Conceitos Preliminares

EDUARDO FREIRE NAKAMURA

Instituto de Computação
Universidade Federal do Amazonas
nakamura@icomp.ufam.edu.br

[1]Este material baseia-se no capítulo 1 do livro: Vieira, N.J. Introdução aos Fundamentos da Computação: Linguagens e Máquinas, Pioneira Thomson Learning (atualmente, CENGAGE), 2006.

Prova de teoremas

OBJETIVO

REVISAR AS PRINCIPAIS TÉCNICAS DE PROVA DE TEOREMAS

Prova de teoremas

- Argumentação indutiva
  - Parte de dados da experiência para concluir que uma dada proposição, provavelmente, é verdadeira
  - Exemplo: se em várias situações, sempre que P é verdade, Q também é, formula-se a conjectura $P \rightarrow Q$

- Argumentação indutiva é uma prova?

Argumentação indutiva

Considere o seguinte exemplo:

Seja o polinômio $p(x) = x^2 + x + 41$, então $\forall x \in \mathbf{N}$, $p(x)$ é primo?

Verificando a conjectura observamos….

x	0	1	2	3	…	20	…	39
$p(x)$	41	43	47	53	…	461	…	1601

Todos primos!

Parece verdade… Podemos assumir válida a conjectura?

Não, $p(40) = 1681$ não é um número primo, 1681 = 41*41!

Outro caso...

Em 1769, Euler conjecturou que $a^4 + b^4 + c^4 = d^4$ não tinha solução no conjunto dos números inteiros positivos

http://en.wikipedia.org/wiki/Leonhard_Euler

http://www.log24.com/log/pix06/060410-Elkies3.jpg

219 anos depois, em 1988, Noam Elkies provou que a conjectura era falsa, pois

$95.800^4 + 217.519^4 + 414.560^4 = 422.481^4$

Mais um…

- Conjectura: $313(x^3+y^3) = z^3$ não tem solução no conjunto dos inteiros positivos
  - Falso, mas o menor contra-exemplo tem mais de 1000 dígitos
  - O computador mais "poderoso" não seria capaz de obter essa solução usando uma estratégia exaustiva

O último teorema de Fermat

- Pierre de Fermat (1601/1607 – 1665)
  - Advogado e, nas horas vagas, matemático
  - Contribuições
    - Cálculo infinitesimal
    - Teoria dos números
    - Geomoetria analítica
    - Probabilidade
    - Ótica
  - Já como advogado …

http://en.wikipedia.org/wiki/Pierre_de_Fermat

O último teorema de Fermat

- Em 1637, ele escreveu o "último teorema de Fermat", como uma nota particular nas margens da obra Arithmetica, escrita pelo matemático grego Diophantus 300 anos A.C.

"É impossível separar um cubo em dois cubos, ou uma quarta potência em duas quartas potências, ou em geral, qualquer potência maior que dois, em duas potências da mesma ordem. Eu descobri uma prova maravilhosa para este problema, mas não cabe nesta margem"

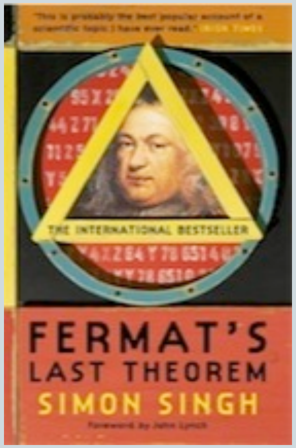
Não existem inteiros positivos a, b, c e n, com $n > 2$ que satisfaçam $a^n = b^n + c^n$

- Fermat morreu em 1665 sem revelar a sua maravilhosa prova!

O último teorema de Fermat

- Andrew Wiles provou o teorema em 1995*
  - Trabalho de sete anos de pesquisa
  - Artigo de 108 páginas
  - Introdução, cinco capítulos, mais apêndice
  - Em 2016, ele recebeu o prêmio Abel - Academia Norueguesa de Ciências e Letras (R$2,7 milhões)

http://en.wikipedia.org/wiki/Wiles'_proof_of_Fermat's_Last_Theorem



Fermat's Last Theorem: The story of a riddle that confounded the world's greatest minds for 358 years
Simon Singh

*http://en.wikipedia.org/wiki/Wiles'_proof_of_Fermat's_Last_Theorem

Um caso em aberto...

- Conjectura de Goldbach (1690–1764)
  - 07/06/1742 carta para Euler
  - "*Todo inteiro par maior que 2 é a soma de dois primos*"
  - Verificada até $4x10^{18}$ (04/04/2012)*
  - Para valores entre $4x10^{18}$ e ∞ ?

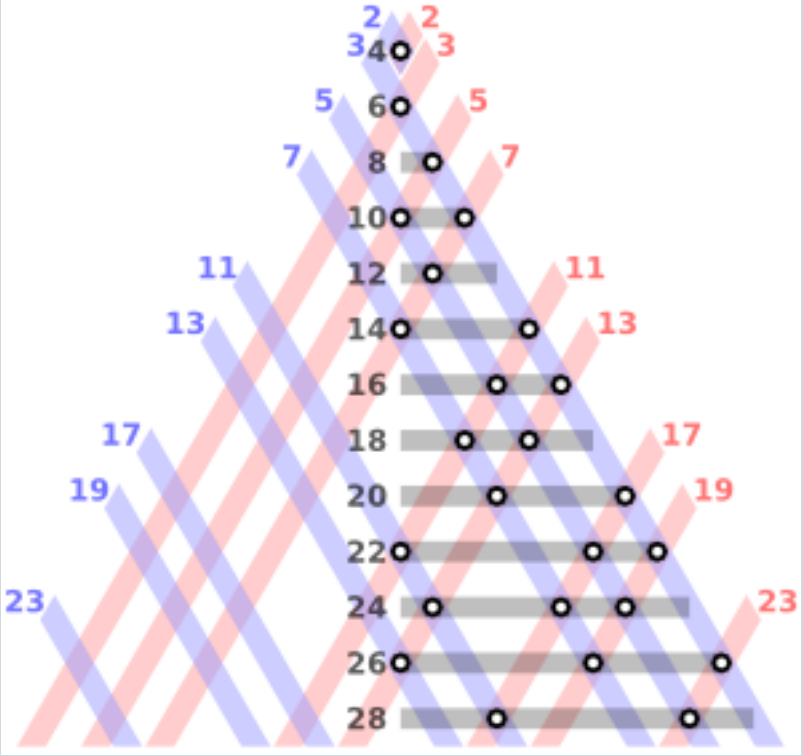
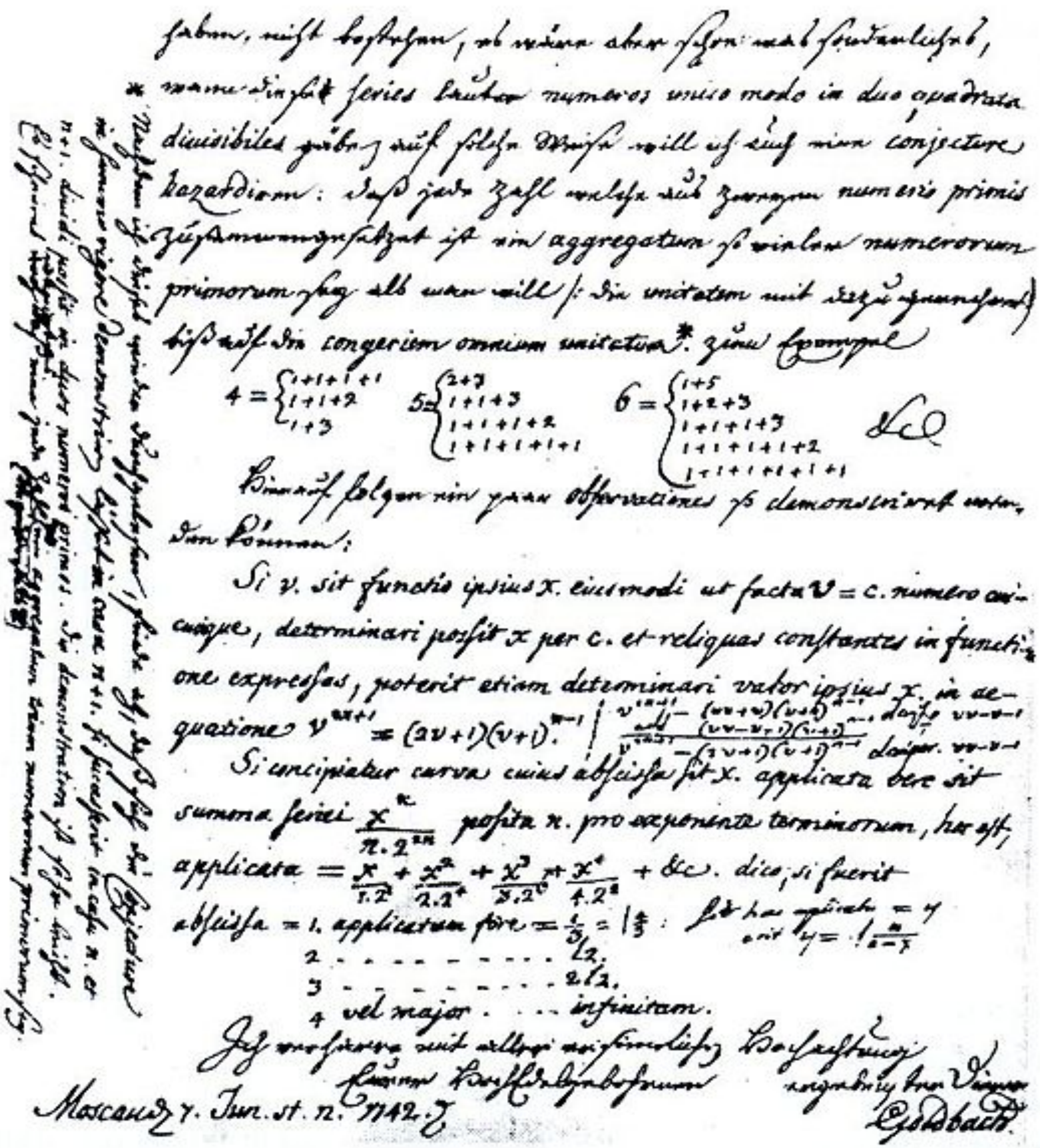


Imagem: http://en.wikipedia.org/wiki/Goldbach's_conjecture

*www.ieeta.pt/~tos/goldbach.html



haben, nicht bestehen, es wäre aber schon mahl hinlänglich, wenn diejenige series lauter numeros unico modo in duo quadrata divisibiles gäbe; auf solche Weise will ich auch eine conjecture hazardiren: daß jede Zahl welche aus zweyen numeris primis zusammengesetzt ist ein aggregatum so vieler numerorum primorum sey als man will (die unitatem mit dazu gerechnet) biß auf die congeriem omnium unitatum.* zum Exempel

$$4=\begin{cases}1+1+1+1\\1+1+2\\1+3\end{cases}\quad 5=\begin{cases}2+3\\1+1+3\\1+1+1+2\\1+1+1+1+1\end{cases}\quad 6=\begin{cases}1+5\\1+2+3\\1+1+1+3\\1+1+1+1+2\\1+1+1+1+1+1\end{cases}\quad \&c.$$

Hierauf folgen ein paar observationes so demonstrirt werden können:

Si v. sit functio ipsius x. eiusmodi ut facta $v = c$. numero cuicunque, determinari possit x per c. et reliquas constantes in functione expressas, poterit etiam determinari valor ipsius x. in aequatione $v^{2x+1} = (2v+1)(v+1)^{x-1}$ [illegible]

Si concipiatur curva cujus abscissa sit x. applicata vero sit summa seriei $\frac{x^n}{n.2^{2n}}$ posita n. pro exponente terminorum, hoc est, applicata $= \frac{x}{1.2^2} + \frac{x^2}{2.2^4} + \frac{x^3}{3.2^6} + \frac{x^4}{4.2^8} + \&c.$ dico, si fuerit abscissa = 1. applicatam fore $= l\frac{4}{3}$. fit hac applicata = y erit $y = l\frac{4}{4-x}$

2 . . . . $l2$.
3 . . . . $2l2$.
4 vel major . . . . infinitam.

Ich verharre mit aller ersinnlichen Hochachtung
Euer Hochedelgebohren
ergebenster Diener
Goldbach.

Moscau d. 7. Jun. st. n. 1742.

* Nachdem ich dieses wieder durchgelesen, finde ich, daß sich die conjecture in summo rigore demonstriren lasse in casu n+1, si successerit in casu n, et n+1 dividi possit in duos numeros primos. Die demonstration ist sehr leicht. Es scheinet wenigstens, daß eine jede Zahl, die grösser ist als 2, ein aggregatum trium numerorum primorum sey.

https://pt.wikipedia.org/wiki/
Ficheiro:Letter_Goldbach-Euler.jpg

Por quê?

- Por que esses problemas são importantes?
  - Achar soluções para tais equações é importante na área de curvas elípticas
  - Curvas elípticas são importantes no estudo de fatoração de inteiros "grandes"
  - Fatorar inteiros "grandes" é importante no estudo de sistemas criptográficos
  - Criptografia é a base de todos os sistemas seguros de comunicação atualmente!

Prova de teoremas

- Argumentação indutiva
  - Apenas para conjecturar

- Argumentação dedutiva
  - Garante que se todas as premissas forem verdadeiras, a conclusão também o será;
  - Exemplo: demonstrar $P \rightarrow Q$ (de conjectura, torna-se teorema);
  - Duas opções
    1. Provar o teorema
    2. Encontrar um contra-exemplo

Eduardo Freire Nakamura (nakamura@icomp.ufam.edu.br)

Prova de teoremas

- Contra-exemplo
  - Apenas um é sufiente para provar a falsidade
  - Se um contra-exemplo não for encontrado, não há garantias de que a conjectura é verdadeira

- Encontre um contra-exemplo para a conjectura
  - Para todo inteiro positivo n, $n! \leq n^2$
  - Todo inteiro menor que 10 é maior do que 5

O que fazer quando não é possível encontrar um contra-exemplo?

Solução:
Buscar uma prova

O que é uma prova?

- Em Matemática temos a prova:
  - Argumentação que mostra, de maneira indiscutível, que uma afirmação é verdadeira
  - As provas matemáticas são estruturadas cuidadosamente e escritas em uma forma estilizada

Técnicas de prova: demonstração exaustiva

Objetivo: Provar que P→Q

- Abordagem
  - Mostrar que P→Q para todos os elementos do domínio individualmente
  - O domínio deve ser um conjunto finito

Para qualquer inteiro positivo menor ou igual a 5, o quadrado do inteiro é menor ou igual à soma de 10 mais 5 vezes o inteiro?

Demonstração

<u>Prova</u>:

Sim, pois:

- $1^2 = 1 \leq 10 + 5(1) = 15$
- $2^2 = 4 \leq 10 + 5(2) = 20$
- $3^2 = 9 \leq 10 + 5(3) = 25$
- $4^2 = 16 \leq 10 + 5(4) = 30$
- $5^2 = 25 \leq 10 + 5(5) = 35$

Eduardo Freire Nakamura (nakamura@icomp.ufam.edu.br)

Técnicas de prova: falsidade por contra-exemplo

Objetivo: Provar que $P \rightarrow Q$

- Abordagem
  - Mostrar que $P \rightarrow Q$ para todos os elementos do domínio individualmente
  - O domínio deve ser um conjunto finito

Para qualquer inteiro positivo, o quadrado do inteiro é menor ou igual à soma de 10 mais 5 vezes o inteiro?

Demonstração

Prova:

Não, pois $7^2 = 49$ é maior que $10 + 5(7) = 45$!

Há outros contra-exemplos?

É preciso mostrar mais de um?

Eduardo Freire Nakamura (nakamura@icomp.ufam.edu.br)

Técnicas de prova: direta

Objetivo: Provar que P→Q

- Abordagem P→Q
  - Supor P (*hipótese*)
  - Derivar Q (*tese*)
- Exemplo A

Prove que o produto de dois inteiros pares é par.

Demonstração

Prova:

P (*hipótese*): x e y são inteiros pares

Q (*tese*): xy é um inteiro par

Sejam os inteiros pares $x = 2m$ e $y = 2n$, onde $m,n \in \mathbf{Z}$. Portanto, $xy = (2m)(2n) = 2(2mn)$. Como $2mn$ é um inteiro, xy é um inteiro par.

Técnicas de prova: direta

Objetivo: Provar que P→Q

- Abordagem P→Q
  - Supor P (*hipótese*)
  - Derivar Q (*tese*)

- Exemplo B

Se um inteiro é divisível por 6, então duas vezes esse inteiro é divisível por 4.

Demonstração

Prova:

P (*hipótese*): $x = 6k$, $k \in \mathbf{Z}$

Q (*tese*): $2x = 4m$, $m \in \mathbf{Z}$

Seja $x = 6k$, tal que $k \in \mathbf{Z}$. Portanto, $2x = 2(6k) = 4(3k)$. Como $3k$ é inteiro, $2x$ é um inteiro divisível por 4.

Técnicas de prova: pela contrapositiva

Objetivo: Provar que P→Q

- Abordagem ¬Q→¬P
  - Supor ¬Q (*hipótese*)
  - Derivar ¬P (*tese*)

- Exemplo A

Se o quadrado de um inteiro é ímpar, então o inteiro tem que ser ímpar.

Demonstração

Prova:

¬Q (*hipótese*): x é par

¬P (*tese*): x^2 é par

Seja $x = 2k$, tal que $k \in \mathbf{Z}$. Portanto, $x^2 = (2k)^2 = 2(2k^2)$. Como $2k^2$ é um inteiro, x^2 é um inteiro par. Logo, se o quadrado de um inteiro é ímpar, então o inteiro tem que ser ímpar.

Técnicas de prova: pela contrapositiva

Objetivo: Provar que P→Q

- Abordagem ¬Q→¬P
  - Supor ¬Q (*hipótese*)
  - Derivar ¬P (*tese*)
- Exemplo B

Se o produto de dois inteiros a e b não é divisível por um inteiro k, então os dois inteiros a e b não são divisíveis por k.

Demonstração

Prova:

¬Q (*hipótese*): ***a* ou *b*** divisíveis por k

¬P (*tese*): ab divisível por k

Caso 1. Sejam $a = mk$ e b, tais que $m, k, b \in \mathbf{Z}$. Assim, $ab = k(bm)$. Como bm é inteiro, ab é um inteiro divisível por k.

Caso 2. Sejam $b = nk$ e a, tais que $a, n, k \in \mathbf{Z}$. Assim, $ab = k(an)$. Como an é inteiro, ab é um inteiro divisível por k.

Técnicas de prova: por contradição

Objetivo: Provar que $P \rightarrow Q$

- Abordagem
  - Supor $P \land \neg Q$ (*hipótese*)
  - Derivar **F**, contradição (*tese*)

- Exemplo A

Se um inteiro somado a ele mesmo é igual a ele mesmo, então esse número é 0.

Demonstração

Prova:

Hipótese: $x+x = x$, $x \neq 0$

Tese: **F**, uma contradição

Seja x um inteiro. Por hipótese, $x + x = x$, ou seja, $x = x - x$ e, portanto, x = 0. Mas por hipótese, $x \neq 0$, uma contradição.

Técnicas de prova: por contradição

Objetivo: Provar que P→Q

- Abordagem
  - Supor $P \land \neg Q$ (*hipótese*)
  - Derivar **F**, contradição (*tese*)
- Exemplo B

O produto de dois inteiros ímpares não é par.

Demonstração

Prova:

Hipótese: *a*, *b* ímpares, *ab* par

Tese: **F**, uma contradição

Sejam $a = 2m+1$ e $b = 2n+1$, tais que $m, n \in \mathbf{Z}$. Portanto, $ab = (2m+1)(2n+1) = 2(2mn + m + n) + 1$. Como, *m* e *n* são inteiros, *ab* é um inteiro ímpar. Mas por hipótese, *ab* é par, uma contradição.

Exercício

Prove as seguintes proposições

1. A soma de um inteiro par com um inteiro ímpar é ímpar.
2. O produto de dois inteiros ímpares é ímpar.
3. O produto de dois inteiros consecutivos é par.
4. Se a e b são números reais, tais que $0 < a < b$, então $a^2 < b^2$.

Conjuntos

OBJETIVO

REVISAR OS CONCEITOS BÁSICOS DE CONJUNTOS

Eduardo Freire Nakamura (nakamura@icomp.ufam.edu.br)

Conjuntos

- Conjunto é uma abstração matemática que visa capturar o conceito de coleção
  - Lista não ordenada de elementos ou membros
  - {1, 2} = {2, 1}

- Notação
  - $a \in A$: *a* **pertence** ao conjunto A
  - $a \notin A$: *a* **não pertence** ao conjunto A

- Exemplos
  - {PAA, FTC, PPCC, IHC, AMMD}

Tipos de conjuntos e conjuntos importantes

- Conjunto vazio: $\varnothing$
- Conjunto unitário
- Conjunto finito e infinito
- **N**: números naturais
- **Z**: números inteiros
- **R**: números reais
- **Q**: números racionais

- Notações
  - $\{ x \mid P(x) \}$
    - Exemplo: $\{ k \mid k = 2n+1 \text{ e } n \in \mathbf{N} \}$
  - $\{ x \in A \mid P(x) \}$
    - Exemplo: $\{ k \in \mathbf{R} \mid 0 \leq k \leq 1 \}$

Relações básicas entre conjuntos

Subconjunto: $A \subseteq B$ se, e somente se, $\forall x\,(x \in A \rightarrow x \in B)$
Subconjunto próprio: $A \subset B$ se, e somente se, $A \subseteq B$ e $A \neq B$

- $\varnothing \subseteq A$
- $\varnothing \subset A$ se $A \neq \varnothing$
- $\varnothing \not\subset \varnothing$
- $\mathbf{N} \subset \mathbf{Z}$
- $\mathbf{N} \subseteq \mathbf{Z}^{+}$
- $\mathbf{R} \not\subset \mathbf{N}$

Operações sobre conjuntos

União

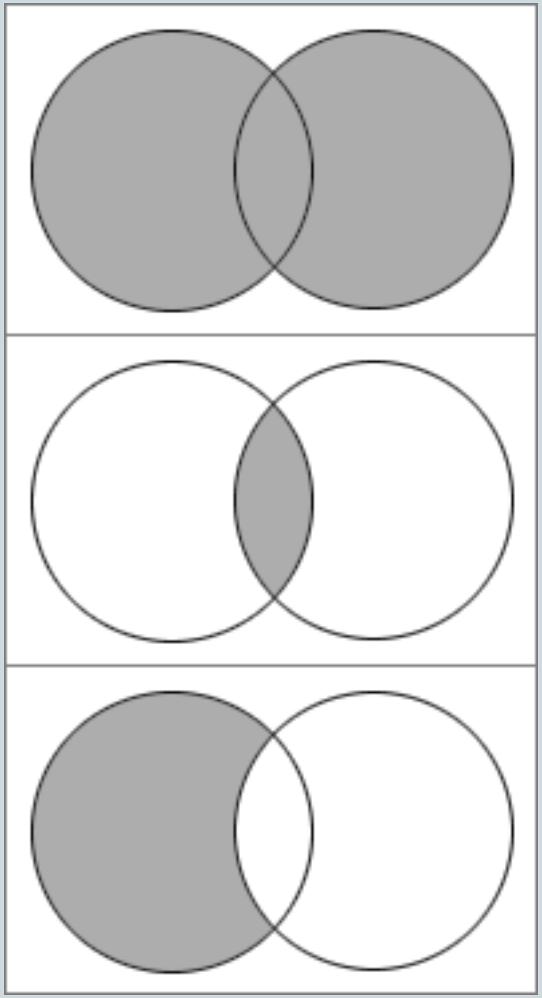
$$A \cup B = \{\, x \mid (x \in A) \vee (x \in B) \,\}$$

Interseção

$$A \cap B = \{\, x \mid (x \in A) \wedge (x \in B) \,\}$$

Diferença

$$A \setminus B = \{\, x \mid (x \in A) \wedge (x \notin B) \,\}$$



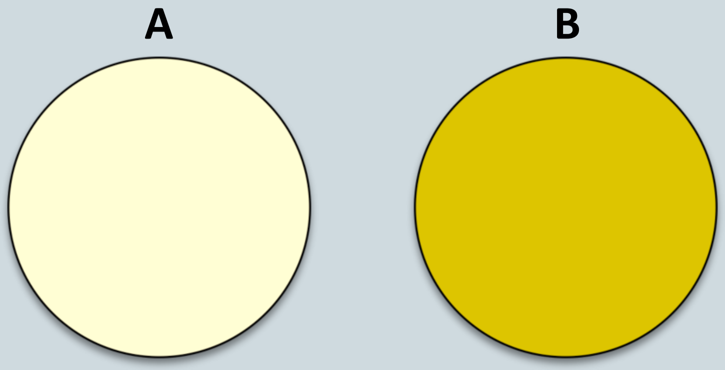
http://namesonnodes.org/ns/math/2009/images/set-operations.png

Eduardo Freire Nakamura (nakamura@icomp.ufam.edu.br)

Conjuntos disjuntos

Definição

Dois conjuntos A e B são disjuntos se, e somente se, $A \cap B = \varnothing$



Exemplos

- {1,2,3} e {5,4,9}
- $A \setminus B$ e $B \setminus A$
- $\mathbf{N}$ e $\mathbf{Z}^{-}$

Algumas identidades

- Identidades sobre conjuntos
  - $A \cap B = B \cap A$
  - $A \cup B = B \cup A$
  - $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
  - $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
  - $(A = B) \leftrightarrow (A \subseteq B) \wedge (B \subseteq A)$

União e interseção generalizadas

União de *n* conjuntos

$$\bigcup_{i=1}^{n} A_i = A_1 \cup A_2 \cup \cdots \cup A_n$$

Interseção de *n* conjuntos

$$\bigcap_{i=1}^{n} A_i = A_1 \cap A_2 \cap \cdots \cap A_n$$

Eduardo Freire Nakamura (nakamura@icomp.ufam.edu.br)

Partição

Partição de um conjunto

Uma partição de A é um conjunto de subconjuntos de A dado por $\{B_1, B_2, \ldots, B_n\}$ tal que

- $B_i \neq \emptyset$, para $1 \leq i \leq n$;
- $B_i \cap B_j = \emptyset$, para $1 \leq i < j \leq n$;
- $\bigcup_{1 \leq i \leq n} B_i = A$

Conjunto potência

Definição

Conjunto potência de A, denotado por $\mathscr{P}(A)$ é o conjunto formado por todos os subconjuntos de A

$$\mathscr{P}(A) = \{ X \mid X \subseteq A \}$$

Exemplo

Que conjunto é $\mathscr{P}(\{1,2,3\})$?

$\{ \varnothing, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\} \}$

Se $|A|$ denota o tamanho de A, qual é o valor de $|\mathscr{P}(A)|$?

$$|\mathscr{P}(A)| = 2^{|A|}$$

Produto cartesiano

Definição

- Produto cartesiano entre dois conjuntos A e B, denotado por $A \times B$ é formado pelo conjunto de pares ordenados (a,b) tais que $a \in A$ e $b \in B$, ou seja,

$$A \times B = \{ (a,b) \mid a \in A \land b \in B \}$$

Exemplos

- $\varnothing \times \{1,2\} = \varnothing$
- $\{1,2\} \times \{3,4\} = \{(1,3), (1,4), (2,3), (2,4)\}$
- $|A \times B| = |A| \cdot |B|$, se A e B finitos
- $A^n = A \times A \times \ldots \times A$ (n vezes)

Relação e função

OBJETIVO

REVER OS CONCEITOS DE RELAÇÃO E FUNÇÃO

O que é uma relação?

Definição informal

- O que significa relacionar dois objetos?
  - Comparar dois objetos segundo uma regra definida
  - Relação é uma comparação entre dois "objetos"

Exemplos

- Matemática
  - "Menor do que"
  - "Maior do que"
  - "É paralelo à"
  - "É um subconjunto de"

O que é uma relação?

Definição formal

Relação de n argumentos sobre $A_1, A_2, \ldots, A_n$

Subconjunto de $A_1 \times A_2 \times \ldots \times A_n$

- Relação binária: $R \subseteq A \times B$
  - Domínio: A
  - Contradomínio: B
  - Imagem: $\{ y \mid (x,y) \in R \text{ para algum } x \}$
- Notação

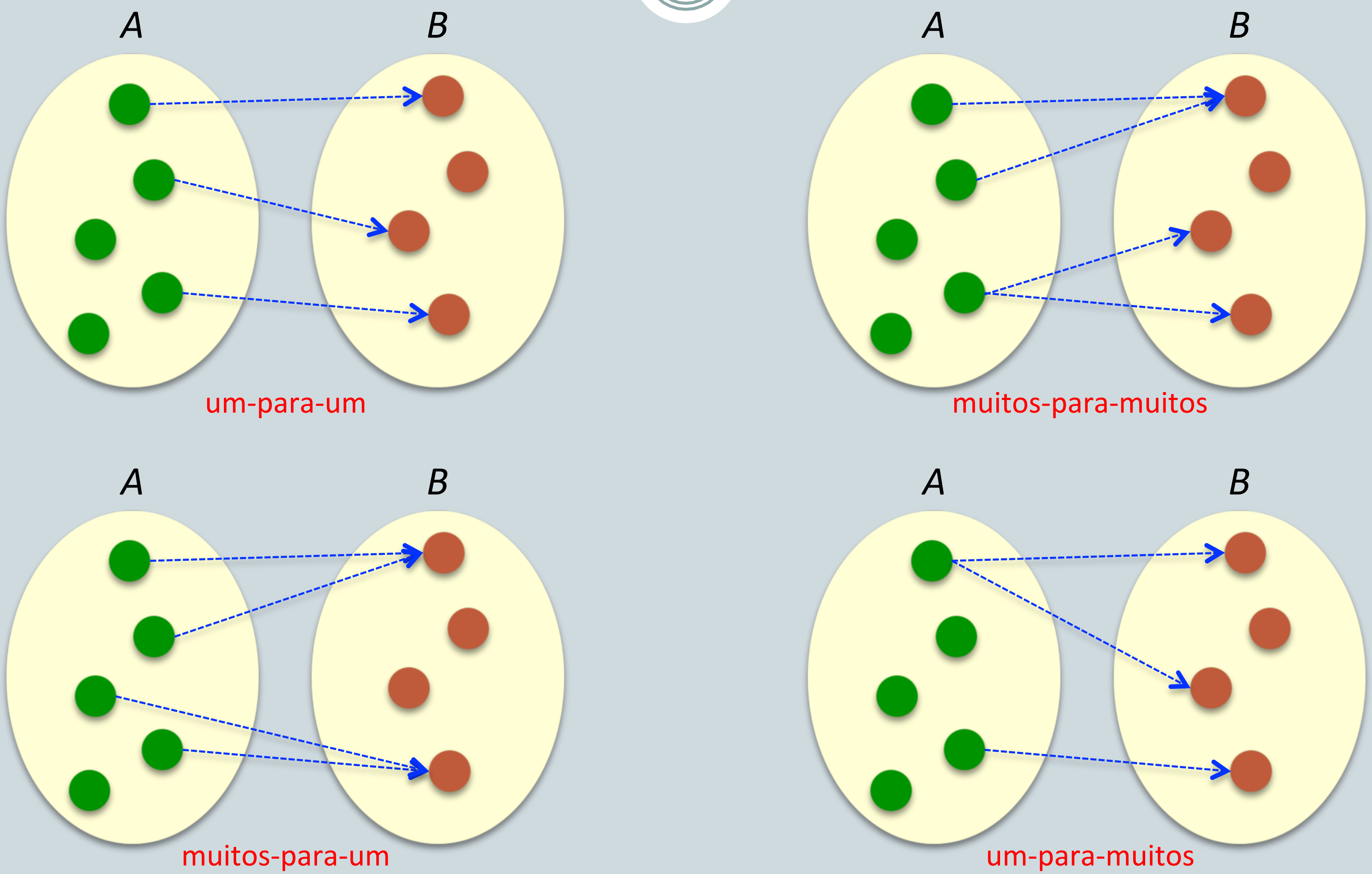
$$(x,y) \in R \quad \text{ou} \quad x\,R\,y$$

Exemplo

- Relação binária: $< \subseteq \mathbf{N} \times \mathbf{N}$
  - Domínio: $\mathbf{N}$
  - Contradomínio: $\mathbf{N}$
  - Imagem: $\mathbf{N} - \{0\}$

    $\{ y \mid (x,y) \in R \text{ para } x \text{ menor que } y \}$

Tipos de relações binárias



Propriedades de uma relação

Inversa de R

$$R^{-1} = \{ (y,x) \mid (x,y) \in R \}$$

Propriedades de uma relação binária $R \subseteq A \times A$

- Reflexiva: $\forall x \in A,\ xRx$
- Simétrica: $\forall x,y \in A,\ (xRy \rightarrow yRx)$
- Transitiva: $\forall x,y,z \in A,\ (xRy \wedge yRz) \rightarrow xRz$

Quais as propriedades das relações abaixo?

- $>$ sobre **N**

  ~~Reflexiva~~, ~~Simétrica~~, Transitiva

- $\geq$ sobre **N**

  Reflexiva, ~~Simétrica~~, Transitiva

- $\subseteq$ sobre $\mathscr{P}$(**N**)

  Reflexiva, ~~Simétrica~~, Transitiva

- $=$ sobre **N**

  Reflexiva, Simétrica, Transitiva

Função

Definição

Função parcial

Uma função $f: A \rightarrow B$ é uma relação $f \subseteq A \times B$, tal que

$$\text{se } (x,y) \in f \text{ e } (x,z) \in f, \text{ então } y = z$$

- $(x,y) \in f$ é o mesmo que $f(x) = y$
- f é indefinida para x, se não existe y tal que $f(x) = y$
- Função **total** definida $\forall x$ no domínio
- Função $f: A_1 \times \ldots \times A_n \rightarrow B$ de n argumentos

Exemplo

Função	Total	Parcial
$+ : \mathbf{N} \times \mathbf{N} \rightarrow \mathbf{N}$	✗	
$* : \mathbf{N} \times \mathbf{N} \rightarrow \mathbf{N}$	✗	
$\div : \mathbf{N} \times \mathbf{N} \rightarrow \mathbf{N}$		✗
$\div : \mathbf{N} \times \mathbf{Z}^+ \rightarrow \mathbf{N}$		✗

Funções compostas

Definição

Composição de duas funções g e f

$$g \circ f = g\big(f(x)\big)$$

Exemplo

$f : \mathbf{Z} \to \mathbf{N}$, tal que $f(x) = |x| + 1$

$g : \mathbf{N} \to \mathbf{Z}$, tal que $g(x) = 2 - x$

$g \circ f : \mathbf{Z} \to \mathbf{Z}$, tal que

$$(g \circ f)(x) = g\big(|x| + 1\big) = 2 - \big(|x| + 1\big) = 1 - |x|$$

$f \circ g : \mathbf{N} \to \mathbf{N}$, tal que

$$(f \circ g)(x) = f\big(2 - x\big) = |2 - x| + 1$$

Tipos de funções

Tipos de funções

Uma função total $f : A \rightarrow B$ pode ser

1. Injetora

   $\forall x,y \in A,\ [\ x \neq y \rightarrow f(x) \neq f(y)\ ]$

   Exemplo: $f : \mathbf{N} \rightarrow \mathbf{N}$, tal que $f(x) = x + 1$

2. Sobrejetora

   $\forall y \in B, \exists x \in A, f(x) = y$, ou seja, B é a imagem de f

   Exemplo: $f : \mathbf{R} \rightarrow \mathbf{R}^+ \cup \{0\}$, tal que $f(x) = x^2$

3. Bijetora

   f é injetora e sobrejetora

   Exemplo: $f : \mathbf{R} \rightarrow \mathbf{R}$, tal que $f(x) = x^3$

Eduardo Freire Nakamura (nakamura@icomp.ufam.edu.br)

Recursividade e Indução Matemática

OBJETIVO

APRENDER A DEFINIR CONJUNTOS RECURSIVAMENTE

APRENDER A PROVAR PROPRIEDADES SOBRE OS INTEIROS USANDO INDUÇÃO MATEMÁTICA

O que é uma definição recursiva?

Definição

Definição Recursiva do Conjunto *A*

a) **Base**: especificação de $B \subset A$

Eduardo Freire Nakamura (nakamura@icomp.ufam.edu.br)

O que é uma definição recursiva?

Definição

Definição Recursiva do Conjunto A

a) **Base**: especificação de $B \subset A$

b) **Passo Recursivo**: como obter elementos de A a partir de outros elementos de A

O que é uma definição recursiva?

Definição

Definição Recursiva do Conjunto *A*

a) **Base**: especificação de $B \subset A$

b) **Passo Recursivo**: como obter elementos de A a partir de outros elementos de A

c) **Fechamento**: só pertencem a A, os elementos obtidos através dos passos **(a)** ou **(b)**.

É possível definir recursivamente qualquer conjunto enumerável!

O que é uma definição recursiva?

Definição

Definição Recursiva do Conjunto *A*

a) **Base**: especificação de $B \subset A$

b) **Passo Recursivo**: como obter elementos de *A* a partir de outros elementos de *A*

c) **Fechamento**: só pertencem a *A*, os elementos obtidos através dos passos **(a)** ou **(b)**.

Exemplo 01: Números naturais

Eduardo Freire Nakamura (nakamura@icomp.ufam.edu.br)

O que é uma definição recursiva?

Definição

Definição Recursiva do Conjunto *A*

a) **Base**: especificação de $B \subset A$

b) **Passo Recursivo**: como obter elementos de A a partir de outros elementos de A

c) **Fechamento**: só pertencem a A, os elementos obtidos através dos passos **(a)** ou **(b)**.

Exemplo 01: Números naturais

Definição

a) $0 \in \mathbf{N}$

b) Se $n \in \mathbf{N}$, então $n + 1 \in \mathbf{N}$

c) Só pertencem a **N**, os números gerados usando (a) ou (b).

O que é uma definição recursiva?

Definição

Definição Recursiva do Conjunto *A*

a) Base: especificação de $B \subset A$

b) Passo Recursivo: como obter elementos de A a partir de outros elementos de A

c) Fechamento: só pertencem a A, os elementos obtidos através dos passos **(a)** ou **(b)**.

Exemplo 02: Fatorial

Definição – $fat : \mathbf{N} \rightarrow \mathbf{N}$

a) $fat(0) = 1$

b) $\forall n \in \mathbf{N}, fat(n+1) = n \times fat(n-1)$

c) implícito

O que é uma definição recursiva?

Definição

Definição Recursiva do Conjunto *A*

a) Base: especificação de $B \subset A$

b) Passo Recursivo: como obter elementos de A a partir de outros elementos de A

c) Fechamento: só pertencem a A, os elementos obtidos através dos passos **(a)** ou **(b)**.

Exemplo 03: Exponencial a^n

Definição – $a^n : \mathbf{N} \rightarrow \mathbf{N}$

a) $a^0 = 1$

b) $\forall n \in \mathbf{N},\ a^{n+1} = a \times a^n$

c) implícito

O que é uma definição recursiva?

Definição

Definição Recursiva do Conjunto *A*

a) Base: especificação de $B \subset A$

b) Passo Recursivo: como obter elementos de A a partir de outros elementos de A

c) Fechamento: só pertencem a A, os elementos obtidos através dos passos **(a)** ou **(b)**.

Exemplo 04: Ling. Proposicional

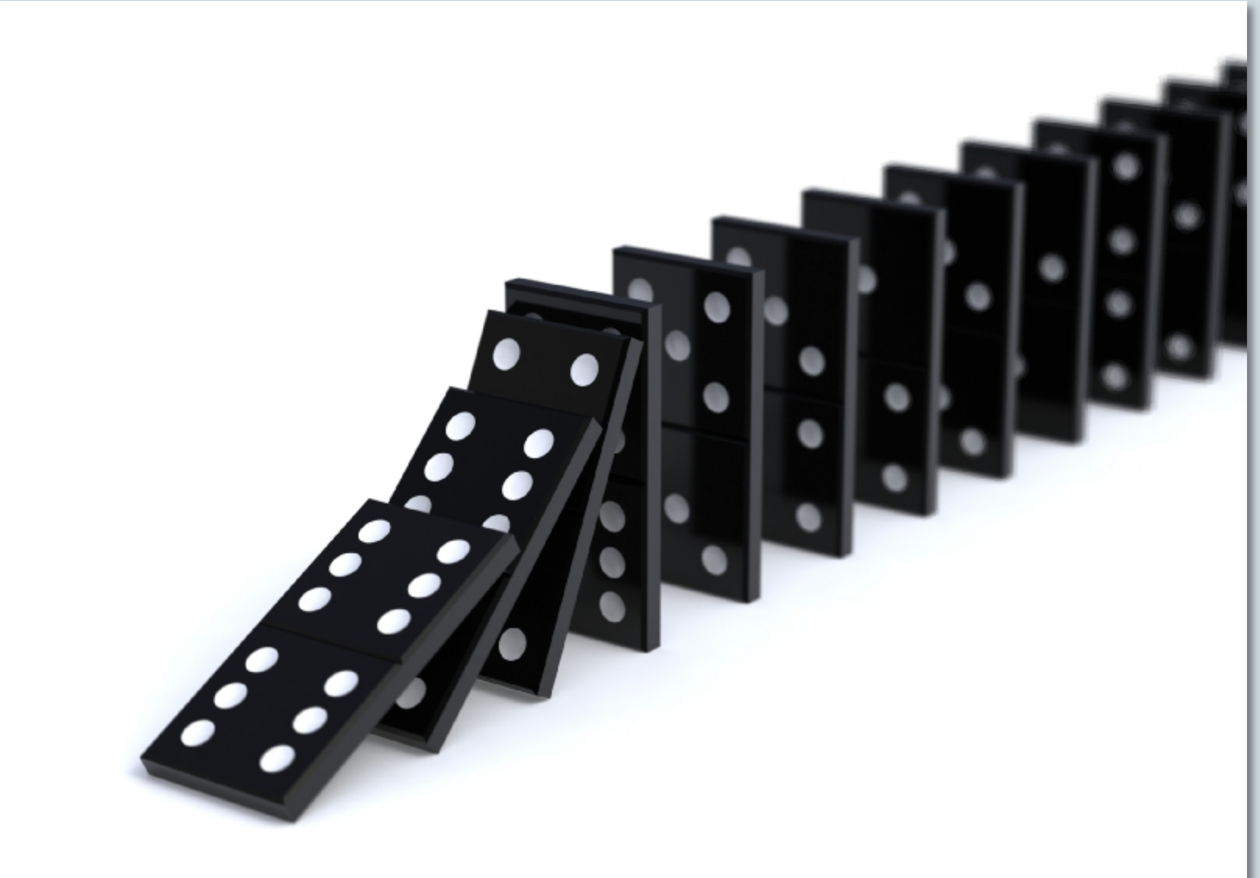
Definição – Ling. proposicional (LP)

a) Toda a variável lógica está na LP

b) Se P e Q, estão na LP, então também estão na LP:
   - $\neg P$
   - $P \wedge Q$
   - $P \vee Q$
   - $P \rightarrow Q$
   - $P \leftrightarrow Q$

c) implícito

Indução matemática

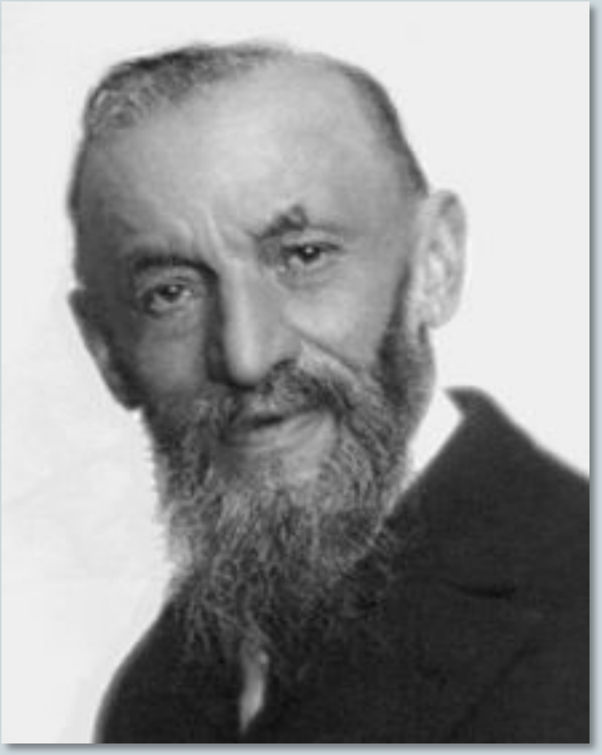


http://meangreenmath.files.wordpress.com/2013/08/dominoes.jpg

Princípio da indução

Nono axioma de Giuseppe Peano

- Se *K* é um conjunto tal que
  1. 0 (zero) pertence a *K*
  2. Para todo natural *k*
     - Se *k* está contido em *K*,
     - Então o sucessor de *k* está em *K*
- Então *K* contém todos os números naturais



http://en.wikipedia.org/wiki/Giuseppe_Peano

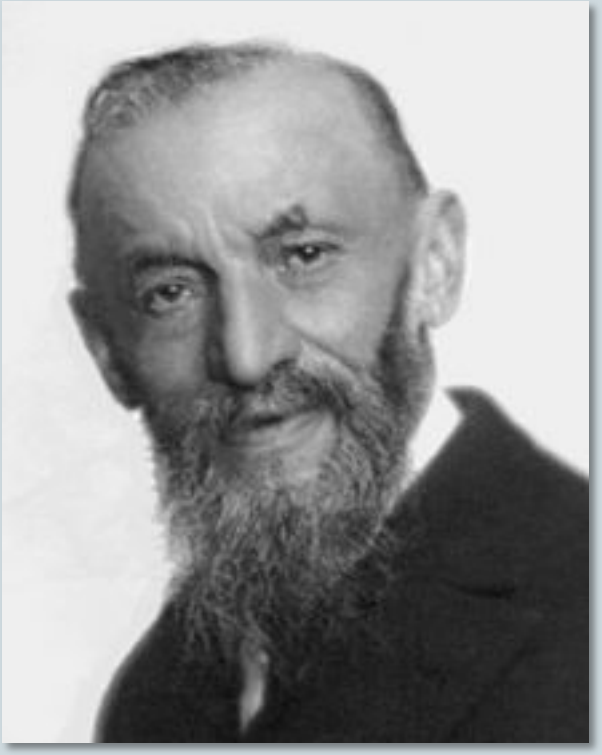
Princípio da indução

Reformulando...

- Se P é um predicado tal que

  1. $P(0)$ é verdade
  2. $\forall k \in \mathbf{N},\ P(k) \rightarrow P(k+1)$

- Então, $P(n)$ é verdadeiro para todo $n \in \mathbf{N}$



http://en.wikipedia.org/wiki/Giuseppe_Peano

Eduardo Freire Nakamura (nakamura@icomp.ufam.edu.br)

Princípio da indução

Reformulando...

- Se P é um predicado tal que

1. $P(0)$ é verdade
2. $\forall k \in \mathbf{N}, P(k) \rightarrow P(k+1)$

- Então, $P(n)$ é verdadeiro para todo $n \in \mathbf{N}$

É possível provar propriedades para conjuntos enumeráveis usando indução matemática!

Eduardo Freire Nakamura (nakamura@icomp.ufam.edu.br)

Princípio da indução fraca

Definição

Princípio da indução fraca

Se

① $P(0)^*$

② $\forall n, P(n) \rightarrow P(n+1)$

Então

✓ $\forall n, P(n)$

*Primeiro elemento do conjunto, não necessariamente 0 (zero)

Estrutura de demonstração

1. Provar $P(0)$ (caso base)
2. Seja $n \geq 0$ abitrário
3. Suponha $P(n)$ (hipótese de indução)
4. Provar $P(n+1)$
5. Concluir $\forall n, P(n)$

Os passos (2) a (4) são chamados de passo indutivo

Princípio da indução fraca

Exemplo 01

Prove que para todo $n \in \mathbf{Z}^+$, temos que a soma $1 + 3 + 5 + \ldots + (2n-1) = n^2$.

1. Caso base $n = 1$
   - $1 = 1^2$
2. Passo indutivo
   - Hipótese:

     $S(n) = 1+3+5+\ldots+(2n-1) = n^2$
   - Tese:

$S(n+1) = 1+3+5+\ldots+(2n-1)+[2(n+1)-1] = (n+1)^2$

$S(n+1) = 1 + 3 + 5 + \ldots + (2n-1) + [2(n+1) - 1]$

Por definição

$S(n) = 1 + 3 + 5 + \ldots + (2n - 1)$

Eduardo Freire Nakamura (nakamura@icomp.ufam.edu.br)

Princípio da indução fraca

Exemplo 01

Prove que para todo $n \in \mathbf{Z}^+$, temos que a soma $1 + 3 + 5 + \ldots + (2n-1) = n^2$.

1. Caso base $n = 1$
   - $1 = 1^2$
2. Passo indutivo
   - Hipótese:

     $S(n) = 1+3+5+\ldots+(2n-1) = n^2$
   - Tese:

$S(n+1) = 1+3+5+\ldots+(2n-1)+[2(n+1)-1] = (n+1)^2$

$$S(n+1) = 1 + 3 + 5 + \ldots + (2n-1) + [2(n+1) - 1]$$
$$= S(n) + [2(n+1) - 1]$$

Por hipótese de indução

$S(n) = n^2$

Eduardo Freire Nakamura (nakamura@icomp.ufam.edu.br)

Princípio da indução fraca

Exemplo 01

Prove que para todo $n \in \mathbf{Z}^+$, temos que a soma $1 + 3 + 5 + \ldots + (2n-1) = n^2$.

1. Caso base $n = 1$
   - $1 = 1^2$
2. Passo indutivo
   - Hipótese:

     $S(n) = 1+3+5+\ldots+(2n-1) = n^2$

   - Tese:

$S(n+1) = 1+3+5+\ldots+(2n-1)+[2(n+1)-1] = (n+1)^2$

$$
\begin{aligned}
S(n+1) &= 1 + 3 + 5 + \ldots + (2n-1) + [2(n+1) - 1] \\
&= S(n) + [2(n+1) - 1] \\
&= n^2 + [2(n+1) - 1]
\end{aligned}
$$

Princípio da indução fraca

Exemplo 01

Prove que para todo $n \in \mathbf{Z}^+$, temos que a soma $1 + 3 + 5 + \ldots + (2n-1) = n^2$.

1. Caso base $n = 1$
   - $1 = 1^2$
2. Passo indutivo
   - Hipótese:

     $S(n) = 1+3+5+\ldots+(2n-1) = n^2$
   - Tese:

$S(n+1) = 1+3+5+\ldots+(2n-1)+[2(n+1)-1] = (n+1)^2$

$$
\begin{aligned}
S(n+1) &= 1 + 3 + 5 + \ldots + (2n-1) + [2(n+1) - 1] \\
&= S(n) + [2(n+1) - 1] \\
&= n^2 + [2(n+1) - 1] \\
&= n^2 + [2n + 2 - 1]
\end{aligned}
$$

Princípio da indução fraca

Exemplo 01

Prove que para todo $n \in \mathbf{Z}^+$, temos que a soma $1 + 3 + 5 + \ldots + (2n-1) = n^2$.

1. Caso base $n = 1$
   - $1 = 1^2$
2. Passo indutivo
   - Hipótese:

     $S(n) = 1+3+5+\ldots+(2n-1) = n^2$
   - Tese:

$S(n+1) = 1+3+5+\ldots+(2n-1)+[2(n+1)-1] = (n+1)^2$

$$
\begin{aligned}
S(n+1) &= 1 + 3 + 5 + \ldots + (2n-1) + [2(n+1) - 1] \\
&= S(n) + [2(n+1) - 1] \\
&= n^2 + [2(n+1) - 1] \\
&= n^2 + [2n + 2 - 1] \\
&= n^2 + 2n + 1
\end{aligned}
$$

$(n + 1)$

Princípio da indução fraca

Exemplo 01

Prove que para todo $n \in \mathbf{Z}^+$, temos que a soma $1 + 3 + 5 + \ldots + (2n-1) = n^2$.

1. Caso base $n = 1$
   - $1 = 1^2$
2. Passo indutivo
   - Hipótese:

     $S(n) = 1+3+5+\ldots+(2n-1) = n^2$
   - Tese:

$S(n+1) = 1+3+5+\ldots+(2n-1)+[2(n+1)-1] = (n+1)^2$

$$
\begin{aligned}
S(n+1) &= 1 + 3 + 5 + \ldots + (2n-1) + [2(n+1) - 1] \\
&= S(n) + [2(n+1) - 1] \\
&= n^2 + [2(n+1) - 1] \\
&= n^2 + [2n + 2 - 1] \\
&= n^2 + 2n + 1 \\
&= (n + 1)^2
\end{aligned}
$$

Logo, para todo $n \in \mathbf{Z}^+$, temos que $1 + 3 + 5 + \ldots + (2n-1) = n^2$.

Eduardo Freire Nakamura (nakamura@icomp.ufam.edu.br)

Princípio da indução fraca

Exemplo 02

Prove que para todo $n \in \mathbf{Z}^+$, o número $2^{2n} - 1$ é divisível por 3.

1. Caso base $n = 1$
   - $2^{2(1)} - 1 = 4 - 1 = 3$ (divisível por 3)
2. Passo indutivo
   - Hipótese: $2^{2n} - 1 = 3m$, para $m,n \in \mathbf{Z}^+$
   - Tese: $2^{2(n+1)} - 1 = 3k$

$$2^{2(n+1)} - 1 =$$

Princípio da indução fraca

Exemplo 02

Prove que para todo $n \in \mathbf{Z}^+$, o número $2^{2n} - 1$ é divisível por 3.

1. Caso base $n = 1$
   - $2^{2(1)} - 1 = 4 - 1 = 3$ (divisível por 3)
2. Passo indutivo
   - Hipótese: $2^{2n} - 1 = 3m$, para $m,n \in \mathbf{Z}^+$
   - Tese: $2^{2(n+1)} - 1 = 3k$, para $k \in \mathbf{Z}^+$

$$2^{2(n+1)} - 1 = 2^{2n+2} - 1$$

Eduardo Freire Nakamura (nakamura@icomp.ufam.edu.br)

Princípio da indução fraca

Exemplo 02

Prove que para todo $n \in \mathbf{Z}^{+}$, o número $2^{2n} - 1$ é divisível por 3.

1. Caso base $n = 1$
   - $2^{2(1)} - 1 = 4 - 1 = 3$ (divisível por 3)
2. Passo indutivo
   - Hipótese: $2^{2n} - 1 = 3m$, para $m,n \in \mathbf{Z}^{+}$
   - Tese: $2^{2(n+1)} - 1 = 3k$, para $k \in \mathbf{Z}^{+}$

$$\begin{aligned} 2^{2(n+1)} - 1 &= 2^{2n+2} - 1 \\ &= 2^{2n}(2^{2}) - 1 \end{aligned}$$

Princípio da indução fraca

Exemplo 02

Prove que para todo $n \in \mathbf{Z}^+$, o número $2^{2n} - 1$ é divisível por 3.

1. Caso base $n = 1$
   - $2^{2(1)} - 1 = 4 - 1 = 3$ (divisível por 3)
2. Passo indutivo
   - Hipótese: $2^{2n} - 1 = 3m$, para $m,n \in \mathbf{Z}^+$
   - Tese: $2^{2(n+1)} - 1 = 3k$, para $k \in \mathbf{Z}^+$

$$
\begin{aligned}
2^{2(n+1)} - 1 &= 2^{2n+2} - 1 \\
&= 2^{2n}(2^2) - 1 \\
&= 2^{2n}(4) - 1
\end{aligned}
$$

Princípio da indução fraca

Exemplo 02

Prove que para todo $n \in \mathbf{Z}^+$, o número $2^{2n} - 1$ é divisível por 3.

1. Caso base $n = 1$
   - $2^{2(1)} - 1 = 4 - 1 = 3$ (divisível por 3)
2. Passo indutivo
   - Hipótese: $2^{2n} - 1 = 3m$, para $m,n \in \mathbf{Z}^+$
   - Tese: $2^{2(n+1)} - 1 = 3k$, para $k \in \mathbf{Z}^+$

$$\begin{aligned} 2^{2(n+1)} - 1 &= 2^{2n+2} - 1 \\ &= 2^{2n}(2^2) - 1 \\ &= 2^{2n}(4) - 1 \\ &= 2^{2n}(3 + 1) - 1 \end{aligned}$$

Princípio da indução fraca

Exemplo 02

Prove que para todo $n \in \mathbf{Z}^+$, o número $2^{2n} - 1$ é divisível por 3.

1. Caso base $n = 1$
   - $2^{2(1)} - 1 = 4 - 1 = 3$ (divisível por 3)
2. Passo indutivo
   - Hipótese: $2^{2n} - 1 = 3m$, para $m,n \in \mathbf{Z}^+$
   - Tese: $2^{2(n+1)} - 1 = 3k$, para $k \in \mathbf{Z}^+$

$$
\begin{aligned}
2^{2(n+1)} - 1 &= 2^{2n+2} - 1 \\
&= 2^{2n}(2^2) - 1 \\
&= 2^{2n}(4) - 1 \\
&= 2^{2n}(3 + 1) - 1 \\
&= 3(2^{2n}) + 2^{2n} - 1
\end{aligned}
$$

Por hipótese de indução:

$2^{2n} - 1 = 3m$

Eduardo Freire Nakamura (nakamura@icomp.ufam.edu.br)

Princípio da indução fraca

Exemplo 02

Prove que para todo $n \in \mathbf{Z}^+$, o número $2^{2n} - 1$ é divisível por 3.

1. Caso base $n = 1$
   - $2^{2(1)} - 1 = 4 - 1 = 3$ (divisível por 3)
2. Passo indutivo
   - Hipótese: $2^{2n} - 1 = 3m$, para $m, n \in \mathbf{Z}^+$
   - Tese: $2^{2(n+1)} - 1 = 3k$, para $k \in \mathbf{Z}^+$

$$
\begin{aligned}
2^{2(n+1)} - 1 &= 2^{2n+2} - 1 \\
&= 2^{2n}(2^2) - 1 \\
&= 2^{2n}(4) - 1 \\
&= 2^{2n}(3 + 1) - 1 \\
&= 3(2^{2n}) + 2^{2n} - 1 \\
&= 3(2^{2n}) + 3m
\end{aligned}
$$

3(

Logo, para todo n $\mathbf{Z}^+$, o número
2 – 1 é divisível por 3

Princípio da indução fraca

Exemplo 02

Prove que para todo $n \in \mathbf{Z}^+$, o número $2^{2n} - 1$ é divisível por 3.

1. Caso base $n = 1$
   - $2^{2(1)} - 1 = 4 - 1 = 3$ (divisível por 3)
2. Passo indutivo
   - Hipótese: $2^{2n} - 1 = 3m$, para $m,n \in \mathbf{Z}^+$
   - Tese: $2^{2(n+1)} - 1 = 3k$, para $k \in \mathbf{Z}^+$

$$
\begin{aligned}
2^{2(n+1)} - 1 &= 2^{2n+2} - 1 \\
&= 2^{2n}(2^2) - 1 \\
&= 2^{2n}(4) - 1 \\
&= 2^{2n}(3 + 1) - 1 \\
&= 3(2^{2n}) + 2^{2n} - 1 \\
&= 3(2^{2n}) + 3m \\
&= 3(2^{2n} + m)
\end{aligned}
$$

$k = (2^{2n} + m) \in \mathbf{Z}^+$

Logo, para todo n $\mathbf{Z}^+$, o número 2 – 1 é divisível por 3

Eduardo Freire Nakamura (nakamura@icomp.ufam.edu.br)

Princípio da indução fraca

Exemplo 02

Prove que para todo $n \in \mathbf{Z}^+$, o número $2^{2n} - 1$ é divisível por 3.

1. Caso base $n = 1$
   - $2^{2(1)} - 1 = 4 - 1 = 3$ (divisível por 3)
2. Passo indutivo
   - Hipótese: $2^{2n} - 1 = 3m$, para $m,n \in \mathbf{Z}^+$
   - Tese: $2^{2(n+1)} - 1 = 3k$, para $k \in \mathbf{Z}^+$

$$
\begin{aligned}
2^{2(n+1)} - 1 &= 2^{2n+2} - 1 \\
&= 2^{2n}(2^2) - 1 \\
&= 2^{2n}(4) - 1 \\
&= 2^{2n}(3 + 1) - 1 \\
&= 3(2^{2n}) + 2^{2n} - 1 \\
&= 3(2^{2n}) + 3m \\
&= 3(2^{2n} + m)
\end{aligned}
$$

Logo, para todo $n \in \mathbf{Z}^+$, o número $2^{2n} - 1$ é divisível por 3.

Princípio da indução forte

Definição

Princípio da indução forte

Se

① $[P(0) \wedge P(1) \wedge \ldots \wedge P(\mathrm{k})] \rightarrow P(k+1)^{*}$

Então

✓ $\forall n, P(n)$

*Primeiro elemento do conjunto, não necessariamente 0 (zero)

Estrutura de demonstração

1. Seja $n \geq 0$ abitrário
2. Suponha $\forall k < n, P(k)$ (hipótese de indução)
3. Provar $P(k+1)$
4. Concluir $\forall n, P(n)$

Eduardo Freire Nakamura (nakamura@icomp.ufam.edu.br)

Princípio da indução forte

Exemplo 01

Prove que todo $n > 1 \in \mathbf{Z}^+$ pode ser escrito como o produto de números primos.

1. Caso base $n = 2$
   - $2 = 2(1)$ (produto de dois primos)
2. Passo indutivo
   - Hipótese: todo $2 \leq r \leq k$, pode ser escrito como o produto de primos
   - Tese: $(k + 1)$ pode ser escrito como o produto de primos

Caso 1: $(k+1)$ é primo

Neste caso $(k+1) = (k+1)(1)$, produto de dois primos.

Princípio da indução forte

Exemplo 01

Prove que todo $n > 1 \in \mathbf{Z}^+$ pode ser escrito como o produto de números primos.

1. Caso base $n = 2$
   - 2 = 2(1) (produto de dois primos)
2. Passo indutivo
   - Hipótese: todo $2 \leq r \leq k$, pode ser escrito como o produto de primos
   - Tese: $(k + 1)$ pode ser escrito como o produto de primos

Caso 2: $(k+1)$ **não** é primo

Se $(k+1)$ não é primo, então $(k+1)$ é composto, ou seja,

$(k+1) = ab$, tal que $2 \leq a \leq b \leq k$.

Por hipótese, todo $2 \leq r \leq k$, é o produto de primos.

Logo, *a* e *b* podem ser escritos como produtos de números primos.

Portanto, $(k+1)$ também pode!

Princípio da indução forte

Exemplo 02

Prove que todo $n \geq 12 \in \mathbf{Z}^+$ pode ser obtido somando-se 4's ou 5's.

1. Caso base n = 12, 13, 14, 15
   - $12 = 4 + 4 + 4$ $\quad$ $13 = 4 + 4 + 5$
   - $14 = 4 + 5 + 5$ $\quad$ $15 = 5 + 5 + 5$
2. Passo indutivo
   - Hipótese: todo $12 \leq r \leq k$ é a soma de 4's ou 5's, onde k>=15
   - Tese: $(k + 1)$ é a soma de 4's ou 5's

Por hipótese, temos que

- $(k - 3)$ pode ser escrito como a soma de 4's ou 5's
- Afinal, $12 \leq (k - 3) \leq k$.

Note que $(k + 1) = (k - 3) + 4$.

Portanto, $(k + 1)$ também pode ser escrito como a soma de 4's ou 5's.

Exercícios de fixação

1. Prove que para todo $n \in \mathbf{Z}^+$ temos que $\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$.

2. Verifique a validade da hipótese: para todo $n \in \mathbf{Z}^+$, temos que

$$1 + 2 + \ldots + n = \frac{n(n+1)}{2}$$

3. Prove que $11^n - 6$ é divisível por 5 para qualquer $n \in \mathbf{Z}^+$.

4. Prove que todo $n \geq 8 \in \mathbf{Z}^+$ pode ser obtido somando-se 3's ou 5's.

5. A função de Fibonacci é dada por $F(n) = \begin{cases} 0, \text{ se } n = 0 \\ 1, \text{ se } n = 1 \\ F(n-1) + F(n-2), \text{ se } n \geq 2 \end{cases}$.

 Prove que

$$F(n) = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right]$$

Exercícios de fixação

- 5 - solução

Proof. We use strong induction. Let n be an arbitrary natural number, and suppose that for all $k < n$,

$$F_k = \frac{\left(\frac{1+\sqrt{5}}{2}\right)^k - \left(\frac{1-\sqrt{5}}{2}\right)^k}{\sqrt{5}}.$$

Case 1. $n = 0$. Then

$$\frac{\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n}{\sqrt{5}} = \frac{\left(\frac{1+\sqrt{5}}{2}\right)^0 - \left(\frac{1-\sqrt{5}}{2}\right)^0}{\sqrt{5}}$$

$$= \frac{1-1}{\sqrt{5}} = 0 = F_0.$$

Exercícios de fixação

Case 2. $n = 1$. Then

$$\frac{\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n}{\sqrt{5}} = \frac{\left(\frac{1+\sqrt{5}}{2}\right)^1 - \left(\frac{1-\sqrt{5}}{2}\right)^1}{\sqrt{5}}$$

$$= \frac{\sqrt{5}}{\sqrt{5}} = 1 = F_1.$$

Case 3. $n \geq 2$. Then applying the inductive hypothesis to $n-2$ and $n-1$, we get

$$\begin{aligned}
F_n &= F_{n-2} + F_{n-1} \\
&= \frac{\left(\frac{1+\sqrt{5}}{2}\right)^{n-2} - \left(\frac{1-\sqrt{5}}{2}\right)^{n-2}}{\sqrt{5}} + \frac{\left(\frac{1+\sqrt{5}}{2}\right)^{n-1} - \left(\frac{1-\sqrt{5}}{2}\right)^{n-1}}{\sqrt{5}} \\
&= \frac{\left[\left(\frac{1+\sqrt{5}}{2}\right)^{n-2} + \left(\frac{1+\sqrt{5}}{2}\right)^{n-1}\right] - \left[\left(\frac{1-\sqrt{5}}{2}\right)^{n-2} + \left(\frac{1-\sqrt{5}}{2}\right)^{n-1}\right]}{\sqrt{5}} \\
&= \frac{\left(\frac{1+\sqrt{5}}{2}\right)^{n-2}\left[1 + \frac{1+\sqrt{5}}{2}\right] - \left(\frac{1-\sqrt{5}}{2}\right)^{n-2}\left[1 + \frac{1-\sqrt{5}}{2}\right]}{\sqrt{5}}.
\end{aligned}$$

Exercícios de fixação

- 5 - solução

Now note that

$$\left(\frac{1+\sqrt{5}}{2}\right)^2 = \frac{1+2\sqrt{5}+5}{4} = \frac{6+2\sqrt{5}}{4} = \frac{3+\sqrt{5}}{2} = 1+\frac{1+\sqrt{5}}{2},$$

and similarly

$$\left(\frac{1-\sqrt{5}}{2}\right)^2 = 1+\frac{1-\sqrt{5}}{2}.$$

Substituting into the formula for F_n, we get

$$F_n = \frac{\left(\frac{1+\sqrt{5}}{2}\right)^{n-2}\left(\frac{1+\sqrt{5}}{2}\right)^2 - \left(\frac{1-\sqrt{5}}{2}\right)^{n-2}\left(\frac{1-\sqrt{5}}{2}\right)^2}{\sqrt{5}}$$

$$= \frac{\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n}{\sqrt{5}}. \qquad \square$$

Conjuntos enumeráveis

OBJETIVO

DEFINIR E APRENDER A RECONHECER CONJUNTOS ENUMERÁVEIS E NÃO ENUMERÁVEIS

Conjunto enumerável

- Tamanho de um conjunto finito A
  - Representado por $|A|$
  - Corresponde ao número de elementos em A

- Dados $A = \{1,2,3,4,5\}$ e $B = \{a,b,c,d,e,f,g,h\}$
  - Quem é maior A ou B?
  - $|A| = 5$, $|B| = 8$

- E se A e B são infinitos? Como compara-los?
  - Quem é maior **N** ou **Z**?
  - Quem é maior **Z** ou **R**?

http://www.kaninekisses.com/sitebuilder/images/great_dane_and_chihuahua-325x245.png

Conjunto enumerável

Cardinalidade

Dois conjuntos A e B, possuem mesma cardinalidade, $card(A) = card(B)$, se existe uma função bijetora de A para B

- Se $card(A) = n$, tal que $n \in \mathbf{N}$, ou ainda, $card(A) = |A|$, então A é finito
- A é infinito se existe $X \subset A$, tal que $card(X) = card(A)$

Conjunto enumerável e conjunto contável

- Um conjunto A é dito enumerável, se $card(A) = card(\mathbf{N})$
- Um conjunto A é dito contável, se A é finito ou enumerável

Conjunto enumerável

Cardinalidade

Dois conjuntos A e B, possuem mesma cardinalidade, $card(A) = card(B)$, se existe uma função bijetora de A para B

A é enumerável se existe uma bijeção $f : \mathbf{N} \to A$, ou uma bijeção $f : A \to \mathbf{N}$

Conjunto enumerável e conjunto contável

– Um conjunto A é dito enumerável, se $card(A) = card(\mathbf{N})$

– Um conjunto A é dito contável, se A é finito ou enumerável

Conjunto enumerável

Cardinalidade

Dois conjuntos A e B, possuem mesma cardinalidade, $card(A) = card(B)$, se existe uma função bijetora de A para B

⬇

Se A é enumerável, então seus elementos podem ser colocados em sequência

⬆

Conjunto enumerável e conjunto contável

– Um conjunto A é dito enumerável, se $card(A) = card(\mathbf{N})$

– Um conjunto A é dito contável, se A é finito ou enumerável

Um exemplo

$\mathbf{Z}^- \rightarrow$		-1	-2	-3	-4	-5	-6	-7	-8	-9	-10	-11	-12	...	$-\infty$
$\mathbf{N} \rightarrow$	0	1	2	3	4	5	6	7	8	9	10	11	12	...	∞
$\mathbf{Z}^+ \cup \{0\} \rightarrow$	0	1	2	3	4	5	6	7	8	9	10	11	12	...	∞

A é enumerável se existe uma bijeção $f : \mathbf{N} \rightarrow A$, ou uma bijeção $f : A \rightarrow \mathbf{N}$

Se A é enumerável, então seus elementos podem ser colocados em sequência

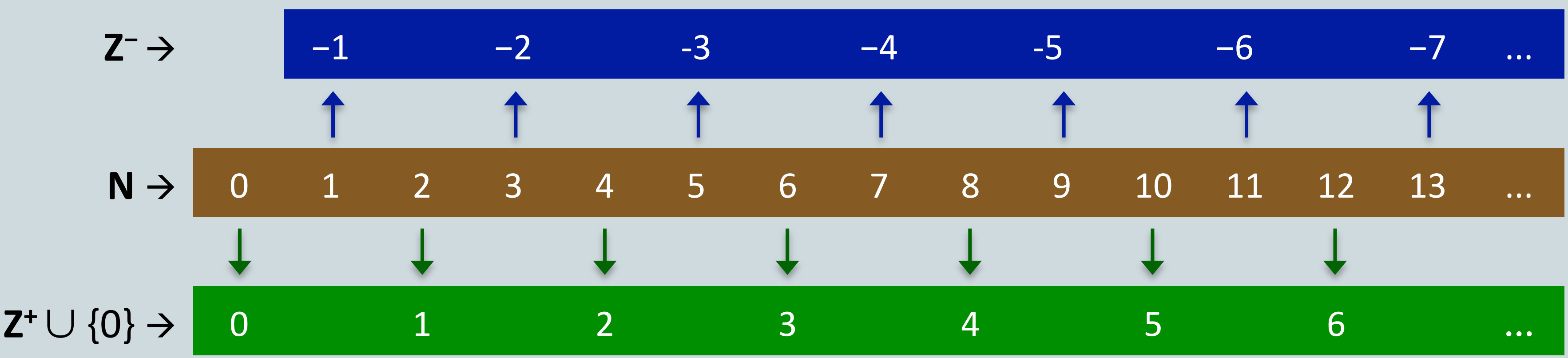
Eduardo Freire Nakamura (nakamura@icomp.ufam.edu.br)

Um exemplo

$\mathbf{Z}^- \rightarrow$	??	−1	−2	−3	−4	−5	−6	−7	−8	−9	−10	−11	−12	...	$-\infty$
$\mathbf{N} \rightarrow$	0	1	2	3	4	5	6	7	8	9	10	11	12	...	∞
	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓		
$\mathbf{Z}^+ \cup \{0\} \rightarrow$	0	1	2	3	4	5	6	7	8	9	10	11	12	...	∞

- $\mathbf{N} \subset \mathbf{Z}$, na verdade, $\mathbf{Z} = \mathbf{N} \cup \mathbf{Z}^-$, então quem é maior?
- Existe uma função bijetora de **Z** para **N**?
- Qual sequência é possível formar?

Um exemplo



- $\mathbf{N} \subset \mathbf{Z}$, na verdade, $\mathbf{Z} = \mathbf{N} \cup \mathbf{Z}^-$, então quem é maior?
- Existe uma função bijetora de **Z** para **N**?
- Qual sequência é possível formar?

Um exemplo

Se *A* é enumerável, então seus elementos podem ser colocados em sequência

N →	0	1	2	3	4	5	6	7	8	9	10	11	12	13	...
	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	
Z →	0	−1	1	−2	2	−3	3	−4	4	−5	5	−6	6	−7	...

Z colocado em uma sequência possível

Um exemplo

Se *A* é enumerável, então seus elementos podem ser colocados em sequência

N →	0	1	2	3	4	5	6	7	8	9	10	11	12	13	...
	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	
Z →	0	−1	1	−2	2	−3	3	−4	4	−5	5	−6	6	−7	...

$f : \mathbf{N} \to \mathbf{Z}$, tal que,

$$f(x) = \begin{cases} \dfrac{x}{2}, & \text{se } x \text{ é par} \\ -\dfrac{x+1}{2}, & \text{se } x \text{ é ímpar} \end{cases}$$

Mais um exemplo

- O conjunto dos racionais positivos $\mathbf{Q}^+$ é enumerável?
  - $\mathbf{Q}^+ = \{\ a/b \mid a \in \mathbf{N}^+ \wedge b \in \mathbf{N}^+ \}$
  - Considere a função $f : \mathbf{Q}^+ \longrightarrow \mathbf{N}$, bijetora, que mapeia a/b em um natural

$f(a,b)$		b					
		1	2	3	4	5	...
a	1	0	1	3	6	10	...
	2	2	4	7	11	...	
	3	5	8	12	...		
	4	9	13	...			
	5	14	...			**N**	
	...	...					

Mais um exemplo

- O racionais positivos $\mathbf{Q}^+$ é enumerável?
  - $\mathbf{Q}^+ = \{\, a/b \mid a \in \mathbf{N}^+ \wedge b \in \mathbf{N}^+ \,\}$
  - Considere a função $f : \mathbf{Q}^+ \longrightarrow \mathbf{N}$, bijetora, que mapeia a/b em um natural

f(*a*,*b*)		*b*					
		1	2	3	4	5	…
a	1	0	1	3	6	10	…
	2	2	4	7	11	…	
	3	5	8	12	…		
	4	9	13	…			
	5	14	…			**N**	
	…	…					

N → 0

↑

Q⁺ → 1/1

Mais um exemplo

- O racionais positivos $\mathbf{Q}^+$ é enumerável?
  - $\mathbf{Q}^+ = \{\ a/b \mid a \in \mathbf{N}^+ \wedge b \in \mathbf{N}^+\ \}$
  - Considere a função $f : \mathbf{Q}^+ \longrightarrow \mathbf{N}$, bijetora, que mapeia a/b em um natural

$f(a,b)$		*b*					
		1	2	3	4	5	…
a	1	0	1	3	6	10	…
	2	2	4	7	11	…	
	3	5	8	12	…		
	4	9	13	…			
	5	14	…			**N**	
	…	…					

N → 0 1

Q⁺ → 1/1 1/2

Mais um exemplo

- O racionais positivos $\mathbf{Q}^+$ é enumerável?
  - $\mathbf{Q}^+ = \{\ a/b \mid a \in \mathbf{N}^+ \wedge b \in \mathbf{N}^+\ \}$
  - Considere a função $f : \mathbf{Q}^+ \longrightarrow \mathbf{N}$, bijetora, que mapeia a/b em um natural

f(*a*,*b*)		*b*					
		1	2	3	4	5	…
a	1	0	1	3	6	10	…
	2	2	4	7	11	…	
	3	5	8	12	…		
	4	9	13	…			
	5	14	…			**N**	
	…	…					

$\mathbf{N} \rightarrow$	0	1	2
	↑	↑	↑
$\mathbf{Q}^+ \rightarrow$	1/1	1/2	2/1

Mais um exemplo

- O racionais positivos $\mathbf{Q}^+$ é enumerável?
  - $\mathbf{Q}^+ = \{ a/b \mid a \in \mathbf{N}^+ \wedge b \in \mathbf{N}^+ \}$
  - Considere a função $f : \mathbf{Q}^+ \longrightarrow \mathbf{N}$, bijetora, que mapeia a/b em um natural

$f(a,b)$		*b*					
		1	2	3	4	5	…
a	1	0	1	3	6	10	…
	2	2	4	7	11	…	
	3	5	8	12	…		
	4	9	13	…			
	5	14	…			**N**	
	…	…					

N →	0	1	2	3
	↑	↑	↑	↑
$\mathbf{Q}^+$ →	1/1	1/2	2/1	1/3

Mais um exemplo

- O racionais positivos $\mathbf{Q}^+$ é enumerável?
  - $\mathbf{Q}^+ = \{\, a/b \mid a \in \mathbf{N}^+ \wedge b \in \mathbf{N}^+ \,\}$
  - Considere a função $f : \mathbf{Q}^+ \longrightarrow \mathbf{N}$, bijetora, que mapeia a/b em um natural

$f(a,b)$		b					
		1	2	3	4	5	…
a	1	0	1	3	6	10	…
	2	2	4	7	11	…	
	3	5	8	12	…		
	4	9	13	…			
	5	14	…			**N**	
	…	…					

N →	0	1	2	3	4
	↑	↑	↑	↑	↑
$\mathbf{Q}^+$ →	1/1	1/2	2/1	1/3	2/2

Mais um exemplo

- O racionais positivos $\mathbf{Q}^+$ é enumerável?
  - $\mathbf{Q}^+ = \{\, a/b \mid a \in \mathbf{N}^+ \wedge b \in \mathbf{N}^+ \,\}$
  - Considere a função $f : \mathbf{Q}^+ \longrightarrow \mathbf{N}$, bijetora, que mapeia a/b em um natural

$f(a,b)$		b					
		1	2	3	4	5	…
a	1	0	1	3	6	10	…
	2	2	4	7	11	…	
	3	5	8	12	…		
	4	9	13	…			
	5	14	…			**N**	
	…	…					

N →	0	1	2	3	4	5
	↑	↑	↑	↑	↑	↑
$\mathbf{Q}^+$ →	1/1	1/2	2/1	1/3	2/2	3/1

Mais um exemplo

- O racionais positivos $\mathbf{Q}^+$ é enumerável?
  - $\mathbf{Q}^+ = \{\, a/b \mid a \in \mathbf{N}^+ \wedge b \in \mathbf{N}^+ \,\}$
  - Considere a função $f : \mathbf{Q}^+ \longrightarrow \mathbf{N}$, bijetora, que mapeia a/b em um natural

$$f(a/b) = \frac{(a+b-1)(a+b-2)}{2} + (a-1)$$

$f(a,b)$		b					
		1	2	3	4	5	…
a	1	0	1	3	6	10	…
	2	2	4	7	11	…	
	3	5	8	12	…		
	4	9	13	…			
	5	14	…			**N**	
	…	…					

N →	0	1	2	3	4	5	6	7	8	9	10	11	12	13	…
	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	
$\mathbf{Q}^+$ →	1/1	1/2	2/1	1/3	2/2	3/1	1/4	2/3	3/2	4/1	1/5	2/4	3/3	4/2	…

Mais sobre conjuntos contáveis

Teorema facilitador

As seguintes afirmações são equivalentes

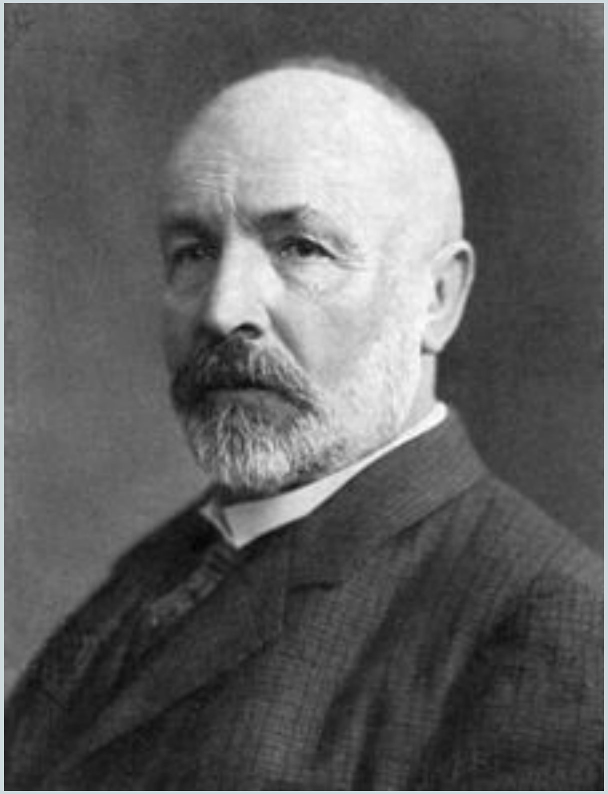
- A é contável
- Existe uma função injetora de A para $\mathbf{N}$
- $A = \varnothing$ ou existe uma função sobrejetora de $\mathbf{N}$ para A

Propriedades

- Se A é contável, então $X \subseteq A$ é contável
- Se A e B são contáveis, então $A \times B$ é contável
- Se A e B são contáveis, então $A \cup B$ é contável

E os números reais?

- O conjunto dos números reais é contável?
  - Não, não é possível enumerar todos os números reais
- A prova, por contradição, foi proposta por Cantor em 1891 (Diagonal de Cantor)



http://en.wikipedia.org/wiki/Georg_Cantor

Diagonal de Cantor

1. Suponha que **R** é contável

2. Considere o conjunto **R'** = { $x \in$ **R** | $0 < x < 1$ }

3. Note que **R'** $\subseteq$ **R**, portanto, se **R** é contável, então **R'** é contável

4. Existe uma bijeção f : **R'** $\rightarrow$ **N** que representa todos elementos de **R'** como uma lista

N	**R'**								
0	r_0	=	0	,	d_{00}	d_{01}	d_{02}	d_{03}	...
1	r_1	=	0	,	d_{10}	d_{11}	d_{12}	d_{13}	...
2	r_2	=	0	,	d_{20}	d_{21}	d_{22}	d_{23}	...
3	r_3	=	0	,	d_{30}	d_{31}	d_{32}	d_{33}	...
$\vdots$	$\vdots$								

Eduardo Freire Nakamura (nakamura@icomp.ufam.edu.br)

Diagonal de Cantor

4. Existe uma bijeção $f : \mathbf{R'} \rightarrow \mathbf{N}$ que representa todos elementos de **R'** como uma lista

N	**R'**	
0	r_0	$= 0 , d_{00}\ d_{01}\ d_{02}\ d_{03}\ \ldots$
1	r_1	$= 0 , d_{10}\ d_{11}\ d_{12}\ d_{13}\ \ldots$
2	r_2	$= 0 , d_{20}\ d_{21}\ d_{22}\ d_{23}\ \ldots$
3	r_3	$= 0 , d_{30}\ d_{31}\ d_{32}\ d_{33}\ \ldots$
$\vdots$	$\vdots$	

$d_{ij} \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$

Por exemplo,
se

$r_0 = 0 , 1\ 0\ 2\ 4\ 9\ 2\ldots$

então

$d_{00} = 1,$
$d_{01} = 0,$
$d_{02} = 2,$
$d_{03} = 4,$
…

Diagonal de Cantor

5. Agora é preciso construir um número que não esteja listado abaixo

N	**R'**
0	$r_0 = 0, d_{00}\ d_{01}\ d_{02}\ d_{03}\ \ldots$
1	$r_1 = 0, d_{10}\ d_{11}\ d_{12}\ d_{13}\ \ldots$
2	$r_2 = 0, d_{20}\ d_{21}\ d_{22}\ d_{23}\ \ldots$
3	$r_3 = 0, d_{30}\ d_{31}\ d_{32}\ d_{33}\ \ldots$
$\vdots$	$\vdots$

Considere o número $a = 0,a_0a_1a_2a_3\ldots$ tal que

$$a_i = 9 - d_{ii}$$

Eduardo Freire Nakamura (nakamura@icomp.ufam.edu.br)

Diagonal de Cantor

5. Agora é preciso construir um número que não esteja listado abaixo

Considere o número $a = 0{,}a_0a_1a_2a_3\ldots$ tal que

$$a_i = 9 - d_{ii}$$

N	R'							
0	r_0	=	0 ,	d_{00}	d_{01}	d_{02}	d_{03}	…
1	r_1	=	0 ,	d_{10}	d_{11}	d_{12}	d_{13}	…
2	r_2	=	0 ,	d_{20}	d_{21}	d_{22}	d_{23}	…
3	r_3	=	0 ,	d_{30}	d_{31}	d_{32}	d_{33}	…
⋮	⋮							

$$a = 0\,,\ a_0\ a_1\ a_2\ a_3\ \ldots$$

Diagonal de Cantor

5. Agora é preciso construir um número que não esteja listado abaixo

Considere o número $a = 0{,}a_0a_1a_2a_3\ldots$ tal que

$$a_i = 9 - d_{ii}$$

N	R'								
0	r_0	=	0	,	$\boxed{d_{00}}$	d_{01}	d_{02}	d_{03}	…
1	r_1	=	0	,	d_{10}	d_{11}	d_{12}	d_{13}	…
2	r_2	=	0	,	d_{20}	d_{21}	d_{22}	d_{23}	…
3	r_3	=	0	,	d_{30}	d_{31}	d_{32}	d_{33}	…
⋮	⋮								
					$\neq$				
	a	=	0	,	$\boxed{a_0}$	a_1	a_2	a_3	…

$$(d_{00} \neq a_0) \longrightarrow (a \neq r_0)$$

Diagonal de Cantor

5. Agora é preciso construir um número que não esteja listado abaixo

Considere o número $a = 0{,}a_0a_1a_2a_3\ldots$ tal que

$$a_i = 9 - d_{ii}$$

$$(d_{11} \neq a_1) \rightarrow (a \neq r_1)$$

N	R'								
0	r_0	=	0 ,	d_{00}	d_{01}	d_{02}	d_{03}	…
1	r_1	=	0 ,	d_{10}	d_{11}	d_{12}	d_{13}	…
2	r_2	=	0 ,	d_{20}	d_{21}	d_{22}	d_{23}	…
3	r_3	=	0 ,	d_{30}	d_{31}	d_{32}	d_{33}	…
⋮	⋮							
				$\neq$	$\neq$			
	a	=	0 ,	a_0	a_1	a_2	a_3	…

Diagonal de Cantor

5. Agora é preciso construir um número que não esteja listado abaixo

Considere o número $a = 0{,}a_0a_1a_2a_3\ldots$ tal que

$$a_i = 9 - d_{ii}$$

$$(d_{22} \neq a_2) \rightarrow (a \neq r_2)$$

$$
\begin{array}{cccccccccc}
\textbf{N} & \textbf{R'} & & & & & & & & \\
0 & r_0 & = & 0 & , & \boxed{d_{00}} & d_{01} & d_{02} & d_{03} & \ldots \\
1 & r_1 & = & 0 & , & d_{10} & \boxed{d_{11}} & d_{12} & d_{13} & \ldots \\
2 & r_2 & = & 0 & , & d_{20} & d_{21} & \boxed{d_{22}} & d_{23} & \ldots \\
3 & r_3 & = & 0 & , & d_{30} & d_{31} & d_{32} & d_{33} & \ldots \\
\vdots & \vdots & & & & & & & & \\
 & & & & & \neq & \neq & \neq & & \\
 & a & = & 0 & , & a_0 & a_1 & \boxed{a_2} & a_3 & \ldots
\end{array}
$$

Diagonal de Cantor

5. Agora é preciso construir um número que não esteja listado abaixo

N	R'						
0	r_0	= 0 ,	d_{00}	d_{01}	d_{02}	d_{03}	…
1	r_1	= 0 ,	d_{10}	d_{11}	d_{12}	d_{13}	…
2	r_2	= 0 ,	d_{20}	d_{21}	d_{22}	d_{23}	…
3	r_3	= 0 ,	d_{30}	d_{31}	d_{32}	d_{33}	…
⋮	⋮						
			$\neq$	$\neq$	$\neq$	$\neq$	
	a	= 0 ,	a_0	a_1	a_2	a_3	…

Considere o número $a = 0,a_0a_1a_2a_3\ldots$ tal que

$$a_i = 9 - d_{ii}$$

$$(d_{33} \neq a_3) \longrightarrow (a \neq r_3)$$

Diagonal de Cantor

5. Agora é preciso construir um número que não esteja listado abaixo

$$
\begin{array}{llcccccccc}
\mathbf{N} & \mathbf{R'} & & & & & & & & \\
0 & r_0 & = & 0 & , & \boxed{d_{00}} & d_{01} & d_{02} & d_{03} & \ldots \\
1 & r_1 & = & 0 & , & d_{10} & \boxed{d_{11}} & d_{12} & d_{13} & \ldots \\
2 & r_2 & = & 0 & , & d_{20} & d_{21} & \boxed{d_{22}} & d_{23} & \ldots \\
3 & r_3 & = & 0 & , & d_{30} & d_{31} & d_{32} & \boxed{d_{33}} & \ldots \\
\vdots & \vdots & & & & & & & & \\
 & & & & & \neq & \neq & \neq & \neq & \ldots \\
 & a & = & 0 & , & a_0 & a_1 & a_2 & a_3 & \ldots
\end{array}
$$

Considere o número $a = 0{,}a_0a_1a_2a_3\ldots$ tal que

$$a_i = 9 - d_{ii}$$

$$\forall i \in \mathbf{N},\ (d_{ii} \neq a_i) \rightarrow (a \neq r_i)$$

Diagonal de Cantor

6. Assim, $a \in \mathbf{R'}$ não está mapeado na bijeção $f : \mathbf{R'} \rightarrow \mathbf{N}$, uma contradição. Portanto, $\mathbf{R'}$ não é contável.

$$
\begin{array}{cccccccccc}
\mathbf{N} & \mathbf{R'} & & & & & & & & \\
0 & r_0 & = & 0 & , & \boxed{d_{00}} & d_{01} & d_{02} & d_{03} & \dots \\
1 & r_1 & = & 0 & , & d_{10} & \boxed{d_{11}} & d_{12} & d_{13} & \dots \\
2 & r_2 & = & 0 & , & d_{20} & d_{21} & \boxed{d_{22}} & d_{23} & \dots \\
3 & r_3 & = & 0 & , & d_{30} & d_{31} & d_{32} & \boxed{d_{33}} & \dots \\
\vdots & \vdots & & & & & & & & \\
 & & & & & \neq & \neq & \neq & \neq & \dots \\
 & a & = & 0 & , & a_0 & a_1 & a_2 & a_3 & \dots
\end{array}
$$

Considere o número $a = 0{,}a_0a_1a_2a_3\dots$ tal que

$$a_i = 9 - d_{ii}$$

$$\forall i \in \mathbf{N},\ (d_{ii} \neq a_i) \rightarrow (a \neq r_i)$$

Logo, $a \in \mathbf{R'}$, mas não está na lista com, supostamente, todos os elementos de $\mathbf{R'}$, uma **contradição** !?

Diagonal de Cantor

7. Como, **R'** $\subseteq$ **R** não é contável, **R** também não é contável.

$$
\begin{array}{cccccccccc}
\mathbf{N} & \mathbf{R'} & & & & & & & & \\
0 & r_0 & = & 0 & , & \boxed{d_{00}} & d_{01} & d_{02} & d_{03} & \dots \\
1 & r_1 & = & 0 & , & d_{10} & \boxed{d_{11}} & d_{12} & d_{13} & \dots \\
2 & r_2 & = & 0 & , & d_{20} & d_{21} & \boxed{d_{22}} & d_{23} & \dots \\
3 & r_3 & = & 0 & , & d_{30} & d_{31} & d_{32} & \boxed{d_{33}} & \dots \\
\vdots & \vdots & & & & & & & & \\
 & & & & & \neq & \neq & \neq & \neq & \dots \\
 & a & = & 0 & , & a_0 & a_1 & a_2 & a_3 & \dots
\end{array}
$$

Considere o número $a = 0{,}a_0a_1a_2a_3\dots$ tal que

$$a_i = 9 - d_{ii}$$

$$\forall i \in \mathbf{N},\ (d_{ii} \neq a_i) \rightarrow (a \neq r_i)$$

Logo, $a \in$ **R'**, mas não está na lista com, supostamente, todos os elementos de **R'**, uma **contradição** !?

Outro exemplo

- Considere o conjunto $\mathcal{F}$ de todas as funções totais $f : \mathbf{N} \to \mathbf{N}$
- $\mathcal{F}$ é finito?
  - Infinito!
- $\mathcal{F}$ é enumerável?
  - Não!
  - É incontável

Outro exemplo

1. Suponha que $\mathcal{F}$ é contável

2. Existe uma bijeção $g : \mathcal{F} \longrightarrow \mathbf{N}$ que ordena os elementos de $\mathcal{F}$ como uma lista

g		**N**				
		0	1	2	3	...
$\mathcal{F}$	f_0	$f_0(0)$	$f_0(1)$	$f_0(2)$	$f_0(3)$	...
	f_1	$f_1(0)$	$f_1(1)$	$f_1(2)$	$f_1(3)$	...
	f_2	$f_2(0)$	$f_2(1)$	$f_2(2)$	$f_2(3)$	...
	f_3	$f_3(0)$	$f_3(1)$	$f_3(2)$	$f_3(3)$	...
	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	

Outro exemplo

3. É preciso encontrar uma função total $h : \mathbf{N} \rightarrow \mathbf{N}$, tal que $h \in \mathcal{F}$ mas não está na lista abaixo

	g	N				
		0	1	2	3	...
$\mathcal{F}$	f_0	$f_0(0)$	$f_0(1)$	$f_0(2)$	$f_0(3)$	...
	f_1	$f_1(0)$	$f_1(1)$	$f_1(2)$	$f_1(3)$	...
	f_2	$f_2(0)$	$f_2(1)$	$f_2(2)$	$f_2(3)$	...
	f_3	$f_3(0)$	$f_3(1)$	$f_3(2)$	$f_3(3)$	...
	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	

Outro exemplo

3. É preciso encontrar uma função total $h : \mathbf{N} \rightarrow \mathbf{N}$, tal que $h \in \mathcal{F}$ mas não está na lista abaixo

Considere $h : \mathbf{N} \rightarrow \mathbf{N}$, tal que

$h(i) = f_i(i) + 1$

g		N				
		0	1	2	3	...
$\mathcal{F}$	f_0	$f_0(0)$	$f_0(1)$	$f_0(2)$	$f_0(3)$	...
	f_1	$f_1(0)$	$f_1(1)$	$f_1(2)$	$f_1(3)$	...
	f_2	$f_2(0)$	$f_2(1)$	$f_2(2)$	$f_2(3)$	...
	f_3	$f_3(0)$	$f_3(1)$	$f_3(2)$	$f_3(3)$	...
	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	

h	$h(0)$	$h(1)$	$h(2)$	$h(3)$	...

Outro exemplo

3. É preciso encontrar uma função total $h : \mathbf{N} \rightarrow \mathbf{N}$, tal que $h \in \mathcal{F}$ mas não está na lista abaixo

g		N				
		0	1	2	3	...
$\mathcal{F}$	f_0	$f_0(0)$	$f_0(1)$	$f_0(2)$	$f_0(3)$	...
	f_1	$f_1(0)$	$f_1(1)$	$f_1(2)$	$f_1(3)$	...
	f_2	$f_2(0)$	$f_2(1)$	$f_2(2)$	$f_2(3)$	...
	f_3	$f_3(0)$	$f_3(1)$	$f_3(2)$	$f_3(3)$	...
	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	
		$\neq$				
	h	$h(0)$	$h(1)$	$h(2)$	$h(3)$	...

Considere $h : \mathbf{N} \rightarrow \mathbf{N}$, tal que

$$h(i) = f_i(i) + 1$$

$$(\ h(0) \neq f_0(0)\ ) \rightarrow (\ h \neq f_0\ )$$

Outro exemplo

3. É preciso encontrar uma função total $h : \mathbf{N} \to \mathbf{N}$, tal que $h \in \mathcal{F}$ mas não está na lista abaixo

Considere $h : \mathbf{N} \to \mathbf{N}$, tal que

$$h(i) = f_i(i) + 1$$

$$(\, h(1) \neq f_1(1)\,) \to (\, h \neq f_1\,)$$

g		N				
		0	1	2	3	...
$\mathcal{F}$	f_0	$f_0(0)$	$f_0(1)$	$f_0(2)$	$f_0(3)$	...
	f_1	$f_1(0)$	$f_1(1)$	$f_1(2)$	$f_1(3)$	...
	f_2	$f_2(0)$	$f_2(1)$	$f_2(2)$	$f_2(3)$	...
	f_3	$f_3(0)$	$f_3(1)$	$f_3(2)$	$f_3(3)$	...
	⋮	⋮	⋮	⋮	⋮	
		$\neq$	$\neq$			
	h	$h(0)$	$h(1)$	$h(2)$	$h(3)$	...

Outro exemplo

3. É preciso encontrar uma função total $h : \mathbf{N} \rightarrow \mathbf{N}$, tal que $h \in \mathcal{F}$ mas não está na lista abaixo

Considere $h : \mathbf{N} \rightarrow \mathbf{N}$, tal que

$$h(i) = f_i(i) + 1$$

$$(\ h(2) \neq f_2(2)\ ) \rightarrow (\ h \neq f_2\ )$$

g		N				
		0	1	2	3	...
$\mathcal{F}$	f_0	$f_0(0)$	$f_0(1)$	$f_0(2)$	$f_0(3)$	...
	f_1	$f_1(0)$	$f_1(1)$	$f_1(2)$	$f_1(3)$	...
	f_2	$f_2(0)$	$f_2(1)$	$f_2(2)$	$f_2(3)$	...
	f_3	$f_3(0)$	$f_3(1)$	$f_3(2)$	$f_3(3)$	...
	⋮	⋮	⋮	⋮	⋮	
		$\neq$	$\neq$	$\neq$		
	h	$h(0)$	$h(1)$	$h(2)$	$h(3)$	...

Outro exemplo

3. É preciso encontrar uma função total $h : \mathbf{N} \to \mathbf{N}$, tal que $h \in \mathcal{F}$ mas não está na lista abaixo

g		$\mathbf{N}$				
		0	1	2	3	...
$\mathcal{F}$	f_0	$f_0(0)$	$f_0(1)$	$f_0(2)$	$f_0(3)$	...
	f_1	$f_1(0)$	$f_1(1)$	$f_1(2)$	$f_1(3)$	...
	f_2	$f_2(0)$	$f_2(1)$	$f_2(2)$	$f_2(3)$	...
	f_3	$f_3(0)$	$f_3(1)$	$f_3(2)$	$f_3(3)$	...
	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	
		$\neq$	$\neq$	$\neq$	$\neq$	
	h	$h(0)$	$h(1)$	$h(2)$	$h(3)$	...

Considere $h : \mathbf{N} \to \mathbf{N}$, tal que

$$h(i) = f_i(i) + 1$$

$$(\ h(3) \neq f_3(3)\ ) \longrightarrow (\ h \neq f_3\ )$$

Outro exemplo

3. É preciso encontrar uma função total $h : \mathbf{N} \to \mathbf{N}$, tal que $h \in \mathcal{F}$ mas não está na lista abaixo

	g	0	1	2	3	...
$\mathcal{F}$	f_0	$f_0(0)$	$f_0(1)$	$f_0(2)$	$f_0(3)$	...
	f_1	$f_1(0)$	$f_1(1)$	$f_1(2)$	$f_1(3)$	...
	f_2	$f_2(0)$	$f_2(1)$	$f_2(2)$	$f_2(3)$	...
	f_3	$f_3(0)$	$f_3(1)$	$f_3(2)$	$f_3(3)$	...
	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	
		$\neq$	$\neq$	$\neq$	$\neq$	...
	h	$h(0)$	$h(1)$	$h(2)$	$h(3)$	...

Considere $h : \mathbf{N} \to \mathbf{N}$, tal que

$$h(i) = f_i(i) + 1$$

$$\forall i \in \mathbf{N},\ (\, h \neq f_i \,)$$

Eduardo Freire Nakamura (nakamura@icomp.ufam.edu.br)

Outro exemplo

4. Logo, $h \in \mathcal{F}$, mas não está mapeada por $g : \mathcal{F} \rightarrow \mathbf{N}$, uma contradição. Portanto, $\mathcal{F}$ não é contável.

g		**N**				
		0	1	2	3	...
$\mathcal{F}$	f_0	$f_0(0)$	$f_0(1)$	$f_0(2)$	$f_0(3)$	...
	f_1	$f_1(0)$	$f_1(1)$	$f_1(2)$	$f_1(3)$	...
	f_2	$f_2(0)$	$f_2(1)$	$f_2(2)$	$f_2(3)$	...
	f_3	$f_3(0)$	$f_3(1)$	$f_3(2)$	$f_3(3)$	...
	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	
		$\neq$	$\neq$	$\neq$	$\neq$	...
	h	$h(0)$	$h(1)$	$h(2)$	$h(3)$	...

Considere $h : \mathbf{N} \rightarrow \mathbf{N}$, tal que

$$h(i) = f_i(i) + 1$$

$$\forall i \in \mathbf{N},\ (h \neq f_i)$$

Logo, $h \in \mathcal{F}$, mas não está na lista com, supostamente, todos os elementos de $\mathcal{F}$, uma **contradição** !?

Exercício de fixação

- Mostre que os conjuntos abaixo são enumeráveis (encontre uma bijeção sobre os naturais)
  1. $\mathbf{Z}^+ = \{1, 2, 3, 4, \ldots\}$
  2. Naturais Pares
  3. Naturais Ímpares
  4. Inteiros Pares

- Mostre que o conjunto abaixo não é contável
  1. $\mathscr{P}(\mathbf{N})$