Tipos de Prova

Dedução
Indução
Contra-exemplos
Contradição
Contrapositiva
Construção
Diagonalização

Provas, lemas, teoremas e corolários

- Uma prova é um argumento lógico de que uma afirmação é verdadeira
- Um teorema é uma afirmação provada verdadeira. Esta afirmação é especial.
- Lemas são afirmações provadas que ajudam a provar afirmações mais importantes (teoremas).
- Quando um teorema ou uma prova nos ajudam a concluir facilmente que outras afirmações são verdadeiras chamamos estas últimas de corolários do teorema.

Prova por Dedução

Consiste de uma seqüência de afirmações cuja verdade nos leva de alguma afirmação inicial, chamada *hipótese* ou *declaração(ões) dada(s),* a uma afirmação *conclusão.*

Teorema da forma "se H então C".

Dizemos que C é deduzido a partir de H.

Exemplo

Teorema: Se x é a soma dos quadrados de quatro inteiros positivos, então $2^x \geq x^2$

Afirmação	Justificativa
(1) $x=a^2+b^2+c^2+d^2$	Dado
(2) $a\geq 1; b\geq 1; c\geq 1; d\geq 1$	Dado
(3) $a^2\geq 1; b^2\geq 1; c^2\geq 1; d^2\geq 1$	(2) e propriedades da aritmética
(4) $x \geq 4$	(1), (3) e propriedades da aritmética
(5) $2^x \geq x^2$	(4) e Teorema*

Teorema*: Se $x \geq 4$, então $2^x \geq x^2$ (provado mais adiante)

Provas por Indução

- Método avançado para mostrar que todos os elementos de um conjunto infinito têm uma propriedade específica.
- Toda prova por indução consiste de 2 partes: a base e o passo de indução.
- Ex: tomemos os números naturais $\mathbb{N}$ e uma propriedade P. Nosso objetivo é provar que P(k) é verdade para todo número natural $k \in \mathbb{N}$.

- Base: Provar que P(1) é verdadeiro.
- Passo de Indução: Para cada $i \geq 1$, assuma que P(i) é verdadeiro (hipótese de indução) e use esta suposição para mostrar que P(i+1) é verdadeiro.
- Exemplo: Vamos provar o Teorema*:

Se $x \geq 4$, então $2^x \geq x^2$

Base: Se x=4, então 2^x e x^2 são ambos 16. Logo, $2^4 \geq 4^2$ é verdadeira – P(1)

Indução: Suponha para algum $x \geq 4$, que $2^x \geq x^2$ - P(i)

Vamos provar que $2^{(x+1)} \geq (x+1)^2$ - P(i+1)

Vamos reescrever P(i+1) de modo que ela possa usar P(i): escrevemos $2^{(x+1)}$ como 2.2^x.

Como $2^x \geq x^2$, podemos concluir que $2^{(x+1)} = 2.2^x \geq 2x^2$.

Mas o que temos de mostrar é que $2^{(x+1)} \geq (x+1)^2$.

Já mostramos que $2^{(x+1)} \geq 2x^2$.

Se mostrarmos que $2x^2 \geq (x+1)^2$, então usamos a transitividade do $\geq$ para mostrar que $2^{(x+1)} \geq 2x^2 \geq (x+1)^2$

Primeiro, simplificamos $2x^2 \geq (x+1)^2$:

$$2x^2 \geq x^2+2x+1 \rightarrow x^2 \geq 2x+1.$$

Dividindo os 2 lados por x:

$$x \geq 2+(1/x)$$

Como, por hipótese, $x \geq 4$, temos que $1/x \leq 1/4$.

Assim, temos no mínimo $4 \geq 2.25$, o que é verdade.

Então também são verdadeiras: $x^2 \geq 2x+1$ e $2x^2 \geq (x+1)^2$, para $x \geq 4$, o que nos permite provar que $2^{(x+1)} \geq (x+1)^2$

Indução Estrutural

Aplicada quando há definições recursivas.

Ex.: Definição recursiva de árvore

Base: Um único nó é uma árvore, e esse nó é a *raiz* da árvore.

Indução: Se T_1, T_2, ...,T_k são árvores, então podemos formar uma nova árvore da seguinte forma:

1. Comece com um novo nó N, a raiz da árvore.
2. Adicione cópias de todas as árvores T_1, ...,T_k.
3. Adicione arestas desde o nó N até as raízes de cada uma das árvores de 2.

Indução Estrutural

Seja S(X) uma afirmação sobre as estruturas X definidas por alguma definição recursiva específica.

1. Como base, prove S(X) para a(s) estrutura(s) de base X.
2. Para a etapa indutiva, tome uma estrutura X que a definição recursiva nos diz que é formada a partir de Y_1, Y_2, ...Y_k. Suponha verdadeiras as afirmações $S(Y_1)$, $S(Y_2)$, ...$S(Y_k)$ e use essas afirmações para provar S(X).

A conclusão é que S(X) é verdadeira para todo X.

Exemplo: Toda árvore tem um nó a mais que seu número de arestas.

Ou: Se T é uma árvore, e T tem *n* nós e *e* arestas, então $n = e + 1$.

Base: T é um único nó. Então $n = 1$ e $e = 0$, logo $n = e + 1$ é verdadeiro.

Indução: Seja T uma árvore construída recursivamente, conforme a definição. Supomos que $S(T_i)$ é verdadeira para i=1,2, ...k. Isso é, seja Ti com n_i nós e e_i arestas; então $n_i = e_i + 1$.

Os nós de T são o nó N e todos os nós das árvores T_i. Desse modo, existem $1 + n_1 + n_2 + \ldots n_k$ nós em T. As arestas de T são as *k* arestas que adicionamos explicitamente na etapa de definição indutiva, mais as arestas das árvores T_i. Conseqüentemente, T tem

$$k + e_1 + e_2 + \ldots + e_k \quad \text{arestas}$$

Se substituirmos n_i por $e_i + 1$ na contagem do número de nós de T, descobriremos que T tem

$$1 + (e_1 + 1) + (e_2 + 1) + \ldots + (e_k + 1) \quad \text{nós}$$

Como existem *k* termos "+1" acima, podemos reagrupar como

$$k + 1 + e_1 + e_2 + \ldots + e_k \quad \text{nós}$$

Essa expressão é exatamente uma unidade maior que a expressão anterior do número de arestas de T. Assim, T tem um nó a mais do que seu número de arestas.

Contra-exemplos

Suposto Teo.: Todos os primos são ímpares (ou: Se o inteiro x é primo, então x é ímpar)

Contra-exemplo: O inteiro 2 é primo, mas é par.

Contra-exemplos

Suposto Teo.: Não existe par de inteiros a e b tais que a mod b = b mod a.

Contra-exemplo: Seja a = b = 2.

Então a mod b = b mod a = 0

No processo de encontrar o contra-exemplo, descobrimos de fato as condições exatas sob as quais o suposto teorema é verdadeiro:

Teorema: a mod b = b mod a se e somente se a = b.

Provas por Contradição

- Uma forma comum de provar um teorema é assumir que o teorema é falso e então mostrar que esta suposição leva a uma conseqüência falsa, chamada contradição.
- Exemplo: Seja U um conjunto infinito, e seja S um subconjunto finito de U. Seja T o complemento de S em relação a U. Então T é infinito.

Prova 1:

- Suponha que T seja finito (ou seja, negamos a tese)

Pela definição de conjunto complemento, se T, finito, é complemento de S, finito, em relação a U, então U deve ser finito.

Mas, por hipótese, U é infinito. Então U seria ao mesmo tempo finito e infinito, o que é um absurdo (uma contradição). Logo, nossa hipótese inicial não pode ser verdadeira.

Portanto, T é infinito (provamos a tese).

Prova 2:

Reduzindo as afirmações às suas definições:

Afirmação original	Nova afirmação
S é finito	$\exists$um inteiro n tal que $\|S\|=n$
U é infinito	Para nenhum inteiro p temos $\|U\|=p$
T é o complemento de S	$S \cup T = U$ e $S \cap T = \varnothing$

Prova:

Sabemos que $S \cup T = U$ e que S e T são disjuntos, e assim $|S| + |T| = |U|$.

Como S é finito, $|S|=n$ para algum n e, como U é infinito, não existe inteiro p tal que $|U|=p$.

Assim, Suponha que T seja finito (ou seja, negamos a tese), ou seja, $|T|=m$ para algum inteiro m.

Então $|U|=|S|+|T|= n+m$, o que contradiz a afirmação de que não existe nenhum inteiro p igual a $|U|$.

Teo 1: Se p^2 é par então p é par

- Provem por contradição

Teo 1: Se p^2 é par então p é par

Suponha que p seja ímpar (negação da tese).
Então $p=2m+1$, para algum $m \in \mathbb{Z}$.

Logo, $p^2=(2m+1)^2 = 4m^2+4m+1 = 2(2m^2+2m)+1$.

Logo, p^2 é ímpar (contradição da hipótese)
=> absurdo

$\therefore$ p é par

Contrapositiva

- Às vezes é mais fácil provar uma afirmação da forma "se H então C" provando-se a afirmação equivalente - contrapositiva:

  "se não C então não H"

(vide Tabela Verdade)

Tabela Verdade

H	C	H → C	~C → ~H
V	V	V	V
V	F	F	F
F	V	V	V
F	F	V	V

Provas por Construção

- Muitos teoremas afirmam que um tipo particular de objeto existe. Um meio de provar tal teorema é demonstrando como construir tal objeto.

Diagonalização

- Cantor (1873) estava preocupado em medir o tamanho de conjuntos infinitos. Se nós temos dois conjuntos infinitos, como podemos dizer se um é maior do que o outro ou se eles têm o mesmo tamanho?
- Para conjuntos finitos, basta contarmos o número de elementos, mas se tentamos contar o número de um conjunto infinito....nós nunca terminaremos.

Proposta de Cantor

- Para conjuntos finitos, emparelhamos os conjuntos, assim comparamos seus tamanhos. Se um deles terminar antes que o outro, então é menor.
- Cantor estendeu esta idéia para conjuntos infinitos. Se for possível emparelhá-los indefinidamente, então eles são de tamanhos iguais.
- Exemplo: números naturais, $\mathbb{N}$, e números pares. Qual é o maior?

Função de mapeamento

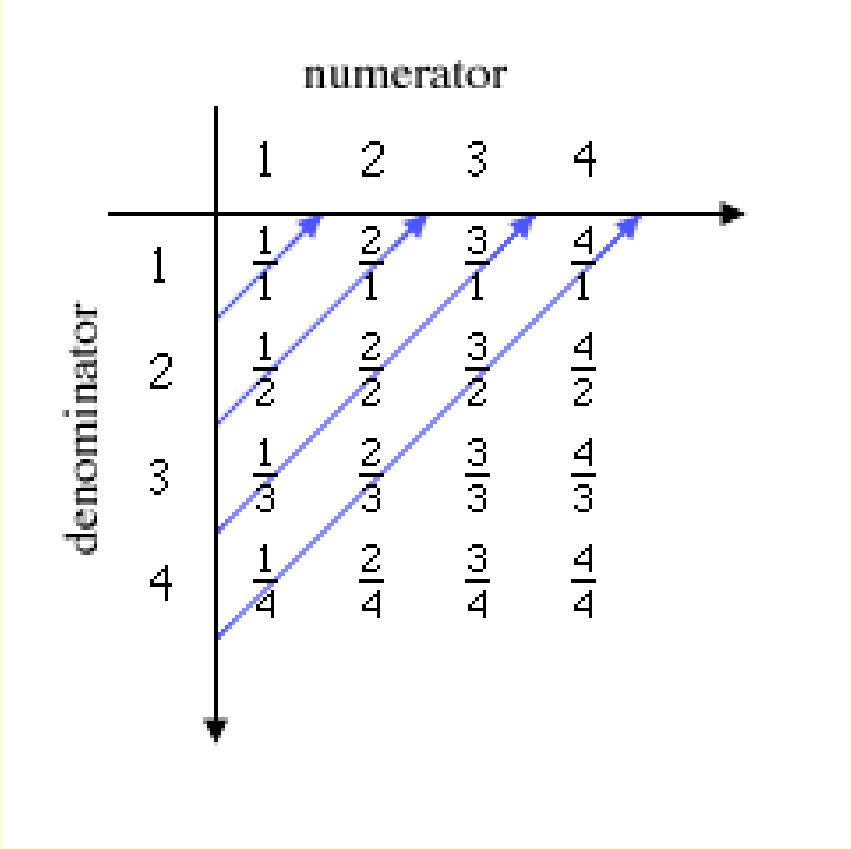
n	f(n)
1	2
2	4
3	6
.	
.	
.	

f(n) = 2n

Embora intuitivamente o conjunto dos pares pareça ser menor que $\mathbb{N}$, já que ele é um subconjunto próprio de $\mathbb{N}$, é possível emparelhar os dois conjuntos e assim declarar que eles têm o mesmo tamanho

Def. Um conjunto é contável se ele é finito ou tem o mesmo tamanho que o conjunto dos naturais, $\mathbb{N}$.

- Q (conjuntos dos números racionais positivos) tem o mesmo tamanho de $\mathbb{N}$.
- A figura ao lado dá a correspondência de $\mathbb{N}$ para Q. Pulamos elementos repetidos e continuando assim obtemos a lista de todos os elementos de Q:



1, 1/2, 2, 1/3, 3, 1/4, 2/3, 3/2, 4,...

Teo (Cantor): O conjunto dos números reais $\mathfrak{R}$ não é contável (é incontável)

- Veja prova por contradição na literatura