UNIVERSIDADE
BEIRA INTERIOR

Teoria da Computação
Aula 1 - Tecnicas de Demonstração

Simão Melo de Sousa

Introdução

prelúdio

Aviso Prévio

- A redacção dos apontamentos da disciplina documento baseou-se fortemente na bibliografia indicada. Parece-nos então óbvio que a leitura e a aprendizagem directa pelas obras originais é recomendada, e mesmo essencial á compreensão profunda das noções aqui apresentadas;
- O português não é a língua materna do autor e o presente documento encontra-se em fase (constante) de elaboração/melhoramento pelo que se agradece e até se incentiva qualquer sugestão ou correcção;

Referencias bibliográficas

- A. Arnold and I. Guessarian. **Mathematics for Computer Science**. Prentice-Hall, 1996.
- David Makinson. **Sets, Logic and Maths for Computing**. Springer Publishing Company, Incorporated, 1 edition, 2008.
- C. H. Papadimitriou, H. R. Lewis. **Elements of the Theory of Computation** por Prentice Hall, 1997. Tradução brasileira: **Elementos de Teoria da Computação**, 2a Edição. Bookman, Porto Alegre, 2000.
- (Uma obra de referência e muito completo... um **must read**) John E. Hopcroft, Rajeev Motwani, Jeffrey D. Ullman. **Introduction to Automata Theory, Languages, and Computation** (3nd Edition). Addison Wesley, 2006 (existe em português do Brasil).
- (Completo e também um **must read**) M. Sipser. **Introducton to the Theory of Computation**. PWS Publishing, 2006.

Tecnicas de Demonstração

Demonstrações Por Contradição

Imagine que pretendemos demonstrar uma propriedade P.

Podemos construir uma argumentação dedutiva que exibe que P é válida a partir de resultados previamente demonstrado, axiomas ou até mesmo do cálculo.

Ou podemos demonstrar que P não pode inválida.

Este processo é designado de **demonstração por contradição**, ou ainda de **demonstração por absurdo** ou de **demonstração por redução ao absurdo** (do latim **reductio ad absurdum**)

Genericamente, o processo de demonstração por contradição duma propriedade P baseia-se na percepção de que **ou temos P ou temos $\neg P$** (ou exclusivo, ou seja nunca os dois simultaneamente) e conduz-se da seguinte forma:

1. Admitir (como hipótese) que o contrário do que pretendemos provar é válido (ou seja admitir $\neg P$)
2. condizir uma dedução que nos leva desta hipótese a uma situção contraditória (dito de outra forma absurda ou ainda impossível).
3. logo a hipótese inicial, $\neg P$, não pode ser válida. Podemos assim concluir que P é válida.

$$\sqrt{2} \in (\mathbb{R} - \mathbb{Q})?$$

Demonstração por absurdo de que $\sqrt{2}$ é irracional:

- Assumimos que $\exists n, m \in \mathbb{N}$, tais que $\sqrt{2} = \frac{n}{m}$, sendo $\frac{n}{m}$ uma fracção irreductível (n e m não tem divisores comuns);
- ou seja $2m^2 = n^2$.
- logo n^2 é par, ou seja n igualmente. Seja $k \in \mathbb{N}$ tal que $n = 2k$, então $2m^2 = 4k^2$.
- assim sendo $m^2 = 2k^2$. O valor m é assim e igualmente par.
- Contradicção. m e n são ambos divisíveis por 2 embora a hipótese inicial afirmasse que não houvesse divisores comuns. $\sqrt{2}$ **só pode ser irracional**.

Um ponto subtil: nunca foi provado que P (no exemplo "$\sqrt{2}$ é irracional") seja válida, mas sim que $\neg P$ ($\sqrt{2}$ é racional) é inválida

ou seja, não se argumentou a validade de P mas sim que não podia ser de outra forma.

Diz-se dessas demonstrações que **não são construtivas** (não se constrói uma prova de P mas sim constata-se formalmente que esta tem de ser válida).

Para os curiosos, ver a discussão sobre a matemática construtiva, o intuicionismo de Brouwer, Heyting e Kolmogorov (os pais desta escola matemática) a as ligações do construtivismo com a algoritmia.

outro exemplo de demonstração não construtiva:

$$\exists \alpha, \beta \in (\mathbb{R} - \mathbb{Q}),\ \alpha^{\beta} \in \mathbb{Q}?$$

Demonstração:
Temos: $\sqrt{2} \notin \mathbb{Q}$. Sejam $\alpha = \beta = \sqrt{2}$

- Ou temos $\alpha^{\beta} = \sqrt{2}^{\sqrt{2}} \in \mathbb{Q}$, *QED*
- Ou temos $\sqrt{2}^{\sqrt{2}} \notin \mathbb{Q}$. Sejam então $\alpha' = \sqrt{2}^{\sqrt{2}}$ e $\beta' = \sqrt{2}$ então $\alpha'^{\beta'} = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^{2} = 2 = \frac{2}{1} \in \mathbb{Q}$, ou seja *QED*

mas $\sqrt{2}^{\sqrt{2}}$ é ou não é racional? Esta demonstração não o diz.

Tecnicas de Demonstração

Princípios da Gaioba de Pombos

Demonstrações pelo princípios da gaiola de pombos

- se A e B são dois conjuntos finito tais que $|A| > |B|$ então não existe nenhuma bijecção entre A e B.
- Por outras palavras (que justificam o nome), se tiver mais pombos do que gaiolas então necessariamente pelo menos uma das gaiolas vai ter de ficar com mais do que um pombo.
- Este princípio simples tem, surpreendentemente, muitas aplicações na matemática, em ciência da computação e em informática.

Demonstrações pelo princípios da gaiola de pombos - Um exemplo

Retirado de `http://en.wikipedia.org/wiki/Pigeonhole_principle`:

> *Although the pigeonhole principle may seem to be a trivial observation, it can be used to demonstrate possibly unexpected results. For example, there must be at least two people in London with the same number of hairs on their heads. Demonstration: a typical head of hair has around 150,000 hairs. It is reasonable to assume that no one has more than 1,000,000 hairs on their head. There are more than 1,000,000 people in London. If we assign a pigeonhole for each number of hairs on a head, and assign people to the pigeonhole with their number of hairs on it, there must be at least two people with the same number of hairs on their heads.*

Demonstrações pelo princípios da gaiola de pombos - Outro exemplo

Seja R uma relação binária sobre um conjunto A. Sejam a e b dois elementos de A. Se existe um caminho entre a e b por R então existe um caminho de comprimento máximo $|A|$.

Demonstração: Seja $a = a_1 a_2, a_3, \cdots, a_n = b$ o caminho mais curto entre a e b. Suponha agora que $n > |A|$. Isto significa que há mais elementos no caminho do que elementos em $|A|$. Pelo princípios da gaiola de pombos sabemos que pelo menos um elemento de A está duas vezes no caminho (se mapeamos os pontos do caminho para elementos do conjunto A, então pelo menos dois pontos do caminho vão ser mapeados para um elemento comum). Digamos $a_i = a_j$ para $1 \leq i < j \leq n$. Mas então $a_1, a_2, \cdots, a_i, a_{j+1}, \cdots, a_n$ é igualmente um caminho, e mais curto. Contradicção. QED.

Tecnicas de Demonstração

Técnica da Diagonal

Princípio da Diagonalização:

Seja R uma relação binária sobre um conjunto A. Seja D o conjunto, designado de **diagonal**, definido por $\{a \mid a \in A \wedge (a, a) \notin R\}$. Para cada $a \in A$, seja $R_a = \{b \mid b \in A \wedge (a, b) \in R\}$. Então D distingue-se de cada R_a.

Este princípio simples é no entanto surpreendentemente poderoso.

Demonstrações por diagonalização

Imagine a seguinte relação R:
$\{(a,b),(a,d),(b,b),(b,c),(c,c),(d,b),(d,c),(d,f),(e,e),(e,f),(f,a),$
$(f,c),(f,d),(f,e)\}$

	a	b	c	d	e	f
a		×		×		
b		×	×			
c			×			
d		×	×		×	×
e					×	×
f	×		×	×	×	

a diagonal é então

a	b	c	d	e	f
	×	×		×	

e o seu complemento

a	b	c	d	e	f
×			×		×

é o **conjunto diagonal,** D de R, ou seja $\{a,d,f\}$. Repare que é diferente de qualquer linha da matriz.

Um exemplo : o Teorema de Cantor sobre a enumerabilidade do conjunto dos subconjuntos.

O conjunto dos subconjutos dum conjunto enumerável não é numerável

Demonstração: Vamos proceder por uma redução ao absurdo e utilizar o princípio da diagonal. Seja $A = \{a_0, a_1, a_2, \cdots\}$. e $S = \{s_0, s_1, s_2\}$. Supomos que S seja numerável. Consideremos então a relação R seguinte: $R \triangleq \{(a, s) \mid a \in A, s \in S, a \in s\}$.

$R \triangleq \{(a, s) \mid a \in A, s \in S, a \in s\}$ induz a matriz (eventualmente infinita) seguinte:

	a_0	a_1	a_2	a_3	$a_4 \cdots$
s_0	×		×		×
s_1	×	□	×		
s_2		×	□	×	×
s_3			×	×	×
s_4	×	×		×	□
⋮					

O conjunto diagonal D é assim $\{a_i \mid a_i \notin s_i\}$ (os elementos assinalados por □). D é um subconjunto de S já que é composto de elementos de A.

- $A = \{a_0, a_1, a_2, \cdots\}$
- $S = \{s_0, s_1, s_2\}$.
- $R \triangleq \{(a, s) \mid a \in A, s \in S, a \in s\}$
- $D \triangleq \{a_i \mid a_i \notin s_i\}$.

Pelo princípio da diagonal, $\forall i \in \mathbb{N}, D \neq s_i$. Logo D não é um subconjunto de A ($D \notin S$). Contradição. QED.
Vejamos esta argumentação com mais cuidado: Porque D não pode ser um dos s_i? Imaginemos que $\exists k \in \mathbb{N}, s_k = D$. Então $a_k \in D$ se e só se $a_k \notin s_k$ (por definição de D).
O conjunto dos subconjuntos não é numerável.

Tecnicas de Demonstração

Indução Estrutural

Esta técnica, muito útil no contexto desta disciplina, já foi abordada anteriormnte e aplica-se ás propriedades sobre conjuntos definidos por indução estrutural.
Damos a seguir dois exemplos.

Seja $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, a função recursiva definida por:

$$f(m,n) \triangleq \begin{cases} n+1 & \text{se } m = 0 \\ f(m-1,1) & \text{se } n = 0 \wedge m \neq 0 \\ f(m-1, f(m,n-1)) & \text{se } n > 0 \wedge m > 0 \end{cases}$$

Vamos demonstrar por indução que $\forall k \in \mathbb{N},\ f(1,k) = k+2$.

Vamos aqui utilizar a definição indutiva standard do inteiros natural (da aritmética de Peano). Neste caso a demonstração por indução deverá seguir o princípio: $((P\ 0) \wedge (\forall n \in \mathbb{N}.P\ n \rightarrow P\ (n+1))) \rightarrow (\forall n \in \mathbb{N}.P\ n)$. Aqui $P\ x \triangleq\ f(1,x) = x+2$

- Caso de Base: Demonstrar que temos $P\ 0$ ou seja $f(1,0) = 2$. Vejamos. $f(1,0) = (regra\ 2)\ \ f(0,1) = (regra\ 1)\ \ 1+1 = 2$
- Passo indutivo: Seja x um valor inteiro. Admitindo que temos $P\ x$ (Hipótese de indução, ou HI), temos de verificar se temos necessariamente $P\ (x+1)$. Vejamos. $f(1,x+1) = (regra3)\ \ f(0,f(1,x)) = (regra1)\ \ f(1,x)+1 = (HI)\ \ x+2+1$ ou seja $(x+1)+2$. Qed.

Conclusão: $\forall k \in \mathbb{N},\ f(1,k) = k+2$

Demonstração por indução estrutural

1. Defina de forma indutiva o conjunto bin_A das árvores binárias **não vazias** de elementos dum conjunto A. Por árvores não vazias, entendemos que as mais pequenas árvores deste conjunto são folhas (árvores com um só elemento do conjunto A);
2. Dê o princípio de indução associada a esta definição indutiva;
3. Defina a função *arestas* que calcula o número de vértice da árvore em parâmetro;
4. Defina a função *nodos* que calcula o número de nodos da árvore em parâmetro;
5. Demonstre que $\forall a \in bin_A, nodos(a) = arestas(a) + 1$.

- Seja A um conjunto. O conjunto das árvores binárias não vazias de elementos de A é o conjunto bin_A definido de forma indutiva a partir do alfabeto $A_A \triangleq A \cup \{"(","),",","\}$ e das regras (B) e (I). De forma equivalente, bin_A é o mais pequeno conjunto X, dos subconjuntos do monóide livre gerado por A_A (ou seja: A_A^*) que verifica:

  (B): $\forall a \in A, a \in X$

  (I): $\forall e, d \in X, \forall a \in A, (e, a, d) \in X$

- O princípio de indução, para uma propriedade P sobre árvores de bin_A, é o seguinte:

$$(\forall x \in A, P(x)) \wedge (\forall e, d \in bin_A, \forall a \in A, P(e) \wedge P(d) \rightarrow P((e, a, d)))$$

$$\rightarrow (\forall ab \in bin_A, P(ab))$$

$$arestas\ n = \begin{cases} 0 & se\ n \in A\ (n\ folha) \\ 2 + arestas(e) + arestas(d) & se\ n = (e, a, d) \end{cases}$$

$$nodos\ n = \begin{cases} 1 & se\ n \in A\ (n\ folha) \\ 1 + nodos(e) + nodos(d) & se\ n = (e, a, d) \end{cases}$$

- Vamos demonstrar por indução que $\forall ab \in bin_A, nodos(ab) = arestas(ab) + 1$. Temos assim de considerar o caso de base e o passo indutivo.

  Base: Demonstrar que para toda a folha $a \in A, nodos(a) = arestas(a) + 1$. Esta demonstração é trivial. Seja a uma folha ($a \in A$) $nodos(a) = 1$ e $arestas(a) = 0$, logo $nodos(a) = arestas(a) + 1$.

Indutivo: Sejam e e d duas árvores de bin_A e a um elemento de A. As hipóteses de indução são as seguintes: (HI1) $nodos(e) = 1 + arestas(e)$ e (HI2) $nodos(d) = 1 + arestas(d)$.

Vamos a seguir demonstrar que (HI1) e (HI2) implicam que $nodos((e, a, d)) = 1 + arestas((e, a, d))$.

$$arestas((e, a, d)) = 2 + arestas(e) + arestas(d) \quad (*)$$

$$\begin{aligned} nodos((e, a, d)) &= 1 + nodos(e) + nodos(d) \\ (porHI1) &= 1 + 1 + arestas(e) + nodos(d) \\ (porHI2) &= 1 + 1 + 1 + arestas(e) + arestas(d) \\ &= 1 + 2 + arestas(e) + arestas(d) \\ (por(*)) &= 1 + arestas((e, a, d)) \end{aligned}$$

QED.

Temos assim $\forall ab \in bin_A, nodos(ab) = arestas(ab) + 1$

Demonstração por indução estrutural

```
type 'a abin =
 | Folha of 'a
 | Nodo  of 'a abin * 'a * 'a abin

let rec arestas = function
 | Folha _         -> 0
 | Nodo (c, x, d) -> (arestas c) + (arestas d) + 2

let rec nodos a =
 match a with
 | Folha _         -> 1
 | Nodo (c, x, d) -> (nodos c) + (nodos d) + 1
```

Tecnicas de Demonstração

Indução Bem Fundada

Demonstração por indução bem fundada

- Pretende-se demonstrar $\forall x \in A, P(x)$.
- Uma ordem $\leq$ bem fundada sobre A é uma relação binária sobre A tal que não exista para nenhum x de A uma sequência $\cdots \leq x_n \leq \cdots x_2 \leq x_1 \leq x$ **estritamente** decrescente infinita.

  Por exemplo

  - $\leq$ é bem fundada sobre $\mathbb{N}$ (qualquer que seja o inteiro n, as sequências estritamente decrescentes acabam no pior caso em 0)
  - $|$ a relação de divisão inteira ($a|b$ significa que a divide b) é bem fundada em $\mathbb{N}$: qualquer que seja o inteiro natural n, a maior sequência de divisores acaba em 1.
- Se o conjunto A dispõe de uma relação de ordem $\leq$ bem fundada então o conjunta dispõe dum principio de indução designado de **bem fundado** definido da seguinte forma:
  $(\forall x \in A, (\forall y \in A, ((y < x) \wedge P(y)) \implies P(x))) \implies \forall x \in A, P(x)$ (onde $y < x \equiv y \leq x \wedge y \neq x$)

Cada inteiro natural tem um descomposição única em números primos (modulo permutação dos elementos da descomposição)

Demonstração da existência: Por indução bem fundada sobre o inteiro n e a ordem $|$ (onde $a|b \triangleq a$ divide b). Esta ordem é bem fundada (todas as cadeias estritamente decrescentes acabam no máximo em 1).

1. Caso em que n é primo. Este caso é trivial (não há descomposição).
2. Caso contrário, existe pelo menos um $d \in \mathbb{N}$ tal que $1 < d < n$ e $d|n$. Seja p_1 o menor destes d. Se p_1 não for primo então e da mesma forma existe um q tal que $1 < q < p_1$ e $q|p_1$ mas neste caso q divide igualmente n. Contradição (porque q é um divisor menor do que p_1). Logo p_1 é primo. Neste caso $n = p_1.n_1$. Se n_1 for primo, então já temos a nossa descomposição. Senão procedemos da mesma forma sobre n_1 e obtemos uma descomposição $n_1 = p_2.n_3$. (etc...).
   Agora, podemos reparar que $\cdots n_i|n_{i-1}|\cdots|n_2|n_1|n$. Como sabemos que esta ordem é bem fundada, esta sequência tem de ser finita: $\exists k$ tal que n_{k-1} primo (que designamos por p_k). Ou seja, $n = p_1.p_2 \cdots p_k$. QED.

Cada inteiro natural tem um descomposição única em números primos (modulo permutação dos elementos da descomposição)

Demonstração da unicidade: Por contradição.

$$n = p_1 p_2 \ldots p_r = q_1 q_2 \ldots q_s$$

Assumimos, sem perda de generalidade que $r \leq s$ e que os factores primos estão ordenados de forma crescente. Ou seja $p_1 \leq p_2 \leq p_3 \leq \ldots \leq p_r$ e $q_1 \leq q_2 \leq q_3 \leq \ldots \leq q_s$. Sabemos que p_1 divide n, ou seja, divide igualmente $q_1 q_2 \ldots q_s$. Como todos os q_is são primos, existe um k tal que $p_1 = q_k$. Logo $p_1 \geq q_1$. Da mesma forma, se olharmos desta vez para q_1 conseguimos demonstrar que $q_1 \geq p_1$. Logo $p_1 = q_1$. Ou seja $p_1 p_2 \ldots p_r = p_1 q_2 \ldots q_s$. Ou ainda $p_2 \ldots p_r = q_2 \ldots q_s$. Podemos repetir este raciocínio até p_r. Logo $1 = q_{r+1} q_{r+2} \ldots q_s$. Esta situação só é possível se $s = r$ (nenhum produto de números primos (que são todos > 1) é igual a 1). Logo $\forall i, p_i = q_i$. QED.

Seja A^* o monoíde livre[1] gerado pelo alfabeto A. Vamos demonstrar que

$$\forall u, v \in A^*.\ (u.v = v.u \quad \leftrightarrow \quad \exists w \in A^*, \exists p, q \in \mathbb{N}.\ u = w^p \quad e \quad v = w^q)$$

$\rightarrow$. Fácil. se $u = w^p$ e $v = w^q$ então
$u.v = w^p.w^q = w^{p+q} = w^q.w^p = v.u$

[1] O conceito de monoíde será definido com mais rigor noutra aula. A utilisação do conceito aqui é marginal

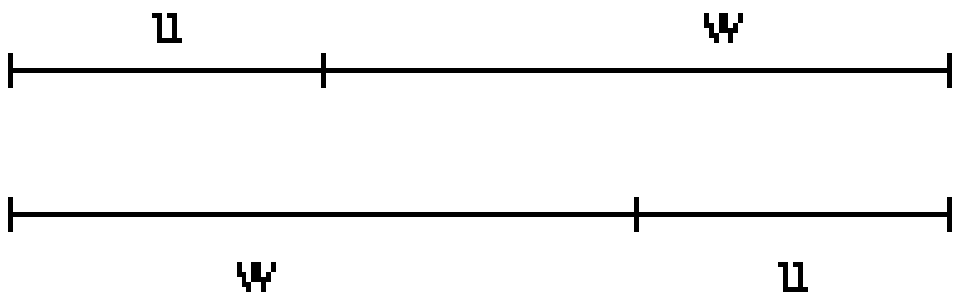
$\leftarrow$. Demonstração por indução bem fundada sobre $|u| + |v|$. Ou seja a propriedade por demonstrar é:

$$P(n) \triangleq \forall u.v \in A^*.|u| + |v| = n, u.v = v.u \rightarrow \exists w \in A^*, \exists p, q \in \mathbb{N}.\ u = w^p \quad e \quad v = w^q$$

. A ordem por utilizar aqui é a ordem natural $\leq$ sobre os inteiros. Esta ordem é bem fundada (não podemos definir cadeias infinitas estritamente decrescentes).
Assim sendo, Por hipótese de indução bem fundada temos: $\forall k < n, P(k)$. Verifiquemos agora que temos então necessariamente $P(n)$.

Sem perder generalidade supomos que $|u| \leq |v|$. Neste caso u é prefixo de v.

Demonstração por indução bem fundada



- Se $u = \epsilon$ ou $u = v$ então basta escolher $w = v$
- Nos outros casos (u é designado de prefixo próprio de v), então existe um v' tal que $v = uv'$ e verifica-se que $v'u = v = uv'$. Visto que $|v'| < |v|$ podemos aplicar a hipótese de indução ao par (u, v') (ou seja $\exists w, p, q.u = w^p \wedge v' = w^q$). Como $v = u.v'$ deduz-se que $v = w^{p+q}$. QED.

Outro caso de utilização privilegiada desta técnica de demonstração é a demonstração de terminação de funções recursivas.
Por exemplo:
Seja $div\_euclides : \mathbb{N} \to \mathbb{N} \to \mathbb{N}$ a função seguinte:

$$div\_euclides\ x\ y = \begin{cases} 0 & if\ x < y \\ x & if\ y = 0 \\ (div\_euclides\ (x - y)\ y) + 1 & otherwise \end{cases}$$

Demonstremos, por indução bem fundada, que a função $div\_euclides$ termina.

Demonstração por indução bem fundada

- Para demonstrar que a função d termina, basta conseguir ligar as chamadas recursivas a uma relação de ordem bem fundada. A ideia é ver que para determinados x e y, $x - y$ é mais pequeno, quando comparado com essa ordem, do que x. Como esta ordem não tem cadeias descendentes infinitas, a função tem de terminar.

  Várias ordens bem fundamentadas são possíveis candidatas. Escolhamos a mais natural de todas: $\leq (\subseteq \mathbb{N} \times \mathbb{N})$. (Podíamos ter escolhido a ordem $\leq_{\mathcal{L}}$ sobre os pares de inteiros. Neste caso teríamos de nos debruçar sobre o par (x, y) e não só sobre x)

  Comecemos por verificar que todos os casos de base terminam. Todos eles se determinam em relação ao valor de y (que não mude durante as diferentes chamadas recursivas).

  1. se $y = 0$ o cálculo de x termina obviamente;
  2. se $x < y$ o cálculo de 0 termina obviamente;

Debrucemo-nos agora sobre o passo indutivo. Temos de verificar:

- que a chamada recursiva faz com um argumento menor estritamente (estritamente menor em relação a ordem bem fundamentada escolhida);
- que se $(d\ (x - y)\ y)$ termina então $(d\ x\ y)$ também termina.

Estes dois pontos são triviais. $(x - y) < x$ quando $y > 0$ (que é o caso, visto $y = 0$ ser um dos casos de base). Somar um a um cálculo por hipótese finito é feito em tempo finito. **QED**