Teoria da Computação

Aula Teórica 5:
Conjuntos finitos e infinitos.

António Ravara

Departamento de Informática

20 de Março de 2019

Funções e conjuntos infinitos

Conjunto extensão de uma função

Conjunto de pares (argumento,resultado) que define a função.

Este conjunto é, em geral, infinito.

Exemplo: função de concatenação de sequências

- Considere as sequências (finitas!) de naturais definidas indutivamente numa aula passada.
- Define-se agora indutivamente a função de concatenação de tais sequências.

$$
\begin{array}{lcl}
concat & \in & SEQ^2 \rightarrow SEQ \\
\text{CEMPTY} & : & s \in SEQ \longrightarrow concat((), s) = s \\
\text{CSTEP} & : & (n \in NAT \wedge u \in SEQ \wedge v \in SEQ) \longrightarrow \\
 & & concat((n, u), v) = (n, concat(u, v))
\end{array}
$$

Um conjunto infinito

Função de concatenação de sequências

Definimos uma função recursiva:

$$\begin{array}{lcl} \mathit{concat} & \in & \mathit{SEQ}^2 \to \mathit{SEQ} \\ \text{CEMPTY} & : & s \in \mathit{SEQ} \longrightarrow \mathit{concat}((), s) = s \\ \text{CSTEP} & : & (n \in \mathit{NAT} \wedge u \in \mathit{SEQ} \wedge v \in \mathit{SEQ}) \longrightarrow \\ & & \mathit{concat}((n, u), v) = (n, \mathit{concat}(u, v)) \end{array}$$

Aplicação da função *concat*

$$\begin{array}{lcl} \mathit{concat}((1,2),(3,4)) & = & (\text{por CSTEP}) \\ (1, \mathit{concat}((2),(3,4))) & = & (\text{por CSTEP}) \\ (1,2, \mathit{concat}((),(3,4))) & = & (\text{por CEMPTY}) \\ (1,2,3,4) & & \end{array}$$

Função: extensão e algoritmo

- A extensão da função *concat* é um conjunto infinito, pois há infinitas sequências (finitas) de naturais.
- Tal conjunto existe (no mundo idealizado da Matemática).
- Como calcular a extensão da função? Será que conseguimos escrever o conjunto?
- Como tem domínio infinito não podemos usar enumeração.
- Conseguimos definir um algoritmo para dadas duas sequências arbitrárias fazer a sua concatenção: é um programa (iterativo ou recursivo) que implementa a definição indutiva da função!
- Usando uma linguagem de programação e um computador conseguimos "mecanizar" o processo - temos um algoritmo que calcula a função, dados dois pares arbitrários.
- Podemos imaginar também um procedimento para calcular todos os *inputs* possíveis...

Funções versus Algoritmos

- Uma função é um conceito matemático, em que a sua extensão pode ser um conjunto infinito.
- Um algoritmo é um conceito informático, que pressupõe a definição de um processo mecânico de cálculo.
- Um algoritmo deve ser executável em tempo finito com recursos finitos (memória, energia, etc.).
- Pode-se definir um algoritmo para calcular automaticamente (executar) qualquer função?

Todas as funções são calculáveis?

Solução de um polinómio de coeficientes inteiros

Considere a função booleana *solution* que diz se dado polinómio tem ou não solução.

- A função é sempre calculável (ou seja, existe um algoritmo)?
- Sim, para polinómios com uma só variável;
- Não, para polinómios com mais que uma variável (é o decimo problema de Hilbert).

Então há funções não calculáveis...

Problemas (in)decidíveis

Existência de algoritmos

Distinguimos então 3 situações:

- Conhece-se o algoritmo para calcular dada função.
- Sabe-se que a função é calculável, mas não se conhece o algoritmo (ainda não se conseguiu desenvolver um).
- Sabe-se que a função *não* é calculável (não existe algoritmo).

Decidibilidade

- Logo, há mais funções que algoritmos!
- As funções (ou *problemas*) não calculáveis dizem-se *indecidíveis*.

Há vários "infinitos"?!

- O conjunto de todas as funções é infinito.
- O conjunto de todos os algoritmos é infinito.
- O cardinal do conjunto de todas as funções é superior ao cardinal do conjunto de todos os algoritmos?!
- Sim.
  Cantor mostrou que existe uma cadeia crescente infinita de cardinais de conjuntos infinitos!

Como determinar qual o cardinal de dado conjunto?

Como determinar cardinais?

- Como contar o número de elementos de um conjunto infinito?
  Como não se podem enumerar, temos que encontrar uma regra...
- Como saber qual dos infinitos é o cardinal de um conjunto infinito?
  Ou seja, como distinguir os cardinais?
  Há mais racionais que naturais? E há mais reais que racionais?
- Como comparar o tamanho de dois conjuntos infinitos?
  A resposta a estas questões foi dada pelos pioneiros da teoria de conjuntos...

Conjunto equipotentes

Definição

Dois conjuntos A e B dizem-se *equipotentes* (têm o "mesmo" número de elementos, finito ou infinito), se existir uma bijecção de A para B.

- A bijecção estabelece uma correspondência única (de um-para-um) entre os elementos de A e os de B.
- A bijecção *testemunha* então que os conjuntos têm basicamente o mesmo número de elementos..
- Se não há tal bijecção, os cardinais dos conjuntos são diferentes.

Conjuntos equipotentes

Exemplos

1. Seja $A \stackrel{\text{def}}{=} \{1, 2\}$ e $B \stackrel{\text{def}}{=} \{3, 4, 5\}$
   Facilmente se prova que não há nenhuma bijecção entre os conjuntos. Logo, não têm então o mesmo cardinal.
2. Seja $A \stackrel{\text{def}}{=} \{n \in \mathbb{N}_0 \mid n\%2 = 0 \wedge n < 10\}$
   e $B \stackrel{\text{def}}{=} \{n \in \mathbb{N}_0 \mid n\%2 \neq 0 \wedge n < 10\}$
   A função $f \stackrel{\text{def}}{=} \{(0, 1), (2, 3), \ldots, (8, 9)\}$ é uma bijecção.
   Logo, os conjuntos têm o mesmo número de elementos.
3. Seja $A \stackrel{\text{def}}{=} \{n \in \mathbb{N}_0 \mid n\%2 = 0\}$ e $B \stackrel{\text{def}}{=} \{n \in \mathbb{N}_0 \mid n\%2 \neq 0\}$
   Facilmente se generaliza a função f anterior e se conclui que A e B têm o mesmo cardinal.

Equipotências surpreendentes

Inclusão não implica cardinal diferente...

1. Seja $A \stackrel{\text{def}}{=} \mathbb{N}_0$ e $B \stackrel{\text{def}}{=} \{n \in \mathbb{N}_0 \mid n\%2 = 0\}$
   - Haverá alguma bijecção entre A e B?
   - Seja $f \stackrel{\text{def}}{=} \{(n, m) \in A \to B \mid m = 2n\}$.
   - Facilmente se mostra que f é uma bijecção!

   Há tantos naturais como naturais pares!
2. E haverá alguma bijecção entre os naturais e os inteiros?
   Encontramos uma se procedermos em *zig-zag*:
   $0 \mapsto 0, 1 \mapsto -1, 2 \mapsto 1, 3 \mapsto -2, 4 \mapsto 2, \ldots$
   A função define-se sem dificuldade: os pares para os naturais e os ímpares para os inteiros negativos.
   Há tantos naturais como inteiros!

Cardinal dos racionais

Números racionais

$$\mathbb{Q} \stackrel{\text{def}}{=} \{x/y \mid x \in \mathbb{Z} \wedge y \in \mathbb{Z} \wedge y \neq 0\}$$

Há mais racionais que naturais?

- Cantor concluiu que não!
- Teorema de Cantor-Bernstein:
  Se existem funções injectivas de A para B e de B para A, então existe uma bijecção de A para B.
- Como $\mathbb{N}_0 \subset \mathbb{Q}$, o cardinal de $\mathbb{N}_0$ é menor ou igual ao de $\mathbb{Q}$.
- Se encontrarmos uma injecção de $\mathbb{Q}$ para $\mathbb{N}_0$ podemos concluir a igualdade dos cardinais.

Pares de Cantor

Uma função injectiva de pares de naturais em naturais

Graficamente, é uma espiral à volta da origem:

$$f = \{((0,0) \mapsto 0), ((1,0) \mapsto 1), ((1,1) \mapsto 2), ((0,1) \mapsto 3), \ldots\}$$

Uma função injectiva de racionais em naturais

- Uma fracção irredutível pode ser representada como um par: (numerador, denominador).
- A seguinte função injectiva garante que $\mathbb{Q}$ e $\mathbb{N}_0$ têm o mesmo cardinal!

$$\begin{array}{lll} f & \subseteq & \mathbb{Z} \times \mathbb{N}_0 \to \mathbb{Q} \\ f & \stackrel{\text{def}}{=} & \{(k,n) \mapsto r \mid r = k/(n+1)\} \end{array}$$

Noções centrais

- Um conjunto é *contável* se tiver uma injecção para os naturais.
- Os conjuntos finitos são obviamente contáveis.
- Se a injecção for sobrejectiva, o conjunto é infinito (contável).

Propriedades

- Todo o subconjunto de um conjunto contável é contável.
  A prova não é simples, mas a ideia é intuitiva - um subconjunto de um conjunto não pode ter cardinal superior.
- Exemplo: o conjunto dos primos é contável:
- Conjunto que contenha um contável pode ou não ser contável.
- Conjunto que contenha um não contável é não contável.
  Um subconjunto de um não contável pode ou não ser contável.

Mais propriedades

- A intersecção de conjuntos contáveis é contável.
  A intersecção de não contáveis pode ou não ser contável.
- A união (contável) de conjuntos contáveis é contável.
- A união de conjuntos não contáveis é não contável.
- O produto cartesiano (finito) de contáveis é contável.
- O produto cartesiano infinito contável de conjuntos infinitos contáveis é não contável.

Provas por Zig-Zag

Uma técnica para definir bijecções com os naturais

Se o domínio é a composição de vários conjuntos, estes *visitam-se alternadamente*.

A união de 3 conjuntos contáveis é contável

- Sejam $A = \{a_0, a_1, a_2, \ldots\}$, $B = \{b_0, b_1, b_2, \ldots\}$ e $C = \{c_0, c_1, c_2, \ldots\}$.
- Obtém-se uma bijecção de $\mathbb{N}_0$ para $A \cup B \cup C$ listando todos os elementos da seguinte forma:
  $a_0, b_0, c_0, a_1, b_1, c_1, a_2, b_2, c_2, \ldots$

Que "Zig-Zagues"?

A união contável de conjuntos contáveis é contável

- A ideia anterior agora não funciona bem:
- visitar um elemento de cada conjunto antes de visitar o segundo elemento do primeiro conjunto não é boa ideia...
- Como o número de conjuntos é infinito, nunca se terminava a primeira iteração!

Outra prova por Zig-Zag

Um exemplo concreto: $\mathbb{N}_0 \times \mathbb{N}_0$ é contável

Note-se que $\mathbb{N}_0 \times \mathbb{N}_0 = \bigcup_{\{i \in \mathbb{N}_0\}} (\{i\} \times \mathbb{N}_0)$.

- A *visita alternada* é agora "mais fina":
- começa-se pelo primeiro elemento do primeiro conjunto, depois vai-se ao segundo elemento do primeiro conjunto e ao primeiro do segundo, etc...
- Enumerando, tem-se $(0,0), (0,1), (1,0), (0,2), (1,1), (2,0), \ldots$

$$\begin{aligned} f &\subseteq \mathbb{N}_0 \times \mathbb{N}_0 \to \mathbb{N}_0 \\ f &\stackrel{\text{def}}{=} \{(i,j) \mapsto r \mid r = \tfrac{1}{2}((i+j)^2 + 3i + j)\} \end{aligned}$$

Todos os conjuntos são contáveis?

- Os reais são "contínuos", mas os naturais são "discretos".
- Deve haver mais reais que racionais...
- Como provar um resultado negativo:
  "não há nenhuma bijecção"?
- Cantor propôs um método (uma técnica geral):
  O Princípio da Diagonalização

Princípio da Diagonalização

Teorema

- Seja R uma relação binária num conjunto A
- e seja $D \stackrel{\text{def}}{=} \{a \in A \mid (a,a) \notin R\}$ o *conjunto diagonal* de R.
- Considerando para todo o $a \in A$ o conjunto $R_a \stackrel{\text{def}}{=} \{a' \in A \mid (a,a') \in R\}$.
- Tem-se que D *é distinto* de todo o R_a.

Esboço de prova: R visto como uma matriz (infinita)

- Cada R_a é uma linha e D é o complemento da diagonal.
- D difere de todas as linhas: por definição, para cada $a \in A$ tem-se que $a \in R_a$ se e só se $a \notin D$.
  Logo, D não é nenhum R_a!

Princípio da Diagonalização

Exemplo de aplicação

Seja R a seguinte relação binária.

	a	b	c
a			$\times$
b	$\times$	$\times$	
c		$\times$	

Note-se que

$$\begin{aligned} R_a &= \{c\} \\ R_b &= \{a, b\} \\ R_c &= \{b\} \\ D &= \{a, c\} \end{aligned}$$

D (o complementar da diagonal) é diferente de qualquer das linhas.

Teorema de Cantor – $\wp(\mathbb{N}_0)$ não é contável!

Prova por absurdo, usando o Princípio da Diagonalização.

1. Assume-se que existe uma enumeração:

$$\wp(\mathbb{N}_0) = \{R_0, R_1, R_2, \ldots\}$$

e considera-se

$$\begin{aligned} R &= \{(i,j) \mid j \in R_i\} \\ D &= \{n \in \mathbb{N}_0 \mid n \notin R_n\} \end{aligned}$$

2. Como D é um conjunto de naturais, tem que estar em $\wp(\mathbb{N}_0)$, ou seja, existe um R_k tal que $D = R_k$. Se tal k existe, então
   - ou $k \in R_k$, mas então $k \notin D$, concluindo-se $D \neq R_k$;
   - ou $k \notin R_k$, mas então $k \in D$, concluindo-se de novo $D \neq R_k$.
3. Como se obtém sempre uma contradição, conclui-se que D não está na enumeração de $\wp(\mathbb{N}_0)$.

Logo, $\wp(\mathbb{N}_0)$ não é contável.

Há mais reais que racionais?

- Cantor mostrou também que sim!
- Na verdade, mostrou mesmo que o cardinal dos reais no intervalo $[0, 1[$ já é superior ao cardinal dos naturais.
- Usou o resultado que se apresenta a seguir, considerando os reais do intervalo real $[0, 1[$ em notação binária: escritos na forma $0.s$, sendo s uma sequência infinita de 0s e 1s.

O conjunto das sequências binárias infinitas não é contável

Considera-se o conjunto $\Pi_{i=1}^{\infty}\{0,1\}$.

1. Considere-se uma enumeração do conjunto das sequências: cada sequência s_i na enumeração pode então ser vista com uma linha (infinita) de uma matriz (infinita) – são os R_i do Princípio.
2. Tome-se para D a sequência obtida "invertendo" cada bit da sequência diagonal.
3. D não é a primeira sequência, porque o primeiro bit é diferente, não é a segunda, porque o segundo bit é diferente, não é a terceira, porque o terceiro bit é diferente..., não é nenhuma das da enumeração, por construção!
4. Como D não pertence à enumeração do conjunto das sequências, e a enumeração é arbitrária, o conjunto não pode ser enumerável, ou seja, não é contável.