Com quantos testes se faz um gabarito?

Um dos problemas de um Torneio das Cidades foi:

Uma prova tem 30 testes do tipo V ou F. Joãozinho não sabe a resposta de nenhum teste, mas pode fazer a mesma prova quantas vezes quiser. Depois da prova ele é informado somente da quantidade de testes que ele acertou (ele não é informado sobre quais testes ele acertou ou errou). Mostre que, após fazer a prova 24 vezes Joãozinho consegue descobrir as respostas, não importando quais sejam os resultados dos testes.

Na prova, houve alunos que mostraram que Joãozinho conseguia descobrir as respostas com 21 tentativas. Até que matemáticos russos se perguntaram "será que dá para melhorar?" e "qual será a menor quantidade de tentativas necessárias?"

Até o momento as respostas para as duas perguntas são "sim" e "não se sabe" (bom, a verdade é que ninguém sabe ainda a resposta para a segunda pergunta).

1. Usamos ou não as respostas anteriores?

Pelo enunciado, em princípio podemos utilizar a informação que temos até o momento para cada tentativa (ou seja, em princípio, podemos usar os resultados das tentativas anteriores para definir a próxima tentativa).

No que se segue, porém, não faremos isso. Ou seja, definiremos as tentativas sem utilizar os resultados das tentativas anteriores.

2. Modelando com coordenadas

Vamos generalizar e transformar tudo em coordenadas. Para facilitar, vamos fixar n, a quantidade de tentativas, e procurar $m(n)$, a quantidade máxima de testes que podemos descobrir com n tentativas. Em particular, o problema do Torneio das Cidades pede para provar que $m(24) \geq 30$. Para simplificar, utilizaremos somente m no lugar de $m(n)$.

É claro que podemos usar, no lugar da quantidade de acertos, a quantidade de acertos menos a quantidade de erros.

Associe a cada *teste* i, $1 \leq i \leq m$ um *vetor de tentativas* $v_i \in \{-1, 1\}^n$ (-1 para marcar F e 1 para marcar V). Note que podemos escolher v_i.

Sejam ϵ_i, $1 \leq i \leq m$, a resposta do teste i. Então não é difícil de verificar que $w = \sum_{i=1}^{m} \epsilon_i v_i$ é igual ao vetor formado pela quantidade de acertos menos a quantidade de erros. A ideia é encontrar um conjunto $\{v_1, v_2, \ldots, v_n\}$ de vetores que, dado w, determine os ϵ_is. Isso é o mesmo que dizer que todos os 2^m vetores $\sum_{i=1}^{m} \epsilon_i v_i$ obtidos ao variar os ϵ_is são distintos. Chamaremos de *solúveis* os conjuntos de vetores que satisfazem a essa condição. Note que agora o que queremos fazer é, dada a dimensão n dos vetores, achar conjuntos solúveis com a maior quantidade de elementos possível (que é o nosso m).

3. Trabalhando com funções, parte 1

Agora vamos desenvolver uma técnica que mostra que um conjunto é solúvel, utilizando funções lineares (funções tais que $f(x + y) = f(x) + f(y)$).

Lema 3.1. *Seja $A = \{v_1, v_2, \ldots, v_m\} \in \{-1, 1\}^n$. Se existirem funções $\phi_i : \{-1, 1\}^n \to R$, $1 \leq i \leq m - 1$, tais que*

$$\phi_i(v_i) > |\phi_i(v_{i+1})| + |\phi_i(v_{i+2})| + \cdots + |\phi_i(v_m)| \quad \text{para} \quad i = 1, 2, \ldots, m - 1$$

então A é solúvel.

Demonstração

Essencialmente temos que, em cada função ϕ_i, o vetor v_i "domina" os de índice maior. De fato, aplicando ϕ_1 em $w = \sum_{i=1}^{m} \epsilon_i v_i$, obtemos

$$\phi_1(w) = \epsilon_1 \phi_1(v_1) + \epsilon_2 \phi_1(v_2) + \cdots + \epsilon_m \phi_1(v_m)$$

Como $\phi_1(v_1)$ "domina" os outros termos, temos $\epsilon_1 = \text{sign}(\phi_1(w))$. Definido ϵ_1, é fácil de achar ϵ_2: $\epsilon_2 = \text{sign}(\phi_2(w) - \epsilon_1\phi_2(v_1))$. Isso continua indutivamente até ϵ_{m-1}. Finalmente, para achar ϵ_m basta usar $w = \sum_{i=1}^{m} \epsilon_i v_i$ e isolar ϵ_m. ∎

Agora, mudamos mais uma vez o que queremos: precisamos encontrar as funções lineares!

4. Trabalhando com funções, parte 2

Agora vamos tomar um valor particular de n: $n = 2^k$. Nesse caso, em vez de pensar em vetores de 2^k dimensões vamos pensar em imagens de funções f de $\{-1,1\}^k$ em $\{-1,1\}$ (colocamos as m-uplas $(\pm 1, \pm 1, \ldots, \pm 1)$ em qualquer ordem). Note que ainda temos total liberdade para escolher as 2^k-uplas, já que podemos escolher as imagens das funções como quisermos.

As funções lineares mais naturais agora são somas parciais de valores das funções f. Sendo $A \subset \{1, 2, \ldots, k\}$ um subconjunto de índices, defina $\sigma_A(f)$ a soma das imagens de f com $x_i = 1$ para $i \in A$ (ou seja, todas as coordenadas em A iguais a 1). Sendo mais direto, $\sigma_A(f) = \sum f(x_1, x_2, \ldots, x_k)$ com $x_i = 1$ sempre que $i \in A$. Note que essa soma tem $2^{k-|A|}$ parcelas. Só para simplificar notação, omitiremos as chaves de conjuntos e também definimos $\sigma(f) = \sigma_\emptyset(f)$ como a soma de todas as imagens de f.

Agora citamos alguns fatos (simples) que ficam como exercício:

Lema 4.1. *Utilizando as notações anteriores,*

- *Se f é ímpar em alguma das variáveis (ou seja, $f(x_1, \ldots, -1, \ldots, x_k) = -f(x_1, \ldots, 1, \ldots, x_k)$ para todos x_is), $\sigma(f) = 0$.*
- *Em geral, se f é ímpar em alguma variável fora de A então $\sigma_A(f) = 0$.*
- *$\sigma_A(f)$ é um número par e pode assumir qualquer valor par em $[-2^{k-|A|}, 2^{k-|A|}]$.*

Com isso, estamos prontos para melhorar o resultado do problema original.

Teorema 4.1. $m(2^k) \geq k + (k-1)\binom{k}{1} + (k-2)\binom{k}{2} + \cdots + \binom{k}{k-1} + 1 = k \cdot 2^k + 1$. *Em particular,* $m(16) \geq 33$, *o que mostra que é possível descobrir as respostas com* 16 *tentativas.*

Demonstração

Primeiro, vamos exibir os vetores, que nesse caso são funções.

Sejam $f^k, f^{k-1}, \ldots, f^1$ funções tais que $\sigma(f^i) = 2^i$ para $1 \leq i \leq k$.

Agora, para cada t entre 1 e $k-1$ e cada subconjunto $A \subset \{1, 2, \ldots, k\}$ com $|A| = t$, construa funções ímpares nas variáveis com índice em A, $f_A^1, f_A^2, \ldots, f_A^{k-t}$ tais que $\sigma_A(f_A^i) = 2^i$ para $1 \leq i \leq k-t$. Note que são $(k-t)\binom{k}{t}$ funções.

Enfim, a última função é $f_{1,2,\ldots,k}$ ímpar em todas as variáveis. Veja que isso totaliza os $k \cdot 2^k + 1$ vetores.

Não é difícil verificar que essas funções existem: de fato, supondo sem perda de generalidade $A = \{1, 2, \ldots, t\}$, tome $f(x_1, \ldots, x_k) = (-1)^j g(x_{t+1}, \ldots, x_k)$ em que j é a quantidade de x_is iguais a 1, $1 \leq i \leq t$ e a função g ajusta os valores de $\sigma_A(f_A^i)$, que já vimos que é possível. Esse argumento também vale se $t = k$, só que dispensamos a função g.

Agora, as funções lineares. A escolha é a natural: para f^i considere σ e para f_A^i considere σ_A. Note que não há problemas em escolher funções repetidas e não precisamos de função linear para $f_{1,2,\ldots,k}$.

Vamos ordenar os vetores: a ordem é

$$f^k, f^{k-1}, \ldots, f^1,$$

depois para cada subconjunto A com 1 elemento (não importa a ordem entre os subconjuntos),

$$f_A^{k-1}, f_A^{k-2}, \ldots, f_A^1,$$

e depois sucessivamente para cada subconjunto com $2, 3, \ldots, m-1$ elementos e, por último, $f_{1,2,\ldots,k}$.

Com isso, podemos aplicar nosso primeiro lema. Para isso, note que se $|A| \leq |B|$ e $A \neq B$ então existe um elemento j de B que não está em A e, por isso, $\sigma_A(f_B^i) = 0$, pois f_B^i é ímpar na variável x_j cujo índice está fora de A. Assim, temos

$$\sigma_A(f_A^i) = 2^i > 2^{i-1} + 2^{i-2} + \cdots + 2 = |\sigma_A(f_A^{i-1})| + |\sigma_A(f_A^{i-2})| + \cdots + |\sigma_A(f_A^1)|$$

e como os demais termos são iguais a zero, a hipótese do lema é satisfeita e temos um conjunto solúvel. ∎

5. Generalizando

Conseguimos um bom valor para potências de 2. Como estender essa ideia para os outros valores?

Teorema 5.1. *Para n inteiro positivo, seja $S_2(n)$ a soma dos dígitos de n na base 2. Defina $B(n) = \sum_{i=1}^{n-1} S_2(i)$ como a soma de todos os algarismos na base 2 de 1 até $n-1$. Então*

$$m(n) \geq B(n) + 1.$$

(note que $B(2^k) = k \cdot 2^k$.)

Não daremos uma prova aqui, mas mostraremos como obter, a partir de $m(8) \geq 13$, os resultados correspondentes $m(7) \geq 10$, $m(6) \geq 8$ e $m(5) \geq 6$.

As 13 funções para $n = 8$ são

$$f^3, f^2, f^1, f_1^2, f_1^1, f_2^2, f_2^1, f_3^2, f_3^1, f_{1,2}^1, f_{1,3}^1, f_{2,3}^1, f_{1,2,3}$$

e as 12 funções lineares são

$$\sigma, \sigma, \sigma, \sigma_1, \sigma_1, \sigma_2, \sigma_2, \sigma_3, \sigma_3, \sigma_{1,2}, \sigma_{1,3}, \sigma_{2,3}$$

Considere o ponto $(-1, -1, -1)$ pertencente ao domínio de cada uma das funções f. Entre as funções lineares, ele só foi considerado em σ (de fato, todos os outros σ_A faziam a soma sobre ternas com algum 1 nas coordenadas). Então descartamos o ponto $(-1, -1, -1)$ de todas as funções f, as funções f^i e σ. As restrições g correspondentes são agora vetores de 7 coordenadas:

$$g_1^2, g_1^1, g_2^2, g_2^1, g_3^2, g_3^1, g_{1,2}^1, g_{1,3}^1, g_{2,3}^1, g_{1,2,3}$$

com funções lineares

$$\sigma_1, \sigma_1, \sigma_2, \sigma_2, \sigma_3, \sigma_3, \sigma_{1,2}, \sigma_{1,3}, \sigma_{2,3}$$

Agora, para $n = 6$, considere o ponto $(1, -1, -1)$. Ele só afeta σ_1, então tiramos o ponto $(1, -1, -1)$ as funções g_1^i e obtemos as restrições h

$$h_2^2, h_2^1, h_3^2, h_3^1, h_{1,2}^1, h_{1,3}^1, h_{2,3}^1, h_{1,2,3}$$

e funções lineares

$$\sigma_2, \sigma_2, \sigma_3, \sigma_3, \sigma_{1,2}, \sigma_{1,3}, \sigma_{2,3}$$

Para $n = 5$, consideramos $(-1, 1, -1)$, que afeta somente σ_2. Com isso, obtemos

$$i_3^2, i_3^1, i_{1,2}^1, i_{1,3}, i_{2,3}, i_{1,2,3}$$

e

$$\sigma_3, \sigma_3, \sigma_{1,2}, \sigma_{1,3}, \sigma_{2,3}$$

Para terminar, poderíamos voltar para $n = 4$ usando esse mesmo procedimento, agora no ponto $(1, 1, -1)$. Tiramos esse ponto e σ_3. Mas note que isso é o mesmo que ignorar a variável x_3, e obtemos a mesma construção do primeiro teorema.

Por fim, para notar a conexão entre base 2 e os pontos, veja que

$$7 = (111)_2 \to (-1, -1, -1),\ 6 = (110)_2 \to (1, -1, -1),\ 5 = (101)_2 \to (-1, 1, -1),\ 4 = (100)_2 \to (1, 1, -1)$$

6. Uma abordagem indutiva

Uma ideia que também mostra uma maneira de obter as soluções é a seguinte:

Lema 6.1. *Se $m(k) \geq n$ então $m(2k) \geq 2n+k-1$. Ou seja, se é possível descobrir as respostas de n testes com k tentativas então é possível descobrir as respostas de $2n+k-1$ testes com $2k$ tentativas.*

Demonstração

Primeiro, note que podemos supor sem perda de generalidade que a primeira tentativa em qualquer processo é responder tudo V. Chamaremos essa tentativa de *tentativa base*.

Considere os $2n+k-1$ testes e divida-os em três conjuntos A, B e C com n, n e $k-1$ testes, respectivamente. Por hipótese, sabemos achar as respostas de A ou de B com k tentativas. Sejam $A_1, A_2, \ldots, A_{k-1}$ os conjuntos de testes que mudamos de V para F em relação à tentativa base nas outras $k-1$ tentativas para descobrir as respostas de A; defina $B_1, B_2, \ldots, B_{k-1}$ de modo análogo. Como nunca usamos os resultados anteriores, é possível descobrir os A_is e B_is de antemão. O conjunto C é dividido em $k-1$ conjuntos unitários $C_1, C_2, \ldots, C_{k-1}$.

As $2k$ tentativas são as seguintes:

- A tentativa base;
- Uma tentativa em que trocamos todos os Vs de A para F; com isso, descobrimos quantas respostas V há no conjunto A;
- $k-1$ tentativas "soma" em que trocamos V por F em $A_i \cup B_i \cup C_i$;
- $k-1$ tentativas "diferença" em que trocamos V por F em $(A \setminus A_i) \cup B_i$.

A soma dos resultados das tentativas $A_i \cup B_i \cup C_i$ e $(A \setminus A_i) \cup B_i$ tem a mesma paridade que o que seria tentar $A \cup C_i$ (o B_i "corta" e o A_i "corta" com $A \setminus A_i$, dando A). Mas já sabemos a quantidade de respostas V em A, então é possível determinar a resposta de C_i. Substituindo e "resolvendo o sistema" com $A_i \cup B_i \cup C_i$ e $(A \setminus A_i) \cup B_i$ (lembre que já temos as quantidades de acertos em A e C_i), obtemos os números de acertos em A_i e B_i. Agora, já temos os números de acertos de A e A_i, mas isso nos dá exatamente os resultados das tentativas $A, A_1, \ldots, A_{k-1}$ que determina todas as respostas de A. Falta achar as respostas de B. Mas sabemos da tentativa base e dos resultados de A e C (é só somar os C_is) quantos acertos tivemos em B. Com $B, B_1, \ldots, B_{k-1}$ conseguimos, por hipótese, as respostas de B. Isso completa a demonstração. ∎

Isso dá um resultado melhor que o das seções anteriores? Para potências de 2, o resultado é exatamente o mesmo! E provavelmente para os outros casos também.

7. Trabalhos futuros

Os procedimentos descritos não provam que esses são os melhores valores. De fato, [1] mostra que uma prova com m testes exige pelo menos $1 + \log_{m/2} \binom{m}{m/2}$ tentativas, que é bem menor do que o valor aproximado $m/\log_2 m$ que obtivemos.

Pelo visto, ninguém sabe ao certo a resposta, embora simulações (como relatadas em [1]) não mostrem possíveis melhorias. Fica para você a oportunidade!

8. Referência bibliográfica

[1] Knop, Mednikov, Testes V ou F: com ou sem computador. Revista Educação Matemática, Rússia (artigo em russo), volume 15, 2010.