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

Notas 1: Demonstrações

Autor: João Ribeiro

Introdução

A teoria da computação é uma área na intersecção da matemática e da informática. Teoremas e demonstrações aparecerão frequentemente nesta cadeira. Nestas notas discutimos como escrever demonstrações de forma rigorosa, mostrando algumas técnicas úteis e alguns exemplos concretos.

1.1 O que é, e o que não é, uma demonstração

Antes de discutirmos o que são demonstrações, é instrutivo começar por dar exemplos do que *não é* considerado uma demonstração em matemática. A função de Collatz $f : \mathbb{N}^+ \to \mathbb{N}^+$ é definida como

$$f(a) = \begin{cases} a/2, & \text{se } a \text{ é par,} \\ 3a+1, & \text{se } a \text{ é ímpar.} \end{cases}$$

A função de Collatz permite-nos definir as seguintes curiosas sequências: Para um dado valor inicial $s_0 = a \in \mathbb{N}^+$, geramos os seguintes elementos $s_1, s_2, \ldots$ da sequência através da relação de recorrência $s_{n+1} = f(s_n)$. Consideramos alguns exemplos:

- Se $a = 1$, obtemos a sequência $(1, \mathbf{4}, \mathbf{2}, \mathbf{1}, \mathbf{4}, \mathbf{2}, \mathbf{1}, \ldots)$.
- Se $a = 3$, obtemos a sequência $(3, 10, 5, 16, 8, \mathbf{4}, \mathbf{2}, \mathbf{1}, 4, 2, 1, \ldots)$.
- Se $a = 6$, obtemos a sequência $(6, 3, 10, 5, 16, 8, \mathbf{4}, \mathbf{2}, \mathbf{1}, 4, 2, 1, \ldots)$.
- Se $a = 7$, obtemos a sequência $(7, 22, 11, 34, 17, 52, 26, 13, 40, 20, 10, 5, 16, 8, \mathbf{4}, \mathbf{2}, \mathbf{1}, 4, 2, 1, \ldots)$.

Em todos os exemplos que testámos, a sequência associada acaba por convergir para o ciclo $4, 2, 1, 4, 2, 1, \ldots$. Será que existe algum valor inicial $a \in \mathbb{N}^+$ tal que a sequência de Collatz associada não converge para este ciclo?

Esta questão tem sido alvo de grande estudo. Em particular, foi verificado que para todos os naturais $a < 2^{68}$ a sequência de Collatz associada eventualmente converge para o ciclo $4, 2, 1$ [Bar21]! Será que esta verificação nos permite dizer que a proposição "Para todo o valor inicial $a \in \mathbb{N}^+$, a sequência de Collatz associada converge para o ciclo $4, 2, 1$" é verdadeira? A resposta é um enfático **não!** Esta verificação, por si só, não impede a existência de um número a muito maior que 2^{68} para o qual esta propriedade não seja satisfeita. Portanto, de um ponto de vista matemático, verificar

apenas alguns (apesar de muitos) casos particulares de uma proposição não é aceite como uma demonstração da sua veracidade. De facto, ainda ninguém conseguiu demonstrar se esta proposição é verdadeira ou falsa! É a a *conjectura de Collatz*, um dos problemas em aberto mais famosos na matemática.

Existem outros cenários em que uma proposição acaba por ser falsa mesmo após termos testado triliões de casos. Consideremos o seguinte exemplo:

> Para qualquer $n \in \mathbb{N}^+$, os números $n^{17} + 9$ e $(n+1)^{17} + 9$ são coprimos.[1]

Esta proposição é falsa! No entanto, tal não seria aparente se tentássemos testar vários casos: o contraexemplo (i.e., um exemplo concreto que mostra a falsidade da proposição) mais pequeno é

$$n = 8424432925592889329288197322308900672459420460792433.$$

Consideramos ainda mais um exemplo. Seja $\pi(x)$ a função que devolve o número de primos menores que x. Esta função é alvo de grande estudo na matemática. Sabemos, por exemplo, que se comporta assimptoticamente como $\frac{x}{\ln x}$ quando $x \to \infty$. Outra importante função especial relacionada é o integral logarítmico $\mathrm{li}(x) = \int_0^x \frac{dt}{\ln(t)}$. Se testássemos vários x, seria natural conjecturarmos que $\pi(x) \leq \mathrm{li}(x)$ para todo o $x > 1$. No entanto, o menor contraexemplo conhecido ocorre perto de $e^{728} > 10^{316}$ (relacionado com o número de Skewes).

O que é uma demonstração. Uma demonstração é uma sequência de deduções lógicas, começando a partir de axiomas, que nos permite concluir a veracidade de uma dada proposição. A escrita de uma boa demonstração é semelhante em vários aspectos à escrita de software legível e correcto, algo a que já estão habituados. De facto, existe software (como Coq, Isabelle, Lean...) que permite a verificação automática de demonstrações. Nestes casos, a construção de tais demonstrações corresponde, essencialmente, à escrita de um programa.

Nesta cadeira, tal como é a norma na matemática e na teoria da computação, vamos escrever demonstrações para serem interpretadas por seres humanos. Mais precisamente, as demonstrações criadas pelos alunos têm como objetivo principal convencer os docentes da veracidade de uma dada proposição! Isto quer dizer que o estilo de escrita e o nível de rigor esperados são diferentes daqueles necessários para uma demonstração ser aceite por software. Naturalmente, existe também uma componente social neste ato de verificação de uma demonstração, pois o leitor humano não é tão literal como uma máquina, e diferentes seres humanos "aceitam" coisas diferentes. Por exemplo, quando é que podemos dizer que algo é "óbvio"? Para o autor, a melhor maneira de se perceber o que é normalmente considerado uma boa demonstração (dirigida a seres humanos) passa pela leitura cuidadosa de muitos exemplos. Segue, então, um exemplo de uma demonstração.

Teorema 1.1 *Para quaisquer dois conjuntos A e B temos $\overline{A \cup B} = \overline{A} \cap \overline{B}$.*

Demonstração: Vamos primeiro demonstrar que $\overline{A \cup B} \subseteq \overline{A} \cap \overline{B}$. Depois demonstramos que $\overline{A} \cap \overline{B} \subseteq \overline{A \cup B}$. A combinação destas duas asserções permite-nos concluir que $\overline{A \cup B} = \overline{A} \cap \overline{B}$.

[1] Dois números a e b dizem-se *coprimos* se o máximo divisor comum de a e b é 1.

Seja $x \in \overline{A \cup B}$ arbitrário. O nosso objectivo é mostrar que $x \in \overline{A} \cap \overline{B}$. Como $x \in \overline{A \cup B}$, então sabemos que $x \notin A \cup B$ pela definição de complemento. Como $A \subseteq A \cup B$, sabemos também que $x \notin A$, e portanto $x \in \overline{A}$ mais uma vez pela definição de complemento. Da mesma maneira, como $B \subseteq A \cup B$ sabemos que $x \notin B$, e portanto $x \in \overline{B}$. Como $x \in \overline{A}$ e $x \in \overline{B}$ concluímos que $x \in \overline{A} \cap \overline{B}$ pela definição da intersecção. Segue então que $\overline{A \cup B} \subseteq \overline{A} \cap \overline{B}$.

Vejamos agora o sentido oposto. Seja $x \in \overline{A} \cap \overline{B}$ arbitrário. O nosso objectivo é mostrar que $x \in \overline{A \cup B}$. Como $\overline{A} \cap \overline{B} \subseteq \overline{A}$, sabemos que $x \in \overline{A}$, e portanto $x \notin A$ pela definição de complemento. Da mesma forma, como $\overline{A} \cap \overline{B} \subseteq \overline{B}$, sabemos que $x \in \overline{B}$, e portanto $x \notin B$ pela definição de complemento. Como $x \notin A$ e $x \notin B$ concluímos que $x \notin A \cup B$ pela definição da união, e portanto $x \in \overline{A \cup B}$ pela definição de complemento. Segue então que $\overline{A} \cap \overline{B} \subseteq \overline{A \cup B}$. ■

Importante! Não existe uma fórmula ou algoritmo que permita criar demonstrações de forma mecânica. O acto de demonstrar (bem!) um teorema requer criatividade e experiência. A melhor maneira de uma pessoa aprender a escrever boas demonstrações consiste em ler (com sentido crítico!) muitas demonstrações criadas por outras pessoas, e criar muitas demonstrações por conta própria, de forma independente. Durante esta cadeira existirão muitos exercícios para praticar a escrita de demonstrações claras e rigorosas.

1.2 Alguns conselhos

Listamos aqui algumas recomendações para a criação de demonstrações:

- Ler toda a asserção que pretende demonstrar com cuidado.
- Ser paciente. Criar uma demonstração requer reflexão. Também é boa ideia fazer pausas de vez em quando e atacar o problema de novo com a mente fresca.
- Quando bloqueado, experimentar demonstrar um caso especial da asserção ($n = 1$, $n = 2$,...) ou encontrar um contraexemplo.
- Considerar vários exemplos, e escrever/ilustrar enquanto se pensa.
- Escrever de forma clara e concisa, sem falhas de lógica. Imaginar que se está a escrever a especificação de um programa que alguém deverá implementar.
- Enquanto se escreve, pôr-se na pele de um "adversário" que tenta encontrar buracos na demonstração. Lembrar-se que o objectivo é convencer outro ser humano adversarial da veracidade da asserção.

1.3 Mais exemplos de demonstrações

Demonstrações por contradição e contra-recíproco. Suponhamos que queremos demonstrar uma proposição da forma "$A \implies B$". Por vezes, a melhor maneira de atacar tal problema é assumir

$\neg B$ (a negação lógica de B) e derivar $\neg A$. Isto é uma demonstração por contrarrecíproco (notamos que $A \implies B$ e $\neg B \implies \neg A$ são equivalentes). Uma estratégia semelhante é a demonstração por contradição: Se queremos demonstrar A, então assumimos $\neg A$ e derivamos algo que é claramente falso.

Teorema 1.2 *O número real $\sqrt{2}$ é irracional.*

Demonstração: Suponhamos, com vista a uma contradição, que $\sqrt{2}$ é racional. Isto quer dizer que existem inteiros a e b com $b \neq 0$ tal que $\sqrt{2} = a/b$. Sem perda de generalidade, podemos assumir que a e b são coprimos (i.e., o máximo divisor comum de a e b é 1). Se este não for o caso, poderíamos cancelar os divisores comuns a a e b no numerador e denominador de a/b.

Como $\sqrt{2} = a/b$, segue que $a^2 = 2b^2$. Em particular, a^2 é par. Isto implica que a é par e que a^2 é divisível por $4 = 2^2$, pois cada divisor de a aparece duplicado em a^2. Argumentamos agora por casos:

- Se b também for par obtemos uma contradição, pois assumimos que a e b são coprimos (o que implica que a e b não podem ser ambos divisíveis por 2).
- Se b for ímpar também obtemos uma contradição, pois $a^2 = 2b^2$ implica que a^2 não é divisível por 4 quando b é ímpar.

Como em cada caso chegamos a uma contradição, concluímos que $\sqrt{2}$ não pode ser racional. ■

Teorema 1.3 *O conjunto dos naturais primos é infinito.*

Demonstração: Demonstramos este teorema por contradição. Suponhamos que o conjunto S dos naturais primos é finito. Seja n a cardinalidade de S e escrevamos $S = \{p_1, p_2, \ldots, p_n\}$.

Pela definição de número primo, sabemos que todos os naturais $m \notin S$ têm de ser divisíveis por algum $p \in S$. Consideremos $m = 1 + p_1 \cdot p_2 \cdots p_n$. Primeiro notamos que $m \in \mathbb{N}$ mas $m \notin S$, pois $m > p_i$ para qualquer $i \in \{1, \ldots, n\}$. Através da nossa hipótese, concluímos que m não pode ser primo, e portanto tem de ser divisível por algum $p \in S$. No entanto, o resto da divisão de m por qualquer $p \in S$ é sempre 1, e portanto m não é divisível por nenhum $p \in S$. Chegámos a uma contradição, e portanto o conjunto S dos naturais primos não pode ser finito. ■

Argumentos combinatoriais. Grande parte da teoria da computação é, inerentemente, discreta. Por vezes teremos de demonstrar teoremas cuja demonstração passa pela contagem de objectos de um certo tipo. Um bom primeiro passo na contagem de objectos consiste em representá-los de uma forma que conduza a uma contagem mais fácil ou intuitiva. Na demonstração abaixo vemos como ao representar subconjuntos como sequências binárias chegamos a um problema de contagem mais intuitivo.

Teorema 1.4 *Seja S um conjunto com n elementos. Então $|\mathcal{P}(S)| = 2^n$.*

Demonstração: Relembramos que $\mathcal{P}(S)$ é o conjunto de todos os subconjuntos de S. Temos, portanto, de contar o número de subconjuntos de S. Como S tem n elementos, podemos representar cada subconjunto T de S por uma sequência binária $v_T = x_1x_2\ldots x_n$ de tamanho n em que $x_j = 1$ se e só se $i_j \in T$. Por exemplo, o conjunto vazio $\varnothing$ corresponde à sequência $v_\varnothing = 00\ldots0$ e o conjunto S corresponde à sequência $v_S = 11\ldots1$. De facto, a função $f : \mathcal{P}(S) \to \{0,1\}^n$ dada por $f(T) = v_T$ é uma bijecção, pois:

1. (sobrejectividade) Cada sequência $v \in \{0,1\}^n$ define um subconjunto $T \in \mathcal{P}(S)$ pela correspondência acima. Por outras palavras, para cada $v \in \{0,1\}^n$ existe T tal que $f(T) = v$;
2. (injectividade) Se $T, T' \in \mathcal{P}(S)$ são distintos, então $v_T \neq v_{T'}$. Como $T \neq T'$, existe i_j que pertence a um deles mas não ao outro. Isto quer dizer que $(v_T)_j \neq (v_{T'})_j$, e portanto $f(T) = v_T \neq v_{T'} = f(T')$.

Como existe uma bijecção entre $\mathcal{P}(S)$ e $\{0,1\}^n$ estes dois conjuntos têm a mesma cardinalidade, e portanto podemos focar-nos em contar o número de sequências binárias de tamanho n. Para cada coordenada $i \in \{1,\ldots,n\}$ existem duas escolhas para o seu valor (0 e 1). Como estas escolhas são independentes para diferentes coordenadas, concluímos que existem $\underbrace{2\cdot 2\cdots 2}_{n \text{ vezes}} = 2^n$ tais sequências. ■

Uma outra técnica combinatorial consiste em contar a mesma colecção de objectos da mesma maneira, de forma a demonstrar que duas quantidades são iguais.

Teorema 1.5 *Para todo o $n \in \mathbb{N}$ temos que $\sum_{i=0}^{n} \binom{n}{i} = 2^n$, onde $\binom{n}{i} = \frac{n!}{i!(n-i)!}$ é o coeficiente binomial que conta o número de maneiras de escolher um subconjunto de i elementos de entre n elementos.*

Demonstração: Consideremos o conjunto $\mathcal{P}(\{1,2,\ldots,n\})$ dos subconjuntos de $\{1,2,\ldots,n\}$. Pelo Teorema 1.4 sabemos que $|\mathcal{P}(\{1,2,\ldots,n\})| = 2^n$. Por outro lado, temos também que

$$|\mathcal{P}(\{1,2,\ldots,n\})| = \binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n} = \sum_{i=0}^{n} \binom{n}{i},$$

pois para contarmos todos os subconjuntos de $\{1,2,\ldots,n\}$ podemos primeiro contar todos os subconjuntos com i elementos, que são $\binom{n}{i}$, e somar esta quantidade de $i = 0$ elementos até $i = n$ elementos. ■

Demonstrações por indução. Indução é uma técnica de demonstração extremamente útil. Suponhamos que pretendemos demonstrar algo da forma "$\forall n \in \mathbb{N} : P(n)$". Dependendo do predicado P, a seguinte estratégia de indução é um bom ponto de partida:

1. Base da indução: Verificar que $P(0)$ é verdadeira.
2. Hipótese de indução: Assumir que $P(n)$ é verdadeira para um dado $n \in \mathbb{N}$.

3. Passo de indução: Usando a hipótese de indução, mostrar que $P(n+1)$ é verdadeira. Por outras palavras, mostramos que $P(n) \implies P(n+1)$ para todo o $n \in \mathbb{N}$.

Teorema 1.6 *Temos que* $\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$.

Demonstração: Demonstramos este teorema por indução em n. No caso base $n = 0$ temos

$$\sum_{i=0}^{0} i = 0 = \frac{0(0+1)}{2},$$

como desejado. Fixemos agora $n \in \mathbb{N}$ qualquer. A nossa hipótese de indução é $\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$. Demonstramos agora o passo da indução, isto é, mostramos que a asserção também é válida para $n+1$ usando a hipótese de indução. Temos que

$$\begin{aligned}\sum_{i=0}^{n+1} i &= (n+1) + \sum_{i=0}^{n} i \\ &= (n+1) + \frac{n(n+1)}{2} \\ &= \frac{(n+1)(n+2)}{2},\end{aligned}$$

onde a segunda igualdade usa a hipótese de indução $\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$. ■

Também é importante perceber que não existe apenas uma maneira correcta de demonstrar um teorema. Por exemplo, vamos re-demonstrar o seguinte teorema por indução.

Teorema 1.7 (Teorema 1.4, repetido) *Seja S um conjunto com n elementos. Então $|\mathcal{P}(S)| = 2^n$.*

Demonstração: Procedemos por indução. Para o caso base $n = 0$ temos $S = \varnothing$, e portanto $|\mathcal{P}(\varnothing)| = |\{\varnothing\}| = 1 = 2^0$. Fixemos $n \in \mathbb{N}$ qualquer e tomemos como hipótese de indução que $|\mathcal{P}(S)| = 2^n$ para qualquer conjunto S de n elementos.

Seja S' um conjunto qualquer com $n+1$ elementos, que podemos escrever como $S' = S \cup \{s\}$ para algum s e algum conjunto S com n elementos. Para construir todos os subconjuntos de S' podemos proceder da seguinte forma: Dado qualquer subconjunto $T \subseteq S$, obtemos de forma única os subconjuntos T e $T \cup \{s\}$ de S'. Isto quer dizer que por cada subconjunto de S existem dois subconjuntos de S', e portanto $|\mathcal{P}(S')| = 2 \cdot |\mathcal{P}(S)| = 2 \cdot 2^n = 2^{n+1}$, onde a segunda igualdade segue da hipótese de indução. ■

1.4 Para explorar

A aula gravada da cadeira "Great Ideas in Theoretical Computer Science" dada pelo Ryan O'Donnell na Carnegie Mellon University em 2016 contém excelentes perspetivas sobre demonstrações e teoria

da computação. Estas notas foram inspiradas por esse vídeo. O livro de Velleman [Vel19] oferece uma excelente e exaustiva introdução à escrita de demonstrações. Aconselhamos também a leitura de [LP97, Section 1.5] e [Sip13, Sections 0.3 and 0.4].

O artigo sobre a conjetura de Collatz na Wikipedia contém uma boa discussão do problema. Os exemplos de "não demonstrações" discutidos nestas notas foram inspirados pelas respostas a esta questão no Mathematics StackExchange.

References

[Bar21] David Barina. Convergence verification of the Collatz problem. *The Journal of Supercomputing*, 77(3):2681–2688, 2021.

[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.

[Vel19] Daniel J. Velleman. *How to Prove It: A Structured Approach*. Cambridge University Press, 3rd edition, 2019.