Teoria da Computação **FCT-UNL, 2º semestre 2023-2024**

Notas 2: Conjuntos contáveis e não contáveis

Autor: João Ribeiro

Introdução

Nestas notas exploramos o conceito de cardinalidade de conjuntos e da comparação da cardinalidade de dois conjuntos, um conceito importante em matemática e, em particular, na teoria da computação. Estudaremos também o princípio da diagonalização, uma ideia importante na teoria da computação muito além dos tópicos aqui discutidos.

2.1 Cardinalidade e conjuntos contáveis e não contáveis

A cardinalidade de um conjunto finito é o número de elementos que este contém. Dados dois conjuntos finitos A e B, é bastante intuitivo comparar as suas cardinalidades – A tem uma cardinalidade maior que B exatamente quando $|A| > |B|$, e estes dois conjuntos têm a mesma cardinalidade quando $|A| = |B|$. No entanto, não é óbvio como estender esta caracterização da cardinalidade para o caso em que A e B são conjuntos infinitos. Por exemplo, como podemos comparar o conjunto dos naturais pares e dos naturais ímpares? Ou $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, e $\mathbb{R}$?

Uma perspectiva importante, introduzida por Georg Cantor no século XIX, consiste em interpretar a comparação da cardinalidade de dois conjuntos A e B através da existência de uma "correspondência" entre os elementos dos dois conjuntos. Por exemplo, seja $A = \{1, 2, 3\}$ e $B = \{a, b, c\}$. Então, temos $|A| = |B|$ pois podemos, de forma unívoca, ligar os elementos de A aos elementos de B da seguinte maneira,

$$\begin{aligned} 1 &\to a \\ 2 &\to b \\ 3 &\to c. \end{aligned}$$

De forma semelhante, o conjunto $A = \{1, 2, 3, 4\}$ é maior que o conjunto $B = \{a, b, c\}$ pois agora não existe tal correspondência unívoca: Para qualquer função $f : A \to B$ existem sempre $x, x' \in A$ distintos tais que $f(x) = f(x')$. Mais geralmente, introduzimos a seguinte definição.

Definição 2.1 *Dois conjuntos A e B têm a mesma cardinalidade se existe uma função bijectiva $f : A \to B$.*

No caso em que A e B são finitos, a Definição 2.1 é equivalente à comparação entre $|A|$ e $|B|$ mencionada acima. No entanto, esta definição faz igualmente sentido quando A e B são infinitos!

Dada esta nova definição, levantamos a seguinte questão: Será que todos os conjuntos infinitos têm a mesma cardinalidade?

Em particular, se um conjunto A tem a mesma cardinalidade que $\mathbb{N}$, então isso quer dizer que podemos "enumerar/contar" os elementos de A. Isto é, existe uma função $f : \mathbb{N} \to A$ tal que podemos escrever

$$A = \{f(0), f(1), f(2), \dots\}.$$

Mais formalmente, definimos o conceito de conjunto *contável*.

Definição 2.2 *Um conjunto A diz-se* contável *se existe uma função sobrejectiva $f : \mathbb{N} \to A$, e* não contável *caso contrário. Isto implica que:*

- *Um conjunto A é contável se e só se existe uma função injectiva $f : A \to \mathbb{N}$.*
- *Um conjunto A é contável se e só se A é finito ou existe uma função bijectiva $f : \mathbb{N} \to A$.*

Temos, agora, várias questões interessantes para estudar. Por exemplo, quais conjuntos são contáveis? E que propriedades satisfazem estes conjuntos? E será que existem conjuntos não contáveis?

2.2 Exemplos de conjuntos contáveis

Começamos por discutir alguns exemplos de conjuntos contáveis.

Exemplo 2.1 *O conjunto dos naturais pares tem a mesma cardinalidade que $\mathbb{N}$.*

Intuitivamente, podemos enumerar os elementos deste conjunto da seguinte forma,

$$0, 2, 4, 6, \dots$$

Para mostrarmos que o conjunto dos naturais pares, chamemos-lhe S, tem a mesma cardinalidade que $\mathbb{N}$ temos de mostrar a existência de uma função bijectiva $f : \mathbb{N} \to S$. Consideramos então $f(n) = 2n$. Primeiro, notamos que $f(n) \in S$ quando $n \in \mathbb{N}$. Resta agora mostrar que f é injectiva e sobrejectiva. Para vermos que f é injectiva, sejam $n, n' \in \mathbb{N}$ naturais distintos. Então, temos que $f(n) = 2n \neq 2n' = f(n')$, o que demonstra a injetividade. Para vermos que f é sobrejectiva, seja $m \in S$ qualquer. Pela definição de número par, segue que m pode ser escrito como $m = 2n$ para algum $n \in \mathbb{N}$. Concluímos que existe $n \in \mathbb{N}$ tal que $f(n) = 2n = m$, o que demonstra a sobrejetividade.

Exemplo 2.2 $\mathbb{Z}$ *é contável.*

Este exemplo pode parecer estranho à partida, pois $\mathbb{Z}$ parece ser muito maior do que $\mathbb{N}$! Depois de pensarmos um bocado, chegamos à conclusão de que, intuitivamente, podemos enumerar os elementos de $\mathbb{Z}$ da seguinte forma,

$$0, -1, 1, -2, 2, -3, 3, \dots$$

Formalmente, para mostrarmos que $\mathbb{Z}$ é contável basta mostrarmos a existência de uma função sobrejectiva $f : \mathbb{N} \to \mathbb{Z}$. Consideramos então a função f dada por

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

Resta mostrar que f é sobrejectiva. Seja $n \in \mathbb{Z}$ qualquer. Se $n \geq 0$, então $f(m) = n$ para $m = 2n$. Se $n < 0$, então $f(m) = n$ para $m = -2n + 1$.

Exemplo 2.3 *O conjunto dos racionais positivos* $\mathbb{Q}^+$ *é contável.*

Este é um exemplo inesperado! Como podemos enumerar todos os racionais? A ideia é usarmos uma "enumeração zig-zag", como a ilustrada na Figura 2.1. Deixamos uma demonstração mais formal como desafio para os alunos.

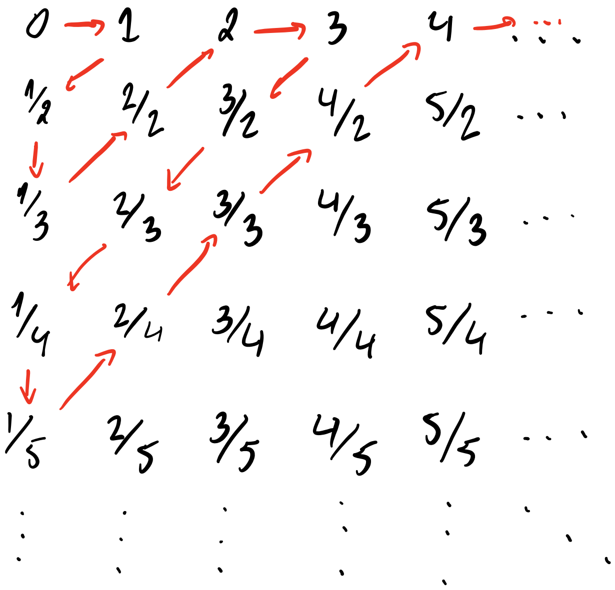

Figure 2.1: Construção de enumeração dos racionais não-negativos.

Finalmente, deixamos um exemplo muito útil (que representamos por um teorema) como desafio para os alunos.

Teorema 2.1 *O conjunto* $\mathbb{N}^2 = \mathbb{N} \times \mathbb{N}$ *é contável.*

Demonstração: Desafio para o aluno. ∎

2.3 Propriedades de conjuntos contáveis e não contáveis

Para entendermos melhor os conceitos de conjunto contável e não contável, demonstramos algumas propriedades úteis.

Teorema 2.2 *Seja A um conjunto contável e $B \subseteq A$. Então B também é contável.*

Demonstração: Sabemos que A é contável se e só se existe uma função injectiva $f : A \to \mathbb{N}$. Como $B \subseteq A$, consideramos a função $g : B \to \mathbb{N}$ dada por $g(x) = f(x)$ para qualquer $x \in B$. Como f é injectiva segue que g também é injectiva, e portanto B é contável. ∎

Teorema 2.3 *Seja A um conjunto não contável e B tal que $A \subseteq B$. Então B também não é contável.*

Demonstração: Este teorema é, simplesmente, o contra-recíproco do Teorema 2.2. Suponhamos que B é contável. Como $A \subseteq B$, o Teorema 2.2 garante que A também tem de ser contável. Isto contradiz a hipótese que A não é contável. ∎

Teorema 2.4 *Sejam A e B conjuntos contáveis. Então $A \cup B$ também é contável.*

Demonstração: Para mostrarmos que $A \cup B$ é contável basta encontrarmos uma função sobrejectiva $f : \mathbb{N} \to A \cup B$. Como A e B são contáveis por hipótese, sabemos que existem funções sobrejectivas $g : \mathbb{N} \to A$ e $h : \mathbb{N} \to B$. Intuitivamente, poderíamos enumerar todos os elementos de $A \cup B$ listando

$$g(0), h(0), g(1), h(1), g(2), h(2), \ldots$$

Com esta intuição em mente, consideremos a função $f : \mathbb{N} \to A \cup B$ dada por

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

Para percebermos que estamos no caminho certo, notamos que $f(0) = g(0), f(1) = h(0), f(2) = g(1), f(3) = h(1), \ldots$.

Resta mostrarmos que f é sobrejectiva. Seja $x \in A \cup B$ qualquer. Se $x \in A$, então existe m tal que $g(m) = x$. Escolhendo $n = 2m$, temos que $f(n) = g(m) = x$, pois n é par. Se $x \in B$, então existe m tal que $h(m) = x$. Escolhendo $n = 2m + 1$, temos que $f(n) = h(m) = x$, pois m é ímpar. ∎

Podemos generalizar a estratégia da demonstração do Teorema 2.4 para obter o seguinte teorema, cuja demonstração fica como desafio.

Teorema 2.5 *Seja $(A_i)_{i \in \mathbb{N}} = A_1, A_2, \ldots$ uma sequência de conjuntos contáveis. Então $\bigcup_{i \in \mathbb{N}} A_i$ também é contável.*

Demonstração: Desafio para o aluno. ∎

Teorema 2.6 *Sejam A e B conjuntos contáveis. Então $A \times B$ também é contável.*

Demonstração: Temos de mostrar a existência de uma função sobrejectiva $f : \mathbb{N} \to A \times B$. Como A e B são contáveis por hipótese, sabemos que existem funções sobrejectivas $g : \mathbb{N} \to A$ e $h : \mathbb{N} \to B$. Pelo Teorema 2.1 sabemos também que $\mathbb{N} \times \mathbb{N}$ é contável, e portanto existe uma função sobrejectiva $r : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$, que podemos escrever como $r(n) = (r_1(n), r_2(n))$ para algumas funções $r_1 : \mathbb{N} \to \mathbb{N}$ e $r_2 : \mathbb{N} \to \mathbb{N}$.

Consideremos a função $f : \mathbb{N} \to A \times B$ dada por

$$f(n) = (g(r_1(n)), h(r_2(n))).$$

Mostramos que f é sobrejectiva. Seja $(x, y) \in A \times B$ qualquer. Sabemos que existem $m_1, m_2 \in \mathbb{N}$ tal que $g(m_1) = x$ e $h(m_2) = y$, pois g e h são sobrejectivas. Como $r = (r_1, r_2)$ também é sobrejectiva, sabemos que existe n tal que $r(n) = (m_1, m_2)$. Temos, então, que

$$f(n) = (g(r_1(n)), h(r_2(n))) = (g(m_1), h(m_2)) = (x, y).$$

■

2.4 O princípio da diagonalização e conjuntos não contáveis

Dados os estranhos exemplos estudados anteriormente, é natural questionarmos se existem de todo conjuntos não contáveis. A existência de tais conjuntos foi estabelecida por Georg Cantor no século XIX através de uma técnica importante na teoria da computação – o princípio da diagonalização.

O objectivo da diagonalização é, dada uma suposta enumeração de um conjunto S, gerar de forma sistemática um elemento de S que não é enumerado. Como exemplo inicial, seja $S = \{0, 1\}^5$ o conjunto das sequências binárias de tamanho 5, e seja

$$\begin{aligned} s^1 &= \mathbf{1}0100 \\ s^2 &= 1\mathbf{0}000 \\ s^3 &= 11\mathbf{1}11 \\ s^4 &= 101\mathbf{1}0 \\ s^5 &= 0110\mathbf{0} \end{aligned}$$

uma suposta enumeração de S. Neste caso é, claro, fácil verificar que existem elementos de S que não aparecem na enumeração. Isto é, existe $s \in S$ tal que $s \neq s^i$ para todo o $i \in \{1, 2, 3, 4, 5\}$. A diagonalização permite-nos construir tal sequência s de forma sistemática da seguinte maneira: Consideremos os dígitos a negrito na enumeração acima, **10110**, que correspondem às posições s_i^i para $i \in \{1, 2, 3, 4, 5\}$. Escolhemos s que difere da diagonal **10110** em todas as posições. Isto implica que $s_i \neq s_i^i$ para $i \in \{1, 2, 3, 4, 5\}$, o que implica também que $s \neq s^i$ para todo o i. Mais precisamente, definimos $s_i = 1 - s_i^i$ (quando $s_i^i = 0$ temos $s_i = 1$, e vice-versa), o que resulta em $s = 01001$. Como $s_1 \neq s_1^1$ por construção de s, segue que $s \neq s^1$. E como $s_2 \neq s_2^2$ por construção de s, segue que $s \neq s^2$. Continuando desta forma, concluímos que $s \neq s^i$ para qualquer $i \in \{1, 2, 3, 4, 5\}$, e portanto s não consta da enumeração.

Usando a estratégia do exemplo acima, podemos provar o seguinte teorema.

Teorema 2.7 *Seja A o conjunto das sequências binárias infinitas. Então A não é contável.*

Demonstração: Suponhamos que A é contável. Isto quer dizer que existe uma função sobrejectiva $f : \mathbb{N} \to A$. Seja $s^n = f(n)$. Sob esta hipótese, podemos escrever $A = \{s^0, s^1, s^2, \dots\}$.

Vamos mostrar, através do princípio da diagonalização, que f não pode ser sobrejectiva através da exibição de uma sequência binária infinita $s \in A$ que não se encontra na lista $s^0, s^1, s^2, \dots$. Por conveniência, nesta demonstração contamos os índices das sequências começando do 0 (i.e., a primeira entrada de uma sequência u é u_0). Consideremos a sequência binária s definida por $s_n = 1 - s^n_n$. Notamos que $s \in A$. Fixemos $n \in \mathbb{N}$ qualquer. Como $s_n \neq s^n_n$, segue que $s \neq s^n$. Concluímos, então, que $s \neq s^n$ para qualquer $n \in \mathbb{N}$, e portanto f não pode ser sobrejectiva. ■

Existem outras incarnações do princípio da diagonalização, conforme ilustrado na demonstração do seguinte teorema.

Teorema 2.8 *O conjunto $\mathcal{P}(\mathbb{N})$ não é contável.*

Demonstração: Suponhamos que $\mathcal{P}(\mathbb{N})$ é contável. Isto quer dizer que existe uma função sobrejectiva $f : \mathbb{N} \to \mathcal{P}(\mathbb{N})$. Seja $S_n = f(n)$, onde cada S_n é um subconjunto de $\mathbb{N}$. Sob esta hipótese, podemos escrever $\mathcal{P}(\mathbb{N}) = \{S_0, S_1, S_2, \dots\}$.

Vamos mostrar, através do princípio da diagonalização, que f não pode ser sobrejectiva através da exibição de um conjunto $S \in \mathcal{P}(\mathbb{N})$ que não se encontra na lista $S_0, S_1, S_2, \dots$. Consideremos o conjunto $S = \{n \in \mathbb{N} \mid n \notin S_n\}$, e mostramos que $S \neq S_n$ para todo o $n \in \mathbb{N}$. Fixamos $n \in \mathbb{N}$ qualquer e procedemos por casos. Se $n \in S_n$, então $n \notin S$ pela definição de S, e por isso $S \neq S_n$. Caso contrário, se $n \notin S_n$ então $n \in S$ pela definição de S, e então $S \neq S_n$. Concluímos que f não pode ser sobrejectiva, pois existe $S \in \mathcal{P}(\mathbb{N})$ tal que $f(n) = S_n \neq S$ para todo o $n \in \mathbb{N}$.

Na realidade, como cada subconjunto de $\mathbb{N}$ pode ser representado univocamente por uma sequência binária infinita, as demonstrações destes dois teoremas são essencialmente iguais, só que com linguagem diferente! ■

Corolário 2.1 *O conjunto $[0, 1[$ não é contável. Segue também que $\mathbb{R}$ não é contável.*

A técnica de demonstração usada para demonstrar o Teorema 2.8 pode ser usada para mostrar o seguinte resultado mais geral, devido a Cantor.

Teorema 2.9 (Teorema de Cantor) *Para qualquer conjunto S, o conjunto $\mathcal{P}(S)$ tem cardinalidade estritamente maior do que S. Em particular, se S é contável e infinito, então $\mathcal{P}(S)$ não é contável.*

2.5 Para explorar

A página da Wikipedia sobre o princípio da diagonalização de Cantor contém uma excelente exposição da história e da utilidade das ideias subjacentes a este método em vários contextos. Aconselhamos também a leitura de [LP97, Section 1.4].

References

[LP97] Harry R. Lewis and Christos H. Papadimitriou. *Elements of the Theory of Computation*. Prentice Hall PTR, USA, 2nd edition, 1997.