Matemática Discreta

Pedro Hokama

Fontes

- Gomide, Anamaria; Stolfi, Jorge. Elementos de Matematica Discreta para Computação.
- Rosen, Kenneth H. Discrete mathematics and its applications. McGraw-Hill Education, 8th Edition, 2019.

Implicação com tese conjuntiva

- Queremos provar que $p \to (q \land r)$
- Que é logicamente equivalente à $(p \to q) \land (p \to r)$
- Basta provar cada uma separadamente.

Implicação com tese conjuntiva

Teorema 4.4: Se 6 divide um inteiro n, então 2 divide n e 3 divide n.
Prova:
Se 6 divide n então existe um inteiro k tal que $n = 6k$. Então, $n = 2(3k)$, logo 2 divide n. Temos também que $n = 3(2k)$, logo 3 divide n. Portanto 2 divide n e 3 divide n.
Fim.

Implicação com hipótese disjuntiva

- Queremos provar $(p \lor q) \to r$
- Equivale à $(p \to r) \land (q \to r)$
- Basta provar cada uma dessas partes.

Implicação com hipótese disjuntiva

Teorema 4.5: Para quaiquer inteiros m e n, se m for par ou n for par, então mn é par.
Prova:
Sejam m e n inteiros quaisquer. Temos dois casos (não exclusivos):

- Caso 1: m é par. Pela definição, existe um inteiro q tal que $m = 2q$. Nesse caso, $mn = (2q)n = 2(nq)$, e portanto mn é par.
- Caso 2: n é par. Pela definição, existe um inteiro r tal que $n = 2r$. Nesse caso $mn = m(2r) = 2(mr)$, e portanto mn é par.

Portanto, se m é par ou n é par, mn é par.
Fim.

Demonstrações de afirmações “se e somente se”

Outro tipo comum de teorema tem a forma $p \leftrightarrow q$, ou seja, “p vale se e somente se q vale.”

- Equivalente à $(p \to q) \land (q \to p)$
- Dividimos a demostração em duas partes.
  - (1) prova que $p \to q$ (ida);
  - (2) prova que $q \to p$ (volta);

Teorema 4.7: Os inteiros x e y são ambos ímpares se, e somente se, o produto xy é ímpar.
Prova:
Sejam x e y inteiros quaisquer.

- Parte (1) ($\to$): provaremos que, se x e y são ímpares, então xy é ímpar.Se x e y são ímpares, por definição existem inteiros r e s tais que $x = 2r + 1$ e $y = 2s + 1$. Portanto $xy = (2r + 1)(2s + 1) = 2(rs + r + s) + 1$. Como $rs + r + s$ é um inteiro, concluímos que xy é ímpar.

- Parte (2) ($\leftarrow$): provaremos que, se xy é ímpar, então x e y são ambos ímpares. Ou seja (pela contrapositiva), que se x é par ou y é par, então xy é par. Temos dois casos (não exclusivos):
  - Caso (a): x é par. Neste caso existe um inteiro r tal que $x = 2r$. Portanto $xy = (2r)y = 2(ry)$. Como ry é inteiro, concluímos que xy é par.
  - Caso (b): y é par. Então existe um inteiro s tal que $y = 2s$. Portanto $xy = x(2s) = 2(xs)$. Como xs é inteiro, concluímos que xy é par.

Fim.

Regras para quantificadores universais

Instanciação universal

- Se provarmos que $(\forall x \in D)\, P(x)$,
- podemos afirmar $P(c)$ para qualquer elemento c do domínio D.
- "para todo inteiro x, $2^x > x^2$", podemos imediatamente concluir que $2^{418} > 418^2$.
- Esta regra é chamada de **instanciação universal**.

Regras para quantificadores universais

Generalização universal

- Agora suponha que desejamos provar $(\forall x \in D)\, P(x)$
- começar supondo que x é um elemento de D escolhido arbitrariamente
- Se, com essa suposição, conseguirmos provar a afirmação $P(x)$, provamos que o teorema original é verdadeiro.
- Este último passo é chamado de **generalização universal** ou **suspensão do quantificador universal**.

Generalização universal

Teorema 4.10: Para quaisquer números reais x e y, $(x + y)^2 - (x - y)^2 = 4xy$.
Prova:
Sejam x e y dois números reais quaisquer.
Pelo teorema do binômio, temos $(x + y)^2 = x^2 + 2xy + y^2$, e $(x - y)^2 = x^2 - 2xy + y^2$.
Portanto, $(x + y)^2 - (x - y)^2 = (x^2 + 2xy + y^2) - (x^2 - 2xy + y^2) = 4xy$.
Fim.

Demonstração por vacuidade

Lembre-se que se E é o conjunto vazio, a afirmação $(\forall x \in E)\, Q(x)$ é verdadeira, qualquer que seja o predicado Q. Esta afirmação é verdadeira **por vacuidade**.

- Queremos demostrar $(\forall x \in D)\, P(x)$ para um domínio arbitrário D.
- Mostrar que ela é equivalente a outra afirmação $(\forall x \in E)\, Q(x)$
- Então mostrar que E é vazio.

Teorema: Para todo número inteiro x, se $x^2 = 5$ então x é par.

- $(\forall x \in \mathbb{Z})\, Q(x) \to P(x)$
- $Q(x)$ significa "$x^2 = 5$", e $P(x)$ é "x é par".
- $E = \{\forall x \in \mathbb{Z} : Q(x)\}$
- equivale à $(\forall x \in E)\, P(x)$.
- ou seja, E é o conjunto dos inteiros cujo quadrado é 5.
- Como E é vazio, a afirmação é verdadeira por vacuidade.

Regras para quantificadores existenciais

- Se provamos que $(\exists x \in D)\, P(x)$,
- podemos supor, dali em diante, que a variável x é um dos elementos cuja existência é afirmada.
- Esta regra é chamada de **instanciação existencial**.
- Exemplo: Considere as seguintes premissas: "Um aluno desse curso não estudou" e "Todos os alunos desse curso foram aprovados" podemos concluir que "Algum aluno não estudou e foi aprovado".

Demonstrações construtivas

- Agora suponha que queremos provar que $(\exists x \in D)\, P(x)$.
- Exibimos um elemento específico a do domínio D (explicitamente, ou através de uma construção algorítmica)
- $P(a)$ é verdadeira, para esse elemento.
- **Demonstração construtiva**

Demonstrações construtivas

Teorema 4.11: Existem três números inteiros positivos tais que $x^2 + y^2 = z^2$.
Prova:
Sejam $x = 3$, $y = 4$, e $z = 5$. Como $x^2 + y^2 = 3^2 + 4^2 = 25 = 5^2 = z^2$, a afirmação é verdadeira.
Fim.

Teorema do deserto de primos: Para todo número inteiro positivo n, existe uma sequência de n números inteiros consecutivos que não são primos.
Prova:
Seja n um inteiro positivo, e seja $x = (n+1)! + 2$. Observe que

$$\begin{aligned} 2 \text{ divide } x &= (n+1)! + 2, && (1) \\ 3 \text{ divide } x+1 &= (n+1)! + 3, && (2) \\ &\dots && (3) \\ n+1 \text{ divide } x+(n-1) &= (n+1)! + n + 1. && (4) \end{aligned}$$

Logo todos os inteiros $x + i$ com $0 \leq i < n$ são não primos; e eles formam uma sequência de n inteiros consecutivos.
Fim.

Exercício:

- Existem 100 inteiros consecutivos que não são quadrados perfeitos.

Demonstrações não construtivas

- Em alguns casos, é possível demonstrar a existência de um elemento que satisfaz uma dada condição mesmo sem exibir explicitamente tal elemento.
- Uma demonstração deste tipo é chamada de **demonstração não construtiva**

Teorema 4.14: Existem dois números reais irracionais x e y tais que x^y é racional.
Prova:
Sabemos que número $\sqrt{2}$ é irracional. Se $(\sqrt{2})^{\sqrt{2}}$ for racional, a afirmação está satisfeita tomando-se $x = \sqrt{2}$ e $y = \sqrt{2}$. Por outro lado, se $(\sqrt{2})^{\sqrt{2}}$ for irracional, podemos tomar $x = (\sqrt{2})^{\sqrt{2}}$ e $y = \sqrt{2}$. Então $x^y = ((\sqrt{2})^{\sqrt{2}})^{\sqrt{2}} = (\sqrt{2})^{\sqrt{2}\cdot\sqrt{2}}$ $= (\sqrt{2})^2 = 2$ que é racional.
Fim.

Demonstração de existência e unicidade

- Queremos provar $(\exists! x \in D)\, P(x)$
- Logicamente equivalente à

$$((\exists x \in D)\, P(x)) \wedge ((\forall x \in D)(\forall y \in D)\, ((P(x) \wedge P(y)) \rightarrow x = y))$$

Portanto, uma demonstração de existência e unicidade pode ser dividida em duas partes:

- **Existência:** prova-se-se que existe pelo menos um x em D que satisfaz $P(x)$.
- **Unicidade:** supõe-se que y também é um elemento de D que satisfaz $P(y)$, e prova-se que ele é igual ao x.

Demonstração de falsidade por contra-exemplo

- Demonstrações de existência são usadas, em particular, para refutar conjeturas da forma $(\forall x \in D)\, P(x)$; pois a negação desta afirmação é $(\exists x \in D)\, \neg P(x)$.
- Neste caso dizemos que o elemento x de D que comprovadamente não satisfaz $P(x)$.
- Portanto mostra a falsidade da conjetura

Considere a seguinte afirmação: “Para todo primo n, o inteiro $2^n - 1$ é primo.” Esta afirmação não é verdadeira, basta ver que o número $n = 11$ é um contra-exemplo, pois $P(11) = 2^{11} - 1 = 2047 = 23 \times 89$.

Exercícios:

Demonstre (por meio de contra-exemplos) que as seguintes conjeturas são falsas:

- Todo inteiro positivo é soma dos quadrados de três inteiros.
- Se n é um número inteiro e $4n$ é par, então n é par.
- O produto de dois números irracionais é um número irracional.

Prove (ou mostre contra exemplos) de que as seguintes proposições são equivalentes

a) $(\forall x \in D)\, P(x) \vee Q(x)$ e $((\forall x \in D)\, P(x)) \vee (\forall x \in D)\, Q(x))$.

b) $(\exists x \in D)\, P(x) \wedge Q(x)$ e $((\exists x \in D)\, P(x)) \wedge (\exists x \in D)\, Q(x))$.