Departamento de Matemática, Universidade de Aveiro

Matemática Discreta (47166)

Ano Letivo 2021/22

Texto de Apoio

Versão: 14 de abril de 2022

Conteúdo

1 Lógica de Primeira Ordem e Demonstração Automática

1.1 Elementos da Lógica Proposicional

Fórmulas

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

- Um número primo ímpar p é soma de dois quadrados se e só se p tem o resto 1 na divisão por 4.
- $\sqrt{2}$ é um número racional.
- $1 + 1 = 3$ e 11 é um número primo.
- A 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 ... »;
- « ... ou dots »;
- « ... não ... »;
- « 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 substituido por « ... e ... »;
- « ... só se ... » pode ser substituido por « ... implica ... » ou « Se ... então ... »;
- « ... excepto se ... » pode ser substituido 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: $\bot$ 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): $p, q, r, \ldots, p_1, p_2, p_3, \ldots$.

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 $\downarrow$).

Definição 1.1.3. 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

$\wedge, \vee, \rightarrow, \neg, \leftrightarrow, \bot, \top$ e às variáveis proposicionais $p, q, r, \ldots$. As fórmulas proposicionais podem então ser definidas inductivamente de acordo com as regras que abaixo se apresentam:

1. cada variável é uma fórmula e $\bot$ 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 1.1.4. 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 precedência inferior aos outros conectivos, ou seja, escreveremos $\neg\varphi \vee \psi$ em vez de $(\neg\varphi) \vee \psi$.

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

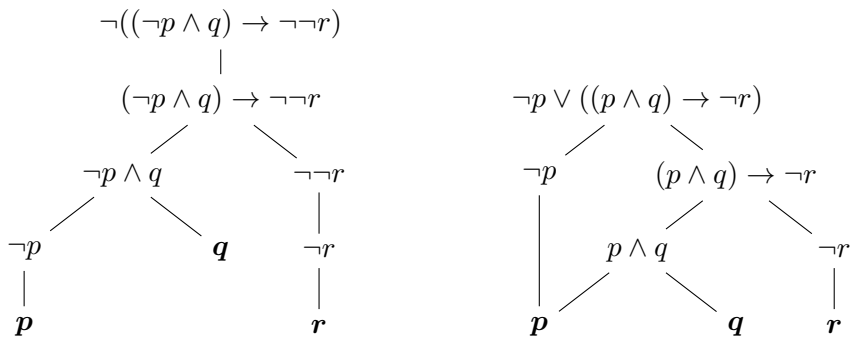
```
<formula> ::= variavel | ⊥ | ⊤
      |   (¬ <formula>)
      |   (<formula> ∧ <formula>)
      |   (<formula> ∨ <formula>)
      |   (<formula> → <formula>)
      |   (<formula> ↔ <formula>)
```

Exemplo 1.1.5. Se considerarmos p, q e r três variáveis, podemos ter os seguintes exemplos de fórmulas:

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

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

Exemplo 1.1.6. As expressões $\neg((\neg p \wedge q) \rightarrow \neg\neg r)$ e $\neg p \vee ((p \wedge q) \rightarrow \neg r)$ são fórmulas. Efectivamente, se considerarmos as variáveis p, q, r, podemos seguir as árvores de construcção ilustradas abaixo.



Semântica, Validade e Equivalência

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

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

Exemplo 1.1.9. Se p e q forem variáveis proposicionais, então uma valoração do conjunto $V = \{p, q\}$ poderá ser a função $v\colon V \to \{0,1\}$ 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 1.1.10. 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 $v\colon V \to \{0,1\}$, onde $V = \{p,q,r\}$, tal que $p, r \mapsto 1$ e $q \mapsto 0$, qual será o valor de verdade da seguinte fórmula?

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

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	$\neg\varphi$
0	1
1	0

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

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

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

Suponhamos agora que temos uma valoração de um conjunto de variáveis proposicionais V, $v\colon V \to \{0,1\}$. 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:

$$v(\bot) = 0$$
$$v(\top) = 1$$
$$v(\varphi \wedge \psi) = v(\varphi) \wedge v(\psi)$$

$$\begin{aligned} v(\varphi \vee \psi) &= v(\varphi) \vee v(\psi) \\ v(\varphi \to \psi) &= v(\varphi) \to v(\psi) \\ v(\varphi \leftrightarrow \psi) &= v(\varphi) \leftrightarrow v(\psi) \\ v(\neg\varphi) &= \neg v(\varphi) \end{aligned}$$

Devemos recordar que podemos pensar nos símbolos conectivos não apenas como partes da fórmula, mas como elementos de combinação dos valores de verdade.

Exemplo 1.1.11. Suponhamos que $V = \{p, q\}$ e que temos uma valoração $v \colon V \to \{0, 1\}$ tal que $p \mapsto 1$ e $q \mapsto 0$. Então,

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

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

p	q	$p \vee q$	$(p \vee q) \to q$
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 $v \colon V \to \{0, 1\}$, 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 $(p \vee q) \to q$. Neste caso, $v((p \vee q) \to q) = 0$.

Definição 1.1.13. Uma fórmula diz-se:

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

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

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 1.1.14. As fórmulas $(p \wedge q) \to q$ e $(p \wedge q) \to p$ são tautologias.

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

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

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

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

p	q	$p \to q$	$\neg p$	$\neg p \vee q$	$(\neg p \vee q) \leftrightarrow (p \to q)$
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	$p \to q$	$\neg q$	$\neg p$	$\neg q \to \neg p$	$(p \to q) \leftrightarrow (\neg q \to \neg p)$
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:

$$(p \wedge q) \equiv (q \wedge p), \qquad (p \vee q) \equiv (q \vee p),$$

$$((p \wedge q) \wedge r) \equiv (p \wedge (q \wedge r)), \qquad ((p \vee q) \vee r) \equiv (p \vee (q \vee r)).$$
$$(p \wedge p) \equiv p, \qquad (p \vee p) \equiv p,$$
$$(p \wedge \top) \equiv p, \qquad (p \vee \bot) \equiv p,$$
$$(p \wedge \bot) \equiv \bot, \qquad (p \vee \top) \equiv \top$$

bem como as leis de distributividade,

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

as leis de De Morgan,

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

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
⋮	⋮	⋮	⋮

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 1^{a}, 4^{a}, 5^{a}, 6^{a} e 8^{a} 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 subconjunto de índices), seja L_j um literal. Então, são equivalentes as seguintes afirmações:*

i) $\bigvee_{j\in J} L_j$ *é uma tautologia.*

ii) $\bigwedge_{j\in J} L_j$ *é uma contradição.*

iii) *Existem índices distintos $j_1, j_2 \in J$ tais que $L_{j_1} = \neg L_{j_2}$.*

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

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

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

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

Nota 1.1.24. A disjunção «vazia» (ou seja, $I = \varnothing$) será a fórmula $\bot$. 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 equiva-

lências lógicas ligadas aos conectivos de implicação e equivalência, assim como das leis de De Morgan e das leis de distributividade:

$$\varphi \to \psi \equiv \neg\varphi \vee \psi, \qquad \varphi \leftrightarrow \psi \equiv (\varphi \to \psi) \wedge (\psi \to \varphi)$$
$$\neg(p \vee q) \equiv (\neg p \wedge \neg q), \qquad \neg(p \wedge q) \equiv (\neg p \vee \neg q),$$

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

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

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. ♦

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

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

vamos colocar φ na FNC:

1. Substituimos as equivalências ($\leftrightarrow$) por implicações ($\to$):

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

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

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

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

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

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

Exemplo 1.1.31. Vamos analisar o sudoku do ponto de vista lógico. Para todos os $i, j, k \in \{1, 2, \ldots, 9\}$, a proposição atómica 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

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

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:

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

- 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

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

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 $\varphi_1, \ldots, \varphi_n$ quando, para toda a valoração, se $\varphi_1, \ldots, \varphi_n$ têm valor 1, então ψ tem valor 1. Neste caso, escrevemos $\varphi_1, \ldots, \varphi_n \vDash \psi$.

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

p	q	$p \vee q$	$p \to q$	$\neg p$	$q \vee \neg p$	
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 $\varphi_1, \ldots, \varphi_n$ e ψ, temos que $\varphi_1, \ldots, \varphi_n \vDash \psi$ se e só se $((\varphi_1 \wedge \cdots \wedge \varphi_n) \to \psi)$ for uma tautologia.*

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

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

($\Leftarrow$) Suponhamos que $((\varphi_1 \wedge \cdots \wedge \varphi_n) \to \psi)$ é válida e seja v uma valoração. Se $v(\varphi_i) = 1$

para cada $i = 1, \ldots, n$, então $v(\varphi_1 \wedge \cdots \wedge \varphi_n) = 1$ e por isso $v(\psi) = 1$. Logo, ψ é consequência semântica de $\varphi_1, \ldots, \varphi_n$. ♦

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

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

$$\varphi \to \psi, \psi \to \theta, \boxed{\cdots}, \varphi \to \theta,$$

onde $\boxed{\cdots}$ representa um conjunto de fórmulas justificadas por $\varphi \to \psi$ e $\psi \to \theta$ através das seguintes **regras de inferência** da lógica proposicional:

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

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

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

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

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

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

1	$\varphi \to \psi$	
2	$\psi \to \theta$	
3	$\quad \varphi$	H
4	$\quad \psi$	$\to$E, 1, 3
5	$\quad \theta$	$\to$E, 2, 4
6	$\varphi \to \theta$	$\to$I, 3, 5

- por hipótese, $\varphi \to \psi$ e $\psi \to \theta$;
- com o objectivo de provar $\varphi \to \theta$, suponhamos φ (temporariamente). Como sabemos $\varphi \to \psi$, temos ψ; por outro lado, como sabemos $\psi \to \theta$, temos θ;
- assim, concluímos $\varphi \to \theta$ (e retiramos φ).

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

1	$\varphi \to \psi$	
2	$\quad \varphi$	H
3	$\quad \psi$	$\to$E, 1, 2
4	$\quad \varphi \wedge \psi$	$\wedge$I, 2, 3
5	$\varphi \to (\varphi \wedge \psi)$	$\to$I, 2, 4

- por hipótese, $\varphi \to \psi$;
- com o objectivo de provar $\varphi \to (\varphi \wedge \psi)$, suponhamos φ (temporariamente). Como sabemos $\varphi \to \psi$, temos ψ, ou seja, podemos ter $\varphi \wedge \psi$;
- assim, concluímos $\varphi \to (\varphi \wedge \psi)$ (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 (Completude). *Toda a consequência semântica do cálculo proposicional é também uma consequência sintáctica.*

Nota 1.1.41. Os enunciados dos últimos resultados podem tomar uma forma mais simples. Para tal, consideremos ψ uma fórmula e $\Gamma = \{\varphi_1, \ldots, \varphi_n\}$ um conjunto de fórmulas. O Teorema da Correcção diz-nos que «tudo o que se prova é válido», i.e., que se $\Gamma \vdash \psi$, então $\Gamma \vDash \psi$. Já o Teorema da Completude diz-nos que «tudo o que é válido se consegue provar», ou seja, que se $\Gamma \vDash \psi$, 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 $\Gamma \vDash \psi$ se e só se $\Gamma \cup \{\neg\psi\}$ é inconsistente.*

Demonstração. Por definição, $\Gamma \vDash \psi$ 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 $v(\neg\psi) = 0$. ♦

A questão principal prende-se com a forma de verificar a inconsistência do conjunto $\Gamma \cup \{\neg\psi\}$. De facto, o problema resolve-se se conseguirmos deduzir uma contradição, ou seja, se conseguirmos obter uma sequência de fórmulas

$$\vartheta_1 \quad \vartheta_2 \quad \cdots \quad \bot,$$

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**:

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

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

$$\frac{\neg\psi \qquad \psi \vee \varphi}{\varphi} \qquad \text{e} \qquad \frac{\neg\psi \qquad \psi}{\bot}$$

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

Nota 1.1.44. Para verificar se $\varphi_1, \ldots, \varphi_n \vDash \psi$ devemos:

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

Exemplo 1.1.45. Vamos verificar $p \to q, q \to r \vDash p \to r$. Comecemos por considerar as fórmulas $p \to q$, $q \to r$ e $\neg(p \to r)$, 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.	$\bot$	Res (4,6)

1.2 Sintaxe e Semântica de lógica de primeira ordem

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

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

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

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

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

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

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

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

Exemplo 1.2.2. O alfabeto da teoria dos espaços vectoriais 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 $t_1, \ldots, t_n$ são termos, então $f(t_1, \ldots, t_n)$ também é um termo.

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

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

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

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

  $$(\varphi \wedge \psi), \quad (\varphi \vee \psi), \quad (\varphi \to \psi), \quad (\neg\varphi), \quad \bot, \quad \top,$$

  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.

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

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

Exemplo 1.2.8. Atentemos nas seguintes fórmulas...

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

- $\forall x\ (\text{gato}(x) \to \text{garras}(x))$: 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** $f^{\mathcal{M}} \colon D^n \to D$;
- a cada símbolo de predicado P (de aridade n), associamos um **subconjunto** $P^{\mathcal{M}} \subseteq D^n$.

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

Dada agora uma interpretação $(\mathcal{M}, v)$ de uma linguagem, é comum definirmos (de forma

recursiva - à semelhança da lógica proposicional) a interpretação dos termos:

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

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

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

temos:

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

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:

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

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

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

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

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

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

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

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

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 valida quando $x = c$ é válida para alguma «modificação» de v em x. Para expressar esta ideia, consideremos a valoração $v^{\frac{x}{a}}$ que interpreta x como a, isto é, $v^{\frac{x}{a}}(x) = a$, e $v^{\frac{x}{a}}$ não altera a interpretação dos outros variáveis. Agora podemos expressar a nossa intuição da forma rigorosa:

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

quando, para algum $a \in D$,

$$(\mathcal{M}, v^{\frac{x}{a}}) \vDash x = c.$$

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

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

e por isso

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

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: $(\mathcal{M}, v) \vDash R(x, y)$.
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 «$\forall y\ (\ldots \text{algo} \ldots)$» é válida nesta interpretação quando «$(\ldots \text{algo}\ldots)$» 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

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

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

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

De facto, $(\mathcal{M}, v^{\frac{y}{1}}) \vDash S(x)$ porque , $v^{\frac{y}{1}}(x) = v(x) = 3 \in S$; no entanto, $(\mathcal{M}, v^{\frac{y}{1}}) \nvDash R(x, y)$ 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

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

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

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

para responder, temos de analisar se

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

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,

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

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
$\forall x\ \ ((x < 4) \to (1 = 0))$	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 $\vDash \psi$ 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 $\varphi_1, \ldots, \varphi_n$ quando, para toda a interpretação $(\mathcal{M}, v)$, se $\varphi_1, \ldots, \varphi_n$ são válidas em $(\mathcal{M}, v)$, então ψ é válida em $(\mathcal{M}, v)$. Neste caso, escrevemos $\varphi_1, \ldots, \varphi_n \vDash \psi$.

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 $\varphi_1, \ldots, \varphi_n \vdash \psi$ e obter

$$\varphi_1, \ldots, \varphi_n \vDash \psi \quad \Longleftrightarrow \quad \varphi_1, \ldots, \varphi_n \vdash \psi.$$

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

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

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

$$\forall x\ (\text{gato}(x) \to \text{garras}(x)),\ \text{gato}(\text{Tom}) \vDash \text{garras}(\text{Tom}).$$

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):

$$\begin{gathered}\forall x\ (\text{gato}(x) \to \text{garras}(x)), \text{gato}(\text{Tom}),\ \text{garras}(\text{Tom}) \\ \Updownarrow \\ \neg\text{gato}(x) \vee \text{garras}(x), \text{gato}(\text{Tom}),\ \neg\text{garras}(\text{Tom}).\end{gathered}$$

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

Por último, começamos a dedução:

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

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,

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

1.3 Formas Normais

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

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

$$\begin{aligned} &(\forall x\ \varphi) \wedge \psi \equiv \forall x\ (\varphi \wedge \psi), \qquad && (\exists x\ \varphi) \wedge \psi \equiv \exists x\ (\varphi \wedge \psi), \\ &(\forall x\ \varphi) \vee \psi \equiv \forall x\ (\varphi \vee \psi), \qquad && (\exists x\ \varphi) \vee \psi \equiv \exists x\ (\varphi \vee \psi). \end{aligned}$$

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

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

Exemplo 1.3.5. Vamos transformar a fórmula

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

para a forma normal prenex.

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

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 $(\varphi \vee \exists x\ \psi) \to \forall z\ \rho$ na FNP.

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

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

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

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 «∃»

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 («∀»).

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 $\vee$-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. substituimos todas as ocorrências livres de x_1 em $Q_2x_2 \cdots Q_nx_n\ \varphi$ por c;
3. eliminamos $\exists x_1$ do prefixo.

- no caso $\forall x_1 \cdots \forall x_{k-1}\ \exists x_k\ Q_{k+1}x_{k+1} \cdots Q_nx_n\ \varphi$ $(k > 1)$:
  1. escolhemos um novo símbolo de função (digamos f) de aridade $k-1$;
  2. substituimos todas as ocorrências livres de x_k em $Q_{k+1}x_{k+1} \cdots Q_nx_n\ \varphi$ por $f(x_1, \ldots, x_{k-1})$;
  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

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

Comecemos 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 $\xi = Qx_1 \cdots Qx_n\ \varphi[x_1, \ldots, x_n]$ (utilizamos esta notação para vincar que a matriz de ξ contém as variáveis $x_1, \ldots, x_n$). Vamos considerar Q_r o primeiro quantificador existencial presente em ξ e, além disso, vamos tomar a fórmula

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

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 $(\mathcal{M}, v) \vDash \xi_*$. Tal diz-nos que, para todos os $x_1, \ldots, x_{r-1}$, existirá pelo menos um elemento (que será $f(x_1, \ldots, x_{r-1})$) de tal forma que

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

seja válida em $(\mathcal{M}, v)$. Assim, ξ será valida 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 $(\mathcal{M}, v) \vDash \xi$. Tal diz-nos que, para todos os $x_1, \ldots, x_{r-1}$, existirá um elemento x_r de forma a que

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

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

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

ou seja, $(\mathcal{M}, v') \vDash \xi_1$, 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 $k = 1, \ldots, m$. 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. ♦

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, Vars $\subseteq$ Term, assim temos a função de inclusão Vars $\hookrightarrow$ Term.

Substituições

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

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

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

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

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

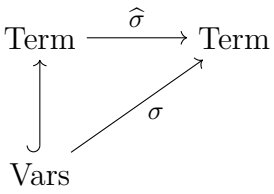
Exemplo 1.4.4. Consideremos a substituição $\sigma = \{f(z)/x, A/y\}$. Explicitamente, a substituição

$$\begin{aligned} \sigma\colon \text{Vars} &\longrightarrow \text{Term} \\ p &\longmapsto \begin{cases} f(z), & \text{se a variável } v \text{ é } x, \\ A, & \text{se a variável } v \text{ é } y, \\ p, & \text{noutros casos.} \end{cases} \end{aligned}$$

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

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

Desta forma, obtemos o seguinte diagrama:



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

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

Felizmente, as extensões não se ficam por aqui! Dada σ: Vars $\to$ Term e uma fórmula E (sem quantificadores), denotaremos por $E\sigma$ a fórmula obtida por aplicação de $\widehat{\sigma}$ a todos os termos de E. Assim sendo, para um conjunto $\mathcal{E} = \{E_1, \ldots, E_n\}$ 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 $\widehat{\theta}$ a t, obtemos:

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

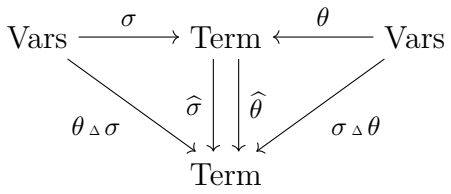
Exemplo 1.4.7. Vamos considerar as fórmulas $E_1 = F(x, y, g(z))$ e $E_2 = P(h(x), z, f(y))$ e a substituição $\theta = \{a/x, f(b)/y, c/z\}$. Então,

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

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

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

De acordo com esta definição, e dadas σ, θ: Vars $\to$ Term, a sua composição pode descrever-se pelo seguinte diagrama.



Nota 1.4.9. Para cada expressão (termo ou fórmula) E, $E(\theta \vartriangle \sigma) = (E\sigma)\theta$.

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

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

a composta $\theta \vartriangle \sigma$ de θ com σ é a substituição dada por

$$\{\widehat{\theta}(\sigma(x_1))/x_1, \ldots, \widehat{\theta}(\sigma(x_n))/x_n\},$$

tendo em conta que, para cada $i = 1, \ldots, n$, se $x_i \notin \{q_1, \ldots, q_j\}$, 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,

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

Apenas para comparação, vamos ainda calcular $\sigma \vartriangle \theta$.

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

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

Rapidamente podemos ver que

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

Lema 1.4.12. *Dada substituições θ, σ: Vars $\to$ Term, então*

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

Demonstração. Consideremos a substituição $\tau = \theta \vartriangle \sigma$ 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 $\widehat{\tau}(x) = \tau(x) = (\theta \vartriangle \sigma)(x) = (\widehat{\theta} \circ \sigma)(x) = \widehat{\theta}(\sigma(x))$ e que $(\widehat{\theta} \circ \widehat{\sigma})(x) = \widehat{\theta}(\widehat{\sigma}(x)) = \widehat{\theta}(\sigma(x))$ (notemos que sendo $t \in$ Vars, $\tau(t) = \widehat{\tau}(t)$);
3. Suponhamos que $t = f(t_1, \ldots t_n)$. Então, $\widehat{\tau}(f(t_1, \ldots, t_n)) = f(\widehat{\tau}(t_1), \ldots, \widehat{\tau}(t_n))$. Nestas condições, para todo o $i \in \{1, \ldots, n\}$, 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 $t_i = f_i(t_{i_1}, \ldots, t_{i_n})$ e o processo repete-se (ou seja, $\widehat{\tau}(t_i) = f_i(\widehat{\tau}(t_{i_1}), \ldots, \widehat{\tau}(t_{i_n}))$ até que se obtenham símbolos de constantes ou variáveis. Em qualquer dos casos vem que $\widehat{\tau}(t) = (\widehat{\theta} \circ \widehat{\sigma})(t)$. ♦

Teorema 1.4.13. *Consideremos S como o conjunto de todas as substituições. Então, a estrutura $\langle S, \vartriangle, \varepsilon \rangle$ 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 $\vartriangle$, admitamos três substituições arbitárias θ, σ, λ. Tendo em conta a Nota 1.4.5 e o Lema 1.4.12:

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

Além disso,

$$\theta \vartriangle \varepsilon = \widehat{\theta} \circ \varepsilon = \theta \quad \text{e} \quad \varepsilon \vartriangle \theta = \widehat{\varepsilon} \circ \theta = \theta.$$ ♦

Unificadores

Definição 1.4.14. Consideremos $\mathcal{E} = \{E_1, \ldots, E_n\}$ um conjunto de expressões (termos, fórmulas). Uma substituição σ: Vars $\to$ Term diz-se um **unificador** de $\mathcal{E}$ quando, para todas as expressões $E_1, \ldots, E_n \in \mathcal{E}$, se tiver $E_1\sigma = \cdots = E_n\sigma$.
Adicionalmente, dizemos que o conjunto $\mathcal{E}$ de expressões é **unificável** quando existir um tal unificador.

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

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

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 substituida por a e, consequentemente, 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 $\mathcal{E} = \{E_1, \ldots, E_n\}$;
Resultado: u.m.g. σ_k de $\mathcal{E}$ (caso exista);

```
k = 0, E_0 = E e σ_0 = ε;
repetir até retornar algo
    se |E_k| = 1 então
        retorna σ_k;
    fim
    determinar o conjunto D_k = {D_1, ...} das diferenças de E_k;
    se existir p ∈ Vars e t ∈ Term tal que {p, t} ⊆ D_k e p não ocorra em t
     então
        σ_{k+1} = (t/p) ▵ σ_k;
        E_{k+1} = E_k(t/p);
        k = k + 1;
    senão
        retorna «E não é unificável»;
    fim
```

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

0. $\mathcal{D}_0 = \{y, x, a\}$, portanto $\sigma_1 = (x/y) \vartriangle \varepsilon = \{x/y\}$, 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 $\sigma_2 = \{a/x\} \vartriangle \sigma_1 = \{a/x, a/y\}$, 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 $\sigma_3 = \{h(a)/z\} \vartriangle \sigma_2 = \{h(a)/z, a/x, a/y\}$, 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 unifivável».

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 unifivável».

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 $\theta = \lambda_k \vartriangle \sigma_k$.

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

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

- se $|\mathcal{E}\sigma_k| = 1$, então o algoritmo termina no passo 4 e, dado que $\theta = \lambda_n \vartriangle \sigma_n$, 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 $\theta = \lambda_n \vartriangle \sigma_n$ 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 $\sigma_{n+1} = (t_n/p_n) \vartriangle \sigma_n$. 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

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

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

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

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

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 1ªOrdem.

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

Definição 1.5.1. Se literais φ e ψ de uma cláusula $C = \varphi \vee \psi \vee \theta \vee \ldots$ admitirem um u.m.g. σ, então $(\psi \vee \theta \vee \ldots)\sigma$ 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 $C_1 = \neg\psi \vee \theta \vee \ldots$ e $C_2 = \varphi \vee \gamma \vee \ldots$ cláusulas sem variáveis em comum. Se ψ e φ admitirem um u.m.g. σ, então a cláusula

$$(\theta \vee \cdots \vee \gamma \vee \ldots)\sigma$$

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:

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

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 $\Gamma \vDash \psi$, 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:

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

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

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

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 $\bot$...

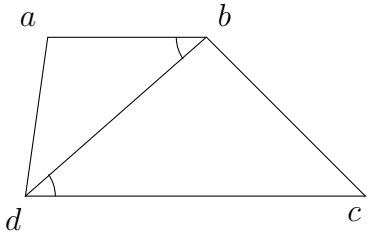
$$\begin{array}{ccccccccc} & & & \text{BR}(1,2) & & \text{BR}(3,4) & & \text{BR}(5,6) & \\ & & & \downarrow & & \downarrow & & \downarrow & \\ P(c) & \neg P(y) \vee I(y) & & I(c) & \neg I(z) \vee \neg S(z) & \neg S(c) & \neg B(x) \vee S(x) & \neg B(c) & B(c) & \bot \\ 1 & & 2 & 3 & 4 & 5 & 6 & 7 & 8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

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 as 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:

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



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.

2 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 $1, \ldots, 9$?
- 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 $x_1 + \cdots + x_n = k$, 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 $f\colon A \to B$ 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 $f\colon A \to B$ diz-se **invertível** quando existir uma função $g\colon B \to A$ tal que $g \circ f = \mathrm{id}_A$ e $f \circ g = \mathrm{id}_B$.

Teorema 2.1.3. *Uma função $f\colon A \to B$ é invertível se e só se é bijectiva.*

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

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

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,

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

Contudo, temos ainda que

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

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

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

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, $f^{-1} \circ f = \mathrm{id}_A$. 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 $f \circ f^{-1} = \mathrm{id}_B$. ♦

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

$$f\colon \{\text{pessoas na sala}\} \longrightarrow \{\text{Janeiro}, \ldots, \text{Dezembro}\}$$

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

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

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

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

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

Demonstração. A prova deste resultado passa por, para cada $k \in \{0, \ldots, n\}$, considerar

$r = k\alpha - \lfloor k\alpha \rfloor \in [0,1]$. De seguida, consideramos ainda a função

$$\begin{aligned} f\colon \{0,\dots,n\} &\longrightarrow \{[0,\frac{1}{n}[, [\frac{1}{n},\frac{2}{n}[, \dots, [\frac{n-1}{n},1[\} \\ k &\longmapsto \text{intervalo } \mathcal{I} \text{ com } r_k \in \mathcal{I} \end{aligned}$$

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

$$\begin{aligned} f\colon \{1,\dots,2n\} &\longrightarrow O. \\ z &\longmapsto \text{aquele único } b \end{aligned}$$

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

$$\begin{aligned} N\colon \{\text{equipas}\} &\longrightarrow \{0,\dots,n-1\} \\ e &\longmapsto \text{total de jogos de } e. \end{aligned}$$

- **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 mk pombos e m gaiolas, então haverá uma gaiola a ter, no mínimo, $k+1$ pombos).

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

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

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 $2,871,133$ pessoas).

Para aplicar o princípio da gaiola dos pombos, vamos considerar a função $f\colon\{\text{Lisboetas}\}\to\{0,\dots,200000\}$ que a cada lisboeta faz corresponder o número de fios de cabelo na cabeça. Como $14\times 200001<2821697$, 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 $f\colon \mathbb{N} \to A$. 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-finitos[1]: 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 $f\colon A \to B$ 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 $f\colon A \to B$ 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 $f\colon A \to B$, então $|A| = |B|$. Tipicamente utilizamos este princípio quando é mais fácil contar os elementos de um destes conjuntos.

[1] Um 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 $A = \{1, 2, \ldots, 9\}$ e o conjunto A^4. De facto, se pensarmos na função $f\colon A^4 \to C$ que a cada quádruplo (a_1, a_2, a_3, a_4) faz corresponder $a_1 10^3 + a_2 10^2 + a_3 10 + a_4$, obtemos a bijecção pretendida.

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

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

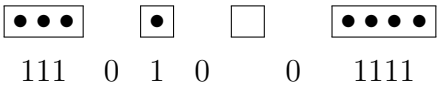
é uma bijecção.

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

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

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

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 sequências binárias com k uns e $n - 1$ zeros.



Por outro lado, o número de sequências 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 ($\mathbb{N} = \{0, 1, 2, \ldots\}$) e o conjunto dos números inteiros ($\mathbb{Z} = \{\ldots, -2, -1, 0, 1, \ldots\}$). 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

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

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

$$\begin{aligned} g\colon\ ]0,1[&\longrightarrow \mathbb{R} \\ x &\longmapsto \tan\left(\pi\left(x - \tfrac{1}{2}\right)\right) \end{aligned}$$

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 $A_1, \ldots, A_n$ conjuntos finitos dois-a-dois disjuntos (i.e., tais que $A_i \cap A_j = \varnothing$, quando $i \neq j$), temos

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

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 $A_1, \ldots, A_n$ conjuntos finitos, a cadinalidade do produto entre estes é igual ao produto das cardinalidades de todos, i.e.,

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

Exemplo 2.4.2.

- 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 $1, \ldots, 9$? Pelo Exemplo 2.3.1, basta determinarmos o tamanho do conjunto $\{1, \ldots, 9\}^4$. Neste caso, existirão $9^4 = 6561$ elementos.
- Qual é o número de números naturais com 4 algarismos que se podem escrever com os

dígitos $0, \ldots, 9$ e que são divisíveis por 5? O conjunto

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

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 «)»;
- $S_2 = \{\text{«}((a))\text{»}, \text{«}((b))\text{»}, \text{«}((c))\text{»}\}$, logo $|S_2| = 3$.

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

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 $r_1 \cdot r_2 \cdot \cdots \cdot r_n$ 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 elemento em $\{1, \ldots, 9\}$. 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, ..., 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 $A_1, \ldots, A_n$ 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

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

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

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

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,

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

♦

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

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

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

$$= 333 + 200 - 66 = 467.$$

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

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

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

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 $p_1, \ldots, p_n$, propriedades aplicáveis aos elementos de X e $N(i_1, i_2, \ldots, i_k)$ o número de elementos de X que têm, pelo menos, as propriedades $p_{i_1}, \ldots, p_{i_k}$.

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 $p_1, \ldots, p_n$ é dado pela expressão

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

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

$$\begin{aligned} |X \setminus A| = {} & |X| - N(1) + \ldots N(n) \\ & + N(1,2) - \cdots - N(n-1,n) \\ & - N(1,2,3) + \cdots + N(n-2,n-1,n) \end{aligned}$$

$$\vdots$$
$$+ (-1)^n N(1, \ldots, n).$$

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.

Smith, Peter (2022). *Beginning Mathematical Logic*. URL: https://www.logicmatters.net/resources/pdfs/LogicStudyGuide.pdf.