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

Notas 0: Revisão de conceitos matemáticos

Autor: João Ribeiro

Introdução

O objetivo destas notas introdutórias é relembrar alguns conceitos matemáticos úteis, tais como operações sobre conjuntos e propriedades de funções e relações. Assumimos familiariedade com os básicos de lógica de primeira ordem.

Estas Notas 0 são apropriadas para auto-estudo. Em paralelo, disponibilizamos também uma ficha com alguns exercícios. Também recomendamos fortemente a revisão da matéria dada na cadeira de Matemática Discreta.

0.1 Conjuntos

Começamos por definir notação para alguns conjuntos importantes que vão ser úteis durante grande parte desta cadeira. Denotamos o conjunto dos números naturais por $\mathbb{N} = \{0, 1, 2, \dots\}$. O conjunto dos naturais *sem o zero* é denotado por $\mathbb{N}^+ = \{1, 2, \dots\}$. O conjunto dos inteiros é denotado por $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$. Denotamos o conjunto dos números reais por $\mathbb{R}$. O conjunto dos números racionais (i.e., números reais que podem ser escritos como uma fração de dois inteiros) é denotado por $\mathbb{Q}$. Por exemplo, $1/2$, $2/3$, e $-3/5$ são racionais, mas π e $\sqrt{2}$ são reais mas irracionais.

0.1.1 Definição de conjuntos

Existem várias maneiras de definir um conjunto. Por exemplo, nos casos em que um conjunto S é finito podemos defini-lo simplesmente através de uma lista dos seus elementos. Se S é o conjunto dos números naturais pares maiores que 1 e menores que 10, então podemos escrever

$$S = \{2, 4, 6, 8\}.$$

Usamos o símbolo $\in$ para denotar pertença a um conjunto. Por exemplo, $2 \in S$, mas $5 \notin S$. Usamos a expressão $A \subseteq B$ para denotar que A é um *subconjunto* de B, o que acontece quando todos os elementos que pertencem a A também pertencem a B. Posto de outra forma, $a \in A$ implica que $a \in B$. Por exemplo, o conjunto S definido acima satisfaz $S \subseteq \mathbb{N}$, e $\mathbb{N} \subseteq \mathbb{Q} \subseteq \mathbb{R}$. Por outro lado, $S \not\subseteq \{2, 6\}$, pois, por exemplo, $4 \in S$ mas $4 \notin \{2, 6\}$.

De uma forma mais geral, nesta cadeira vamos precisar de definir conjuntos *por compreensão*. Por exemplo, um subconjunto $S \subseteq \mathbb{N}$ definido por compreensão toma a forma

$$S = \{n \in \mathbb{N} \mid P(n)\}, \tag{0.1}$$

onde P é uma fórmula de lógica de primeira ordem. Devemos ler a expressão na Equação (0.1) como querendo dizer que os elementos de S são exactamente os elementos n de $\mathbb{N}$ para os quais $P(n)$ é verdadeira. Por exemplo, para definir o conjunto dos números naturais pares por compreensão temos de escolher P tal que $P(n)$ seja verdadeira exactamente quando $n \in \mathbb{N}$ é par. Uma escolha válida seria definir $P(n) = \exists k (k \in \mathbb{N} \wedge n = 2k)$. Por palavras, $P(n)$ é verdadeira exactamente quando existe um natural k tal que $n = 2k$, o que é equivalente à afirmação de que n é par. Portanto, podemos definir o subconjunto S dos naturais pares por compreensão como

$$S = \{n \in \mathbb{N} \mid \exists k \in \mathbb{N} : n = 2k\}.$$

Esta notação é muito importante em informática, em particular quando queremos criar especificações lógicas precisas de sistemas para serem interpretadas por computadores. Como este não é o foco desta cadeira, e com vista a não complicar as nossas discussões desnecessariamente, em casos em que o contexto é claro também faz sentido definirmos conjuntos através de linguagem "humana" (mas sempre clara e não ambígua!). Por exemplo, seria igualmente aceitável escrever

$$S = \{n \in \mathbb{N} \mid \text{existe } k \in \mathbb{N} \text{ tal que } n = 2k\}$$

ou "S é o conjunto dos naturais pares", exceto quando é pedido explicitamente num exercício para definir o conjunto formalmente por compreensão.

Geralmente, denotamos a *cardinalidade* de um conjunto S por $|S|$. No caso em que S é um conjunto finito, $|S|$ corresponde ao número de elementos do conjunto. Por exemplo, se $S = \{a, b, c\}$, então $|S| = 3$, e, se $S = \varnothing$, então $|S| = 0$. Mais tarde estudaremos a cardinalidade de conjuntos infinitos.

0.1.2 Operações sobre conjuntos

Intersecção. A intersecção de dois conjuntos A e B, que denotamos por $A \cap B$, é o conjunto dos elementos que pertencem simultaneamente a A e a B, i.e.,

$$A \cap B = \{x \mid x \in A \wedge x \in B\}.$$

União. A união de dois conjuntos A e B, que denotamos por $A \cup B$, é o conjunto dos elementos que pertencem a pelo menos um de A e B, i.e.,

$$A \cup B = \{x \mid x \in A \vee x \in B\}.$$

Diferença. A diferença de um conjunto A por um conjunto B, que denotamos por $A \setminus B$, é o conjunto dos elementos de A que não pertencem a B, i.e.,

$$A \setminus B = \{x \mid x \in A \wedge x \notin B\}.$$

Armados com a notação da diferença de conjuntos, podemos definir o conjunto dos racionais como $\mathbb{Q} = \{\frac{a}{b} \mid a \in \mathbb{Z} \wedge b \in \mathbb{Z} \setminus \{0\}\}$ e o conjunto dos irracionais $\overline{\mathbb{Q}} = \mathbb{R} \setminus \mathbb{Q}$. O conjunto dos números inteiros negativos corresponde ao conjunto $\mathbb{Z} \setminus \mathbb{N}$.

Produto cartesiano e sequências. O produto cartesiano entre dois conjuntos A e B, que denotamos por $A \times B$, é o conjunto de pares (x, y) tal que $x \in A$ e $y \in B$, i.e.,

$$A \times B = \{(x, y) \mid x \in A \land y \in B\}.$$

Esta definição pode ser facilmente estendida a mais do que dois conjuntos. O produto cartesiano $A_1 \times A_2 \times \cdots \times A_k$ corresponde às sequências $(x_1, x_2, \ldots, x_k)$ em que $x_i \in A_i$ para cada $i \in \{1, \ldots, k\}$.

No decorrer desta cadeira será muito comum estudarmos conjuntos de *sequências* de símbolos de um dado conjunto Σ, a que também chamamos de alfabeto. O conjunto das sequências de tamanho k sobre Σ corresponde ao produto cartesiano

$$\Sigma^k = \underbrace{\Sigma \times \Sigma \times \cdots \times \Sigma}_{k \text{ vezes}}.$$

Uma sequência $v \in \Sigma^k$ é da forma $v = (v_1, v_2, \ldots, v_k)$, onde $v_i \in \Sigma$ para todo o $i \in \{1, \ldots, k\}$. Normalmente, quando não introduz ambiguidade, omitimos os parênteses e as vírgulas e escrevemos apenas $v = v_1 v_2 \ldots v_k$. Um cenário importante é quando $\Sigma = \{0, 1\}$, caso em que os elementos de $\{0, 1\}^k$ são as sequências binárias (ou *bitstrings*) de tamanho k. Por exemplo,

$$\{0, 1\}^3 = \{000, 001, 010, 011, 100, 101, 110, 111\}.$$

Outro caso importante corresponde a Σ^0, que definimos como $\Sigma^0 = \{\varepsilon\}$ para qualquer Σ, onde ε denota a *sequência vazia* (de comprimento 0).

Geralmente, dada uma sequência v sobre Σ, usamos a notação v_i para denotar o i-ésimo símbolo de v, e usamos $|v|$ para denotar o tamanho de v (i.e., o número total de símbolos).

Uniões e intersecções indexadas. Vamos precisar também de trabalhar com intersecções e uniões de um número de conjuntos potencialmente infinito. Seja $I \subseteq \mathbb{N}$ um conjunto qualquer, que vemos como um conjunto de índices. Suponhamos que para cada índice $i \in I$ temos um conjunto A_i correspondente. A intersecção indexada por I, que denotamos por $\bigcap_{i \in I} A_i$, é dada por

$$\bigcap_{i \in I} A_i = \{x \mid \forall i \in I (x \in A_i)\}.$$

Por palavras, $\bigcap_{i \in I} A_i$ contém exactamente os elementos x que pertencem a *todos* os conjuntos indexados. De forma análoga, definimos a união indexada por I, que denotamos por $\bigcup_{i \in I} A_i$, como

$$\bigcup_{i \in I} A_i = \{x \mid \exists i \in I (x \in A_i)\}.$$

Por palavras, $\bigcup_{i \in I} A_i$ contém exactamente os elementos x que pertencem a *pelo menos um* dos conjuntos indexados.

Normalmente, consideraremos intersecções e uniões indexadas com conjunto de indíces $I = \mathbb{N}$. Por exemplo, se $I = \mathbb{N}$ e $A_i = \{i\}$ para cada $i \in I$, então $\bigcup_{i \in \mathbb{N}} A_i = \mathbb{N}$. Se $I = \mathbb{N}$ e $A_i = \{0, i\}$, então $\bigcap_{i \in \mathbb{N}} A_i = \{0\}$. Se $I = \mathbb{Z}$ e $A_i = \{-i, i\}$, então $\bigcup_{i \in \mathbb{N}} A_i = \mathbb{Z}$.

Estrela de Kleene. Uma operação sobre conjuntos comum em teoria da computação, e que usa uniões indexadas, é a estrela de Kleene. Dado um conjunto Σ, o seu fecho de Kleene Σ^* é definido por

$$\Sigma^* = \bigcup_{i \in \mathbb{N}} \Sigma^i = \Sigma^0 \cup \Sigma \cup \Sigma^2 \cup \cdots .$$

Por palavras, Σ^* é o conjunto de todas as sequências *finitas* com símbolos de Σ.

Por exemplo, temos $\{0,1\}^* = \{\varepsilon, 0, 1, 00, 01, 10, 11, 000, 001, \ldots\}$.

Conjunto das partes. Dado um conjunto S, o seu *conjunto das partes* $\mathcal{P}(S)$ é o conjunto de todos os subconjuntos de S. Mais formalmente,

$$\mathcal{P}(S) = \{T \mid T \subseteq S\}.$$

Por exemplo, temos

$$\mathcal{P}(\{0,1\}) = \{\varnothing, \{0\}, \{1\}, \{0,1\}\}$$

e

$$\mathcal{P}(\{0,1,2\}) = \{\varnothing, \{0\}, \{1\}, \{2\}, \{0,1\}, \{1,2\}, \{0,2\}, \{0,1,2\}\}.$$

Em ambos os casos, $\varnothing$ denota o *conjunto vazio*.

0.2 Relações e funções

Dados dois conjuntos A e B, uma relação R de A para B é, simplesmente, um subconjunto $R \subseteq A \times B$. Podemos escrever $a \sim_R b$ quando $(a,b) \in R$. No caso especial em que $A = B$, as seguintes propriedades são úteis:

- Uma relação R de A para A diz-se *reflexiva* quando $a \sim_R a$ para qualquer $a \in A$. Por exemplo, a relação de igualdade $R = \{(a,b) \in A \times A \mid a = b\}$ é reflexiva.
- Uma relação R de A para A diz-se *simétrica* quando $a \sim_R b$ implica $b \sim_R a$ para quaisquer $a, b \in A$. Por exemplo, para $A = \mathbb{Z}$, a relação $R = \{(a,b) \in \mathbb{Z} \times \mathbb{Z} \mid a - b \text{ é par}\}$ é simétrica, enquanto que a relação $R' = \{(a,b) \in \mathbb{Z} \times \mathbb{Z} \mid a > b\}$ não é simétrica, pois, por exemplo, $(2,1) \in R'$ mas $(1,2) \notin R'$.
- Uma relação R de A para A diz-se *transitiva* quando $a \sim_R b$ e $b \sim_R c$ implicam que $a \sim_R c$ para quaisquer $a, b, c \in A$. Por exemplo, para $A = \mathbb{Z}$, a relação $R' = \{(a,b) \in \mathbb{Z} \times \mathbb{Z} \mid a > b\}$ é transitiva, pois se $a > b > c$, então sabemos, em particular, que $a > c$.

Uma função é um bem conhecido caso especial de uma relação. Escrevemos $f : A \to B$ para denotar a função total f que mapeia elementos de A para elementos de B. Posto de outra forma, f corresponde à relação $R_f = \{(a,b) \in A \times B \mid b = f(a)\}$. Esta relação R_f satisfaz a propriedade que para cada $a \in A$ existe um único b tal que $(a,b) \in R_f$. Também consideraremos funções $f : A \to B$ que não estão definidas para todo o $a \in A$, ditas funções parciais.

As seguintes propriedades de funções serão importantes nesta cadeira:

- Uma função $f : A \to B$ diz-se *injetiva* se inputs distintos levam a outputs distintos. Mais formalmente, f é injetiva se $f(a) = f(a')$ implica que $a = a'$. Por exemplo, a função $f : \mathbb{Z} \to \mathbb{Z}$ dada por $f(n) = 2n$ é injetiva (pois $2n = 2n'$ implica que $n = n'$), enquanto que a função $g : \mathbb{Z} \to \mathbb{Z}$ dada por $g(n) = n^2$ não é injetiva (pois $g(-1) = 1 = g(1)$).

- Uma função $f : A \to B$ diz-se *sobrejetiva* se para qualquer $b \in B$ existe $a \in A$ tal que $f(a) = b$. Por exemplo, a função $f : \mathbb{Z} \to \mathbb{Z}$ dada por $f(n) = 2n$ não é sobrejetiva pois não existe $n \in \mathbb{Z}$ tal que $f(n) = 1$, enquanto que a função $g : \mathbb{Z} \to \mathbb{Z}$ dada por $g(n) = n - 10$ é sobrejetiva (pois para qualquer $b \in \mathbb{Z}$ temos, para $a = b + 10$, que $g(a) = b$).

- Uma função diz-se bijetiva se é simultaneamente injetiva e sobrejetiva. Por exemplo, a função $f : \mathbb{Z} \to \mathbb{Z}$ dada por $f(n) = -n$ é bijetiva. Começamos por argumentar que f é injetiva. Suponhamos que $f(n) = f(n')$ para alguns $n, n' \in \mathbb{Z}$. Então isto quer dizer que $-n = -n'$, o que é equivalente a $n = n'$, e portanto f é injetiva. Para vermos a sobrejetividade de f, seja $b \in \mathbb{Z}$ qualquer. Então, tomando $a = -b \in \mathbb{Z}$, temos que $f(a) = -a = b$.

0.3 Para explorar

Se quiserem apreciar outras perspetivas sobre os conteúdos destas notas, sugerimos a leitura de [Sip13, Section 0.2] e [LP97, Sections 1.1 and 1.2]

References

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

[Sip13] Michael Sipser. *Introduction to the Theory of Computation*. CEngage Learning, 3rd edition, 2013.