O que é uma prova?

Em matemática, uma prova[1] é uma argumentação que procura convencer o leitor de que uma certa proposição,[2] previamente enunciada, está correta. Em outras palavras, uma prova é uma narrativa que ajuda o leitor a entender por que uma dada proposição é verdadeira.

Em geral, as proposições têm a forma "se A então B", sendo A a *hipótese* e B a *tese* da proposição. Mas às vezes a hipótese não é dada explicitamente.

Qual a estrutura de uma prova? Uma prova é um texto, escrito em língua natural (português, ou inglês, ou russo, ou chinês, etc.), que consiste em uma sequência de sentenças gramaticalmente completas. Mais precisamente, uma prova é uma sequência de afirmações em que cada afirmação decorre logicamente das anteriores. A primeira afirmação é a hipótese da proposição e a última afirmação é a tese.

Exemplo 1

Considere a configuração do jogo *Minesweeper* à direita. Cada "B" representa uma bomba. As posições em branco não têm bombas e as posições marcadas com "?" podem ou não ter bombas. Uma posição marcada com um número k não tem bomba mas é vizinha de exatamente k bombas. (Cada posição tem até 8 vizinhos: ao norte, a nordeste, a leste, ..., a noroeste.) Nosso problema é decidir se uma dada posição "?" tem uma bomba ou não.

?	?	1	2	B
?	?	2	3	B
?	?	3	B	2
?	?	B	2	1
?	?	2	1	0
?	?	3	1	0
2	B	B	1	0
1	2	2	1	0

Cada posição do tabuleiro é especificada por suas coordenadas. Assim, por exemplo, o extremo superior esquerdo do tabuleiro tem coordenadas $(1,1)$ e o cruzamento da primeira linha com a segunda coluna tem coordenadas $(1,2)$.

Proposição: A posição $(1,2)$ da configuração da figura não tem bomba.

Prova, por contradição:

Suponha, por um momento, que há uma bomba em $(1,2)$.

A posição $(2,3)$ é vizinha de duas bombas e há uma bomba em $(3,4)$.

Logo, as posições $(2,2)$ e $(3,2)$ não têm bomba alguma.

Portanto, o "3" na posição $(3,3)$ garante que há uma bomba em $(4,2)$.

[1] prova = demonstração
[2] proposição = afirmação

Agora, o "2" na posição $(5, 3)$ garante que não há bomba em $(5, 2)$ nem em $(6, 2)$.

Mas isso é inconsistente com o "3" na posição $(6, 3)$.

Esta contradição mostra que $(1, 2)$ não pode ter uma bomba.

Exemplo 2

Proposição: Não existem números inteiros positivos p e q tais que $p/q = \sqrt{2}$. Em outras palavras, a raiz quadrada de 2 é irracional.

Prova, por contradição:

Suponha que existem números inteiros positivos p e q tais que $(p/q)^2 = 2$.

Escolha p e q de modo que eles não tenham divisor comum.

Portanto, não existe número inteiro maior que 1 que divida tanto p quanto q.

O número p^2 é par, pois $p^2 = 2q^2$.

O número p é par, pois o produto de quaisquer dois números ímpares é ímpar.

Seja s o número inteiro $p/2$.

O número q^2 é par, pois $q^2 = p^2/2 = (2s)^2/2 = 2s^2$.

O número q é par, pois o produto de dois ímpares é ímpar.

Os números p e q são divisíveis por 2.

Isso contradiz a maneira como escolhemos p e q.

A contradição mostra que a raiz quadrada de 2 é irracional.

Exemplo 3

Proposição: Se n é um número inteiro positivo então $1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{1}{6}\,n(n+1)(2n+1)$.

Prova, por indução em n:

Suponha que $n = 1$ (esta é a base da indução).

Nesse caso, os dois lados da identidade valem 1 e portanto são iguais.

Suponha agora que $n > 1$ (aqui começa o passo da indução).

Por hipótese de indução, $1^2 + 2^2 + \cdots + (n-1)^2 = \frac{1}{6}\,(n-1)n(2n-1)$.

Portanto, $1^2 + 2^2 + \cdots + n^2 =$

$$= 1^2 + 2^2 + \cdots + (n-1)^2 + n^2$$
$$= \tfrac{1}{6}\,(n-1)n(2n-1) + n^2$$

$$
\begin{aligned}
&= \tfrac{1}{6}\, n\left((n-1)(2n-1)+6n\right)\\
&= \tfrac{1}{6}\, n\left(2n^2-3n+1+6n\right)\\
&= \tfrac{1}{6}\, n\left(2n^2+3n+1\right)\\
&= \tfrac{1}{6}\, n\,(n+1)(2n+1)\,, \text{ como queríamos demonstrar.}
\end{aligned}
$$

Mau exemplo. Veja uma maneira *feia* de organizar a indução. Ela é feia porque vai na direção errada, de $n+1$ para n, e assim termina com uma expressão que não é idêntica à tese.

Suponha que $n = 1$ (esta é a base da indução).

Então os dois lados da identidade valem 1 e portanto são iguais.

Suponha agora que a identidade vale para n (aqui começa o passo da indução).

Vamos provar a identidade para $n+1$:

$$
\begin{aligned}
&1^2+2^2+\cdots+n^2+(n+1)^2 =\\
&\quad= \tfrac{1}{6}\, n(n+1)(2n+1)+(n+1)^2\\
&\quad= \tfrac{1}{6}\,(n+1)\left(n(2n+1)+6(n+1)\right)\\
&\quad= \tfrac{1}{6}\,(n+1)\left(2n^2+7n+6\right)\\
&\quad= \tfrac{1}{6}\,(n+1)\,(n+2)(2n+3)\\
&\quad= \tfrac{1}{6}\,(n+1)(n+2)(2(n+1)+1)).
\end{aligned}
$$

Exemplo 4

O *grau* de um vértice v num grafo é o número de arestas que têm ponta v. O grau de um vértice v é denotado por $g(v)$.

Proposição: Em qualquer grafo, a soma dos graus dos vértices é igual ao dobro do número de arestas. Em outras palavras, se (V, E) é um grafo então $\sum_{v\in V} g(v) = 2|E|$.

Prova, por indução em $|E|$:

Base da indução: $|E| = 0$.

Nesse caso, $\sum g(v) = 0$, e portanto $\sum g(v) = 2|E|$.

Passo da indução: $|E| > 0$.

Suponha que a identidade vale em todo subgrafo próprio de (V, E)
(esta é a hipótese de indução).

Seja xy uma aresta do grafo.

Seja F o conjunto $E - \{xy\}$.

Seja $g'(v)$ o grau de v no grafo (V, F).

Por hipótese de indução, $\sum g'(v) = 2|F|$.

Temos $g(x) = 1 + g'(x)$, $g(y) = 1 + g'(y)$ e $g(v) = g'(v)$ para todo v diferente de x e y.

Portanto, $\sum g(v) = 1 + 1 + \sum g'(v) = 2 + 2|F|$.

Mas $2 + 2|F| = 2|E|$.

Portanto, $\sum g(v) = 2|E|$, como queríamos demonstrar.

Errado. Eis uma versão errada da indução. Ela *supõe* a tese e *acrescenta* uma aresta ao grafo em vez de tirar uma.

Base da indução: $|E| = 0$.

Então $\sum g(v) = 0$, e portanto $\sum g(v) = 2|E|$.

Passo da indução: suponha que $\sum g(v) = 2|E|$ para um grafo (V, E).

Acrescente ao grafo uma nova aresta xy.

Seja E' o novo conjunto de arestas.

Denote por g' os graus dos vértices no grafo (V, E').

Temos $g'(x) = 1 + g(x)$, $g'(y) = 1 + g(y)$ e $g'(v) = g(v)$ para todo v diferente de x e y.

Portanto, $\sum g'(v) = 1 + 1 + \sum g(v) = 2 + 2|E|$.

Mas $2 + 2|E| = 2|E'|$, e assim $\sum g'(v) = 2|E'|$.

Exemplo 5

Um *emparelhamento* num grafo é um conjunto de restas que incide no máximo uma vez em cada vértice. Dizemos que um emparelhamento M *satura* um vértice v se M incide em v.

Proposição: Em qualquer grafo, todo vértice não isolado é saturado por algum emparelhamento máximo.

Prova:

Seja G um grafo e u um vértice não isolado de G.

Seja M um emparelhamento máximo em G.

Se M satura u então nada mais temos que provar.

Suponha agora que M não satura u.

Seja uv qualquer uma das arestas que incidem em u.

O emparelhamento M satura v (pois é máximo).

Seja vw a aresta de M que incide em v.

O conjunto $(M \cup \{uv\}) - \{vw\}$ é um emparelhamento.

Esse emparelhamento é máximo (pois tem o mesmo tamanho que M).

Esse emparelhamento satura u.

Observações finais

É claro que você não precisa seguir fielmente o formato dos exemplos acima: o texto da prova pode ser complementado com comentários e observações que tornem a leitura mais fácil. (A propósito, veja o artigo de Reuben Hersh.)

Exercícios

1. Prove, por indução em k, que $2^0 + 2^1 + \cdots + 2^k = 2^{k+1} - 1$.

2. Seja a um número positivo qualquer. Afirmo que $a^{n-1} = 1$ para todo inteiro positivo n. Eis a prova (por indução em n). Se $n = 1$ então $a^{n-1} = a^0 = 1$ e portanto a afirmação está correta nesse caso. Agora tome $n > 1$ e suponha, a título de hipótese de indução, que $a^{k-1} = 1$ para $k = n-1, n-2, \ldots, 1$. Então
$$a^{n-1} = a^{n-2}\, a^1 = a^{n-2}\, a^{n-2}/a^{n-3} = 1 \times 1/1 = 1.$$
Portanto, a afirmação está correta para todo n, como queríamos provar. Onde está o erro dessa prova? [D.E. Knuth, "Fundamental Algorithms"]

3. Afirmo que $\sum_{i=1}^{n-1} 1/(i\,(i+1)) = 3/2 - 1/n$ para todo número inteiro positivo n. Eis a prova, por indução em n. Para $n = 1$, ambos os lados da equação valem $1/2$ e portanto a afirmação está correta nesse caso. Agora tome $n > 1$ e suponha, como hipótese de indução, que $\sum_{i=1}^{n-2} 1/(i(i+1)) = 3/2 - 1/(n-1)$. Teremos então
$$\begin{aligned}\sum_{i=1}^{n-1} \frac{1}{i\,(i+1)} &= \sum_{i=1}^{n-2} \frac{1}{i\,(i+1)} + \frac{1}{(n-1)\,n} \\ &= \frac{3}{2} - \frac{1}{n-1} + \frac{1}{(n-1)\,n} \\ &= \frac{3}{2} - \frac{1}{n-1} + \frac{1}{n-1} - \frac{1}{n} \\ &= \frac{3}{2} - \frac{1}{n}\,.\end{aligned}$$
Onde está o erro da prova? Alguma coisa deve estar errada, pois quando $n = 6$ o lado esquerdo da equação vale $5/6$ enquanto o lado direito vale $4/3$. [D.E. Knuth, "Fundamental Algorithms"]

4. Imagine uma barra retangular de chocolate que consiste em quadradinhos dispostos em m linhas e n colunas. Uma tal barra pode ser quebrada ao longo de uma linha ou de uma coluna, produzindo assim duas barras menores. Qual o número mínimo de quebras necessário para reduzir uma barra aos seus quadradinhos constituintes? [Manuel Blum]

5. Imagine uma jarra contendo um certo número de bolas brancas e bolas pretas. Suponha também que você tem um suprimento ilimitado de bolas brancas fora da jarra. Agora repita o seguinte procedimento enquanto ele fizer sentido: retire duas bolas da jarra; se as duas tiverem a mesma cor, coloque uma bola branca na jarra; se as duas tiverem cores diferentes, coloque uma bola preta na jarra. Qual a cor da última bola a sobrar na jarra? [Manuel Blum]

Bibliografia e material suplementar

- Quora: "What are the most common mistakes people make when writing mathematical proofs?"
- Keith Devlin, What is a mathematical proof?, blog da MAA (Mathematical Association of America)
- Reuben Hersh, Math Lingo vs. Plain English: Double Entendre, *The American Mathematical Monthly*, v.104 (1997), pp. 48-51 (também http://www.jstor.org/stable/2974822)
- Leslie Lamport, How to Write a 21st Century Proof, 2011 [Aula no Heidelberg Laureat Forum em 2015-09-23]
- Günter Rote, The Book of False Proofs
- Wikipedia: List of incomplete proofs
- Wikipedia: List of mathematical jargon

---

www.ime.usp.br/~pf/amostra-de-prova/
Paulo Feofiloff
Departamento de Ciência da Computação
Instituto de Matemática e Estatística da USP
2022-03-25