Mapeando Reais para Inteiros

Domingos Dellamonica Jr.
Orientador: Yoshiharu Kohayakawa

8 de agosto de 2004

Resumo

Demonstraremos que é possível mapear uma seqüência de números reais para uma seqüência de números inteiros preservando certas somas de elementos da seqüência. Por exemplo, podemos desejar que uma tripla da seqüência de reais, digamos (s_i, s_j, s_k), com $s_k = s_i + s_j$, seja mapeada a uma tripla de inteiros (t_i, t_j, t_k) com $t_k = t_i + t_j$.

Seja $S = \{s_1, \ldots, s_n\}$ uma seqüência de reais – para simplificar a notação, definimos $\mathbf{s} = (s_1, \ldots, s_n)$. As propriedades de somas que trataremos são do tipo $a_1 s_1 + a_2 s_2 + \cdots + a_n s_n = 0$, com $a_i \in \mathbb{Q}$. Seguindo o exemplo dado, $s_k = s_i + s_j$ é codificado como $1s_i + 1s_j - 1s_k = 0$.

Seja $\mathcal{P} \subset \mathbb{Q}^n$ um conjunto finito e não-vazio que codifica propriedades de somas de S, ou seja, para todo $\mathbf{a} \in \mathcal{P}$, temos $\langle \mathbf{a}, \mathbf{s} \rangle = 0$. Nosso lema mostra que podemos obter uma seqüência de inteiros $\{t_1, \ldots, t_n\}$ com as seguintes características:

1. para todo $\mathbf{a} \in \mathcal{P}$ temos $\langle \mathbf{a}, (t_1, \ldots, t_n) \rangle = 0$, ou seja, as propriedades de somas são preservadas pelo mapa;
2. $t_i = t_j$ somente se $s_i = s_j$;
3. $t_i = 0$ somente se $s_i = 0$.

A partir desse resultado provaremos uma generalização de um teorema de Erdős e a solução de um problema olímpico.

Forme uma matriz $\mathbf{M}$ cujas linhas são os vetores de $\mathcal{P}$. É evidente que $\mathbf{Ms} = \mathbf{0}$ e, por definição, os elementos de $\mathbf{M}$ são todos racionais.

Sendo assim, quando tratamos $\mathbf{M}$ como uma transformação linear nos reais, $\ker(\mathbf{M}) \neq \emptyset$, ou seja $\ker(\mathbf{M})$ tem dimensão maior ou igual a 1. Observe que essa dimensão deve ser a mesma quando $\mathbf{M}$ é vista como uma transformação linear nos racionais.

Tome B como uma base de vetores racionais para $\ker(\mathbf{M})$. Note que B é base também para $\ker(\mathbf{M})$ nos reais, já que os vetores de B também são linearmente independentes sobre os reais (se isto não for claro, aplique eliminação Gaussiana nos vetores de B e veja que eles devem ser LI sobre os reais).

Escolha $\mathbf{u} \in \ker(\mathbf{M}) \cap \mathbb{Q}^n$ com $\#\{(i,j) \mid u_i = u_j\}$ mínimo. Vamos mostrar que $\mathbf{u}$ é um vetor racional com $u_i = u_j$ somente se $s_i = s_j$.

Suponha que $s_i \neq s_j$ mas $u_i = u_j$. Existe $\mathbf{v} \in \ker(\mathbf{M}) \cap \mathbb{Q}^n$ com $v_i \neq v_j$, caso contrário, todo vetor de B teria as coordenadas i e j iguais e isso invalidaria $s_i \neq s_j$.

Seja $\lambda \in \mathbb{Q}^*$. Vamos analisar as coordenadas de $\mathbf{u} + \lambda\mathbf{v}$. Veja que $u_i + \lambda v_i \neq u_j + \lambda v_j$ e que, para cada par (k,l), $u_k + \lambda v_k = u_l + \lambda v_l$ se e somente se $u_k - u_l = \lambda(v_l - v_k)$, e isso ocorre se e somente se $u_k = u_l, v_k = v_l$ ou

$$\lambda = \frac{u_k - u_l}{v_l - v_k}, v_k \neq v_l. \tag{1}$$

Note que podemos escolher algum λ que não satisfaça a equação (1) para nenhum par (k,l), com $u_k \neq u_l$. Mas então, para tal escolha de λ, $\mathbf{u} + \lambda\mathbf{v}$ tem menos coordenadas repetidas que $\mathbf{u}$, o que contradiz a suposição inicial.

Temos então um vetor racional $\mathbf{u}$ que satisfaz as propriedades de somas e é tal que $u_i = u_j$ somente se $s_i = s_j$. Resta mostrar que podemos exigir que u_k seja nulo somente se s_k também é nulo.

A idéia é basicamente uma repetição do argumento anterior. Suponha $s_k \neq 0$ e $u_k = 0$. Deve existir $\mathbf{w} \in \ker(\mathbf{M}) \cap \mathbb{Q}^n$ com $w_k \neq 0$, senão, todo vetor de B seria nulo na k'ésima coordenada e isso contraria a suposição $s_k \neq 0$.

Considere vetores do tipo $\mathbf{u} + \mu\mathbf{w}$, com $\mu \in \mathbb{Q}^*$. Note que $u_k + \mu w_k = \mu w_k \neq 0$. Além disso, $u_l + \mu w_l = 0$ se e somente se $u_l = w_l = 0$ ou

$$\mu = -\frac{u_l}{w_l} \tag{2}$$

e, para um par (i,j), com $s_i \neq s_j$, devemos ter $u_i \neq u_j$ e, portanto, $u_i + \mu w_i = u_j + \mu w_j$ se e somente se

$$\mu = \frac{u_i - u_j}{w_j - w_i}, w_i \neq w_j. \tag{3}$$

Desta forma, é possível escolher μ que nunca satisfaça as equações (2) e (3).

Aplicando a idéia acima sucessivas vezes, eliminamos toda coordenada nula de $\mathbf{u}$ que não seja correspondida no vetor $\mathbf{s}$. Isso conclui a demonstração do lema,

já que basta multiplicar o vetor por um inteiro que seja múltiplo dos denominadores das coordenadas de $\mathbf{u}$ para obter um vetor de inteiros que satisfaça as características enumeradas acima.

COROLÁRIO 1: Seja $\{s_1, \ldots, s_n\}$ um conjunto de reais, existe $A \subset S$, livre de somas e com cardinalidade $|A| > n/3$.

Dizemos que um conjunto S é livre de somas quando não existem $a, b, c \in S$, tais que $a + b = c$. O seguinte teorema foi demonstrado por Erdős em 1965:

TEOREMA: *Todo conjunto $B = \{b_1, \ldots, b_n\}$ de inteiros não nulos contém um subconjunto A, livre de somas, de tamanho $|A| > n/3$.*

Dem.: Seja $p = 3k + 2$ um primo satisfazendo $p > 2 \max_{1 \leq i \leq n} |b_i|$ e defina $C = \{k + 1, k + 2, \ldots, 2k + 1\} \subset \mathbb{Z}_p$. Veja que C é livre de somas em $\mathbb{Z}_p$ e que

$$\frac{|C|}{p-1} = \frac{k+1}{3k+1} > \frac{1}{3}.$$

Escolha um elemento aleatório x, de $\mathbb{Z}_p^*$, conforme uma distribuição uniforme. Defina $d_i = xb_i \mod p$, $1 \leq i \leq n$. Note que como p é primo e $b_i \not\equiv 0 \pmod p$, $\varphi_i(x) = xb_i$ é uma função bijetiva e, portanto, $\Pr[d_i \in C] = |C|/(p-1) > 1/3$. O número esperado de elementos b_i tais que $d_i \in C$ é maior que $n/3$. Logo, existe um $x \in \mathbb{Z}_p^*$ e $A \subset B$ de cardinalidade $|A| > n/3$ tal que $xy \mod p \in C$ para todo $y \in A$. Mas A é livre de somas, pois se $a_1, a_2, a_3 \in A$ são tais que $a_1 + a_2 = a_3$, então $xa_1 + xa_2 \equiv xa_3 \pmod p$, o que contradiz o fato de que C é livre de somas. $\diamond$

Para aplicar o lema, tome $\mathcal{P} = \{\mathbf{e}_i + \mathbf{e}_j - \mathbf{e}_k \mid s_i + s_j = s_k\}$, onde $\mathbf{e}_i$ é o vetor com 1 na i'ésima coordenada e 0 em todas as demais. Verifique também que o lema garante um mapa de um *conjunto S*, de n reais, para um *conjunto T*, de n inteiros, pois $t_i = t_j$ somente se $s_i = s_j$.

COROLÁRIO 2: Se $\{s_1, \ldots, s_n\}$ é uma seqüência de reais na qual para toda sub-seqüência de tamanho $a > 1$, existe uma sub-seqüência de tamanho $b > a$ com mesma média aritmética, e $a \nmid b$, então $s_1 = s_2 = \ldots = s_n$.

A partir do lema, podemos mapear a seqüência de reais para uma seqüência de inteiros onde a propriedade das sub-seqüências se mantém. Basta observar que, se

$$\frac{s_{i_1} + \cdots + s_{i_a}}{a} = \frac{s_{j_1} + \cdots + s_{j_{a+1}}}{b},$$

então podemos atribuir a esta condição o vetor $\mathbf{c}$, onde $c_{i_k} = b$, para $1 \leq k \leq a$, $c_{j_l} = -a$, para $1 \leq l \leq b$ e todos os demais componentes são nulos.

Para completar, note que o número de sub-seqüências é finito e, portanto, o número de vetores formados é finito, ou seja, aplicando o lema, basta provar que uma seqüência $\{t_1, \ldots, t_n\}$ de inteiros que satisfaça tais propriedades é constante (já que $t_i = t_j$ somente se $s_i = s_j$).

Primeiramente, vamos mostrar que $t_1 = t_2 = \cdots = t_{a+1}$. Para isso, observe que podemos assumir, sem perda de generalidade, que $t_1 \leq t_2 \leq \cdots \leq t_n$. Temos

$$\begin{aligned} \frac{t_1 + \cdots + t_a}{a} = \frac{t_{i_1} + \ldots t_{i_b}}{b} &\geq \frac{t_1 + \cdots + t_b}{b}, \\ b(t_1 + \cdots + t_a) &\geq a(t_1 + \cdots + t_b), \\ (b-a)(t_1 + \cdots + t_a) &\geq a(t_{a+1} + \cdots + t_b). \end{aligned} \tag{4}$$

Notando que $(b-a)(t_1 + \cdots + t_a) \leq a(b-a)t_a$ e $a(t_{a+1} + \cdots + t_b) \geq a(b-a)t_{a+1}$, concluímos que $t_a \geq t_{a+1}$, portanto, $t_a = t_{a+1}$. Substituindo em (4), temos

$$\begin{aligned} (b-a)(t_1 + \cdots + t_a) \geq a(t_{a+1} + \cdots + t_b) &\geq a(b-a)t_a \\ t_1 + \cdots + t_a &\geq at_a, \end{aligned}$$

logo, $t_1 = t_2 = \cdots = t_{a+1}$.

Podemos assumir que a seqüência é não-negativa; se não for, basta somar uma constante positiva α para todos os elementos da seqüência. Esse processo acrescenta α a todas as médias aritméticas e, portanto, as propriedades de somas desejadas são mantidas.

Tome $\{t_1, \ldots, t_n\}$ como uma seqüência não-constante e não-negativa de inteiros, em ordem crescente, com as somas desejadas e com $t_1 + \cdots + t_n$ mínimo. Sabemos que $t_1 = t_2 = \cdots = t_{a+1} = 0$, senão, poderíamos subtrair t_1 de todos os termos, manter as propridades desejadas e reduzir a soma dos termos. Mas então, para todo k,

$$\frac{t_k + (t_1 + \cdots + t_{a-1})}{a} = \frac{t_k}{a} = \frac{t_{i_{k,1}} + \cdots + t_{i_{k,b}}}{b},$$

o que nos diz que $a' \mid t_k$, onde $a' = a/\operatorname{mdc}(a,b) > 1$.

Note que, se todos os termos da seqüência são múltiplos de a', ao dividirmos todos eles por a', formamos uma nova seqüência de inteiros, não-constante e não-negativa, em ordem crescente e também com as somas desejadas, pois, ao dividir todos os termos por a', estamos dividindo todas as médias aritméticas por a'. Mas isso contraria a hipótese de que $t_1 + \cdots + t_n$ é mínimo e, portanto, a seqüência deve ser constante (já que nenhuma outra suposição feita acarreta perda de generalidade).

Para concluir, veja que se tivermos a condição $a \mid b$, é simples formular uma seqüência na qual para toda sub-seqüência de tamanho a existe uma sub-seqüência de tamanho b de mesma média aritmética. Tome, por exemplo, uma seqüência contendo b 0's e b 1's, e $b = ac$ para algum c. As médias possíveis das sub-seqüências de tamanho a são k/a, com $0 \leq k \leq a$, mas, para qualquer um desses valores, é possível formar uma sub-seqüência de tamanho b, com kc 1's e os demais elementos nulos. Tal sub-seqüência tem média aritmética $(kc)/b = k/a$.