uma delas exactamente um índice j entre 0 e 8 que corresponde ao número de apertos de mão que deu.

Utilizando o seguinte grafo:



Portanto:

- O vértice n_0 tem grau $d(n_0) = 0$; portanto, nenhuma aresta pode ter um extremo em n_0 .
- Uma vez que o n_8 deu 8 apertos de mão, ele apertou a mão a toda a gente, com exceção dele(a) próprio(a) e da mulher/do marido ... logo, n_0 e n_8 são casados.

Já temos $d(n_0) = 0$, $d(n_8) = 8$ e $d(n_1) = 1$, pelo que não pode haver mais arestas com extremos nestes vértices.

- Por sua vez, n_7 só não apertou a mão a ele próprio, a n_0 e n_1 (uma vez que este último só deu um aperto de mão e foi a n_8).

Logo, n_7 e n_1 são casados e já temos $d(n_2) = 2$.

- Por sua vez, n_6 só não deu apertos de mão a si próprio, a n_0 , n_1 e n_2 (note-se que este último deu um aperto de mão a n_8 e n_7).

Logo, n_2 e n_6 são casados e já temos $d(n_3) = 3$.

- O n_5 apertou a mão de n_8 , n_7 , n_6 , n_4 e ao Sr. Silva e, conseqüentemente, é casado com n_3 .

Assim, n_4 é a Sra. Silva (que, naturalmente, não deu um aperto de mão ao Sr. Silva) e ficam determinados todos os apertos de mão.

\therefore O Sr. Silva apertou a mão a n_8 , n_7 , n_6 e n_5 .

Definição 5.2.6. Seja $G = (V, E, \psi)$ um grafo (finito). A **matriz de incidência** (aresta-vértice) de G é a matriz do tipo $\nu \times \varepsilon$ definida por

$$V \times E \longrightarrow \mathbb{R}, \quad (v, e) \longmapsto \begin{cases} 0 & \text{se } v \notin \psi(e), \\ 1 & \text{se } \psi(e) = \{u, v\} \text{ com } u \neq v, \\ 2 & \text{se } \psi(e) = \{v\}. \end{cases}$$

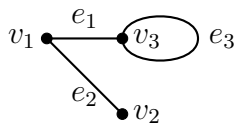
Nota 5.2.7. Para cada $a \in E$, a soma sobre todos os elementos da «coluna e » é 2. Para cada $v \in V$, a soma sobre todos os elementos da «linha v » é o grau de v .

Seja $\vec{G} = (V, E, \psi)$ um digrafo (finito) sem lacetes. A **matriz de incidência** (aresta-vértice) de \vec{G} é a matriz do tipo $\nu \times \varepsilon$ definida por

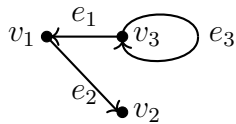
$$V \times E \longrightarrow \mathbb{R}, \quad (v, e) \longmapsto \begin{cases} -1 & \text{se existe } u \in V \text{ com } (u, v) = \psi(e), \\ 1 & \text{se existe } u \in V \text{ com } (v, u) = \psi(e), \\ 0 & \text{nos outros casos.} \end{cases}$$

Nota 5.2.8. Para cada $e \in E$, a soma sobre todos os elementos da «coluna e » é 0. Para cada $v \in V$, a soma sobre todos os elementos da «linha v » é igual a $d^+(v) - d^-(v)$.

Exemplo 5.2.9.



	e_1	e_2	e_3
v_1	1	1	0
v_2	0	1	0
v_3	1	0	2



	e_1	e_2	e_3
v_1	-1	1	0
v_2	0	-1	0
v_3	1	0	0

Teorema 5.2.10. Para todo o grafo $G = (V, E, \psi)$ finito, a soma dos graus dos seus vértices é igual ao dobro do número de arestas, i.e.,

$$\sum_{v \in V} d(v) = 2|E|.$$

Demonstração. Somamos de duas maneiras diferentes as entradas da matriz de incidência de G :

- Para cada «linha v », a soma das entradas desta linha é igual ao $d(v)$. Portanto, a soma de todas as entradas da matriz de incidência é igual à $\sum_{v \in V} d(v)$.
- Para cada «coluna e », a soma das entradas desta coluna é igual à 2. Portanto, a soma de todas as entradas da matriz de incidência é igual à $2|E|$. ♦

Corolário 5.2.11. *O número de vértices de grau ímpar é par.*

Teorema 5.2.12. *Para todo o digrafo $\vec{G} = (V, E, \psi)$ finito,*

$$\sum_{v \in V} d^+(v) = \sum_{v \in V} d^-(v) = |E|.$$

Definição 5.2.13. • Seja $G = (V, E, \psi)$ um grafo (finito). A **matriz de adjacência** de G é a matriz do tipo $\nu \times \nu$ com entrada (u, v) igual a **número de arestas entre u e v (cada lacete conta duas vezes)**., ou seja,

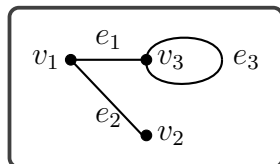
$$V \times V \mapsto \mathbb{R}, \quad (u, v) \mapsto \begin{cases} |\{a \in E \mid \psi(a) = \{u, v\}\}| & \text{se } u \neq v; \\ 2|\{a \in E \mid \psi(a) = \{u, u\}\}| & \text{se } u = v. \end{cases}$$

Nota: Esta matriz é simétrica e a soma sobre os elementos da coluna u (ou linha u) é igual ao grau de u .

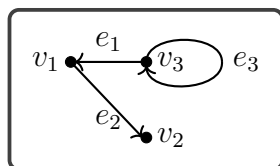
- Seja $\vec{G} = (V, E, \psi)$ um digrafo (finito). A **matriz de adjacência** de \vec{G} é a matriz do tipo $\nu \times \nu$ definida pela aplicação

$$V \times V \mapsto \mathbb{R}, \quad (u, v) \mapsto |\{a \in E : \psi(a) = (u, v)\}|.$$

Exemplo 5.2.14.



	v_1	v_2	v_3
v_1	0	1	1
v_2	1	0	0
v_3	1	0	2



	v_1	v_2	v_3
v_1	0	1	0
v_2	0	0	0
v_3	1	0	1

5.3 Homomorfismos, Isomorfismos e Sub-Grafos

Definição 5.3.1. Sejam $G = (V_G, E_G, \psi_G)$ e $H = (V_H, E_H, \psi_H)$ dois grafos. Um **homomorfismo** de G em H é um par $f: V_G \rightarrow V_H$ e $h: E_G \rightarrow E_H$ de funções tais que, para todos os $e \in E_G$ e $u, v \in V_G$,

$$(\psi_G(e) = \{u, v\}) \implies (\psi_H(h(e)) = \{f(u), f(v)\}).$$

(No caso dos digrafos, escrevemos (u, v) em lugar de $\{u, v\}$.)

Nota 5.3.2. Caso exista um homomorfismo $G \rightarrow H$, dizemos que G é **homomorfo** a H , ou ainda que G é **H -colorável**.

Exemplo 5.3.3. • Para cada grafo $G = (V, E, \psi)$, as identidades $\text{id}_V: V \rightarrow V$ e $\text{id}_E: E \rightarrow E$ definem um homomorfismo de G em G .

- As compostas de homomorfismos são homomorfismos.

Nota 5.3.4. No caso de grafos simples, e denotando as arestas da forma « uv », a função h acima é completamente determinada por f :

$$h(uv) = f(u)f(v).$$

Portanto, um homomorfismo entre grafos simples (V_G, E_G) e (V_H, E_H) é dado por uma função $f: V_G \rightarrow V_H$ tal que, para todos os $u, v \in V_G$:

$$uv \in E_G \implies f(u)f(v) \in E_H.$$

Definição 5.3.5. Dizemos que um homomorfismo de G para H é **injectivo** (i.e., nunca transforma dois vértices distintos de G num mesmo vértice de H) se e só se G for um sub-grafo de H .

Definição 5.3.6. Um homomorfismo de G em H é um **isomorfismo** de G em H se tem um homomorfismo de grafos inverso.

Nota 5.3.7. De acordo com o escrito imediatamente acima, um isomorfismo de G em H é um par (f, h) funções bijetivas onde $f: V_G \rightarrow V_H$, $h: E_G \rightarrow E_H$, de tal forma que, para todos os $e \in E_G$ e $u, v \in V_G$,

$$(\psi_G(e) = \{u, v\}) \iff (\psi_H(h(e)) = \{f(u), f(v)\}).$$

Um isomorfismo entre grafos simples (V_G, E_G) e (V_H, E_H) é dado por uma função bijetiva $f: V_G \rightarrow V_H$ tal que, para todos os $u, v \in V_G$:

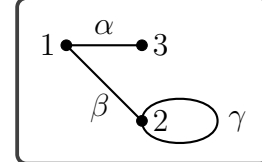
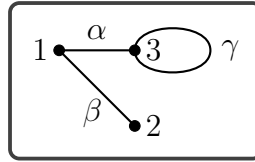
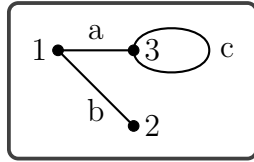
$$uv \in E_G \iff f(u)f(v) \in E_H.$$

Exemplo 5.3.8. • Para cada grafo $G = (V, E, \psi)$, as identidades $\text{id}_V: V \rightarrow V$ e $\text{id}_E: E \rightarrow E$ definem um isomorfismo de G em G .

- Para cada isomorfismo de G em H , as funções $f^{-1}: V_H \rightarrow V_G$ e $h^{-1}: E_H \rightarrow E_G$ definem um isomorfismo de H em G .
- As compostas de isomorfismos são isomorfismos.

Definição 5.3.9. (Di)grafos dizem-se **isomorfos** quando existe um isomorfismo entre eles.

Nota 5.3.10. Intuitivamente, grafos isomorfos são «iguais a menos da etiquetação dos vértices e aresta».



Nota 5.3.11. Grafos isomorfos tem «as mesmas propriedades de grafos».

Mais concretamente, sendo o par $f: V_G \rightarrow V_H$ e $h: E_G \rightarrow E_H$ um isomorfismo entre os grafos $G = (V_G, E_G, \psi_G)$ e $H = (V_H, E_H, \psi_H)$ (finitos). Então:

- Os grafos têm a mesma ordem e a mesma dimensão:

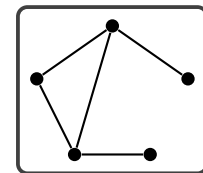
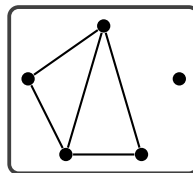
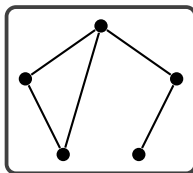
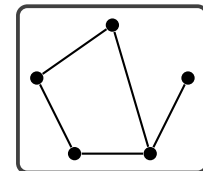
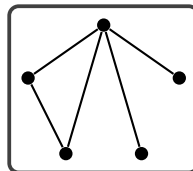
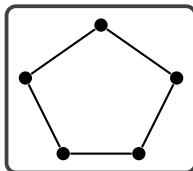
$$\nu(G) = \nu(H) \quad \text{e} \quad \varepsilon(G) = \varepsilon(H).$$

- G é simples se e só se H é simples.
- Vértices correspondentes têm o mesmo grau:

$$\text{para cada } v \in V_G, d_G(v) = d_H(\varphi(v)).$$

- Portanto: $\Delta(G) = \Delta(H)$ e $\delta(G) = \delta(H)$.

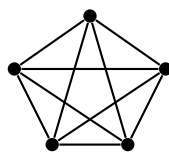
Exemplo 5.3.12. Representação gráfica de todos os grafos simples não isomorfos, com 5 vértices e 5 arestas:



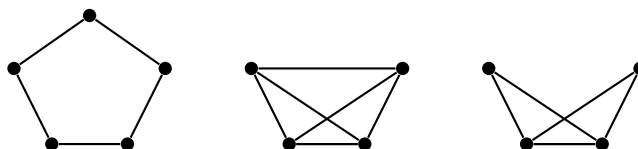
Definição 5.3.13. Sejam $G = (V_G, E_G, \psi_G)$ e $H = (V_H, E_H, \psi_H)$ grafos. O grafo H diz-se **sub-grafo** de G quando $V_H \subseteq V_G$, $E_H \subseteq E_G$, e ψ_H é a restrição de ψ_G ao conjunto E_H . Neste caso, dizemos também que G é um **super-grafo** de H .

Nota 5.3.14. Cada grafo é sub-grafo de si próprio. Se H é um sub-grafo de G e $H \neq G$, então dizemos que H é um **sub-grafo próprio** de G .

Exemplo 5.3.15. Consideremos o seguinte grafo G :



Alguns sub-grafos de G :



Definição 5.3.16. Um sub-grafo $H = (V_H, E_H, \psi_H)$ de $G = (V_G, E_G, \psi_G)$ diz-se **abran-
gente** quando $V_H = V_G$.

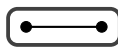
Definição 5.3.17. Seja $G = (V, E, \psi)$ um grafo e sejam $\hat{V} \subseteq V$ e $\hat{E} \subseteq E$.

- O **sub-grafo** $G[\hat{V}]$ de G **induzido por** \hat{V} é o grafo cujo conjunto de vértices é \hat{V} e cujo conjunto de arestas é o conjunto das arestas de G com extremos em \hat{V} .
- O **sub-grafo** $G[\hat{E}]$ de G **induzido por** \hat{E} é o grafo cujo conjunto de arestas é \hat{E} e cujo conjunto de vértices é constituído pelos vértices extremos das arestas de \hat{E} .

Nota 5.3.18. Tem-se que $G = G[V]$ mas, em geral, $G[E] \neq G$. Para perceber tal questão, atentemos no seguinte grafo G :



Aqui, $G[E]$ é o grafo



De facto, $G[E] = G$ se e só se G não possuir vértices isolados.

- Por definição, $G[V - \hat{V}]$ é o sub-grafo gerado pelo complemento de \hat{V} , e escrevemos simplesmente $G - \hat{V}$. Adicionalmente, se $\hat{V} = \{v\}$, escrevemos simplesmente $G - v$.
- Denotamos por $G - \hat{E}$ o sub-grafo **abran-
gente** cujo conjunto de arestas é $E - \hat{E}$. Caso $\hat{E} = \{e\}$, escrevemos simplesmente $G - e$.

Atenção: Em geral $G[E - \hat{E}]$ e $G - \hat{E}$ são distintos.

5.4 Alguns conceitos métricos

Durante este capítulo preocupamo-nos várias vezes com questões de conexidade e de distância entre os vértices de um grafo, ou seja, questões como «Será possível caminhar de u para v ?», e, se sim, «Qual é o caminho mais curto/rápido/barato?». Para tratar estas questões, começamos com os seguintes conceitos.

Definição 5.4.1. Seja $G = (V, E, \psi)$ um grafo. Um **passeio** em G é uma sequência finita

$$P = (v_0, e_1, v_1, e_2, \dots, e_k, v_k)$$

onde $v_0, v_1, \dots, v_k \in V$, $e_1, e_2, \dots, e_k \in E$ e, para cada $i = 1, 2, \dots, k$, $\psi(e_i) = v_{i-1}v_i$. Neste caso diz-se que P é um passeio entre os vértices v_0 e v_k . O vértice v_0 designa-se por **vértice inicial** do passeio P e v_k designa-se por **vértice final** do passeio P . Os vértices v_1, \dots, v_{k-1} designam-se por **vértices intermédios**.

Nota 5.4.2. Num grafo simples, um passeio é determinado pela sequência dos sucessivos vértices; isto é, basta considerar

$$P = (v_0, v_1, \dots, v_k).$$

Definição 5.4.3. Seja G um grafo.

- Um **trajeto** em G é um passeio sem arestas repetidas.
- Um trajeto em G diz-se **fechado** quando tem pelo menos uma aresta e o vértice inicial coincide com o vértice final ($v_0 = v_k$). Um trajeto fechado diz-se também **circuito**.
- Um **caminho** em G é um trajeto em G que não repete vértices.
- Um **ciclo** P em G é um circuito com pelo menos uma aresta onde o vértice inicial e os vértices intermédios são diferentes dois a dois, ou seja, $P = (v_0, e_1, v_1, e_2, v_2, \dots, v_{k-1}, e_k, v_k)$ é um circuito tal que $(v_1, e_2, v_2, \dots, v_{k-1})$ é um caminho.

Nota 5.4.4. Um passeio P em G é um ciclo se e somente se

1. P é um lacete $P = (v_0, e, v_0)$, ou
2. $P = (v_0, a, v_1, b, v_0)$ com $v_0 \neq v_1$ e $a \neq b$, ou
3. $P = (v_0, e_1, v_1, e_2, v_2, \dots, e_k, v_k, e_{k+1}, v_0)$ é um passeio com $k \geq 2$ e $(v_0, e_1, v_1, e_2, v_2, \dots, e_k, v_k)$ é um caminho.

Portanto, num grafo simples, um ciclo tem pelo menos três vértices.

Definição 5.4.5. Sejam G um grafo e $P = (v_0, e_1, v_1, e_2, \dots, e_k, v_k)$ um passeio de G . Então, o **comprimento** de P , denotado por $\text{comp}(P)$, é definido por

$$\text{comp}(P) = k;$$

ou seja, $\text{comp}(P)$ é o número de arestas (com eventual repetição) que o constitui.

Nota 5.4.6. No caso dos caminhos e dos trajetos, o comprimento coincide com o número de arestas.

Exemplo 5.4.7. Uma aresta com pontos extremos diferentes é um caminho de comprimento 1 e um vértice é um caminho de comprimento 0.

Agora podemos introduzir o conceito de distância entre vértices de um grafo.

Definição 5.4.8. Seja $G = (V, E, \psi)$ um grafo. Para $x, y \in V$, consideremos o conjunto

$$\mathcal{P}_{x,y} = \{\text{os caminhos entre } x \text{ e } y\}.$$

Designa-se por **distância** entre vértices de G a função

$$\begin{aligned} \text{dist}: V \times V &\longrightarrow \{0, 1, \dots, \nu(G), \infty\} \\ (x, y) &\longmapsto \begin{cases} \min\{\text{comp}(P) \mid P \in \mathcal{P}_{x,y}\} & \text{se } \mathcal{P}_{x,y} \neq \emptyset, \\ \infty & \text{se } \mathcal{P}_{x,y} = \emptyset. \end{cases} \end{aligned}$$

Nota 5.4.9. Na definição de distância acima podia-se igualmente usar passeios em lugar de caminhos porque um passeio de comprimento mínimo é necessariamente um caminho.

Nota 5.4.10. A função de distância introduzida na Definição 5.4.8 tem as propriedades esperadas:

$$\text{dist}(x, x) = 0, \quad \text{dist}(x, y) + \text{dist}(y, z) \geq \text{dist}(x, z),$$

e $\text{dist}(x, y) = \text{dist}(y, x)$, para todos os $x, y, z \in V$.

O seguinte resultado afirma a existência de certos caminhos/ciclos «compridos» num grafo finito.

Teorema 5.4.11. *Seja G um grafo simples finito.*

- G contém um caminho P tal que $\text{comp}(P) \geq \delta(G)$.
- Se $\delta(G) \geq 2$, então G contém um ciclo C tal que $\text{comp}(C) \geq \delta(G) + 1$.

Demonstração. Como G é finito, só há um número finito de caminhos em G . Seja $P = (v_0, v_1, \dots, v_k)$ um caminho de maior comprimento em G . Portanto, todos os vizinhos de

v_k pertencem ao caminho porque, se não, podia-se prolongar o caminho. Portanto,

$$\text{comp}(P) \geq d(v_k) \geq \delta(G).$$

Seja $i = \min\{j \mid v_j v_k \in E\}$. Então, $C = (v_i, v_{i+1}, \dots, v_k, v_i)$ é um ciclo (note-se que $(v_i, v_{i+1}, \dots, v_k)$ tem pelo menos três vertices porque $d(v_k) \geq 2$) de comprimento $d(v_k) + 1 \geq \delta(G) + 1$. \blacklozenge

Definição 5.4.12. Seja $G = (V, E, \psi)$ um grafo finito com $V \neq \emptyset$.

- A **cintura** $g(G)$ de G é o comprimento de um ciclo de menor comprimento em G se existe pelo menos um ciclo em G ; caso contrario $g(G) = \infty$.
- Seja $v \in V$. A maior distância entre v e todos os vértices de G designa-se por **excentricidade** de v e denota-se por $e(v)$, isto é,

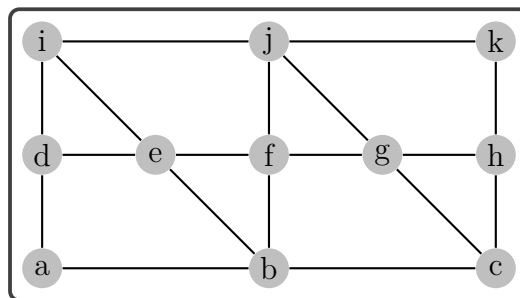
$$e(v) = \max_{u \in V} \text{dist}(u, v).$$

- A maior excentricidade dos seus vértices designa-se por **diâmetro** de G e denota-se por $\text{diam}(G)$.

Nota: $\text{diam}(G) = \max_{x,y \in X} \text{dist}(x, y)$.

- A menor excentricidade dos vértices de G designa-se por **raio** e denota-se por $r(G)$.
- Um vértice v diz-se **central** quando $e(v) = r(G)$. O conjunto dos vértices centrais designa-se por **centro** do grafo.

Exemplo 5.4.13. Considere o seguinte grafo G .



1. Determine a cintura do grafo G .
2. Determine a excentricidade dos vértices de G .
3. Determine o raio e o diâmetro de G .
4. Determine o centro de G .

Exemplo 5.4.14. Seja $G = (V, E, \psi)$ um grafo finito com $V \neq \emptyset$. Então,

$$r(G) \leq \text{diam}(G) \leq 2r(G).$$

Recordamos que:

- $r(G) = \min_{x \in V} \max_{y \in V} \text{dist}(x, y)$.
- $\text{diam}(G) = \max_{x, y \in V} \text{dist}(x, y)$.
- $\text{dist}(x, y) = \text{comprimento do menor caminho entre } x \text{ e } y \text{ (ou } \infty)$.

Logo, $r(G) \leq \text{diam}(G)$.

Caso 1: Suponhamos que existem $x, y \in V$ com $\text{dist}(x, y) = \infty$. Então, para todo $z \in V$, $\text{dist}(z, x) = \infty$ ou $\text{dist}(z, y) = \infty$ e por isso $r(G) = \infty$ e $\text{diam}(G) = \infty$.

Caso 2: Suponhamos que $\text{dist}(x, y) < \infty$, para todos os $x, y \in V$. Sejam x, y vértices com a maior distância $\text{dist}(x, y) = \text{diam}(G)$ e seja z um vértice central (ou seja, $e(z) = r(G)$). Portanto:

$$\text{diam}(G) = \text{dist}(x, y) \leq \text{dist}(x, z) + \text{dist}(z, y) \leq 2e(z) = 2r(G).$$

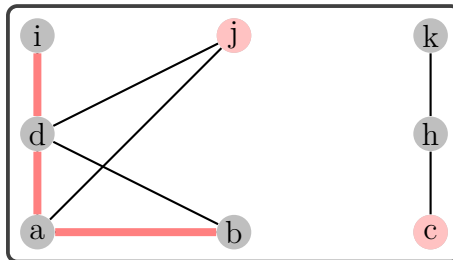
5.5 Conexidade

Definição 5.5.1. Seja G um grafo. Os vértices u e v de G dizem-se **conexos** quando existe um caminho entre eles em G . O grafo G diz-se **conexo** quando G tem pelo menos um vértice e todos os seus vértices são conexos.

Um grafo não conexo diz-se **desconexo**.

Nota 5.5.2. De forma semelhante ao que foi dito na Nota 5.4.9, os vértices u e v são conexos se e só se existe um passeio em G entre eles.

Exemplo 5.5.3. No grafo seguinte, os vértices i e b são conexos, mas os vértices j e c não são conexos.



Nota 5.5.4. Intuitivamente, um grafo conexo deve ter «um número suficiente» de arestas para ligar todos os vértices; ou, por outras palavras, não pode ter vértices a mais. De facto,

como verificaremos mais adiante num contexto ligeiramente mais geral (ver o Lema 5.5.9), num grafo finito conexo verifica-se a fórmula $\nu(G) \leq \varepsilon(G) + 1$.

Nota 5.5.5. A **relação de conexidade** num grafo $G = (V, W, \psi)$ definida por

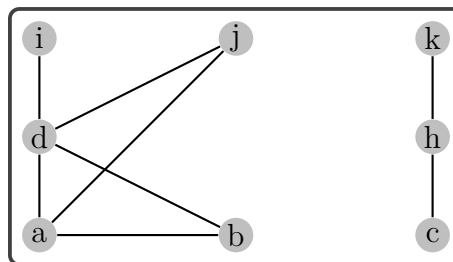
$$u \sim v \text{ quando } u \text{ e } v \text{ são conexos}$$

é uma relação de equivalência em V . Isto é, para todos os vértices u, v, w ,

- $u \sim u$;
- se $u \sim v$, então $v \sim u$;
- se $u \sim v$ e $v \sim w$, então $u \sim w$.

Definição 5.5.6. Os subgrafos induzidos pelas classes de equivalência da relação de conexidade dizem-se **componentes conexas**. O número de componentes conexas de G denota-se por $cc(G)$.

Exemplo 5.5.7. O grafo G representada pela seguinte figura tem duas componentes conexas, ou seja, $cc(G) = 2$.



Nota 5.5.8. • Um grafo G é conexo se e só se $cc(G) = 1$.

- As componentes conexas de um grafo são precisamente os subgrafos (induzidos) conexos *maximais*.

Lema 5.5.9. Para cada grafo finito G ,

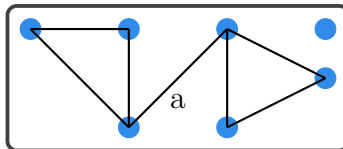
$$\nu(G) \leq \varepsilon(G) + cc(G).$$

Demonstração. Provamos esta afirmação utilizando indução sobre o número m de arestas de G . Se o grafo G tem zero arestas, então $\nu(G) = cc(G)$. Seja agora $m > 0$, e suponhamos que a afirmação é verdadeira para cada grafo com menos do que m arestas. Escolhemos uma aresta a de G ; por hipótese, $\nu(G - a) \leq \varepsilon(G - a) + cc(G - a)$. Portanto:

$$\nu(G) = \nu(G - a) \leq \varepsilon(G - a) + cc(G - a) \leq \varepsilon(G) - 1 + cc(G) + 1 = \varepsilon(G) + cc(G). \quad \blacklozenge$$

Definição 5.5.10. Uma aresta a de um grafo G diz-se **ponte** (ou uma **aresta de corte**) de G quando os pontos extremos de a são desconexos em $G - a$.

Exemplo 5.5.11. No grafo seguinte, a aresta a é uma ponte.

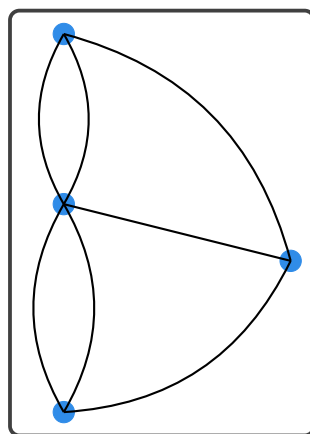


Portanto, uma aresta a de G com pontos extremos u e v é uma ponte precisamente quando a é a «única ligação» entre u e v , ou seja, se e só se a componente conexa de u e v em G , com a aresta a removida, é um subgrafo desconexo de $G - a$. Portanto, num grafo finito G , uma aresta a de G é uma ponte se e só se $cc(G - a) > cc(G)$, mais concretamente, se e só se $cc(G - a) = cc(G) + 1$. O seguinte resultado fornece mais uma descrição de uma aresta de corte.

Teorema 5.5.12. Uma aresta a de um grafo G é uma ponte se e só se a não pertence a nenhum ciclo de G .

Demonstração. Sejam u e v os pontos extremos da aresta a de G . Se existia um caminho u, e_1, \dots, e_k, v entre u e v em $G - a$, então $u, e_1, \dots, e_k, v, a, u$ é um ciclo em G . Por outro lado, se u, a, v, e, \dots, u é um ciclo em G , então v, e, \dots, u é um caminho entre v e u em $G - a$, logo, u e v são conexos em $G - a$. ♦

Com o conhecimento adquirido até este momento, podemos resolver agora o problema das pontes de Königsberg: será possível caminhar pela esta cidade, começando e terminando na mesma margem/ilha, de modo que atravessássemos cada ponte exatamente uma vez? Recordamos que a informação essencial do plano da cidade reduz-se ao grafo seguinte,



e, utilizando a linguagem de grafos, a questão é se este grafo admite um circuito que envolve todas as arestas.

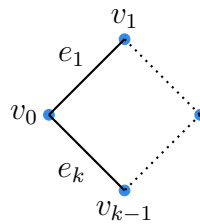
Definição 5.5.13. Seja G um grafo finito. Um circuito em G diz-se **circuito de Euler** quando contém todas as arestas de G .

O seguinte teorema dá-nos um critério útil para resolver o problema das pontes de Königsberg.

Teorema 5.5.14. *Seja G um grafo finito e conexo. Então, G tem um circuito de Euler se e só se todos os vértices de G tem grau par.*

Demonstração. Para simplificar a apresentação do argumento, tiramos primeiro todas as lacetes de G . Notamos que isto não altera a paridade do grau dos vértices de G , nem a propriedade de ter um circuito de Euler.

Suponha que G tem um circuito de Euler $C = (v_0, e_1, v_1, \dots, e_k, v_0)$.

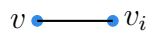


Seja v um vértice de G . Em cada ocorrência de v em C encontramos duas arestas com um ponto extremo em v . Como C tem cada aresta de G precisamente uma vez, deduzimos que o grau de v é par.

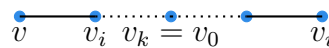
Suponha agora que todos os vértices de G tem grau par. Seja P



um trajeto de maior comprimento em G . Logo, P contém todas as arestas com um vértice em v_k porque, no caso contrário, se podia prolongar o trajeto P . Logo, como $d(v_k)$ é par, $v_0 = v_k$. Suponha que existe uma aresta fora de P ; neste caso existe uma aresta

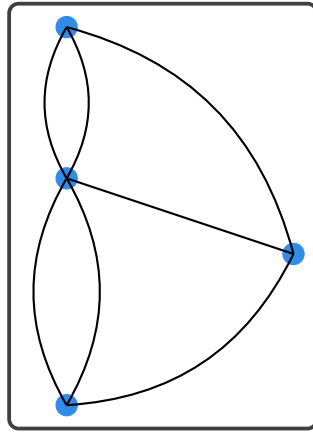


fora de P com v_i em P . Então,



é um trajeto de comprimento maior que o comprimento de P , uma contradição. ◆

Exemplo 5.5.15. No grafo



que representa o plano da cidade de Königsberg, os vértices tem grau 3, 5, 3 e 3, respetivamente. Logo, não existe um circuito de Euler.

Sabendo agora que um tal passeio não existe, pode-se ainda perguntar se seria possível passar exatamente uma vez por todas as pontes, possivelmente acabar o passeio numa outra margem ou ilha. No entanto, a resposta é a mesma, como se pode verificar com métodos muito semelhantes.

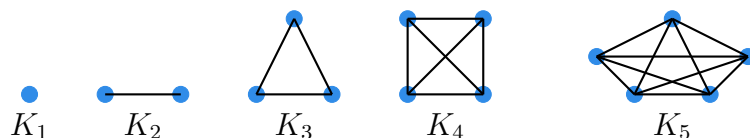
Definição 5.5.16. Seja G um grafo finito. Um trajeto em G diz-se **trajeto de Euler** quando contém todas as arestas de G .

Teorema 5.5.17. *Seja G um grafo finito e conexo. Então, G tem um trajeto de Euler se e só se o número de vértices de grau ímpar é 0 ou 2.*

5.6 Grafos particulares

Definição 5.6.1. Um grafo simples G diz-se **completo** quando todos os pares de vértices diferentes são adjacentes. Um grafo G diz-se **nulo** quando não tem arestas.

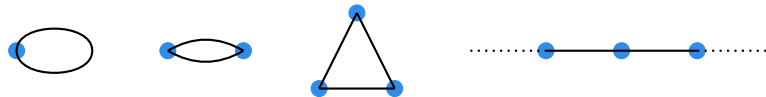
Nota 5.6.2. • A menos de isomorfismo, existe um único grafo completo de ordem $n \in \mathbb{N}$. Denota-se este grafo por K_n , e tem-se $e(K_n) = \binom{n}{2}$.



- Cada grafo nulo é simples, de facto, os grafos nulos são precisamente os grafos complementares dos grafos completos. Portanto, denotamos o grafo nulo com n vértices por K_n^c .

Definição 5.6.3. Seja $k \in \mathbb{N}$. Um grafo G diz-se **k -regular** quando todos os seus vértices têm grau k . Um grafo G diz-se **regular** quando G é k -regular para algum $k \in \mathbb{N}$.

Exemplo 5.6.4 (Grafos 2-regulares).



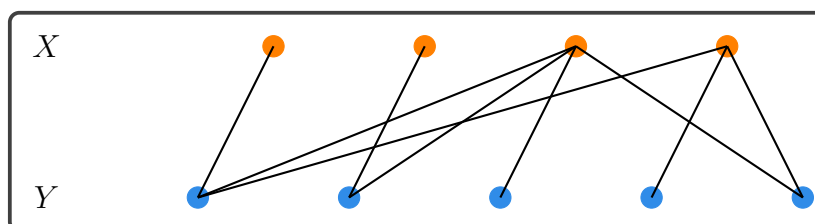
Nota 5.6.5. • Os grafos 3-regulares designam-se também por grafos cúbicos.

- O grafo K_n é $(n-1)$ -regular. De facto, um grafo simples G com n vértices é $(n-1)$ -regular se e só se G é completo.
- Um grafo G é 0-regular se e só se G é um grafo nulo.

Definição 5.6.6. Um grafo $G = (V, E, \psi)$ diz-se **bipartido** quando existem subconjuntos $X, Y \subseteq V$ de V com $V = X \cup Y$ e $X \cap Y = \emptyset$ tais que os grafos $G[X]$ e $G[Y]$ são nulos. O par (X, Y) designa-se por **bipartição dos vértices**. Neste caso denota-se G por (X, Y, E, ψ) (ou simplesmente (X, Y, E) se G é simples).

Nota 5.6.7. Num grafo bipartido, não existem arestas entre qualquer par de vértices de X nem entre qualquer par de vértices de Y ; ou seja, cada aresta de G tem um extremo em X e outro em Y .

Exemplo 5.6.8. A seguir apresentamos um grafo bipartido.



Teorema 5.6.9. Um grafo G é bipartido se e só se G não tem ciclos de comprimento ímpar.

Demonstração. Suponha primeiro que G é bipartido, com as partes X e Y . Seja

$$P: \begin{array}{c} e_1 \\ v_0 \text{---} v_1 \text{---} \dots \text{---} v_{k-1} \text{---} v_k = v_0 \\ e_k \end{array}$$

um ciclo em G . Sem perda de generalidade, suponhamos que $v_0 \in X$. Então, $v_1 \in Y, v_2 \in X, \dots, v_{k-1} \in Y$ e $v_k \in X$. Portanto, há um número ímpar de vértices em P e por isso um número par de arestas.

Suponha agora que $G = (V, E, \psi)$ não tem ciclos de comprimento ímpar. Suponhamos que G é conexo; se for desconexo, pode-se tratar cada componente conexa separadamente. Seja $x_0 \in V$. Consideremos $V = X \cup Y$, $X \cap Y = \emptyset$ dada por

$$X = \{x \in V \mid \text{dist}(x, x_0) \text{ é par}\}, \quad Y = \{y \in V \mid \text{dist}(y, x_0) \text{ é ímpar}\}.$$

Suponhamos que existem $x, x' \in X$ adjacentes, com a aresta $a \in E$. Sejam

$$P: \quad x_0 \text{ --- } \cdots \text{ --- } x \quad \quad P': \quad x_0 \text{ --- } \cdots \text{ --- } x'$$

caminhos de menor comprimento entre x_0 e x e entre x_0 e x' , respetivamente. Como $x, x' \in X$, estes caminhos tem necessariamente um comprimento de valor par. Portanto,

$$x_0 \text{ --- } \cdots \text{ --- } x' \xrightarrow{a} x \text{ --- } \cdots \text{ --- } x_0$$

é um passeio fechado de comprimento ímpar. Seja z o último vértice comum de P e de P' . A parte (x_0, \dots, z) , tanto em P como em P' , é um caminho de menor comprimento entre x_0 e z , logo estas partes têm o mesmo comprimento.

$$x_0 \text{ --- } \cdots \text{ --- } z \xrightarrow{a} x' \text{ --- } \cdots \text{ --- } z \text{ --- } \cdots \text{ --- } x_0$$

Portanto, $(z, \dots, x, a, x', \dots, z)$ é um ciclo de comprimento ímpar em G , uma contradição. Do mesmo modo justifique-se que nenhuma aresta de G tem ambos os pontos extremos em Y . Logo G é bipartido. \blacklozenge

5.7 Problemas de caminho de custo mínimo em grafos

Nesta secção consideremos o problema de encontrar, por exemplo, a melhor ligação entre duas cidades ou duas casas como, por exemplo, na Figura 5.1. Para descrever o problema matematicamente, é útil representar o mapa por um grafo, onde os vértices representam cruzamentos e as arestas representam estradas. No entanto, falta ainda a informação sobre o comprimento das estradas, ou o tempo (médio) da viagem numa estrada, ou outra informação, depende das preferências. Estas considerações motivam a seguinte definição.

Definição 5.7.1. Um **grafo com custos não negativos nas arestas** $G = (V, E, W)$ é dado por um grafos simples (V, E) e uma **matriz de custos**

$$W: V \times V \longrightarrow [0, \infty]$$

tais que, $W(u, v) = W(v, u)$, $W(u, u) = 0$ e, para todos os $u \neq v \in V$, $W(u, v) = \infty$ se $uv \notin E$.

Para um caminho $P = (v_0, v_1, \dots, v_k)$ em G , o **custo de P** é

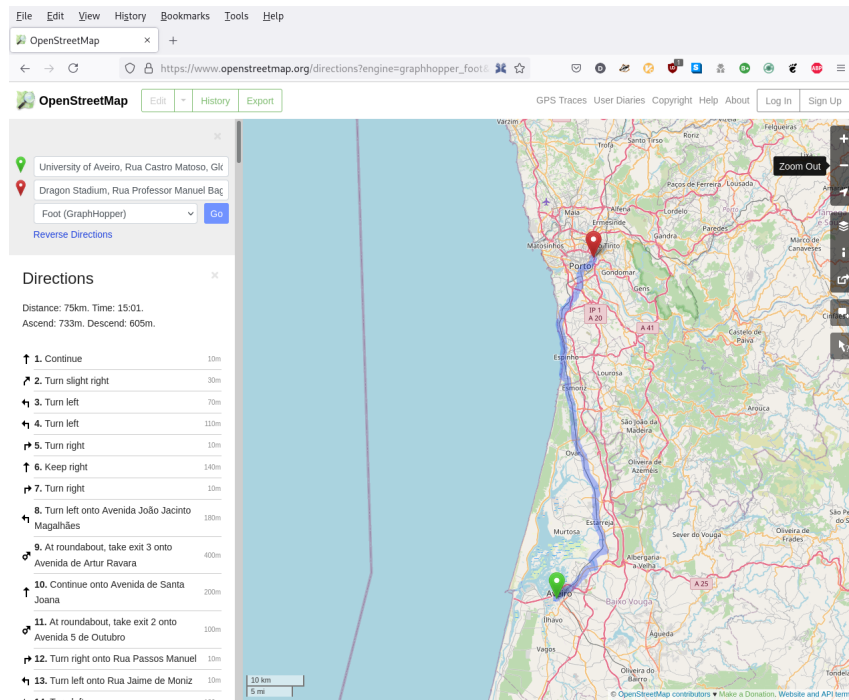


Figura 5.1: Caminho entre Aveiro e Porto

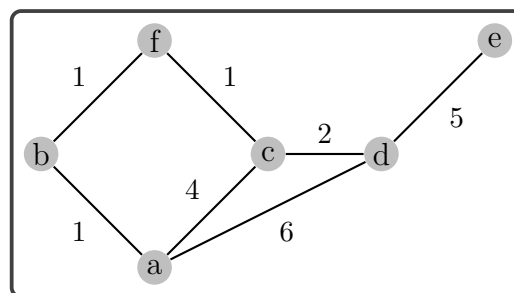
$$W(P) = \sum_{i=0}^{k-1} W(v_i, v_{i+1})$$

(onde $\alpha + \infty = \infty = \infty + \alpha$).

Nota 5.7.2. Como $W(u, u) = 0$, $W(u, v) = W(v, u)$ e $W(u, v) = \infty$ se $uv \notin E$ e $u \neq v$, em lugar de $W: V \times V \rightarrow [0, \infty]$ pode-se equivalentemente considerar uma função $W: E \rightarrow [0, \infty]$.

Nota 5.7.3. No que se segue, não é necessário distinguir entre «as arestas não existentes» (recordamos que $W(u, v) = \infty$ se $uv \notin E$) e as arestas uv em G com $W(u, v) = \infty$. Sendo assim, podemos dispensar E e apenas considerar o par $G = (V, W)$.

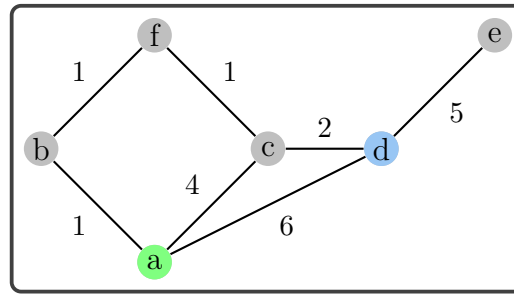
Exemplo 5.7.4. A seguir apresentamos uma representação gráfica de um grafo com custos não negativos nas arestas.



Dada um grafo (V, W) com custos não negativos nas arestas e dois vértices, o nosso objetivo é encontrar *um caminho de menor custo* entre estes dois vértices. Apresentamos a solução

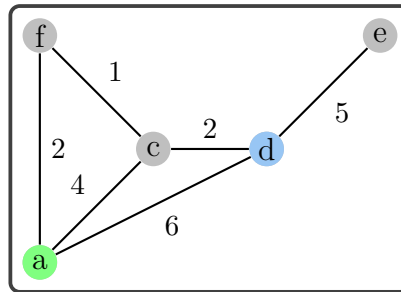
proposta pelo cientista da computação holandês Edsger Wybe Dijkstra em 1956, conhecido como *o algoritmo de Dijkstra*. Notamos primeiro que, se $(v_0, v_1, \dots, v_{k-1}, v_k)$ é um caminho de menor custo entre os vértices v_0 e v_k , então $(v_0, v_1, \dots, v_{k-1})$ é um caminho de menor custo entre v_0 e v_{k-1} ; ou seja, o algoritmo tem de encontrar também o caminho de menor custo entre v_0 e os vértices intermédios. De facto, a partir do vértice inicial, o algoritmo procura o caminho de menor custo para (todos) os outros vértices do grafo, e termina quando o caminho de menor custo para o vértice terminal é conhecido. Para explicar melhor a ideia, apresentamos primeiro um exemplo simples.

Exemplo 5.7.5. Consideremos o grafo G com custos não negativos nas arestas representada na seguinte figura, com o vértice inicial a e o vértice terminal d .



G

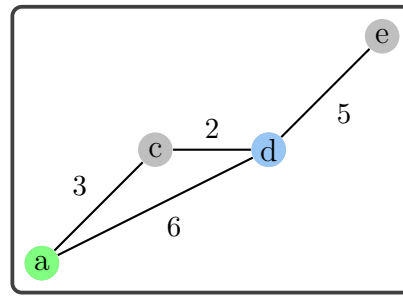
Neste caso não é difícil de ver que o caminho de menor custo entre a e d é (a, b, f, c, d) ; no entanto, tentamos agora encontrar este caminho de forma sistemática. Consideremos primeiro todos os vizinhos do vértice inicial a : passar de a para b tem custo 1, de a para c tem custo 4 e de a para d tem custo 6. Portanto, sabemos que (a, b) é o caminho de menor custo entre a e b , com custo 1, porque todos os outros caminhos a partir de a tem custo pelo menos 1, de facto, neste caso maior do que 1. Também concluímos que (a, b, f) é o caminho de menor custo entre a e f em G com o *penúltimo vértice* b , e este caminho tem custo 2. Consequentemente, podemos dispensar o vértice b e considerar o grafo com custos não negativos nas arestas G_1 representado na seguinte figura.



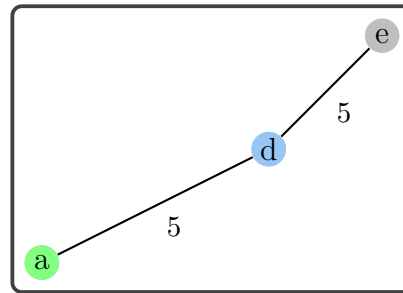
G_1

Agora repetimos o argumento. O vértice f é o vizinho de a de menor custo em G_1 , portanto, (a, f) é o caminho de menor custo entre a e f em G , com custo 2. Além disso, (a, f, c) é o caminho de menor custo com o *penúltimo vértice* f entre a e c em G_1 , com custo 3. Tal

como no passo anterior, podemos dispensar o vértice f e passar para o grafo com custos não negativos nas arestas G_2 representado na seguinte figura.

 G_2

De mesmo modo, c é o vizinho de menor custo de a em G_2 , portanto, (a, b, f, c) é o caminho de menor custo entre a e c , e (a, b, f, c, d) é o caminho com o penúltimo vértice c de menor custo entre a e d , com custo 5. Apagando c , consideremos

 G_3

Neste grafo, d é o único vizinho de a , portanto (a, d) é o caminho de menor custo entre a e d em G_3 . Logo, (a, b, f, c, d) é o caminho de menor custo em G entre a e d , com custo 5.

Nota 5.7.6. No exemplo acima, em cada passo houve um *único* vizinho de menor custo e portanto encontramos o caminho de menor custo entre a e d . No entanto, em geral pode haver vários caminhos entre o vértice inicial e o vértice terminal com custos iguais. No desenvolvimento do algoritmo, se num dos passos existem vizinhos com custos iguais, escolhe-se um destes.

Formulamos agora o algoritmo de Dijkstra detalhadamente. A partir do vértice inicial, descobre-se sucessivamente um caminho mais curto entre este vértice e certos vértices do grafo. Para organizar a informação pertinente, vamos utilizar as seguintes variáveis:

- **start** = o vértice inicial.
- Para cada vértice v :
 - **marca**(v) = o custo do caminho de menor custo, obtido até o momento, entre **start** e v .

- $\text{ant}(v)$ = o antecessor de $v \neq \text{start}$ no caminho de menor custo, obtido até o momento, entre start e v .
- temp = a lista dos vértices com valores temporários, ou seja os vértices para os quais ainda não se conhece um caminho de menor custo.
- menor = o vértice com o caminho de menor custo, neste momento, a partir do vértice start .

A seguir descrevemos o desenvolvimento do algoritmo de Dijkstra.

Algoritmo: O algoritmo de Dijkstra

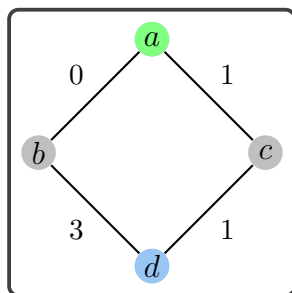
Entrada: Um grafo $G = (V, W)$ com custos nas arestas, um vértice inicial start e um vértice terminal end ;

Resultado: Um caminho de menor custo entre start e end em G ;

```

1  marca(start) = 0;
2  ant(start) = -;                                /* start não tem antecessor */
3  temp =  $V \setminus \{\text{start}\}$ ;
4  para todo  $v \in \text{temp}$  faça
5      |  marca( $v$ ) =  $\infty$ ;
6      |  ant( $v$ ) = -;                                /* Ainda não tem antecessor */
7  fim
8  menor = start;
9  repita
10     |   $c_{\text{aux}} = \infty$ ;
11     |  para todo  $v \in \text{temp}$  faça
12         |  se marca( $v$ ) > marca(menor) +  $W(\text{menor}, v)$  então
13             |  marca( $v$ ) = marca(menor) +  $W(\text{menor}, v)$ ;
14             |  ant( $v$ ) = menor;
15         |  fim
16         |  se marca( $v$ ) <  $c_{\text{aux}}$  então
17             |   $c_{\text{aux}} = \text{marca}(v)$ ;
18             |   $v_{\text{aux}} = v$ ;
19         |  fim
20     |  fim
21     |  temp = temp  $\setminus \{v_{\text{aux}}\}$ ;
22     |  menor =  $v_{\text{aux}}$ ;
23 até menor = end;
```

Exemplo 5.7.7. No grafo



com custos nas arestas, procuramos o caminho de menor custo entre o vértice **start** = a e o vértice **end** = d . Organizamos os passos do algoritmo nas linhas da seguinte tabela onde, para cada vértice v , indicamos o par $(\text{marca}(v), \text{ant}(v))$.

a	b	c	d	menor	temp
$(0, -)$	$(\infty, -)$	$(\infty, -)$	$(\infty, -)$	a	$\{b, c, d\}$
	$(0, a)$	$(1, a)$	$(\infty, -)$	b	$\{c, d\}$
		$(1, a)$	$(3, b)$	c	$\{d\}$
			$(2, c)$	d	\emptyset

Portanto, concluímos que o caminho de menor custo entre a e d tem custo 2 (a primeira entrada de $(2, c)$ na coluna d), e este caminho acabe com (\dots, c, d) . Pela última entrada da coluna c , o vértice anterior é a , o que de facto é o vértice inicial. Portanto, a caminho de menor custo de a para d , encontrado pelo algoritmo, é (a, c, d) .

5.8 Árvores e florestas

Definição 5.8.1. Um grafo simples G diz-se uma **floresta** se G não contém ciclos. Uma floresta conexa designa-se por **árvore**.

Nota 5.8.2. Uma floresta é um grafo simples cujas componentes conexas são árvores. Mais intuitiva: uma floresta é uma coleção de árvores.

Teorema 5.8.3. Para um grafo G com pelo menos um vértice, as seguintes afirmações são equivalentes.

- (i) G é uma árvore.
- (ii) G não tem lacetes e entre cada par de vértices em G existe um único caminho.
- (iii) G é «minimamente conexo»; ou seja, G é conexo e cada aresta é uma ponte.
- (iv) G é «maximamente acíclico», ou seja, G não contém ciclos, mas acrescentando uma aresta obtém-se um ciclo.

Demonstração. (i) \implies (ii). Se G é uma árvore, então G não tem ciclos, em particular G não tem lacetes. Sejam u e v dois vértices de G . Como G é conexo, existe um caminho entre u e v . Suponha que P e P' são dois caminhos diferentes entre u e v . Portanto, existe uma aresta a em P que não ocorre em P' . Portanto, o subgrafo H dado por P e P' , mas sem a aresta a , é conexo. Sejam x e y os pontos extremos de a . Logo, existe um caminho $Q = (x, \dots, y)$ entre x e y em H . Consequentemente, (x, \dots, y, a, x) é um ciclo em G , uma contradição.

(ii) \implies (iii). Suponha agora que G não tem lacetes e entre cada par de vértices em G existe um único caminho. Em particular, G é conexo e simples. Seja a uma aresta em G com pontos extremos u e v . Por hipótese, (u, a, v) é o único caminho entre u e v em G , logo, u e v são desconexos em $G - a$, isto é, a é uma ponte.

(iii) \implies (i). Se G é conexo e cada aresta é uma ponte, então G não contém ciclos (ver o Teorema 5.5.12) e por isso é uma árvore.

(iii) \iff (iv). Como já observamos, se G é conexo e cada aresta em G é uma ponte, então G não contém ciclos; além disso, como G é conexo, acrescentar uma aresta produz um ciclo. Por outro lado, se G não tem ciclos, então cada aresta é uma ponte, se G também é «maximamente acíclico», então todos os vértices em G já estão ligados, ou seja, G é conexo. \blacklozenge

Definição 5.8.4. Seja G um grafo. Um subgrafo abrangente T de G diz-se **árvore abrangente** de G quando T é uma árvore.

Nota 5.8.5. Cada grafo finito conexo admite uma árvore abrangente. Por exemplo, podemos escolher um subgrafo «maximamente acíclico».

Continuamos o nosso estudo de árvores com uma observação simples mas extremamente útil.

Lema 5.8.6. *Cada árvore finita com pelo menos dois vértices tem pelo menos dois vértices de grau um.*

Demonstração. Considere, por exemplo, os vértices extremos de um caminho de maior comprimento do grafo. \blacklozenge

Nota 5.8.7. Os vértices de grau um de uma árvore diz-se **folhas**.

Se v é uma folha da árvore T com pelo menos dois vértices, então o subgrafo $T - v$ também é uma árvore. Este facto permite reduzir o «tamanho» de uma árvore e portanto aplicar argumentos indutivos. Esta técnica já é útil na prova do seguinte resultado.

Lema 5.8.8. *Uma árvore com n vértices tem precisamente $n - 1$ arestas.*

Demonstração. Provamos esta afirmação utilizando indução sobre o número n de vértices da árvore T . Sendo conexo, T tem pelo menos um vértice. Se $n = 1$, então T não tem arestas porque, sendo um grafo acíclico, não tem lacetes. Seja agora $n \geq 2$ e suponha que a afirmação é verdadeira para todas as árvores com menos do que n vértices. Seja v

uma folha de T . Portanto, $T - v$ é uma árvore; por hipótese da indução, $T - v$ tem $n - 2$ arestas. Logo, T tem $n - 1$ arestas. \blacklozenge

De facto, esta relação entre o número de arestas e o número de vértices caracteriza as árvores entre os grafos conexos.

Teorema 5.8.9. *Um grafo finito G conexo com n vértices é uma árvore se e só se G tem $n - 1$ arestas.*

Demonstração. Suponha que G tem n vértices e $n - 1$ arestas e seja T uma árvore abrangente de G . Logo, T tem $n - 1$ arestas, portanto $G = T$ é uma árvore. \blacklozenge

Temos um resultado muito semelhante para grafos acíclicos:

Teorema 5.8.10. *Um grafo finito G sem ciclos com $n \geq 1$ vértices é uma árvore se e só se G tem $n - 1$ arestas.*

Como um grafo sem ciclos é uma floresta, o teorema acima pode-se justificar utilizando o seguinte resultado.

Teorema 5.8.11. *Um grafo finito G é uma floresta se e só se*

$$\epsilon(G) = \nu(G) - \text{cc}(G).$$

Demonstração. Suponhamos que G é uma floresta e sejam G_1, \dots, G_k as componentes conexas de G . Logo, $\text{cc}(G) = k$ e

$$\epsilon(G) = \epsilon(G_1) + \dots + \epsilon(G_k) \quad \text{e} \quad \nu(G) = \nu(G_1) + \dots + \nu(G_k).$$

Para cada $i = 1, 2, \dots, k$, $\epsilon(G_i) = \nu(G_i) - 1$ (ver o Lema 5.8.8), portanto,

$$\epsilon(G) = \nu(G) - k.$$

Suponha agora que $\epsilon(G) - \nu(G) + \text{cc}(G) = 0$ e sejam G_1, \dots, G_k as componentes conexas de G . Logo,

$$0 = \underbrace{(\epsilon(G_1) - \nu(G_1) + 1)}_{\geq 0} + \dots + \underbrace{(\epsilon(G_k) - \nu(G_k) + 1)}_{\geq 0};$$

ou seja, $\epsilon(G_i) - \nu(G_i) + 1 = 0$, para cada $i = 1, \dots, k$. Pelo Teorema 5.8.9, cada componente conexa é uma árvore. Portanto, G é uma floresta. \blacklozenge

Nota 5.8.12. Se G é uma árvore, então obtemos a fórmula já conhecida:

$$\epsilon(G) = \nu(G) - 1.$$

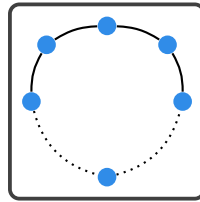
Portanto, num grafo conexo obtemos outra vez (ver a Nota 5.5.4)

$$\epsilon(G) \geq \epsilon(\text{uma árvore abrangente}) = \nu(G) - 1.$$

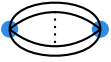
Definição 5.8.13. Para um grafo finito G , $\tau(G)$ denota o **número de árvores abrangentes de G** .

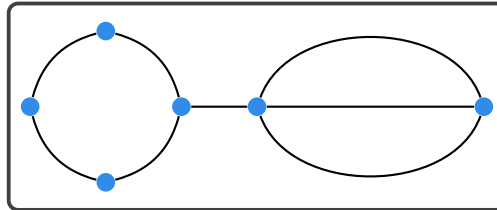
Exemplo 5.8.14. Para alguns grafos particulares G , calculamos agora o número $\tau(G)$.

- Para cada grafo conexo G , $\tau(G) \geq 1$, se G é desconexo, então $\tau(G) = 0$. Portanto, $\tau(G) = 0$ se e só se G é desconexo.
- Se G é uma árvore, então $\tau(G) = 1$ porque a única árvore abrangente de G é G .
- Se G é um ciclo com k arestas, então $\tau(G) = k$



As árvores abrangentes de G são da forma $G - a$.

- Se $G =$  (k arestas paralelas), então $\tau(G) = k$. As árvores abrangentes de G são precisamente as arestas de G .
- Se $G =$ dois subgrafos G_1 e G_2 unidos por uma ponte ou por um único vértice em comum, então $\tau(G) = \tau(G_1) \cdot \tau(G_2)$.



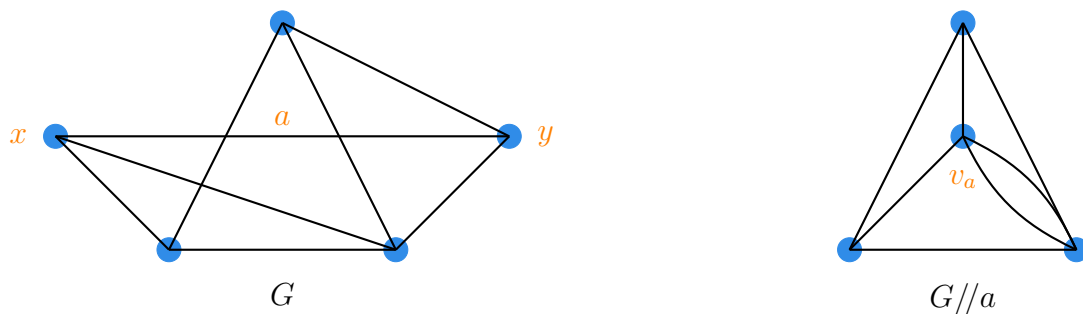
De facto, as árvores abrangentes de G correspondem aos pares (T_1, T_2) onde T_1 é uma árvore abrangente de G_1 e T_2 é uma árvore abrangente de G_2 .

Apresentamos agora uma construção com grafos que reduz o número de arestas e assim é útil para calcular o número de árvores abrangentes *recursivamente*.

Seja $G = (V, E, \psi)$ um grafo e seja $a \in E$ com $\psi(a) = \{x, y\}$. Denotamos por $G//a$ o grafo obtido a partir de G por **fusão** de x e y . Mais concretamente, $G//a = (V', E', \psi')$ onde

$$V' = V \setminus \{x, y\} \cup \{v_a\}, \quad E' = E \setminus \{a\}$$

e $\psi(e) = \psi'(e)$ para toda a aresta $e \in E$ com $\psi(e) \cap \{x, y\} = \emptyset$, em todos os outros casos $\psi'(e)$ é dado por $\psi(e)$ com v_a em lugar de x respetivamente y .

Exemplo 5.8.15.

Nota 5.8.16. Seja G um grafo finito e seja a uma aresta de G . Por definição,

$$\epsilon(G//a) = \epsilon(G) - 1.$$

Nota 5.8.17. Seja G um grafo finito e sejam a, b arestas distintas de G . Então,

$$(G//a) - b = (G - b)//a,$$

ou seja, a operação de fusão de extremos de arestas comuta com a operação de eliminação de arestas.

Teorema 5.8.18. *Seja G um grafo finito e conexo seja a uma aresta de G que não é um lacete. Então,*

$$\tau(G) = \tau(G - a) + \tau(G//a).$$

Demonstração. De facto

$$\tau(G) = |\{\text{as árvores sem } a\}| + |\{\text{as árvores com } a\}| = \tau(G - a) + \tau(G//a). \quad \blacklozenge$$

Nota 5.8.19. • Se a em um lacete em G , então $\tau(G) = \tau(G - a)$.

- Para $\begin{array}{c} a \\ \bullet \text{---} \bullet \\ v_0 \quad v_1 \end{array}$ em G com $d(v_1) = 1$: $\tau(G) = \tau(G - v_1)$.

Exemplo 5.8.20. Apresentamos um pequeno exemplo onde utilizamos o Teorema 5.8.18 para calcular o número de árvores abrangentes de um grafo G . Para simplificar a notação, no que se segue não escrevemos os «nomes» dos vértices. Começamos por recordar que

$$\tau \left(\begin{array}{c} \bullet \\ \diagup \quad \diagdown \\ \bullet \quad \bullet \\ \diagdown \quad \diagup \\ \bullet \end{array} \right) = 4.$$

Portanto, selecionando a aresta «vermelha», calculamos:

$$\tau \left(\begin{array}{c} \bullet \\ \diagup \quad \diagdown \\ \bullet \quad \bullet \\ \diagdown \quad \diagup \\ \bullet \end{array} \right) = \tau \left(\begin{array}{c} \bullet \\ \diagup \quad \diagdown \\ \bullet \quad \bullet \\ \diagdown \quad \diagup \\ \bullet \end{array} \right) + \tau \left(\begin{array}{c} \bullet \quad \bullet \\ \text{---} \quad \text{---} \\ \bullet \quad \bullet \end{array} \right)$$

$$= 4 + 2 \cdot 2 = 8.$$

Apresentamos ainda mais uma fórmula para o cálculo do número de árvores abrangentes de um grafo, conhecido como a fórmula de Cayley.¹

Teorema 5.8.21. *Para cada $n \geq 1$, o número de árvores com n vértices (etiquetadas) é n^{n-2} .*

Tiramos logo uma consequência importante:

Corolário 5.8.22. *Para cada $n \geq 1$, $\tau(K_n) = n^{n-2}$.*

Existem várias maneiras de justificar o Teorema 5.8.21, apresentamos aqui uma técnica introduzida pelo matemático alemão Heinz Prüfer em 1918.

Para $n = 1$, temos $\tau(K_1) = 1 = 1^{-1}$. Sejam $n \geq 2$ e V um conjunto de n elementos. Vamos estabilizemos uma bijeção entre

o conjunto de todas as árvores $T = (V, E)$

e

o conjunto de todas as sequências $(a_1, a_2, \dots, a_{n-2})$ em V de comprimento $n - 2$.

Daqui segue imediatamente que o número de árvores $T = (V, E)$ é n^{n-2} .

Para simplificar a notação, no que se segue consideremos que $V \subseteq \mathbb{N}$, assim temos naturalmente uma ordem total em V . Em primeiro lugar, definimos a função **pruefer** que, para cada árvore $T = (V, E)$ com $|V| = n \geq 2$, calcula uma certa sequência $(a_1, a_2, \dots, a_{n-2})$ em V , de modo que esta sequência permite reconstruir a árvore T . Por exemplo, se V tem precisamente dois elementos, então só há uma única árvore (V, E) onde os dois vértices estão ligados. A esta árvore associamos a lista vazia $()$. Se $|V| = 3$, então dois dos vértices são folhas e o terceiro vértice tem grau dois, ambas as folhas estão ligadas a este vértice. Portanto, para reconstruir T neste caso, basta saber qual dos vértices em V não é uma folha. Neste sentido, associamos à T a sequência

(o único vértice de T que não é folha)

¹Arthur Cayley (1821 – 1895), matemático britânico.

(o único vizinho da menor folha de T),

$\text{pruefer}(\text{uma \u00e1rvore de dois v\u00e9rtices}) = \text{a lista vazia } () \text{ em } V$
 $\text{pruefer}(T) = (u, \text{pruefer}(T - v)) \text{ em } V$
 onde
 $v = \text{a menor folha de } T$
 $u = \text{o \u00fanico vizinho de } v \text{ em } T$

Algoritmo: A codificação de Prüfer

Resultado: O código $(a_1, a_2, \dots, a_{n-2})$ de Prüfer de T ;

2 $i = 1;$

3 enquanto T tem mais do que dois vértices faça

4 procurar o menor vértice v em T com grau 1 (a menor folha);

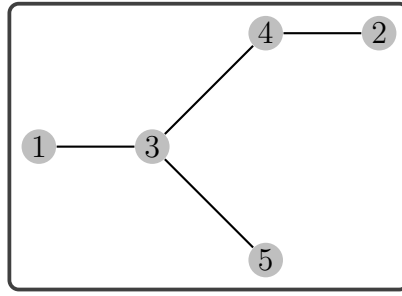
5 $a_i =$ o único vizinho de v ;

```
6 |  $T = T - v$  ;           /* o que ainda é uma árvore */
```

7	$i = i + 1;$
----------	--------------

8 fim

Exemplo 5.8.23. O código de Prüfer da árvore T dada por



é a sequência $\text{pruefer}(T) = (3, 4, 3)$ em $V = \{1, 2, 3, 4, 5\}$.

Nota 5.8.24. Cada vértice v de uma árvore T aparece $d(v) - 1$ no código de Prüfer (a_1, \dots, a_{n-2}) de T . Em particular, um vértice $v \in V$ é uma folha de $T = (V, E)$ se e somente se v não ocorre em (a_1, \dots, a_{n-2}) .

Procedemos agora à descrição da função inversa unpruefer de pruefer que, dada um conjunto V de n vértices e uma sequência $(a_1, a_2, \dots, a_{n-2})$ em V , calcula a árvore correspondente. Notamos primeiro que

- se $n = 2$, então a sequência é vazia e a árvore correspondente liga os dois vértices de V ,
- os elementos de V que não ocorrem em $(a_1, a_2, \dots, a_{n-2})$ são precisamente as folhas da árvore correspondente. Para $n > 2$, sendo v o menor elemento de V que não ocorre em $(a_1, a_2, \dots, a_{n-2})$, então a árvore com vértices em V e com o código $(a_1, a_2, \dots, a_{n-2})$ é a árvore em $V \setminus \{v\}$ com o código (a_2, \dots, a_{n-2}) , ligando ainda v e a_1 .

Portanto, definimos:

$\text{unpruefer}(\text{a lista vazia em } V) = \text{a única árvore } (V, E)$

$\text{unpruefer}((a, \text{resto}) \text{ em } V) = \text{unpruefer}(\text{resto em } V \setminus \{v\}) + \text{ligar } v \text{ e } a$

onde

$v = \text{o menor elemento de } V \text{ que}$

$\text{não ocorre em } (a, \text{resto})$

Teorema 5.8.25. *Seja $V \subseteq \mathbb{N}$ um conjunto com $|V| = n \geq 2$. Para cada sequência (a_1, \dots, a_{n-2}) em V a cada árvore $T = (V, E)$, verificam-se as igualdades*

$$\begin{aligned} \text{pruefer}(\text{unpruefer}((a_1, \dots, a_{n-2}) \text{ em } V)) &= (a_1, \dots, a_{n-2}) \text{ em } V, \\ \text{unpruefer}(\text{pruefer}(T)) &= T. \end{aligned}$$

Portanto, pruefer e unpruefer definem funções bijetivas entre o conjunto de todas as árvores $T = (V, E)$ e o conjunto de todas as sequências $(a_1, a_2, \dots, a_{n-2})$ em V de comprimento $n - 2$.

O algoritmo de decodificação de Prüfer podemos também descrever da forma iterativa.

Algoritmo: A decodificação de Prüfer;

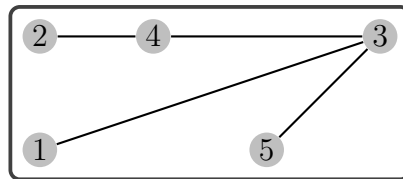
Entrada: Uma sequência $(a_1, a_2, \dots, a_{n-2})$ em V com $|V| = n \geq 2$;

Resultado: A árvore (V, E) com o código $(a_1, a_2, \dots, a_{n-2})$

```

1  $P = (a_1, a_2, \dots, a_{n-2})$ ;
2  $L$  = a lista ordenada dos vértices (de comprimento  $n$ );
3  $E = \emptyset$ ;
4 enquanto  $L$  tem mais do que dois elementos faça
5    $x$  = o menor elemento em  $L$  que não pertence a  $P$ ;
6    $y$  = o primeiro elemento de  $P$ ;
7   Ligar  $x$  e  $y$ , ou seja,  $E = E \cup \{xy\}$ ;
8    $L = L$  tirando  $x$ ;
9    $P = P$  tirando  $y$ ;
10 fim
11 Ligar os dois elementos de  $L$ , ou seja,  $E = E \cup \{\text{os dois elementos de } L\}$ ;
```

Exemplo 5.8.26. Com $P = (3, 4, 3)$ e $L = (1, 2, 3, 4, 5)$, obtemos a árvore



porque, sucessivamente, ligamos

1. 3 e 1,
2. 4 e 2,
3. 3 e 4 e,

finalmente, 3 e 5.

5.9 Árvores abrangentes de custo mínimo

I Nesta secção consideremos apenas grafos finitos.

Tal como na Secção 5.7, consideremos nesta secção grafos (finitos) $G = (V, E)$ com uma função

$$W: E \longrightarrow [0, \infty]$$

de custos não negativos nas arestas. Dada um subgrafo H de G , com o conjunto de arestas

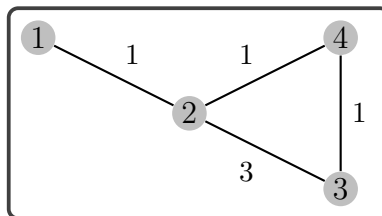
$E' \subseteq E$, definimos o custo de H como

$$\sum_{e \in E'} W(e).$$

Dada um tal grafo G , procuramos uma árvore abrangente de custo mínimo em G . Para resolver este problema, apresentamos dois algoritmos: o algoritmo de Prim² e o algoritmo de Kruskal³. Estes algoritmos são muito semelhantes, e começamos por explicar a ideia comum. Primeiro, alguma notação.

Definição 5.9.1. Sejam $G = (V, E)$ um grafo conexo com custos não negativos nas arestas $W: E \rightarrow [0, \infty]$ e $E' \subseteq E$ um conjunto de arestas que faz parte de uma árvore abrangente de G de custo mínimo. Uma aresta $a \in E$ diz-se **segura para E'** quando $E' \cup \{a\}$ faz parte de uma árvore abrangente de G de custo mínimo.

Exemplo 5.9.2. Considere o grafo G representada pela seguinte figura.



Com $E' = \{12\}$, a aresta 24 é segura para E' , mas a aresta 23 não é segura para E' .

De modo geral, ambos os algoritmos utilizem o seguinte princípio, apenas diferem na escolha da aresta segura no passo 2.

1. $E' = \emptyset$.
2. **Enquanto** $T = (V, E')$ não é uma árvore abrangente de G :
 - Encontre uma aresta $a \in E \setminus E'$ segura para E' .
 - $E' = E' \cup \{a\}$.
 - **Saltar para** o início de 2.
3. Devolver a árvore abrangente (V, E') de G de custo mínimo.

Uma aresta $a \in E \setminus E'$ segura para E' realmente existe? E se sim, como encontrar? Para poder responder a estas questões, introduzimos ainda mais notação.

Definição 5.9.3. Seja $G = (V, E)$ um grafo conexo com $W: E \rightarrow [0, \infty]$.

- Um **corte** de G é uma partição $\{S, V \setminus S\}$ de V .

²Robert Clay Prim (1921 – 2021) matemático e informático estadunidense.

³Joseph Bernard Kruskal (1928 – 2010) matemático, estatístico, informático e psicometrista estadunidense.

- Uma aresta $a \in E$ **ultrapassa o corte** quando um extremo pertence ao S e o outro ao $V \setminus S$.
- Um corte $\{S, V \setminus S\}$ **respeita** um conjunto $E' \subseteq E$ de arestas quando nenhuma aresta de E' ultrapassa o corte.
- Finalmente, uma aresta $a \in E$ diz-se **leve ultrapassando o corte** $\{S, V \setminus S\}$ quando a ultrapassa o corte e tem custo mínimo entre todas as arestas que ultrapassam o corte.

O seguinte resultado descreve um critério para determinar uma aresta segura.

Teorema 5.9.4. *Seja $G = (V, E)$ um grafo conexo com $W: E \rightarrow [0, \infty]$. Suponha que $E' \subseteq E$ faz parte de uma árvore abrangente de G de custo mínimo e seja $\{S, V \setminus S\}$ um corte de V que respeita E' . Se $uv \in E$ é leve ultrapassando o corte; então, uv é segura para E' .*

Demonstração. Seja T uma árvore abrangente de G de custo mínimo que inclui E' . Se uv pertence à T , então uv é segura para E' .

Suponha que uv não pertence à T . Procuramos uma árvore abrangente T' de G de custo mínimo que inclui $E' \cup \{uv\}$.

Como T é uma árvore, existe um único caminho entre u e v em T . Juntando uv a este caminho obtém-se um ciclo em G . Como a aresta uv ultrapassa o corte $\{S, V \setminus S\}$, uma aresta do caminho entre u e v em T também ultrapassa o corte $\{S, V \setminus S\}$; digamos a aresta xy . Temos que $xy \notin E'$ porque o corte respeita E' . Portanto, $T' = T - xy + uv$ é uma árvore abrangente de G que inclui $E' \cup \{uv\}$.

Como uv é uma aresta leve ultrapassando o corte e xy também ultrapassa o corte, $W(uv) \leq W(xy)$. Portanto,

$$W(T') = W(T) - W(xy) + W(uv) \leq W(T);$$

mas, como T é de custo mínimo, $W(T) = W(T')$. Portanto, T' é uma árvore abrangente de G de custo mínimo. ♦

Corolário 5.9.5. *Seja $G = (V, E)$ um grafo conexo com $W: E \rightarrow [0, \infty]$. Suponha que $E' \subseteq E$ faz parte de uma árvore abrangente de G de custo mínimo, e seja $C = (V_C, E_C)$ uma componente conexa (ou seja, árvore) da floresta (V, E') . Se $a \in E$ é uma aresta leve que liga C a uma outra componente conexa de (V, E') , então a é segura para E' .*

Demonstração. Considere o corte $(V_C, V \setminus V_C)$. ♦

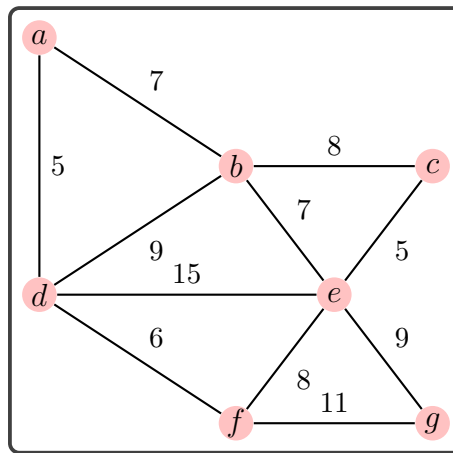
Aos algoritmos de Kruskal e de Prim utilizam ambos o Corolário 5.9.5 para determinar uma aresta segura, mas de forma diferente. Começamos por explicar o algoritmo de Kruskal.

Algoritmo: O algoritmo de Kruskal**Entrada:** Um grafo conexo $G = (V, E)$ com $W: E \rightarrow [0, \infty]$;**Resultado:** Uma árvore abrangente (V, E') de G de custo mínimo;

- 1 Ordenar as arestas de G por ordem não decrescente do seu custo: (a_1, \dots, a_m) com $W(a_1) \leq W(a_2) \leq \dots \leq W(a_m)$;
- 2 $E' = \emptyset$;
- 3 $i = 1$;
- 4 **enquanto** $T = (V, E')$ não é conexa **faça**
- 5 **se** $(V, E' \cup \{a_i\})$ não tem ciclos **então**
- 6 $E' = E' \cup \{a_i\}$;
- 7 **fim**
- 8 $i = i + 1$;
- 9 **fim**

Notamos que o algoritmo acrescenta em cada passo uma aresta de menor custo que ligue duas componentes conexas da floresta (V, E') , por isso é segura pelo Corolário 5.9.5.

Exemplo 5.9.6. Consideremos o seguinte grafo $G = (V, E)$ com custos não negativos nas arestas.



Para aplicar o algoritmo de Kruskal, começamos por ordenar as arestas de G por ordem não decrescente do seu custo:

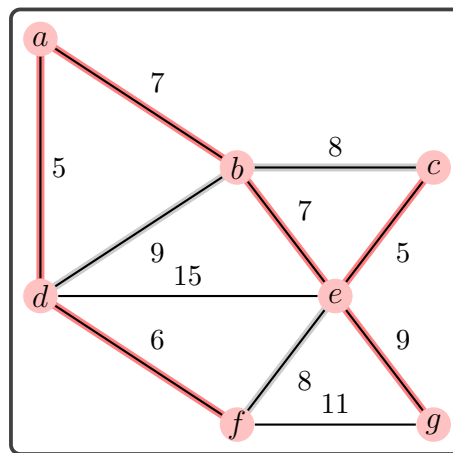
ad, ce, df, ab, be, bc, ef, bd, eg, fg, de.

Agora obtemos:

1. $E' = \emptyset$
2. $E' = \{ad\}$
3. $E' = \{ad, ce\}$

4. $E' = \{ad, ce, df\}$
5. $E' = \{ad, ce, df, ab\}$
6. $E' = \{ad, ce, df, ab, be\}$
7. $E' = \{ad, ce, df, ab, be\}$, $bc \notin E'$
8. $E' = \{ad, ce, df, ab, be\}$, $ef \notin E'$
9. $E' = \{ad, ce, df, ab, be\}$, $bd \notin E'$
10. $E' = \{ad, ce, df, ab, be, eg\}$

Neste momento observamos que o grafo (V, E') é conexo,



portanto, $T = (V, E')$ é uma árvore abrangente de G de custo mínimo, com $W(T) = 39$.

Finalmente, apresentamos o algoritmo de Prim.

Algoritmo: O algoritmo de Prim

Entrada: Um grafo conexo $G = (V, E)$ com $W: E \rightarrow [0, \infty]$;

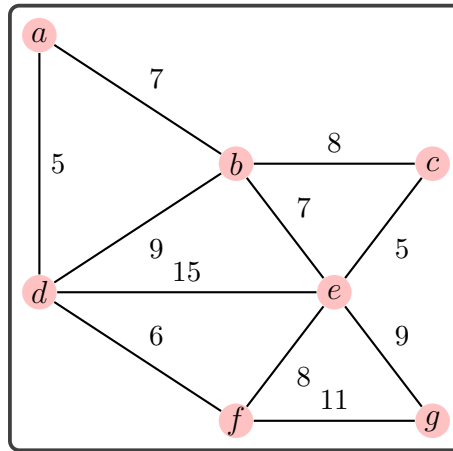
Resultado: Uma árvore abrangente (V, E') de G de custo mínimo;

- 1 Escolher um vértice $u \in V$;
 - 2 $V' = \{u\}$;
 - 3 $E' = \emptyset$;
 - 4 **enquanto** $V' \neq V$ **faça**
 - 5 Entre todas as arestas $vw \in E$ com $v \in V'$ e $w \notin V'$, determinar uma aresta v^*w^* de menor custo;
 - 6 $V' = V' \cup \{w^*\}$;
 - 7 $E' = E' \cup \{e^*\}$;
 - 8 **fim**
-

Notamos que o algoritmo acrescenta em cada passo uma aresta de menor custo que ligue a componente conexa V' de (V, E') a um elemento de $V \setminus V'$, por isso é segura pelo Corolá-

rio 5.9.5.

Exemplo 5.9.7. Consideremos outra vez o grafo (V, E) com custos não negativos nas arestas do Exemplo 5.9.6.



Escolhemos, por exemplo, o vértice d , e:

1. $V' = \{d\}$, $E' = \emptyset$
2. $V' = \{d, a\}$, $E' = \{ad\}$
3. $V' = \{d, a, f\}$, $E' = \{ad, df\}$
4. $V' = \{d, a, f, b\}$, $E' = \{ad, df, ab\}$
5. $V' = \{d, a, f, b, e\}$, $E' = \{ad, df, ab, be\}$
6. $V' = \{d, a, f, b, e, c\}$, $E' = \{ad, df, ab, be, ec\}$
7. $V' = \{d, a, f, b, e, c, g\}$, $E' = \{ad, df, ab, be, ec, eg\}$

Como $V' = V$, podemos terminar aqui e $T = (V, E')$ é uma árvore abrangente de G de custo mínimo, com $W(T) = 39$.

Bibliografia

- BAUER, ANDREJ (2016). «Five stages of accepting constructive mathematics». Em: *Bulletin of the American Mathematical Society* **54**.(3), pp. 481–498. URL: <http://www.ams.org/journals/bull/2017-54-03/S0273-0979-2016-01556-4/>.
- CARDOSO, DOMINGOS e CARVALHO, PAULA (2007). «Noções de Lógica Matemática». Universidade de Aveiro.
- CARDOSO, DOMINGOS, SZYMANSKI, JERZY e ROSTAMI, MOHAMMAD (2009). *Matemática discreta: Combinatória, Teoria dos Grafos e Algoritmos*. Escolar Editora.
- CAROLL, LEWIS (1896). *Symbolic Logic*. URL: <http://www.gutenberg.org/ebooks/28696#bibrec>.
- CHANG, CHIN-LIANG e LEE, RICHARD CHAR-TUNG (1973). *Symbolic Logic and Mechanical Theorem Proving*. Elsevier. 331 pp.
- CORMEN, THOMAS H., LEISERSON, CHARLES E., RIVEST, RONALD L. e STEIN, CLIFFORD (2009). *Introduction to Algorithms*. 3ª ed. The MIT Press. URL: <http://staff.ustc.edu.cn/~csli/graduate/algorithms/book6/toc.htm>.
- LASTARIA, FEDERICO G. (2000). «An invitation to combinatorial species». URL: <http://math.unipa.it/~grim/ELastaria221-230.PDF>.
- SMITH, PETER (2022). *Beginning Mathematical Logic. A Study Guide*. Logic Matters. x + 194. URL: <https://www.logicmatters.net/resources/pdfs/LogicStudyGuide.pdf>.
- STANLEY, RICHARD P. (2010). *Enumerative Combinatorics*. Vol. 2. Cambridge University Press. xii + 600.
- STANLEY, RICHARD P. (2012). *Enumerative Combinatorics*. Vol. 1. Cambridge University Press. xiii + 642.
- WORRELL, JAMES (2016). *Introduction to Logic*. URL: <https://www.cs.ox.ac.uk/people/james.worrell/lectures.html>. Lecture notes, Department of Computer Science, University of Oxford.