Princípio das casas de pombo*

Márcia R. Cerioli
IM e COPPE, UFRJ

Renata de Freitas
IME, UFF

Petrucio Viana
IME, UFF

Maio de 2014

1 Introdução

Neste texto, apresentamos e exemplificamos o Princípio das Casas de Pombo, PCP, tanto como um *resultado matemático*, quanto como um *método de prova*.

Como um resultado matemático, o PCP é bastante simples e intuitivo e parece, à primeira vista, ser de pouca aplicabilidade. Mas, como veremos, através de exemplos, quando usado como um método de prova, o PCP se torna uma ferramenta extremamente poderosa na resolução de problemas cujo objetivo é garantir a existência de configurações de objetos satisfazendo a certas propriedades.

Na Seção 2 e na Seção 3 motivamos e enunciamos o PCP. Na Seção 4 e na Seção 5, apresentamos alguns exemplos de aplicação do PCP na resolução de problemas. Na Seção 6, apresentamos alguns exemplos clássicos de aplicação do PCP na prova de teoremas. Na Seção 7, apresentamos uma prova do PCP baseada no Princípio da Adição, PA. Encerramos essa última seção estudando a relação lógica entre o PA e o PCP. Em particular mostramos que, embora o PA possa ser usado para provar o PCP, a recíproca não é verdadeira.

*Um resumo deste trabalho foi publicado no Jornal Dá Licença 48, UFF, Niterói, 2011, pp. 8-9.

2 A ideia do PCP

Considere o seguinte enunciado:

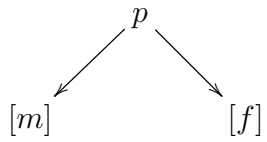
> Em um conjunto de 3 pombos, existem pelo menos 2 do mesmo sexo.

Este enunciado é, obviamente, verdadeiro e nem carece de justificativa. Mas, uma justificativa detalhada para ele pode ser a seguinte:

Justificativa:

Em primeiro lugar, observe que queremos provar a existência de um certo subconjunto dos pombos dados (2 pombos), cujos elementos satisfazem a uma certa propriedade (são do mesmo sexo).

Para isto, consideramos os 3 pombos dados e duas casas de pombo, uma rotulada m (macho) e a outra rotulada f (fêmea). Vamos agora colocar os pombos nas casas de pombo, de acordo com o sexo. Isto é, cada pombo vai para uma das casas, de acordo com o seguinte critério: se o pombo é macho, ele vai para a casa m; se o pombo é fêmea (uma pomba, na verdade), ela vai para a casa f.



Como temos 3 pombos e 2 casas de pombo para colocá-los, uma das casas deverá conter mais do que $\frac{3}{2} = 1,5$ pombos. Mais especificamente, uma das casas deverá conter 2 pombos. Ou seja, ou temos 2 pombos machos ou temos 2 pombos fêmeas. $\lhd$

A resolução deste problema simples ilustra a ideia principal associada ao PCP: o PCP dá origem a um método que pode ser usado na prova de que uma certa configuração (objetos que possuem uma certa propriedade) existe. Para isto, alguns objetos são considerados como pombos, outros como casas de pombo, e os pombos são colocados nas casas de pombo. O PCP, simplesmente, garante que existe uma casa de pombos que contém mais do que um certo número de pombos. Esta casa de pombos, obtida pelo PCP, usualmente nos leva à configuração procurada.

Para formalizar esta ideia, usamos as noções de *função* e de *imagem inversa de um elemento por uma função.*

3 Enunciado do PCP

Sejam P e C conjuntos finitos e não vazios. Uma *função* de P em C relaciona elementos de P a elementos de C, de maneira que:

- cada elemento de P está associado a algum elemento de C;
- nenhum elemento de P está associado a mais do que um elemento de C.

Assim, f é uma função de P em C, quando cada elemento de P está associado a um e exatamente um elemento de C por f. Funções são, usualmente, dadas por *conjuntos de pares ordenados* ou *leis algébricas*.

Dados os conjuntos P e C, escrevemos $f : P \to C$ para dizer que f é uma função de P em C. Além disso, dados $f : P \to C$, $p \in P$ e $c \in C$, escrevemos $f(p) = c$ para dizer que c é o único elemento de C associado a p por f.

Sejam P e C conjuntos, $f : P \to C$ e $c \in C$. A *imagem inversa* de c por f é o conjunto de todos os elementos de P que f associa a c, ou seja, é o conjunto

$$\{p \in P : f(p) = c\}.$$

Dados $f : P \to C$ e $c \in C$, escrevemos $f^{-1}(c)$ para denotar a imagem inversa de c por f. Observe que $f^{-1}(c)$ é um subconjunto de P.

A ideia central na formulação do PCP é a de que, se estabelecemos uma função de um conjunto P em um conjunto C, mesmo que tenhamos feito uma distribuição equitativa dos elementos de P entre os elementos de C, há um elemento de C que é o correspondente de, no mínimo, uma quantidade igual a divisão de $|P|$ (o número de elementos de P) por $|C|$ (o número de elementos de C).

Mais formalmente temos:

Princípio das Casas de Pombo:
Seja P um conjunto finito e não vazio (de pombos) e C um conjunto finito e não vazio (de casas de pombo).
Se $f : P \to C$ é uma função (que coloca os pombos nas casas de pombo), então existe c em C (uma casa de pombo), tal que

$$|f^{-1}(c)| \geq \frac{|P|}{|C|}$$

(a casa c possui ao menos $\frac{|P|}{|C|}$ pombos).

Antes de mais nada, observe que:

- O PCP garante que existe uma casa de pombo c que possui ao menos $\frac{|P|}{|C|}$ pombos, mas não mostra qual é a casa e nem quais são os pombos que estão nela.
- Usualmente, o PCP é enunciado com a restrição de que $|P| > |C|$, ou seja, de que existem mais pombos do que casas de pombo.

  Embora estes sejam os casos que interessam na maioria das vezes, esta restrição não é necessária. De fato, se temos menos pombos do que casas, ou seja, se $|P| < |C|$, o PCP afirma que existe uma casa que possui pelo menos $1 > \frac{|P|}{|C|} > 0$ pombo e, portanto, está correto. Além disso, se temos tantos pombos quanto casas, ou seja, se $|P| = |C|$, o PCP também está correto, pois afirma que existe uma casa que possui pelo menos $1 = \frac{|P|}{|C|}$ pombo.

4 Primeiras aplicações do PCP

Nos exemplos mais diretos de aplicação, o PCP dá origem a um método de prova, da seguinte maneira:

1. Queremos provar a existência de uma certa configuração cuja existência não é fácil provar, à primeira vista.
2. Analisamos o problema de modo a determinar um certo conjunto de objetos P (pombos) e um outro conjunto de C (casas de pombo).

3. Determinamos o número $|P|$ de pombos e o número $|C|$ de casas de pombo.

4. Aplicamos o PCP e concluímos que existe uma casa de pombos c que possui ao menos $\frac{|P|}{|C|}$ pombos.

5. A partir da casa de pombos c, determinamos a configuração procurada.

Como um exemplo imediato da aplicação desta estratégia, vamos justificar os seguintes enunciados.

Exemplo 4.1 Em um grupo de 40 pessoas, existem ao menos 4 que fazem aniversário no mesmo mês.

Justificativa:

Observe que queremos provar a existência de um certo subconjunto das pessoas (4 pessoas) cujos elementos possuem uma certa propriedade (fazem aniversário no mesmo mês).

Vamos considerar P como sendo o conjunto das pessoas e C como sendo o conjunto dos meses do ano. Sabemos que $|P| = 40$ e $|C| = 12$. Consideremos também a função $f : P \to C$ tal que $f(p)$ é o mês de aniversário da pessoa p.

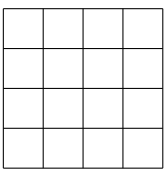
Assim, pelo PCP, existe uma casa c que possui ao menos $4 > 3,333\ldots = \frac{40}{12} = \frac{|P|}{|C|}$ pombos. Ou seja, temos ao menos 4 pessoas que fazem aniversário no mesmo mês. $\lhd$

Exemplo 4.2 Se escolhemos 17 pontos aleatoriamente dentro de um quadrado de área 16, então existem ao menos 2 pontos cuja distância de um para o outro é menor ou igual a $\sqrt{2}$.

Justificativa:

Observe que queremos provar a existência de um certo subconjunto dos pontos (2 pontos) cujos elementos estão em uma certa relação (distam um do outro de no máximo $\sqrt{2}$).

Vamos considerar P como sendo o conjunto dos pontos e C como sendo o conjunto dos quadrados unitários desenhados dentro do quadrado de área 16:



Sabemos que $|P| = 17$ e $|C| = 16$. Consideremos também a função $f : P \to C$ tal que $f(p)$ é o quadrado unitário ao qual o ponto p pertence.

Assim, pelo PCP, existe uma casa c que possui ao menos $2 > 1,0625 = \frac{17}{16} = \frac{|P|}{|C|}$ pombos.

Como a diagonal do quadrado unitário mede $\sqrt{2}$, os pontos em c estão a uma distância menor ou igual a $\sqrt{2}$, um do outro. $\lhd$

5 Segundas aplicações do PCP

Os exemplos da Seção 4 sugerem que a parte mais difícil na aplicação do PCP é determinar, de acordo com os dados do problema, qual é o conjunto de pombos e qual é o conjunto de casas de pombo. Nesta seção vamos considerar alguns exemplos mais complexos nos quais determinar P e C não é uma tarefa tão direta e exige alguma esperteza por parte de quem está aplicando o PCP.

Exemplo 5.1 Considere um conjunto X contendo 10 números naturais não nulos menores que 100. Ou seja, $X \subseteq \{1, 2, 3, \ldots, 99\}$ e $|X| = 10$. Temos que existem dois subconjuntos Y e Z de X tais que $Y \neq \emptyset$, $Z \neq \emptyset$, $Y \cap Z = \emptyset$ e $\sum_{y \in Y} y = \sum_{z \in Z} z$.

Justificativa:

Considere P como sendo o conjunto dos subconjuntos não vazios de X, e C como sendo o conjunto dos resultados possíveis dos somatórios dos subconjuntos não vazios de X, isto é, $C = \{\sum_{a \in A} a : A \subseteq X \text{ e } A \neq \emptyset\}$. Sabemos que $|P| = 2^{10} - 1$, pois $|X| = 10$ mas o conjunto vazio não pertence a P. Não temos informação suficiente para calcular $|C|$ com precisão. Mas uma cota superior para o valor de $|C|$ será suficiente para os nossos propósitos. Para calcular esta cota, observe que, como todos os 10 elementos de X são menores ou iguais a 99, temos que $\sum_{x \in X} x < 990$. Logo, se $A \subseteq X$, então $\sum_{a \in A} a < 990$. Ou seja, os resultados possíveis dos somatórios dos subconjuntos não vazios de X são valores entre 1 e 990, isto é, $|C| < 990$.

Assim, pelo PCP, existe uma casa c que possui ao menos $2 \geq \frac{1023}{990} = \frac{|P|}{|C|}$ pombos. Isto é, existem dois subconjuntos não vazios A e B de X tais que $\sum_{a \in A} a = \sum_{b \in B} b$.

Não podemos garantir que $A \cap B = \emptyset$ mas, a partir destes conjuntos, é fácil obter dois subconjuntos não vazios Y e Z de A com todas as propriedades desejadas. Basta considerar $Y = A - (A \cap B)$ e $Z = B - (A \cap B)$. Temos então que $Y \cap Z = \emptyset$ e $\sum_{y \in Y} y = \sum_{z \in Z} z$. $\lhd$

Exemplo 5.2 Seja A um conjunto finito e não vazio de números naturais, com m elementos. Temos que existe um subconjunto B de A tal que m divide a soma dos elementos de B.

Justificativa:

Seja $A = \{a_1, a_2, \ldots, a_m\}$. Observe que queremos provar a existência de um certo subconjunto $B = \{b_1, b_2, \ldots, b_n\}$ de A, $n \leq m$, cuja soma dos elementos $b_1 + b_2 + \ldots + b_n$ é um múltiplo de m. Para isto, vamos considerar as somas

$$a_1$$

$$a_1 + a_2$$

$$a_1 + a_2 + a_3$$

$$a_1 + a_2 + a_3 + a_4$$

$$\vdots$$

$$a_1 + a_2 + a_3 + a_4 + \cdots + a_m$$

Temos dois casos.

Se m divide uma das somas $a_1 + a_2 + a_3 + \cdots + a_i$, $1 \leq i \leq m$, basta considerar o conjunto $B = \{a_1, a_2, a_3, \ldots, a_i\}$.

Se nenhuma das somas $a_1 + a_2 + a_3 + \cdots + a_i$, $1 \leq i \leq m$ é um múltiplo de m, consideramos P como sendo o conjunto das somas e C como sendo o conjunto $\{1, 2, 3, \ldots, m-1\}$ dos possíveis restos quando dividimos as somas por m. Sabemos que $|P| = m$ e $|C| = m - 1$.

Assim, pelo PCP, existe uma casa c que possui ao menos $2 > \dfrac{m}{m-1} = \dfrac{|P|}{|C|}$ pombos.

Sejam $a_1 + a_2 + a_3 + \cdots + a_i$ e $a_1 + a_2 + a_3 + \cdots + a_j$, com $i < j$, estas somas. Temos que $a_1 + a_2 + a_3 + \cdots + a_i$ e $a_1 + a_2 + a_3 + \cdots + a_j$ deixam o mesmo resto na divisão por m.

Ora, se dois números a e b, com $a > b$ deixam o mesmo resto na divisão por m, então m divide a diferença $a - b$.

De fato, se $a = q_1 m + r$ e $b = q_2 m + r$, com $q_1 > q_2$, então $a - b = (q_1 m + r) - (q_2 m + r) = q_1 m - q_2 m = (q_1 - q_2)m$, que é um múltiplo de m.

Assim, temos que m divide $a_{i+1} + a_{i+2} + \cdots + a_j = (a_1 + a_2 + a_3 + \cdots + a_j) - (a_1 + a_2 + a_3 + \cdots + a_i)$.

Basta, então, considerar o conjunto $B = \{a_{i+1}, a_{i+2}, \ldots, a_j\}$. $\lhd$

Exemplo 5.3 Seja $s = (a_1, a_2, \ldots, a_{2n+1})$ uma sequência de $2n+1$ números inteiros, $n \in \mathbb{N}$, e $p = (a_{i1}, a_{i2}, \ldots, a_{i(2n+1)})$ uma permutação de s. Temos que o produto

$$(a_{i1} - a_1)(a_{i2} - a_2)(a_{i3} - a_3) \ldots (a_{i(2n+1)} - a_{2n+1})$$

é um número par.

Justificativa:

Observe que

o produto $(a_{i1} - a_1)(a_{i2} - a_2)(a_{i3} - a_3) \ldots (a_{in} - a_{2n+1})$ é par
se, e somente se,
existe um fator $a_{ij} - a_j$, $1 \leq j \leq 2n+1$, que é um número par
se, e somente se,
existe um número j, $1 \leq j \leq 2n+1$, tal que os números a_{ij} e a_j
são ambos pares ou ambos ímpares.

Para isto, vamos considerar P como sendo o conjunto cujos elementos são os números $a_1, a_2, \ldots, a_{2n+1}$ e C como sendo o conjunto cujos elementos são as palavras 'par' e 'ímpar'.

Sabemos que $|P| = 2n+1$ e $|C| = 2$.

Assim, pelo PCP, existe uma casa c que possui ao menos $n+1 > \dfrac{2n+1}{2} = \dfrac{|P|}{|C|}$ pombos.

Sejam $b_1, b_2, \ldots, b_{n+1}$ estes números. Temos que $b_1, b_2, \ldots, b_{n+1}$ são todos pares ou todos ímpares.

Sejam, também, $c_1, c_2, \ldots, c_{n+1}$ os elementos que correspondem aos elementos $b_1, b_2, \ldots, b_{n+1}$, segundo a permutação p.

Observe que $\{b_1, b_2, \ldots, b_{n+1}\} \cap \{c_1, c_2, \ldots, c_{n+1}\} \neq \emptyset$. De fato, se fosse $\{b_1, b_2, \ldots, b_{n+1}\} \cap \{c_1, c_2, \ldots, c_{n+1}\} = \emptyset$, então a união $\{b_1, b_2, \ldots, b_{n+1}\} \cup \{c_1, c_2, \ldots, c_{n+1}\}$ teria $(n+1) + (n+1) = 2n+2 > 2n+1$ elementos, uma contradição.

Agora, seja $d \in \{b_1, b_2, \ldots, b_{n+1}\} \cap \{c_1, c_2, \ldots, c_{n+1}\}$. Ou seja, $d = b_k = c_l$, onde $1 \leq k, l \leq n+1$.

Temos que, $c_l - b_l = b_k - b_l$ é par, pois b_k e b_l são ambos pares ou ambos ímpares.

Como $c_l - b_l$ é um fator de $(a_{i1} - a_1)(a_{i2} - a_2)(a_{i3} - a_3) \ldots (a_{i(2n+1)} - a_{2n+1})$, temos que este último produto é par. $\lhd$

6 Algumas aplicações clássicas do PCP

Uma das razões pelas quais o PCP merece destaque é que ele é, usualmente, empregado como método de prova na justificativa de vários teoremas importantes. Vamos deixar para o leitor a tarefa de procurar na bibliografia especializada de combinatória, os vários exemplos de uso do PCP neste contexto. Para uma leitura inicial, sugerimos os livros [1] e [4] e os artigos [2] e [6].

Nesta seção, apresentamos três exemplos clássicos de aplicação do PCP na prova de teoremas. Apresentamos a prova do Teorema de Erdös-Szekeres sobre subsequências monotônicas, a prova do Lema de Dilworth sobre ordens parciais e a prova do Teorema de Ramsey sobre subgrafos monocromáticos, seguindo [2].

6.1 O PCP e a prova do Teorema de Erdös-Szekeres

Para enunciar o Teorema de Erdös-Szekeres, utilizamos os conceitos a seguir.

Seja $s = (x_1, \ldots, x_n)$ uma sequência de números reais.

1. s é *monotônica crescente* se $x_1 \leq \cdots \leq x_n$.
2. s é *monotônica decrescente* se $x_1 \geq \cdots \geq x_n$.
3. s é *monotônica* se é monotônica crescente ou monotônica decrescente.
4. $s' = (y_1, \ldots, y_m)$ é uma *subsequência* de s se $m \leq n$ e, para todos y_i, y_j em s' tais que $i < j$, temos que existem x_k, x_l em s tais que $y_i = x_k$, $y_j = x_l$ e $k < l$.

Teorema 6.1 (Erdös-Szekeres) *Se $s = (x_1, \cdots, x_n)$ é uma sequência de números reais, então s contém uma subsequência monotônica com $\sqrt{n}$ termos.*

Prova. Seja $s = (x_1, \cdots, x_n)$ uma sequência de números reais.

Suponhamos, para uma contradição, que toda subsequência monotônica de s possui no máximo $\sqrt{n} - 1$ termos.

Podemos então definir uma função

$$f : \{1, \ldots, n\} \to \{1, \ldots, \sqrt{n} - 1\} \times \{1, \ldots, \sqrt{n} - 1\}$$

tal que $f(i) = (c_i, d_i)$, onde c_i é o tamanho da maior subsequência monotônica crescente iniciada em x_i e d_i é o tamanho da maior subsequência monotônica decrescente iniciada em x_i.

Para a aplicação do PCP, consideramos

$$P = \{1, \ldots, n\} \text{ e } C = \{1, \ldots, \sqrt{n} - 1\} \times \{1, \ldots, \sqrt{n} - 1\},$$

donde $|P| = n$ e $|C| = (\sqrt{n} - 1)^2$. Pelo PCP, temos que existe $(c, d) \in C$ tal que

$$|f^{-1}(c, d)| \geq \frac{|P|}{|C|} = \frac{n}{(\sqrt{n} - 1)^2} = \frac{n}{n - 2\sqrt{n} + 1} > 1.$$

Assim, existem dois termos x_j e x_k da sequência s tais que $c_j = c_k = c$ e $d_j = d_k = d$.

Temos duas possibilidades: $x_j < x_k$ ou $x_j > x_k$. Se $x_j < x_k$, então a maior subsequência monotônica crescente iniciada em x_j possui ao menos um termo a mais do que a maior subsequência monotônica crescente iniciada em x_j. Ou seja, $c_j > c_k$, o que é uma contradição. Se $x_j > x_k$, então a maior subsequência monotônica decrescente iniciada em x_j possui ao menos um termo a mais do que a maior subsequência monotônica decrescente iniciada em x_j. Ou seja, $d_j > d_k$, o que também é uma contradição.

Assim, s contém uma subsequência monotônica com $\sqrt{n}$ termos. ■

6.2 O PCP e a prova do Lema de Dilworth

Para enunciar o Lema de Dilworth, utilizamos os conceitos de ordem, cadeia e anticadeia.

Dizemos que $\leq$ é uma *relação de ordem* em um conjunto A se $\leq$ é uma relação binária em A que é reflexiva, antissimétrica e transitiva. Se, ao contrário, todos os elementos de A são incomparáveis segundo $\leq$, isto é, dados $a, b \in A$, temos que $a \not\leq b$ e $b \not\leq a$, dizemos que $\leq$ é uma *anticadeia*.

Lema 6.1 (Dilworth) *Seja A um conjunto finito e $\leq$ uma relação de ordem em A. Se $|A| = n$, com $n \geq 2$, então existe um subconjunto $B \subseteq A$ tal que $|B| = \sqrt{n}$ e B é uma cadeia ou uma anticadeia.*

Prova. Suponhamos que A não contém nenhuma cadeia de tamanho $\sqrt{n}$. Para a aplicação do PCP, consideramos $P = A$ e $C = \{1, 2, \ldots, \sqrt{n} - 1\}$. Temos que $|P| = n$ e $|C| = \sqrt{n} - 1$.

Podemos definir uma função $f : P \to C$ tal que $f(x) = m$ se m é o tamanho da maior cadeia em A que tem x como último elemento.

Pelo PCP, existe $c \in C$ tal que

$$|f^{-1}(c)| \geq \frac{n}{\sqrt{n} - 1}.$$

Como $n \geq 2$, temos que $|f^{-1}(c)| \geq \sqrt{n}$. De fato, se $|f^{-1}(c)| \leq \sqrt{n} - 1$, teríamos que

$$\sqrt{n} - 1 \geq |f^{-1}(c)| \geq \frac{n}{\sqrt{n} - 1},$$

donde $n - 2\sqrt{n} + 1 \geq n$, uma contradição. Logo, $|f^{-1}(c)| > \sqrt{n} - 1$, isto é, $|f^{-1}(c)| \geq \sqrt{n}$. Agora vamos mostrar que $B = f^{-1}(c)$ é uma anticadeia. Suponhamos, para uma contradição, que existem $x, y \in B$ tais que $x \leq y$. Daí teríamos $f(x) > f(y)$, ou seja, $f(x) \neq f(y)$, uma contradição, pois, se $x, y \in f^{-1}(c)$, então $f(x) = f(y) = c$. Assim, $f^{-1}(c)$ é uma anticadeia de tamanho mínimo $\sqrt{n}$. ■

6.3 O PCP e a prova do Teorema de Ramsey

O Teorema de Ramsey trata de coloração de grafos.

Um *grafo* é um conjunto finito de vértices ligados por arestas, de modo que:

- não haja laços, isto é, um vértice nunca está ligado a si mesmo por uma aresta, e
- não haja arestas múltiplas, isto é, um mesmo par de vértices está ligado por no máximo uma aresta.

Dado um grafo G, denotamos por $V(G)$ o conjunto de vértices de G e por $A(G)$ o conjunto de arestas de G. As arestas de G são representadas por pares de vértices de G. Dizemos que um grafo G é *completo* se existe uma aresta entre cada par de vértices, isto é, para todos $u, v \in V(G)$, temos que $(u, v) \in A(G)$. Um grafo completo com n vértices é denominado K_n. Dizemos que um grafo H é *subgrafo* de um grafo G se $V(H) \subseteq V(G)$ e $A(H) \subseteq A(G)$.

Uma *bicoloração* de um grafo G é uma assinalação de cores às arestas de G com uma ou duas cores. Uma bicoloração pode ser vista como uma função

$$f : A(G) \to \{\mathsf{vermelho}, \mathsf{amarelo}\},$$

onde $A(G)$ é o conjunto das arestas de G. Um subgrafo H de G é *monocromático* segundo uma bicoloração f se f é constante em $A(H)$. Se H é monocromático, dizemos que H é *vermelho* ou *amarelo*.

Dados $a, b \in \mathbb{N}$ tais que $a, b \geq 2$, o *número de Ramsey* para a e b, denotado por $R(a, b)$, é o menor natural tal que, para qualquer bicoloração f de $K_{R(a,b)}$, temos um subgrafo K_a vermelho segundo f ou um subgrafo K_b amarelo segundo f.

Vejamos o caso em que $a = b = 3$. O número de Ramsey para estes valores é $R(3, 3) = 6$. Em geral, a prova de que $R(a, b) = n$ é feita em

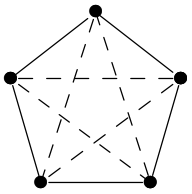


Figure 1: $R(3,3) \leq 6$

duas partes: (1) prova-se que $R(a,b) \geq n$, exibindo uma bicoloração de K_{n-1} segundo a qual nenhum subgrafo K_a é vermelho e nenhum subgrafo K_b é amarelo, e (2) prova-se que $R(a,b) \leq n$, usando-se argumentos de contagem, como o PCP, por exemplo.

Proposição 6.1 *$R(3,3) \geq 6$.*

Prova. A Figura 1 apresenta uma bicoloração de K_5 segundo a qual nenhum subgrafo K_3 é vermelho e nenhum subgrafo K_3 é amarelo, isto é, nenhum subgrafo K_3 é monocromático. ■

Proposição 6.2 *$R(3,3) \geq 6$.*

Prova. Considere uma bicoloração para K_6. Seja v um vértice em K_6. Considere os conjuntos $P = V(K_6) \setminus \{v\}$ e $C = \{\mathsf{vermelho}, \mathsf{amarelo}\}$, e a função $f : P \to C$ tal que $f(u)$ é a cor da aresta que liga o vértice u ao vértice v. Temos que $|P| = 5$ e $|C| = 2$. Logo, pelo PCP, temos que existe uma cor $c \in C$ tal que

$$|f^{-1}(c)| \geq \frac{|P|}{|C|} = \frac{5}{2},$$

ou seja, existem pelo menos 3 vértices de K_6 ligados a v por vértices da mesma cor c, digamos vermelho. Agora temos dois casos a considerar.
Caso 1. Se estes 3 vértices estiverem ligados entre si por arestas amarelas, então temos um subgrafo K_3 amarelo.
Caso 2. Caso contrário, ou seja, se existir uma aresta vermelha entre dois destes vértices, então estes dois vértices, juntamente com v, formam um subgrafo K_3 vermelho.

Em qualquer caso, temos um subgrafo K_3 vermelho ou um subgrafo K_3 amarelo. Logo, $R(3,3) \leq 6$. ■

O Teorema de Ramsey afirma que, no caso geral, sempre existe um natural n tal que $R(a,b) \leq n$. Em outras palavras, para todos $a, b \geq 2$, existe um valor mínimo $R(a,b)$.

Teorema 6.2 (Ramsey) *Se $a, b \in \mathbb{N}$ e $a, b \geq 2$, então $R(a, b)$ existe.*

PROVA. Por indução em a.

BASE. Vamos mostrar que, qualquer que seja $b \geq 2$, existe um valor mínimo $R(2, b) \in \mathbb{N}$ tal que, para qualquer bicoloração de $K_{R(2,b)}$, temos um subgrafo vermelho K_2 ou um subgrafo amarelo K_b.

Seja $b \geq 2$. Vamos mostrar que $R(2, b) = b$. Considere uma bicoloração de K_b. Se K_b for amarelo segundo esta coloração, temos um subgrafo amarelo K_b. Se não, existem pelo menos uma aresta vermelha ligando dois vértices em K_b. Estes dois vértices constituem um subgrafo vermelho K_2.

HIPÓTESE. Seja $a \geq 2$ tal que, qualquer que seja $b \geq 2$, existe um valor mínimo $R(a, b) \in \mathbb{N}$ tal que, para qualquer bicoloração de $K_{R(a,b)}$, temos um subgrafo vermelho K_a ou um subgrafo amarelo K_b.

PASSO. Vamos mostrar que, qualquer que seja $b \geq 2$, existe um valor mínimo $R(a + 1, b) \in \mathbb{N}$ tal que, para qualquer bicoloração de $K_{R(a+1,b)}$, temos um subgrafo vermelho K_{a+1} ou um subgrafo amarelo K_b. Apresentamos uma prova por indução em b.

> Base. É fácil ver que $R(a, b) = R(b, a)$, para todos $a, b \in \mathbb{N}$. Além disso, como foi mostrado na BASE, temos que $R(2, a + 1) = a + 1$. Assim, $R(a + 1, 2) = R(2, a + 1) = a + 1$.
>
> Hipótese. Seja $b \geq 2$ para o qual existe um valor mínimo $R(a+1, b) \in \mathbb{N}$ tal que, para qualquer bicoloração de $K_{R(a+1,b)}$, temos um subgrafo vermelho K_{a+1} ou um subgrafo amarelo K_b.
>
> Passo. Vamos mostrar que existe um valor mínimo $R(a+1, b+1) \in \mathbb{N}$ tal que, para qualquer bicoloração de $K_{R(a+1,b+1)}$, temos um subgrafo vermelho K_{a+1} ou um subgrafo amarelo K_{b+1}.
>
> Pela HIPÓTESE, existe um valor mínimo $R(a, b + 1)$ tal que, para qualquer bicoloração de $K_{R(a,b+1)}$, temos um subgrafo vermelho K_a ou um subgrafo amarelo K_{b+1}.
>
> Pela Hipótese, existe um valor mínimo $R(a+1, b)$ tal que, para qualquer bicoloração de $K_{R(a+1,b)}$, temos um subgrafo vermelho K_{a+1} ou um subgrafo amarelo K_b.
>
> Vamos mostrar que $R(a + 1, b + 1) \leq R(a + 1, b) + R(a, b + 1)$.
>
> Consideremos $n = R(a + 1, b) + R(a, b + 1)$ e uma bicoloração para o grafo completo K_n. Seja v um vértice em K_n, k o número de vértices

ligados a v por arestas vermelhas e l o número de vértices ligados a v por arestas amarelas. Assim, $k+l = n-1 = R(a, b+1)+R(a+1, b)-1$.

Agora vamos analisar dois casos.

Caso 1. $k \geq R(a, b+1)$. Neste caso, pela HIPÓTESE, o (sub)grafo K_k de K_n constituído pelos k vértices ligados a v por arestas vermelhas possui um subgrafo K_a vermelho ou um subgrafo K_{b+1} amarelo. Se acrescentarmos v aos vértices que compõem o subgrafo K_a vermelho, teremos um subgrafo K_{a+1} vermelho.

Caso 2. $k < R(a, b+1)$. Neste caso, como

$$k + l = R(a, b+1) + R(a+1, b) - 1,$$

temos que $l > R(a+1, b)-1$, donde $l \geq R(a+1, b)$. Daí, pela Hipótese, o (sub)grafo K_l de K_n constituído pelos k vértices ligados a v por arestas amarelas possui um subgrafo K_{a+1} vermelho ou um subgrafo K_b amarelo. Se acrescentarmos v aos vértices que compõem o subgrafo K_b amarelo, teremos um subgrafo K_{b+1} amarelo.

Assim, para quaisquer $a, b \in \mathbb{N}$ tais que $a, b \geq 2$, existe um valor mínimo $R(a, b) \in \mathbb{N}$ tal que, para qualquer bicoloração de $K_{R(a,b)}$, temos um subgrafo vermelho K_a ou um subgrafo amarelo K_b. Além disso, quando $a, b \geq 3$, temos que $R(a, b) \leq R(a, b-1) + R(a-1, b)$. ■

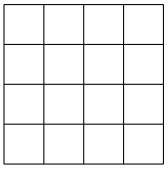
7 Prova do PCP

Nesta seção, vamos apresentar uma prova formal do PCP — isto é, uma justificativa para o PCP, logicamente encadeada, que emprega conceitos e resultados matemáticos considerados como já estabelecidos. Vamos, também, discutir a relação lógica do PCP com o principal resultado matemático usado nesta prova, o Princípio da Adição.

7.1 Princípio da Adição

A prova do PCP que vamos apresentar, é baseada em um resultado matemático conhecido como Princípio da Adição, PA. Como o PCP, o PA é um resultado bastante simples e pode ser motivado pelo problema a seguir.

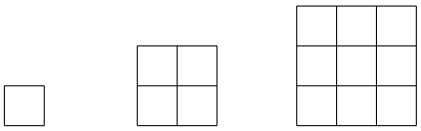
Exemplo 7.1 Determine o número total de quadrados que podem ser desenhados, de modo que os lados de cada quadrado estejam sobre as linhas da figura abaixo (chamada *grade*), composta de 16 quadrados (chamados *células*).



Resolução:

Seja X o conjunto de todos os quadrados que podem ser desenhados sobre as linhas da grade.

Observe que cada elemento de X é um quadrado formado por 1, 4, 9 ou 16 células, respectivamente. Ou seja, a própria grade e as figuras:



Considere o conjunto A_1 dos quadrados que usam 1 célula; A_2 o conjunto dos quadrados que usam 4 células; A_3 o conjunto dos quadrados que usam 9 células; e A_4 o conjunto dos quadrados que usam 16 células.

Como cada quadrado em X pertence a exatamente um dos conjuntos A_1, A_2, A_3 ou A_4, se determinamos $|A_1|$, $|A_2|$, $|A_3|$ e $|A_4|$, o problema está resolvido, pois para determinar $|X|$ basta somar $|A_1|$ com $|A_2|$, com $|A_3|$ e com $|A_4|$. De acordo com o enunciado do problema, $|A_1| = 16$, $|A_2| = 9$, $|A_3| = 4$ e $|A_4| = 1$.

Assim, temos $|X| = 16 + 9 + 4 + 1 = 30$. $\lhd$

A resolução deste problema simples ilustra a ideia principal do PA: o PA pode ser usado na determinação do número de elementos de um dado conjunto X, simplesmente pela troca de X por vários conjuntos menores A_1, A_2, ..., A_n, que possuem todos os elementos de X e que não possuem elementos em comum, para os quais sabemos determinar $|A_1|$, $|A_2|$, ..., $|A_n|$.

Para enunciar o PA de maneira formal (e correta) precisamos da noção de *partição*.

Uma coleção de subconjuntos forma uma partição de um conjunto dado, quando cada elemento do conjunto dado pertence a exatamente um destes subconjuntos.

Sejam X um conjunto finito e $A_1, A_2, \ldots, A_n$ subconjuntos de X.

(1) Dizemos que $A_1, A_2, \ldots, A_n$ *exaurem* X se, para cada elemento x de X, existe i, com $1 \leq i \leq n$, tal que $x \in A_i$; ou seja, se $A_1 \cup A_2 \cup \ldots \cup A_n = X$.

(2) Dizemos que $A_1, A_2, \ldots, A_n$ são *disjuntos dois a dois* se, quando examinados aos pares, eles não possuem elementos em comum; ou seja, $A_i \cap A_j = \emptyset$, para todos i, j com $1 \leq i \neq j \leq n$.

(3) Dizemos que $A_1, A_2, \ldots, A_n$ são uma *partição* de X se $A_1, A_2, \ldots, A_n$ exaurem X e são disjuntos dois a dois.

Neste caso, também dizemos que $A_1, A_2, \ldots, A_n$ são os *blocos* da partição e que a cada elemento de X corresponde a um e somente um dos blocos A_i, onde $i \in \{1, 2, \ldots, n\}$.

A ideia central na formulação do PA é a de que, se separamos os elementos de X em conjuntos $A_1, A_2, \ldots, A_n$, de maneira que cada elemento de X está em exatamente um dos conjuntos Ai, ou seja, se estabelecemos uma partição de X nos conjuntos $A_1, A_2, \ldots, A_n$, então a soma do número de elementos de A_1 com o número de elementos de A_2 com $\ldots$ com o número de elementos de A_n é igual ao número de elementos de X.

Mais formalmente, temos:

Princípio da Adição (PA):
Seja X um conjunto finito.
Se $A_1, A_2, \ldots, A_n$ são uma partição de X, então

$$|X| = |A_1| + |A_2| + \ldots + |A_n|.$$

Na prática, o PA deve ser aplicado na seguinte situação:

1. Queremos determinar o número de elementos de um conjunto X que não é fácil determinar, à primeira vista.

2. Transformamos, através de uma partição, o conjunto X em n subconjuntos $A_1, A_2, \ldots, A_n$ cujos números de elementos já sabemos determinar.

3. Aplicamos o PA e concluímos que o número de elementos de X é igual ao somatório do número de elementos dos A_i, com $1 \leq i \leq n$.

7.2 Prova do PCP usando o PA

Vamos ver como podemos usar o PA para provar o PCP.

Teorema 7.1 (Princípio das Casas de Pombo) *Sejam P e C conjuntos finitos e não vazios. Se $f : P \to C$ é uma função, então existe c em C, tal que*

$$|f^{-1}(c)| \geq \frac{|P|}{|C|}.$$

Prova. Vamos provar o PCP por redução ao absurdo, usando o PA.

Assim, vamos supor, para uma contradição, que o PCP é falso. Isto é, vamos supor que existem conjuntos finitos e não vazios $P = \{p_1, p_2, \ldots, p_m\}$ e $C = \{c_1, c_2, \ldots, c_n\}$, e função $f : P \to C$ tais que, para cada c em C:

$$|f^{-1}(c)| < \frac{|P|}{|C|}.$$

Sejam $d_1, d_2, \ldots, d_k$, $k \leq n$, os elementos de C aos quais f associa algum elemento de P. A primeira coisa a observar é que, como $f : P \to C$ é uma função, os conjuntos $f^{-1}(d_1), f^{-1}(d_2), \ldots, f^{-1}(d_k)$ são uma partição de P. De fato, como cada elemento de P está associado a algum elemento de C por f, dado $p \in P$, existe algum elemento d_i em C, $1 \leq i \leq k$, tal que $f(p) = d_i$. Assim, $p \in f^{-1}(d_i)$, ou seja, cada elemento de P pertence a algum dos conjuntos em $f^{-1}(d_i)$, $1 \leq i \leq k$. Além disso, como nenhum elemento de P está associado a mais do que um elemento de C por f, dados $f^{-1}(d_i)$ e $f^{-1}(d_j)$, $1 \leq i \neq j \leq k$, temos que $f^{-1}(d_i) \cap f^{-1}(d_j) = \emptyset$.

Assim, pelo PA, temos

$$|P| = |f^{-1}(d_1)| + |f^{-1}(d_2)| + \cdots + |f^{-1}(d_k)|.$$

E daí, podemos concluir que

$$\begin{aligned} m = |P| &= |f^{-1}(c_1)| + |f^{-1}(c_2)| + \cdots + |f^{-1}(c_k)| \\ &< \underbrace{\frac{|P|}{|C|} + \frac{|P|}{|C|} + \cdots + \frac{|P|}{|C|}}_{k \text{ vezes}} \\ &\leq \underbrace{\frac{m}{n} + \frac{m}{n} + \cdots + \frac{m}{n}}_{n \text{ vezes}} \\ &= n \times \frac{m}{n} \\ &= m, \end{aligned}$$

ou seja, $m < m$, uma contradição com $m = m$. ■

7.3 Generalizando a prova anterior

Com relação à prova apresentada na seção anterior, observe que os únicos conceitos matemáticos que foram usados na sua formulação foram:

- os números racionais e suas propriedades aritméticas;
- conjuntos e a noção de partição;
- funções e suas propriedades;
- a função $|\ |$, que associa a cada conjunto finito X o seu número de elementos $|X|$. A função $|\ |$ possui duas propriedades fundamentais que foram usadas na prova acima:

  (i) para todo conjunto finito X, $|X| = 0$ se, e somente se, $X = \emptyset$;

  (ii) para todos os conjuntos finitos $X, A_1, A_2, \ldots, A_n$, temos que se $A_1, A_2, \ldots, A_n$ são uma partição de X, então $|X| = |A_1| + |A_2| + \ldots + |A_n|$.

A propriedade (i) foi usada, por exemplo, para garantir o uso das frações $\frac{|P|}{|C|}$ que aparecem na prova. A propriedade (ii) é, exatamente, o PA.

Além disso, a propriedade (ii) foi usada apenas em um ponto muito específico da prova, para concluir que $|P| = |f^{-1}(d_1)| + |f^{-1}(d_2)| + \ldots + |f^{-1}(d_k)|$. Agora, observe que a prova acima pode ser diretamente adaptada para provar que um resultado análogo ao PCP vale para toda função g, que associa conjuntos finitos a números naturais, que satisfaz a propriedades análogas a estas propriedades fundamentais da função $|\ |$.

Formalmente, vamos definir:

> Seja g uma função dos conjuntos finitos nos números naturais.
> Dizemos que g é *normal aditiva* se satisfaz às seguintes condições:
>
> (1) para todo conjunto finito X, $g(X) = 0$ se, e somente se, $X = \emptyset$;
>
> (2) para todos os conjuntos finitos $X, A_1, A_2, \ldots, A_n$, se $A_1, A_2, \ldots, A_n$ são uma partição de X, então $g(X) = g(A_1) + g(A_2) + \ldots + g(A_n)$.

Duas propriedades básicas das funções normais aditivas são necessárias no segue:

Teorema 7.2 *Se g é uma função normal aditiva, então:*
(i) $1 \leq g(X)$*, para todo conjunto unitário X;*
(ii) $|X| \leq g(X)$*, para todo conjunto finito X.*

Prova. (i) Se X é unitário, temos que $X \neq \emptyset$. Assim, pela propriedade (1) da definição de função normal aditiva, $g(X) \neq 0$. Como g é uma função dos conjuntos finitos nos números naturais, temos $g(X) \geq 1$.
(ii) Suponha agora que $X = \{x_1, x_2, \ldots, x_n\}$. Como $\{x_1\}$, $\{x_2\}$, $\ldots$, $\{x_n\}$ são uma partição de X, pela propriedade (2) da definição de função normal aditiva, $g(X) = g(\{x_1\}) + g(\{x_2\}) + \ldots + g(\{x_n\}) \geq \underbrace{1 + 1 + \ldots + 1}_{n \text{ vezes}} = n = |X|$. Para justificar a desigualdade, usamos (i). ■

Dada uma função normal aditiva, g, qualquer, estamos prontos para provar o seguinte:

Teorema 7.3 (PCP para g) *Para todos os conjuntos finitos e não vazios P e C, e para toda função $f : P \to C$, existe c em C, tal que*

$$g(f^{-1}(c)) \geq \frac{g(P)}{g(C)}.$$

PROVA. Vamos adaptar de maneira direta a prova do PCP usando o PA, para obter uma prova do PCP para g.

Assim, vamos supor, para uma contradição, que o PCP para g é falso. Isto é, vamos supor que existem conjuntos finitos e não vazios $P = \{p_1, p_2, \ldots, p_m\}$ e $C = \{c_1, c_2, \ldots, c_n\}$, e função $f : P \to C$ tais que, para cada c em C:

$$g(f^{-1}(c)) < \frac{g(P)}{g(C)}.$$

Sejam $d_1, d_2, \ldots, d_k$, $k \leq n$, os elementos de C aos quais f associa algum elemento de P. Como já sabemos, do fato que $f : P \to C$ é uma função, temos que os conjuntos $f^{-1}(d_1), f^{-1}(d_2), \ldots, f^{-1}(d_k)$ são uma partição de P. Assim, pela propriedade de g e pelo PA, temos

$$g(P) = g(f^{-1}(d_1)) + g(f^{-1}(d_2)) + \ldots + g(f^{-1}(d_k)).$$

E daí, podemos concluir que

$$\begin{aligned} g(P) &= g(f^{-1}(c_1)) + g(f^{-1}(c_2)) + \ldots + g(f^{-1}(c_k)) \\ &< \underbrace{\frac{g(P)}{g(C)} + \frac{g(P)}{g(C)} + \ldots + \frac{g(P)}{g(C)}}_{k \text{ vezes}} \\ &\leq \underbrace{\frac{g(P)}{g(C)} + \frac{g(P)}{g(C)} + \ldots + \frac{g(P)}{g(C)}}_{n \text{ vezes}} \\ &= n \times \frac{g(P)}{g(C)}, \end{aligned}$$

ou seja, $g(P) < n \times \dfrac{g(P)}{g(C)}$. Mas isto acarreta $g(C)g(P) < ng(P)$ e, como $g(P) \neq 0$, $g(C) < n$. Mas esta última desigualdade é o mesmo que $g(C) < |C|$, uma contradição com o Teorema 7.2(ii). ■

7.4 Relação lógica do PA com o PCP

O PA e o PCP podem ser vistos como propriedades importantes da função $|\ |$ que associa conjuntos finitos a números naturais, contando o número de elementos dos conjuntos. Na seção anterior provamos que o PA (quando visto deste modo), juntamente com propriedades usuais dos números racionais e

conjuntos, acarreta o PCP (quando este também é visto como uma propriedade de $|\ |$). Na verdade, mostramos um resultado um pouco mais forte que garante que, dadas as propriedades usuais dos números racionais e conjuntos, qualquer função normal aditiva tem uma propriedade análoga à do PCP, quando visto como uma propriedade da função $|\ |$. Uma pergunta que cabe fazer neste contexto é se o PA também é uma consequência do PCP, ou seja, se os dois princípios são, na verdade, equivalentes.

Veremos agora que este não é o caso, isto é, veremos que não é possível provar o PA a partir do PCP, juntamente com propriedades usuais dos números racionais e conjuntos.

A ideia principal da justificativa deste fato é a de que, se pudéssemos provar o PA a partir do PCP, de uma maneira análoga a que fizemos no caso da prova do PCP a partir do PA, a prova apresentada poderia ser generalizada para provar que qualquer função satisfazendo o PCP para g e as propriedades que foram usadas na prova, também deveria satisfazer uma versão do PA para g, ou seja, deveria satisfazer a propriedade:

Propriedade 7.1 (PA para g) *Para todos os conjuntos finitos X, A_1, A_2, ..., A_n, se $A_1, A_2, \ldots, A_n$ são uma partição de X, então $g(X) = g(A_1) + g(A_2) + \ldots + g(A_n)$.*

Observe que o PA para g é exatamente a condição (ii) da definição de função normal aditiva. Assim, se pretendemos provar que o PCP não acarreta o PA, devemos relaxar o espaço de funções e considerar funções que não satisfazem, necessariamente, esta propriedade.

Formalmente, vamos definir:

> Seja g uma função dos conjuntos finitos nos números naturais.
> Dizemos que g é *normal* se, para todo conjunto finito X, $g(X) = 0$ se, e somente se, $X = \emptyset$.

Finalmente, vamos provar o seguinte resultado que mostra que o PCP não acarreta o PA:

Teorema 7.4 *Existe uma função normal, g, que satisfaz o* PCP *para g mas não satifaz o* PA *para g.*

Prova. Basta tomar a função que associa conjuntos a números naturais do seguinte modo:

$$g(X) = \begin{cases} 0 \text{ se } X = \emptyset, \\ 1 \text{ se } X \neq \emptyset. \end{cases}$$

Em primeiro lugar, por definição, temos que $g(X) = 0$ se, e somente se, $X = \emptyset$. Assim, g é normal.

Agora, se P e C são conjuntos finitos não vazios e $f : P \to C$ é uma função, existe p em P e c em C tais que $f(p) = c$, ou seja, $p \in f^{-1}(c)$. Assim, $f^{-1}(c) \neq \emptyset$ e temos: $g(f^{-1}(c)) = 1 = \dfrac{1}{1} \geq \dfrac{g(P)}{g(C)}$. Ou seja, o PCP para g é verdadeiro.

Por outro lado, tomando, $X = \{a, b\}$, $A_1 = \{A\}$ e $A_2 = \{b\}$, temos: $g(X) = 1 \neq 2 = 1 + 1 = g(A_1) + g(A_2)$. Ou seja, o PA para g é falso. ■

References

[1] M. Aigner e G.M. Ziegler, *A Provas estão n'O Livro*. Segunda Edição. Edgard Blucher, São Paulo, 2002.

[2] M. Erickson, An Introduction to Combinatorial Existence Theorems. *Mathematics Magazine*, 67(1994), 118–123.

[3] G. Garbi, Sobre múltiplos "irados", *Revista do Professor de Matemática* **78**:2-4, 2012.

[4] L. Lovász, J. Pelikán e K. Vesztergombi, *Matemática Discreta*. Coleção Textos Universitários. SBM, Rio de Janeiro, 2003.

[5] A.C. de O. Morgado, J.B.P. de Carvalho, P.C.P. Carvalho e P. Fernandez, Análise Combinatória e Probabilidade: com as soluções dos exercícios. Sexta edição. SBM, Rio de Janeiro, 2004.

[6] K.R. Rebman, The Pigeonhole Principle (What It Is, How It Works, and How It Applies to Map Coloring. *The Two-Year College Mathematics Journal*, 10(1979), 3–13.

[7] J.P.O. Santos, M.P. de Mello e I.T.C. Murari, Introdução à Análise Combinatória. 4ª edição revista. Ciência Moderna, Rio de Janeiro, 2007.