

Matemática Discreta

2010/11

Vítor H. Fernandes

Departamento de Matemática
FCT/UNL

Parcialmente baseados em slides elaborados pelo Prof. Dr. Jorge André

Programa

1 Parte 1 - Conjuntos e Aplicações

- 1 Conjuntos, relações binárias e indução matemática
- 2 Funções
- 3 Divisibilidade
- 4 Congruências lineares
- 5 Relações de recorrência

2 Parte 2 - Grafos e Aplicações

- 1 Generalidades
- 2 Conexidade
- 3 Árvores
- 4 Grafos Eulerianos
- 5 Grafos Hamiltonianos
- 6 Matrizes e grafos

1.1 Conjuntos, relações binárias e indução matemática

Representamos por:

- $\mathbb{N} = \{1, 2, 3, \dots\}$, o conjunto dos números naturais;
- $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$, o conjunto dos números inteiros;
- $\mathbb{Q} = \{\frac{p}{q} \mid p \in \mathbb{Z}, q \in \mathbb{Z} \text{ e } q \neq 0\}$, o conjunto dos números racionais;
- $\mathbb{R}$, o conjunto dos números reais;
- $\emptyset$, o conjunto vazio, i.e. o conjunto sem quaisquer elementos.

Sejam A e B dois conjuntos. Recordemos que:

- A e B são iguais se têm os mesmos elementos, i.e. $(\forall x) x \in A \Leftrightarrow x \in B$;
- A está contido em B , e denotamos por $A \subseteq B$, se todo o elemento de A é também um elemento de B , i.e. $(\forall x) x \in A \Rightarrow x \in B$.

- A é subconjunto próprio de B (ou que A está estritamente contido em B), e denotamos por $A \subsetneq B$, se A está contido em B e A é diferente de B ;
- $A = B$ se e só se $A \subseteq B$ e $B \subseteq A$;
- A união de A com B é o conjunto

$$A \cup B = \{x \mid x \in A \text{ ou } x \in B\};$$

- A intersecção de A com B é o conjunto

$$A \cap B = \{x \mid x \in A \text{ e } x \in B\};$$

- O complementar de B em A é o conjunto

$$A \setminus B = \{x \mid x \in A \text{ e } x \notin B\};$$

- Fixado um universo U , o complementar de $A \subseteq U$ é o conjunto

$$\bar{A} = \{x \in U \mid x \notin A\},$$

ou seja, $\bar{A} = U \setminus A$ (o complementar de A em U).

Sejam x e y dois elementos. Definimos o **par ordenado** formado por x e y como sendo o conjunto

$$(x, y) = \{\{x\}, \{x, y\}\}.$$

A propriedade fundamental deste conceito é a seguinte: dados elementos x, y, u e v , temos

$$(x, y) = (u, v) \text{ se e só se } x = u \text{ e } y = v.$$

Recorde que o **produto cartesiano** de dois conjuntos A e B é o conjunto de pares ordenados

$$A \times B = \{(a, b) \mid a \in A \text{ e } b \in B\}.$$

Mais geralmente, um **n -uplo ordenado** define-se por

$$(x_1, x_2, \dots, x_n) = (x_1, (x_2, (\dots, (x_{n-1}, x_n))))$$

e o **produto cartesiano** dos conjuntos $A_1, \dots, A_n$ é o conjunto

$$A_1 \times A_2 \times \dots \times A_n = \{(a_1, a_2, \dots, a_n) \mid a_i \in A_i \text{ e } i \in \{1, \dots, n\}\}.$$

Se $A = A_1 = A_2 = \dots = A_n$ representamos $A_1 \times A_2 \times \dots \times A_n$ por A^n .

Definição

Seja X um conjunto. Chamamos **relação binária** sobre X a todo o subconjunto de $X \times X$.

Mais geralmente, uma **relação n -ária** ($n \in \mathbb{N}$) sobre X é um subconjunto de X^n .

Exemplos

- Seja $X = \{1, 2, 3\}$. O conjunto $R = \{(1, 1), (2, 3), (3, 2)\}$ é uma relação binária sobre X .
- Sejam $X = \{1, 2, 3, 4\}$. O conjunto $R = \{(x, y) \in X^2 \mid x + y \leq 5\}$ é uma relação binária sobre X .

Notação

Sejam X um conjunto e R uma relação binária sobre X . Dado um par $(x, y) \in X \times X$, escrevemos também **xRy** para designar que $(x, y) \in R$.

Seja A um conjunto. Recorde que o **conjunto das partes** de A é o conjunto (de conjuntos)

$$\mathcal{P}(A) = \{X \mid X \subseteq A\}.$$

Observe que, $\emptyset \in \mathcal{P}(A)$ e $A \in \mathcal{P}(A)$.

Considere agora um conjunto de conjuntos $\mathcal{A}$ (i.e. $\mathcal{A} \subseteq \mathcal{P}(A)$, para algum conjunto A) não vazio. Definimos a **união de $\mathcal{A}$** e a **intersecção de $\mathcal{A}$** por

$$\cup \mathcal{A} = \{x \mid (\exists X \in \mathcal{A}) x \in X\} \text{ e } \cap \mathcal{A} = \{x \mid (\forall X \in \mathcal{A}) x \in X\},$$

respectivamente. Se $\mathcal{A} = \{A_i \mid i \in I\}$, também escrevemos

$$\cup \mathcal{A} = \bigcup_{i \in I} A_i \text{ e } \cap \mathcal{A} = \bigcap_{i \in I} A_i.$$

Se $\mathcal{A} = \{A_1, A_2, \dots, A_n\}$ então

$$\cup \mathcal{A} = \bigcup_{i=1}^n A_i = A_1 \cup A_2 \cup \dots \cup A_n \text{ e } \cap \mathcal{A} = \bigcap_{i=1}^n A_i = A_1 \cap A_2 \cap \dots \cap A_n.$$

Definição

Sejam X e Y dois conjuntos. Uma **relação de X em Y** é um subconjunto de $X \times Y$. (No caso particular em que $X = Y$ temos uma relação binária sobre X .)

Seja R uma relação de X em Y . Chamamos **domínio** de R ao conjunto

$$\text{dom} R = \{x \in X \mid (\exists y \in Y) (x, y) \in R\},$$

e **imagem** de R ao conjunto

$$\text{im} R = \{y \in Y \mid (\exists x \in X) (x, y) \in R\}.$$

A **relação inversa** de R é a relação R^{-1} de Y em X definida por

$$R^{-1} = \{(y, x) \mid (x, y) \in R\}.$$

A **relação composta** da relação R de X em Y com a relação S de Y em Z é a relação $S \circ R$ de X em Z definida por

$$S \circ R = \{(x, z) \mid (\exists a \in Y) (x, a) \in R \text{ e } (a, z) \in S\}.$$

Representação de uma relação binária

Seja R uma relação binária sobre um conjunto finito $X = \{x_1, \dots, x_n\}$.

- 1 Através de uma **matriz de adjacências**:

a matriz de adjacências de R é a matriz $A = [a_{ij}]_{n \times n} \in \mathcal{M}_{n \times n}(\{0, 1\})$ definida por:

$$a_{ij} = \begin{cases} 1 & \text{se } (x_i, x_j) \in R \\ 0 & \text{se } (x_i, x_j) \notin R \end{cases}$$

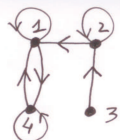
- 2 Através de um **diagrama**:

os elementos de X são representados por pontos e dois pontos do diagrama que representam x_i e x_j estão unidos por uma seta, com orientação de x_i para x_j , se $(x_i, x_j) \in R$.

Exemplo

Sejam $X = \{1, 2, 3, 4\}$ e $R = \{(1, 1), (1, 4), (2, 1), (2, 2), (3, 2), (4, 1), (4, 4)\}$. A matriz das adjacências de R (considerando $x_i = i$, $i = 1, 2, 3, 4$) é a matriz

$$\begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix} \text{ e}$$



é um diagrama que representa R .

- A relação R definida em $\mathbb{R}$ por, para quaisquer $x, y \in \mathbb{R}$,

$$xRy \Leftrightarrow x^2 = y^2,$$

é uma relação de equivalência.

- Em $\mathbb{Z}$ a relação $\sim$ definida por, para quaisquer $m, n \in \mathbb{Z}$,

$$m \sim n \Leftrightarrow |m| = |n|,$$

é uma relação de equivalência

- Sejam X um conjunto e $\Delta = \{(x, x) \mid x \in X\}$. Então Δ é uma relação de equivalência sobre X (denominada **relação identidade** sobre X).
- Sejam X um conjunto e $\Omega = \{(x, y) \mid x, y \in X\}$. Então Ω é uma relação de equivalência sobre X (denominada **relação universal** sobre X).
- Para cada $x \in \mathbb{R}$, denotemos por $\lfloor x \rfloor$ o maior número inteiro y tal que $y \leq x$ (parte inteira de x). A relação $\sim$ definida em $\mathbb{R}$ por, para quaisquer $x, y \in \mathbb{R}$,

$$x \sim y \Leftrightarrow \lfloor x \rfloor = \lfloor y \rfloor,$$

é uma relação de equivalência.

Definição

Dizemos que uma relação binária R sobre X é:

- reflexiva** se $(\forall x \in X) xRx$;
- irreflexiva** se $(\forall x \in X) (x, x) \notin R$;
- simétrica** se $(\forall x, y \in X) xRy \Rightarrow yRx$;
- anti-simétrica** se $(\forall x, y \in X) xRy \wedge yRx \Rightarrow x = y$;
- transitiva** se $(\forall x, y, z \in X) xRy \wedge yRz \Rightarrow xRz$.

Definição

Uma relação binária reflexiva, simétrica e transitiva diz-se uma **relação de equivalência**.

Exemplos

- Seja $X = \{1, 2, 3, 4\}$. A relação $R = \{(1, 1), (1, 2), (4, 1), (2, 2), (3, 3), (1, 4), (2, 1), (4, 4)\}$ não é uma relação de equivalência.

Definição

Dados uma relação de equivalência R num conjunto X e um elemento $a \in X$, chamamos **classe de equivalência** de a (módulo R), que representamos usualmente por $[a]_R$ (ou, se não houver ambiguidade, simplesmente por $[a]$ ou, em certos casos, por $\bar{a}$), ao conjunto dos elementos x de X tais que $(x, a) \in R$, isto é a

$$[a]_R = \{x \in X \mid xRa\}.$$

Ao conjunto cujos elementos são as classes de equivalência $[a]_R$, com $a \in X$, chamamos **conjunto cociente** de X por R e representamo-lo por X/R .

Exemplo

Seja $X = \{1, 2, 3, 4, 5\}$. A relação $R = \{(1, 1), (2, 2), (3, 3), (4, 4), (5, 5), (1, 2), (2, 1), (1, 5), (5, 1), (2, 5), (5, 2)\}$ é uma equivalência sobre X e temos $[1] = \{1, 2, 5\} = [2] = [5]$, $[3] = \{3\}$, $[4] = \{4\}$, donde $X/R = \{\{1, 2, 5\}, \{3\}, \{4\}\}$.

Exemplo

Fixado $n \in \mathbb{N}$, em $\mathbb{Z}$ definimos uma relação de equivalência $\equiv_n$ da seguinte forma: para quaisquer $x, y \in \mathbb{Z}$,

$$x \equiv_n y \iff (\exists k \in \mathbb{Z}) x - y = kn.$$

Designamos esta relação em $\mathbb{Z}$ por **relação de congruência módulo n** .

Para indicar que $x \equiv_n y$, usualmente escrevemos $x \equiv y \pmod{n}$.

No capítulo 1.4 (Congruências lineares), estudaremos alguns aspectos desta relação de equivalência. Por exemplo, mostraremos que

$$\begin{aligned} \overline{0} &= \{\dots, -2n, -n, 0, n, 2n, \dots\} = n\mathbb{Z}, \\ \overline{1} &= \{\dots, 1-2n, 1-n, 1, 1+n, 1+2n, \dots\} = 1 + n\mathbb{Z}, \\ &\vdots \\ \overline{k} &= \{\dots, k-2n, k-n, k, k+n, k+2n, \dots\} = k + n\mathbb{Z}, \\ &\vdots \\ \overline{n-1} &= \{\dots, -n-1, -1, n-1, 2n-1, 3n-1, \dots\} = (n-1) + n\mathbb{Z}, \end{aligned}$$

donde $\mathbb{Z}_n = \mathbb{Z}/R = \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}$.

Definição

Seja X um conjunto. Dizemos que um conjunto não vazio $\{X_i \mid i \in I\}$ de subconjuntos não vazios de X é uma **partição** de X se:

- ① $X = \bigcup_{i \in I} X_i$
- ② $i \neq j \implies X_i \cap X_j = \emptyset$, para quaisquer $i, j \in I$.

Exemplos

- Seja X um conjunto. Se $A \in \mathcal{P}(X)$ é tal que $\emptyset \subsetneq A \subsetneq X$, então $\{A, \overline{A}\}$ é uma partição de X .
- Seja $X = \{1, 2, 3, 4\}$. Então, por exemplo,

$$\{\{1\}, \{2\}, \{3\}, \{4\}\}, \quad \{\{1, 2\}, \{3, 4\}\}, \quad \{\{1, 3\}, \{2\}, \{4\}\} \quad \text{e} \quad \{\{1, 2, 3, 4\}\}$$

são partições de X . Pelo contrário, por exemplo,

$$\{\{1, 2\}, \{3\}\} \quad \text{e} \quad \{\{1, 2\}, \{1, 3, 4\}\}$$

não são partições de X .

Proposição

Sejam X um conjunto e R uma relação de equivalência sobre X . Para quaisquer $a, b \in X$, as seguintes afirmações são equivalentes:

- ① bRa ;
- ② $b \in [a]_R$;
- ③ $[b]_R = [a]_R$.

Teorema

Sejam X um conjunto e R uma relação de equivalência sobre X . Temos:

- ① Para qualquer $x \in X$, $[x]_R \neq \emptyset$;
- ② Para quaisquer $x, y \in X$, $[x]_R = [y]_R$ ou $[x]_R \cap [y]_R = \emptyset$;
- ③ $X = \bigcup_{x \in X} [x]_R$;
- ④ A relação R fica determinada pelas suas classes de equivalência.

Teorema

- ① Se R é uma relação de equivalência sobre X , então o conjunto cociente X/R é uma partição de X .
- ② Se $\mathcal{P} = \{X_i \mid i \in I\}$ é uma partição de X e R é a relação binária sobre X definida por

$$xRy \iff (\exists i \in I) x, y \in X_i,$$

para quaisquer $x, y \in X$, então:

- R é relação de equivalência sobre X ;
- $\mathcal{P} = X/R$.

Exemplo

Seja $X = \{1, 2, 3, 4, 5\}$ e consideremos a partição $\mathcal{P} = \{\{1, 2\}, \{3, 5\}, \{4\}\}$ de X . Então, $\mathcal{P}$ determina a seguinte relação de equivalência sobre X :

$$R = \{(1, 1), (2, 2), (1, 2), (2, 1), (3, 3), (5, 5), (3, 5), (5, 3), (4, 4)\}.$$

Definição

Uma relação binária reflexiva, anti-simétrica e transitiva diz-se uma **relação de ordem parcial** (abreviadamente: r.o.p.).

As r.o.p. são usualmente denotadas pelos símbolos $\leq$ ou por $\subseteq$.

Definições

Seja $\leq$ uma relação de ordem parcial sobre um conjunto X . Dizemos que:

- Os elementos x e y de X são **comparáveis** se $x \leq y$ ou $y \leq x$;
- $\leq$ é uma **relação de ordem total** se quaisquer dois elementos de X são comparáveis.

Sejam $\leq$ uma r.o.p. sobre X e $x, y \in X$. Escrevemos $x < y$ para significar que $x \leq y$ e $x \neq y$.

Definição

Sejam X um conjunto e $\leq$ uma r.o.p. sobre X . Dizemos que o par $(X, \leq)$ é um **conjunto parcialmente ordenado** (abreviadamente: c.p.o.). Se $\leq$ for uma ordem total, dizemos que $(X, \leq)$ é um **conjunto totalmente ordenado** ou uma **cadeia** (abreviadamente: c.t.o.).

Diagrama de Hasse

Sejam $X = \{x_1, x_2, \dots, x_n\}$ e $\leq$ uma r.o.p. em X . A relação $\leq$ pode ser representada através de um diagrama (denominado **diagrama de Hasse**) construído do seguinte modo: os elementos de X são os pontos do diagrama e, para quaisquer $x, y \in X$, se y **cobre** x , colocamos o ponto que representa y “acima” do ponto que representa x e unimo-os com um segmento de recta:



Exemplos

- Consideremos o c.p.o. $(\{1, 2, 3, 4\}, \leq)$, em que $\leq$ é a ordem usual. Esta cadeia tem o seguinte diagrama de Hasse:



Exemplos

- Seja $\leq$ a relação de ordem usual em $\mathbb{R}$. Então $(\mathbb{R}, \leq)$ é uma cadeia. Também $(\mathbb{N}, \leq)$, $(\mathbb{Z}, \leq)$ e $(\mathbb{Q}, \leq)$ são cadeias (para a ordem usual).
- Seja X um conjunto. A relação de inclusão $\subseteq$ definida sobre $\mathcal{P}(X)$ é uma relação de ordem parcial em $\mathcal{P}(X)$, pelo que $(\mathcal{P}(X), \subseteq)$ é um c.p.o..
- Em $\mathbb{N}$ definimos a seguinte relação binária (relação de divisibilidade) $|$:

$$a|b \text{ (a divide b)} \iff (\exists c \in \mathbb{N}) ac = b,$$

para quaisquer $a, b \in \mathbb{N}$. Então, $(\mathbb{N}, |)$ é um c.p.o..

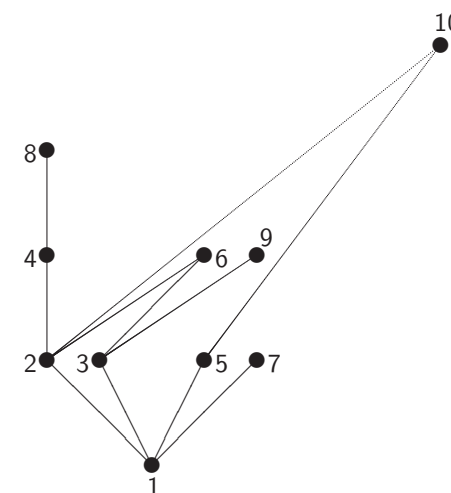
Definição

Seja $(X, \leq)$ um c.p.o.. Dados $x, y \in X$, dizemos que y **cobre** x (relativamente a $\leq$) se $x \leq y$ e não existe $z \in X$ tal que $x < z < y$, i.e., equivalentemente, se $x \leq y$ e, para qualquer $z \in X$,

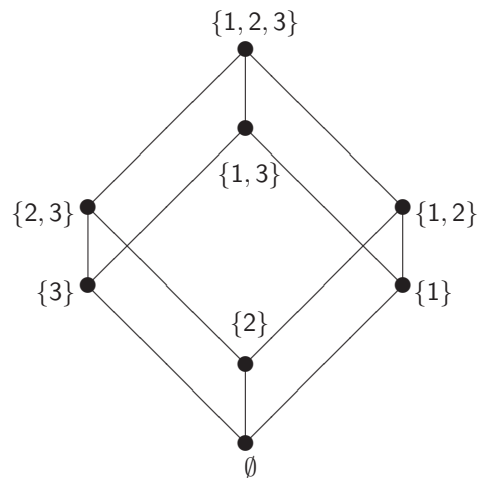
$$x \leq z \leq y \Rightarrow z = x \vee z = y.$$

Escrevemos $x << y$ para denotar que y cobre x .

- O c.p.o. $(\{1, 2, \dots, 10\}, |)$, em que $|$ é relação de divisibilidade, tem o seguinte diagrama de Hasse:



- O c.p.o. $(\mathcal{P}(\{1, 2, 3\}), \subseteq)$ possui o seguinte diagrama de Hasse:



Definição

Sejam $(X, \leq)$ um c.p.o. e $Y \subseteq X$.

- Dizemos que $a \in X$ é um **minorante** [resp. **majorante**] de Y se $a \leq y$ [resp. $y \leq a$], para qualquer $y \in Y$.
- Chamamos **primeiro elemento** de Y (ou **mínimo** de Y) a um elemento $a \in Y$ tal que $a \leq y$, para qualquer $y \in Y$.
- Chamamos **último elemento** de Y (ou **máximo** de Y) a um elemento $b \in Y$ tal que $y \leq b$, para qualquer $y \in Y$.
- Dizemos que $a \in Y$ é um **elemento minimal** [resp. **maximal**] de Y se não existe $b \in Y$ tal que $b < a$ (resp. $a < b$).
- Dizemos que $a \in X$ é o **ínfimo** [resp. **supremo**] de Y se a é o maior (i.e. o máximo) dos minorantes [resp. o menor (i.e. o mínimo) dos majorantes].

(Exemplos no quadro)

Exemplo

$2n + 1 \leq 2^n$, para qualquer natural $n \geq 3$.

Teorema (Segundo Princípio de Indução / Princípio de Indução Completa)

Sejam $k \in \mathbb{N}_0$, $\mathbb{N}_k = \{n \in \mathbb{N} \mid n \geq k\}$ e S um subconjunto de $\mathbb{N}_k$ tal que:

- $k \in S$;
- Para qualquer $n \in \mathbb{N}_k$, se $t \in S$, para todo o $t \in \{k, \dots, n\}$, então $n + 1 \in S$ (i.e. $(\forall n \in \mathbb{N}_k) [(\forall t \in \{k, \dots, n\}) t \in S] \implies n + 1 \in S$).

Então, $S = \mathbb{N}_k$.

Exemplo

Consideremos a sucessão $(a_n)_{n \geq 0}$ definida por

$$\begin{cases} a_0 = 1 \\ a_1 = 2 \\ a_n = 4a_{n-1} - 4a_{n-2} \end{cases} \quad . \quad \text{Então } a_n = 2^n, \text{ para qualquer } n \in \mathbb{N}_0.$$

Axioma (Princípio da Boa Ordenação dos Números Naturais)

O conjunto parcialmente (totalmente) ordenado $(\mathbb{N}, \leq)$, em que $\leq$ é a relação de ordem usual, é um conjunto bem ordenado, i.e. todo o subconjunto não vazio de $\mathbb{N}$ possui primeiro elemento.

Como provar que a soma dos primeiros n números naturais é $\frac{1}{2}n(n+1)$, para qualquer $n \in \mathbb{N}$?

Teorema (Princípio de Indução)

Sejam $k \in \mathbb{N}_0$, $\mathbb{N}_k = \{n \in \mathbb{N} \mid n \geq k\}$ e S um subconjunto de $\mathbb{N}_k$ tal que:

- $k \in S$;
- Para qualquer $n \in \mathbb{N}_k$, se $n \in S$ então $n + 1 \in S$.

Então, $S = \mathbb{N}_k$.

O Princípio de Indução pode ser reformulado utilizando uma condição de variável natural:

Princípio de Indução. *Sejam $k \in \mathbb{N}$ e $\Phi(n)$ uma condição, com $n \in \mathbb{N}_k$, tal que:*

- ① $\Phi(k)$ é uma proposição verdadeira;
- ② $\forall n \in \mathbb{N}_k, \Phi(n) \implies \Phi(n+1)$ é uma proposição verdadeira.

Então,

$$(\forall n \in \mathbb{N}_k) \Phi(n)$$

é uma proposição verdadeira.

Princípio de Indução Completa. *Sejam $k \in \mathbb{N}$ e $\Phi(n)$ uma condição, com $n \in \mathbb{N}_k$, tal que:*

- ① $\Phi(k)$ é uma proposição verdadeira;
- ② $\forall n \in \mathbb{N}_k, [(\forall k \leq t \leq n) \Phi(t)] \implies \Phi(n+1)$ é uma proposição verdadeira.

Então,

$$(\forall n \in \mathbb{N}_k) \Phi(n)$$

é uma proposição verdadeira.

Dado um conjunto finito X , denotamos por $|X|$ o número de elementos (cardinal) de X .

Teorema

Seja X um conjunto com n elementos ($n \in \mathbb{N}$). Então, $|\mathcal{P}(X)| = 2^n$.

Demonstração. Efectuamos a demonstração por indução em $|X|$.

Se $|X| = 0$ então $X = \emptyset$ e, portanto, $\mathcal{P}(X) = \{\emptyset\}$, pelo que $|\mathcal{P}(X)| = 1 = 2^0$.

Admitamos então (por hipótese de indução) que, para certo $n \geq 0$, $|\mathcal{P}(Y)| = 2^n$, para qualquer conjunto Y com n elementos.

Seja X um conjunto com $n+1$ elementos. Então, em particular, $X \neq \emptyset$.

Tomemos pois $x \in X$. Seja $Y = X \setminus \{x\}$. Então $|Y| = n$, pelo que, por hipótese de indução, $|\mathcal{P}(Y)| = 2^n$. Como

$$\mathcal{P}(X) = \mathcal{P}(Y) \cup \{Z \cup \{x\} \mid Z \in \mathcal{P}(Y)\},$$

com $\mathcal{P}(Y) \cap \{Z \cup \{x\} \mid Z \in \mathcal{P}(Y)\} = \emptyset$, temos

$$|\mathcal{P}(X)| = |\mathcal{P}(Y)| + |\{Z \cup \{x\} \mid Z \in \mathcal{P}(Y)\}| = 2^n + 2^n = 2 \cdot 2^n = 2^{n+1},$$

como queríamos demonstrar. □