$p \vee (p \wedge q) \equiv p$ $p \wedge (p \vee q) \equiv p$	Leis da absorção
$(p \vee q) \vee r \equiv p \vee (q \vee r)$ $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	Leis da associatividade
$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$ $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	Leis da distributividade
$\neg(p \wedge q) \equiv \neg p \vee \neg q$ $\neg(p \vee q) \equiv \neg p \wedge \neg q$	Leis de De Morgan
$p \rightarrow q \equiv \neg p \vee q$	

$p \vee \neg p \equiv \mathsf{V}$ $p \wedge \neg p \equiv \mathsf{F}$	Lei do terceiro excluído Lei da contradição
$p \wedge \mathsf{V} \equiv p$ $p \vee \mathsf{F} \equiv p$	Leis da identidade
$p \vee \mathsf{V} \equiv \mathsf{V}$ $p \wedge \mathsf{F} \equiv \mathsf{F}$	Leis do elemento dominante
$p \vee p \equiv p$ $p \wedge p \equiv p$	Leis da idempotência
$\neg(\neg p) \equiv p$	Lei da dupla negação
$p \vee q \equiv q \vee p$ $p \wedge q \equiv q \wedge p$	Leis da comutatividade

MP (modus ponens)

$$\frac{p \rightarrow q,\ p}{\therefore q}$$

MT (modus tollens)

$$\frac{p \rightarrow q,\ \neg q}{\therefore \neg p}$$

Conj (conjunção)

$$\frac{p,\ q}{\therefore p \wedge q}$$

Ad (adição)

$$\frac{p}{\therefore p \vee q}$$

SD (silogismo disjuntivo)

$$\frac{p \vee q,\ \neg p}{\therefore q}$$

SH (silogismo hipotético)

$$\frac{p \rightarrow q,\ q \rightarrow r}{\therefore p \rightarrow q}$$

A é uma tautologia se e só se $A(p/\mathsf{V})$ e $A(p/\mathsf{F})$ são tautologias.

Método de Quine

A é uma contradição se e só se $A(p/\mathsf{V})$ e $A(p/\mathsf{F})$ são contradições.

A é contingência se e só se A(p/V) e A(p/F) têm valores lógicos diferentes.

diz-se um *argumento correcto* se $A_1 \wedge A_2 \wedge \cdots \wedge A_n \rightarrow B$ for uma tautologia. Neste caso também se costuma escrever

$$A_1, A_2, \ldots, A_n \models B$$

Um literal é uma variável proposicional ou a sua negação; por exemplo, p e $\neg p$ são literais (ditos *literais complementares*).

Uma fbf diz-se uma *forma normal disjuntiva* (FND) se for da forma $C_1 \vee C_2 \vee \cdots \vee C_n$, onde cada C_i é uma conjunção de literais (chamada *conjunção fundamental*).

Analogamente, uma fbf diz-se uma *forma normal conjuntiva* (FNC) se for da forma $D_1 \wedge D_2 \wedge \cdots \wedge D_n$, onde cada D_i é uma disjunção de literais (chamada *disjunção fundamental*).

p	q	$f(p,q)$	Partes FND	Partes FNC
V	V	V	$p \wedge q$	
V	F	V	$p \wedge \neg q$	
F	V	F		$p \vee \neg q$
F	F	V	$\neg p \wedge \neg q$	

Assim, $f(p,q)$ pode ser escrita nas formas:

$$f(p,q) \equiv (p \wedge q) \vee (p \wedge \neg q) \vee (\neg p \wedge \neg q) \quad \text{(FND)}$$

$$f(p,q) \equiv p \vee \neg q \quad \text{(FNC)}.$$

Um conjunto de conectivos lógicos diz-se *completo* se toda a fbf do cálculo proposicional é equivalente a uma fbf onde figuram apenas conectivos desse conjunto. É claro que

$$\{\neg, \wedge, \vee, \rightarrow\}$$

é completo, por definição.

$$\neg[\exists x\, P(x)] \equiv \forall x\, [\neg P(x)], \quad \neg[\forall x\, P(x)] \equiv \exists x\, [\neg P(x)].$$

Predicados unários

Sentença atómica	Interpretação
$Tet(a)$	a é um tetraedro
$Cube(a)$	a é um cubo
$Dodec(a)$	a é um dodecaedro
$Small(a)$	a é pequeno
$Medium(a)$	a é médio
$Large(a)$	a é grande

Predicados binários

Sentença atómica	Interpretação
$SameSize(a,b)$	a tem o mesmo tamanho que b
$SameShape(a,b)$	a tem a mesma forma que b
$Larger(a,b)$	a é maior que b
$Smaller(a,b)$	a é menor que b
$SameCol(a,b)$	a está na mesma coluna que b
$SameRow(a,b)$	a está na mesma linha que b
$Adjoins(a,b)$	a e b estão localizados em casas adjacentes (mas não na diagonal)
$LeftOf(a,b)$	a está numa coluna à esquerda de b
$RightOf(a,b)$	a está numa coluna à direita de b
$FrontOf(a,b)$	a está numa linha à frente de b
$BackOf(a,b)$	a está numa linha atrás de b

Predicados ternários

Sentença atómica	Interpretação
$Between(a,b,c)$	a, b e c estão na mesma coluna, linha ou diagonal, e a está entre b e c.

Princípio de Indução Matemática (PIM). *Seja $P(n)$, $n \in \{a, a+1, \ldots\}$, uma proposição. Para provar que $P(n)$ é verdadeira para qualquer $n \geq a$ basta:*

(1) (Passo inicial) *Mostrar que $P(a)$ é verdadeira.*

(2) (Passo indutivo) *Mostrar que a implicação $P(k) \rightarrow P(k+1)$ é verdadeira para qualquer $k \geq a$.*

(1) *Distributividade:* $\sum_{i \in I} c\, a_i = c \sum_{i \in I} a_i$.

(2) *Associatividade:* $\sum_{i \in I} (a_i + b_i) = \sum_{i \in I} a_i + \sum_{i \in I} b_i$.

(3) *Comutatividade:* $\sum_{i \in I} a_i = \sum_{i \in I} a_{p(i)}$ *para qualquer bijecção (permutação)* $p : I \to I$.

(4) *Progressão constante:* $\sum_{i \in I} c = c\,|I|$.

$$\sum_{k=b}^{n} 1 = n - b + 1$$

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

(5) *Aditividade dos índices:* $\sum_{i \in I} a_i + \sum_{i \in J} a_i = \sum_{i \in (I \cup J)} a_i + \sum_{i \in (I \cap J)} a_i$ *(sendo J um conjunto finito também).*

(6) *Mudança de variável:* $\sum_{i \in I} a_{f(i)} = \sum_{j \in J} a_j$, *para qualquer função bijectiva* $f : I \to J$; *mais geralmente, para qualquer função* $f : I \to J$, $\sum_{i \in I} a_{f(i)} = \sum_{j \in J} \left(a_j \cdot \#(f^{-1}(\{j\}))\right)$.

Grafos:

Grafo simples: Não tem arestas múltiplas nem lacetes e tem arestas sem direção.

Multigrafo: Tem arestas múltiplas e sem direção, não tem lacetes.

Pseudografo: Tem arestas múltiplas e sem direção, tem lacetes.

Grafo dirigido simples: Grafo simples com arestas com direção.

Grafo dirigido: Pseudografo com arestas com direção.

Arestas múltiplas: $\forall v_0 \in V(G), \forall v_1 \in V(G), v_0 \neq v_1$: existe mais do que 1 aresta que liga v_0 e v_1.

Caminho: Seja (V,E) um grafo. Um caminho de comprimento n em (V,E) é uma sucessão $v_0, a_1, v_1, \dots, v_{n-1}, a_n, v_n$, onde cada v_j é um vértice em V e cada a_j uma aresta que liga v_{j-1} e v_j.

Matriz de incidência: Suponhamos $G=(V,E)$ um grafo tal que $V=\{v_1,\dots,v_n\}$ e $E=\{a_1,\dots,a_m\}$. A matriz de incidência B de G tem n linhas e m colunas e as entradas de B são 0 ou 1. No lugar (i,j) de B temos 1 se e só se $v_i \in a_j$. Relembrar que as arestas são da forma $a_j=\{v_i,v_j\}$ se a_j ligar v_i e v_j.

Matriz de adjacência: Suponhamos $G=(V,E)$ um grafo tal que $V=\{v_1,\dots,v_n\}$. A matriz de adjacência A é uma matriz $n\times n$ com entrada (i,j) igual ao número de arestas que ligam v_i e v_j.

Grau de um vértice v ($\deg(v)$/grau(v)/$g(v)$): O grau de um vértice v é o número de arestas que conectam com v (sendo que lacetes contam como 2 conexões distintas).

Lema dos apertos de mão: Seja $G=(V,E)$ um grafo com n vértices e m arestas e B a sua matriz de incidência:

$$\sum_{i=1}^{n} \deg(v_i) = \sum_{i=1}^{n} \begin{pmatrix}\text{soma dos elementos}\\ \text{na linha } i \text{ de } B\end{pmatrix} = \begin{pmatrix}\text{soma das}\\ \text{entradas de } B\end{pmatrix} = \sum_{j=1}^{m} \begin{pmatrix}\text{soma dos elementos}\\ \text{da coluna } j \text{ de } B\end{pmatrix} = \sum_{j=1}^{m} 2 = 2\sum_{j=1}^{m} 1 = 2(m-1+1) = 2m$$

Logo, o nº de arestas de um grafo é dado por $\frac{1}{2}\sum_{v\in G} \deg(v)$.

- Seja $G=(V,E)$ um grafo com n vértices e matriz de adjacência A. A entrada (i,j) de A^m, $m\in\mathbb{N}$ é o número de caminhos de comprimento m que unem v_i e v_j. Se $m=1$, é o número de caminhos de comprimento 1, ou seja, o número de arestas que ligam V_i e V_j. Se $m=0$, $A^0=I_n$, ou seja, é o número de caminhos de comprimento 0, estes caminhos apenas existem entre V_i e V_i.

Grafo euleriano: Um grafo G é euleriano se existe um caminho fechado (começa e acaba no mesmo vértice) tal que cada aresta aparece exatamente uma vez neste caminho. G é euleriano $\Leftrightarrow$ G for conexo e o grau de qualquer vértice de G for par.

Grafo conexo: Um grafo é conexo se para qualquer par de vértices de G existir um caminho que os liga.

Grafo completo: Um grafo é completo se para qualquer par de vértices distintos de G, existe exatamente uma aresta que os liga.

Grafos isomorfos: Os grafos G_1 e G_2 são isomorfos se existe uma bijeção f de vértices de G_1 para vértices de G_2 tal que o número de arestas entre $V \in G_1$ e $U \in G_1$ é igual ao número de arestas entre $f(v) \in G_2$ e $f(u) \in G_2$.

Grafo regular: Um grafo G é regular de grau d se cada vértice de G tem grau d. Todos os grafos completos são regulares. Num grafo regular temos, pelo lema dos apertos de mão, que $\#\text{arestas} = (d/2) \times \#\text{vértices}$. Assim n é par ou d é par.

Grafo semi-euleriano: Um grafo é semi-euleriano se existe um caminho tal que cada aresta aparece exatamente uma vez neste caminho. G é semi-euleriano é euleriano $\Leftrightarrow$ G for conexo e todos os vértices têm grau par ou exatamente 2 vértices têm grau ímpar.

Árvore: Uma árvore é um grafo conexo sem ciclos (um ciclo é um caminho fechado sem arestas repetidas). Um grafo G é uma árvore $\Leftrightarrow$ entre qualquer par de vértices existe exatamente um caminho que os liga sem arestas repetidas.

Árvore com raiz: Seja G uma árvore. Fixamos um vértice r como raiz de G e orientamos as arestas de G:

- Orientamos cada aresta que sai de r na direção oposta de r.
- Se já temos uma aresta orientada que entra em $v \in G$, orientamos todas as outras arestas que saiam de v na direção oposta de v.

Profundidade: A profundidade de $V \in G$, sendo G uma árvore com raiz, é:

- $\text{prof}(r) = 0$
- Sejam $V, U \in G$ vértices tal que $V \longrightarrow U$, então $\text{prof}(U) = \text{prof}(V) + 1$
- U é ascendente de $V \Leftrightarrow \text{prof}(U) = \text{prof}(V) - 1$.
- U é descendente de $V \Leftrightarrow \text{prof}(U) = \text{prof}(V) + 1$.

Grafo bipartido: Um grafo $G = (V, E)$ é bipartido se podemos separar V em V_1 e V_2, $V_1 \neq V_2$, tal que, para qualquer aresta de G, esta liga dois vértices de subconjuntos diferentes.

- Se uma árvore G tem n vértices, então:
  - G tem $n-1$ arestas.
  - $\sum_{v \in V} \deg(v) = 2\#\text{arestas} = 2(n-1)$.
  - n_d é o número de vértices em G com grau d. Se $d \geq n$ temos sempre $n_d = 0$.
  - $2(n-1) = 2\#\text{arestas} = \sum_{v \in V} \deg(v) = \sum_{d=1}^{n-1} (d \times n_d)$ e $\sum_{d=1}^{n-1} n_d = n$.

Teoria dos números

Divisão com resto: $\forall n,d \in \mathbb{Z}, d \neq 0, \exists q,r \in \mathbb{Z}: n = q \times d + r \wedge 0 \leq r \leq |d| - 1$

- Divisão de n por d, $d<0$: $n = q \times (-d) + r \Rightarrow n = (-q) \times d + r$

- Divisão de n por d, $n<0$: $(-n) = q \times d + r \Rightarrow n = (-q) \times d - r = (-q) \times d - d + d - r = (-q-1) \times d + (d-r)$. ($r<d \Rightarrow >0$)

- Divisão de n por d, $d,n<0$: $(-n) = q \times (-d) + r \Rightarrow n = (-q) \times (-d) - r = (-q) \times (-d) + d - d - r = (-q-1) \times (-d) + (-d-r) =$ ($d<0 \Rightarrow -d>0 \wedge d>r \Rightarrow >0$)
  $= (q+1) \times d + (-d-r)$.

Divisor de um inteiro: $d \in \mathbb{Z}$ é divisor dum inteiro $n \in \mathbb{Z}$ se $\exists q \in \mathbb{Z}: n = q \times d$

Números primos: Um número primo é um inteiro positivo p diferente de 1 com apenas 2 divisores inteiros (1 e p).
Se $p \geq 11$, então o último algarismo de p é 1, 3, 7 ou 9.

Factorização prima: $\forall n \in \mathbb{N}, n \neq 0$ pode ser escrito como um produto $p_1 \times \dots \times p_k$, com $p_1, \dots, p_k$ números primos. Se $p_1 \times \dots \times p_k = q_1 \times \dots q_m$, com $p_1, \dots, p_k, q_1, \dots, q_m$ números primos, então $k=m$ e $q_1, \dots, q_k$ é uma permutação de $p_1, \dots, p_k$.

Maior divisor comum: Dizemos que d é o maior divisor comum de m e n, $m,n \in \mathbb{N}$ se d é um divisor de m e de n e se d' também o for, $d \geq d'$. $d = mdc(m,n)$.
- Suponhamos que $m = 2^{k_2} \times 3^{k_3} \times 5^{k_5} \times \dots \times p^{k_p}$ e $n = 2^{i_2} \times 3^{i_3} \times 5^{i_5} \times \dots \times p^{i_p}$, então $mdc(m,n) =$
$= 2^{\min(k_2,i_2)} \times 3^{\min(k_3,i_3)} \times 5^{\min(k_5,i_5)} \times \dots \times p^{\min(k_p,i_p)}$.

Algoritmo de Euclides: $mdc(m,n) = mdc(m, n \bmod m)$, onde $n \bmod m$ é o resto da divisão inteira de n por m, $n \geq m$.

- Para $m \in \mathbb{N}, m \geq 2$, definimos $\mathbb{Z}_m = \{0, 1, \dots, m-1\}$:
  - $a +_m b = (a+b) \bmod m$
  - $a -_m b = (a-b) \bmod m$
  - $a \times_m b = (a \times b) \bmod m$
  - $a +_m x = b \Leftrightarrow x = (b-a) \bmod m$
  - $a -_m x = b \Leftrightarrow x = a +_m b = (a+b) \bmod m$
  - $a =_m b \Leftrightarrow a \bmod m = b \bmod m$
  - $a \times_m x = b$, resolvemos $a \times_m y = 1$ sendo que $y = a^{-1}$ e $x = y \times_m b$

Contagem:

- Seja A um conjunto finito, $|A|$ ou $\#A$ é o número de elementos em A.
- Sejam A e B dois conjuntos, $A \times B$ é o conjunto de pares (a,b), $a \in A$, $b \in B$.

Princípio da multiplicação: $|A \times B| = |A| \times |B|$

Princípio da adição: Se $A \cap B = \emptyset \Rightarrow |A \cup B| = |A| + |B|$.

Permutações: Seja S um conjunto com n elementos. Uma permutação de S, r a r, é uma sucessão $(s_1, \ldots, s_r)$ de elementos distintos de S e o número de permutações é $P(n,r) = \frac{n!}{(n-r)!}$.

$$\begin{pmatrix}\text{Permutação de } \{1,\ldots,n\},\\ r+1 \text{ a } r+1 \text{ que começam}\\ \text{com } j\end{pmatrix} \overset{1:1}{\leftrightarrow} \begin{pmatrix}\text{Permutação de}\\ \{1,\ldots,n-1\},\\ r \text{ a } r\end{pmatrix}$$

$$j\, s_2 \ldots s_{r+1} \leftrightarrow \begin{cases} s_2, \text{ se } s_2 < j \\ s_2 - 1, \text{ se } s_2 > j \end{cases} \ldots \begin{cases} s_{r+1}, \text{ se } s_{r+1} < j \\ s_{r+1} - 1, \text{ se } s_{r+1} > j \end{cases}$$

Combinações: Seja S um conjunto com n elementos. $C(n,r)$ é o número de combinações de S, r a r, e é igual a $\frac{n!}{(n-r)!r!}$. Assim, $C(n,r)r! = P(n,r) \Leftrightarrow C(n,r)P(r,r) = P(n,r)$.

- $(x+y)^n$, $n \in \mathbb{N}, n \geq 1$: O coeficiente de $x^k y^{n-k}$ é $C(n,k)$.

Permutações com repetição: $\overline{P}(n,r) = n^r$

Multi-subconjunto: Um multi-subconjunto de S é um conjunto onde permitimos a repetição de elementos de S.

-Exemplos:

- $\{1,1,2,2,2\}$ é um multi-subconjunto de $\{1,2,3\}$. Podemos abreviar $\{1,1,2,2,2\}$ para $\{2\times 1, 3\times 2, 0\times 3\}$.

- Conjunto $\{a_1, a_2, a_3, a_4\}$:
  - Multi-subconjuntos: $\{a_1, a_1, a_2, a_4, a_4, a_4\}$ e $\{a_2, a_2, a_3, a_3, a_3, a_3\}$ (por exemplo)
  - Representações: $**|*||***$ e $|**|*****|$

Combinações com repetição: Escrevemos $\overline{C}(n,r)$ para o número de multi-subconjuntos de r elementos dum conjunto com n elementos e $\overline{C}(n,r) = C(n+r-1, n-1) = C(n+r-1, r)$.