Matemática Recreativa

Editor
António Machiavelo

Ainda o Totobola[1]

«O singular caso dos 5» (à la Dante Alighieri, em marcha atrás)

António Machiavelo e **Rogério Reis**

Departamentos de *Matemática* e *Ciência dos Computadores*

Faculdade de Ciências da Universidade do Porto

---

1. Introdução

No número anterior, foi apresentado o problema do totobola e algum do seu contexto histórico [MR09]. Mostrou-se como resolver o problema para os casos em que o número de jogos é $3, 4, 13$ (e, em geral, os números da forma $\frac{3^k-1}{2}$) e afirmou-se ser há muito conhecida a solução para o caso 5. Para um inteiro pequeno como o número 5, é difícil imaginar que o problema conduza já ao limiar da intratabilidade computacional. Mas, como mais à frente se verá, o totobola com esta dimensão resiste a um ataque de força bruta, por muito rápidos que sejam os computadores usados e necessita portanto de uma abordagem mais subtil.

Um primeiro majorante pode ser trivialmente obtido à custa da solução para o caso dos quatros jogos (ver Proposição 1 do artigo anterior), com uma «tripla» no quinto jogo, o que conduz a uma solução com 27 chaves.

[1] A escrita deste artigo não resulta de qualquer forma de encomenda, patrocínio ou pressão por parte da Santa Casa da Misericórdia ou da Federação Portuguesa de Futebol.

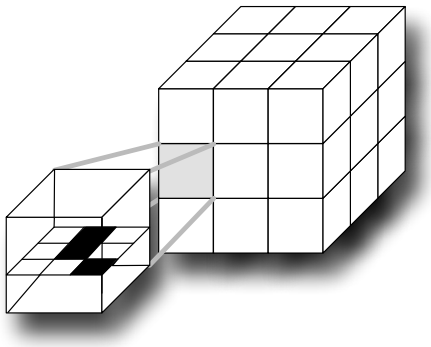
Em 1967, H. J. L. Kamps e J. H. van Lint mostraram em [KL67] que este é, de facto, o mínimo. Pretende-se aqui expôr algumas das ideias centrais dessa demonstração, não seguindo à letra o percurso desse artigo, que não é de fácil leitura, mas optando por alguns argumentos alternativos que nos parecem mais claros e um pouco mais elegantes. Limitar-nos-emos a pormenorizar a dedução da inexistência de uma cobertura com 25 chaves, deixando o caso restante, para o qual as técnicas aqui introduzidas são suficientes, para o leitor mais aventuroso.

Esta exposição não tem apenas um interesse histórico. Na nossa opinião, o processo de solução de instâncias de maior dimensão do problema do totobola assentará em técnicas similares às que aqui apresentamos.

2. O problema da visualização (do problema)

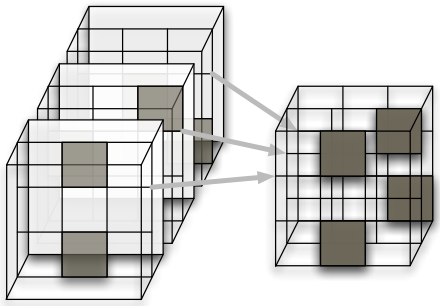
A primeira grande dificuldade, antes mesmo de poder atacar o problema, é encontrar um bom modelo de visualização no qual seja cómodo trabalhar, dado que o caso dos 5 jogos reside naturalmente num espaço de dimensão 5.

Imaginemos um cubo $3 \times 3 \times 3$ formado por 27 pequenos cubos (tal como o cubo de Rubik), em que cada pequeno cubo contém um plano 3×3 constituído por 9 células. A cada célula estão associadas, portanto, cinco coordenadas com valores 1, 2 ou 3: as três coordenadas no cubo, mais as duas no plano em que ela se encontra. Uma célula corresponde assim a uma chave do totobola com 5 jogos.



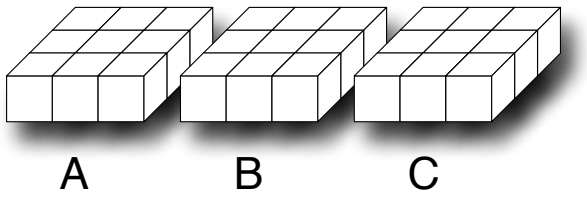
Cada célula (ou seja, chave) cobre, no sentido de garantir pelo menos quatro resultados certos, para além dela própria, todas as células que dela diferem numa única coordenada. Assim, cobre 5 células no plano onde reside e, para cada uma das direcções dos 3 eixos coordenados, 2 células em cada um dos outros dois cubos dessa direcção.

Será por vezes útil considerar outros cubos, estes formados pelos 3 planos que partilham 2 coordenadas no grande cubo, que designaremos por *pilhas*.



A vantagem deste modelo de células em planos dentro de pequenos cubos que constituem um grande cubo $3 \times 3 \times 3$ é a de, reorientando os planos dentro dos seus cubos, podermos executar a construção destas pilhas de 3 modos diferentes.

Será também útil considerar o corte do grande cubo em 3 fatias e dispô-los horizontalmente como sugere a figura seguinte.



Estas fatias serão denotadas A, B, C por forma a poder referir os planos pelo conjunto de coordenadas ilustrado na figura seguinte.

A_{11}	A_{12}	A_{13}
A_{21}	A_{22}	A_{23}
A_{31}	A_{32}	A_{33}

B_{11}	B_{12}	B_{13}
B_{21}	B_{22}	B_{23}
B_{31}	B_{32}	B_{33}

C_{11}	C_{12}	C_{13}
C_{21}	C_{22}	C_{23}
C_{31}	C_{32}	C_{33}

3. Olhando de cima, de frente ou de lado

Por *cobertura* entenda-se um conjunto de células (chaves) que garante pelo menos 4 (em 5) resultados certos. Nesta secção consideramos as estruturas formadas pelas pilhas numa determinada direcção.

Proposição 1 *Seja C uma cobertura com t células, e seja x o número de células dessa cobertura numa certa pilha, X. Sejam a (respectivamente b)*

o número de células de C nas restantes pilhas da mesma linha (respectivamente, da mesma coluna), e seja $c = t - a - b - x$, o número de células no «antagonista» de X (as que não estão nem na mesma linha, nem na mesma coluna).

x	a
b	c

Tem-se:

$$\begin{aligned} a + b &\geq 27 - 7x \\ c &\leq 6x - (27 - t)\,. \end{aligned}$$

Demonstração. A primeira desigualdade resulta facilmente do facto de cada elemento de C em X cobrir 7 células dessa mesma pilha, e portanto ficarem por cobrir pelo menos $27 - 7x$, que têm de ser cobertas pelas células das restantes pilhas dessa linha e coluna.

A segunda desigualdade resulta imediatamente da primeira e da definição de c. □

Proposição 2 *Dada uma cobertura com t células, cada linha ou coluna de pilhas contém pelo menos $\dfrac{81 - t}{8}$ células dessa cobertura.*

Demonstração. Denote-se o número de células em cada uma das pilhas da seguinte forma:

x	a	b
y	c	d
z	e	f

Da segunda desigualdade do lema anterior, obtém-se

$$\begin{aligned} c + d + e + f &\leq 6x - (27 - t) \\ a + b + e + f &\leq 6y - (27 - t) \\ a + b + c + d &\leq 6z - (27 - t)\,. \end{aligned}$$

Adicionando estas três desigualdades, tem-se

$$2(t - (x + y + z)) \leq 6(x + y + z) - 3\,(27 - t)\,,$$

de onde resulta o que se afirmou. □

Proposição 3 *Dada uma cobertura com t células, cada diagonal generalizada de pilhas (um conjunto de três pilhas que não partilham nenhuma coordenada) tem de conter pelo menos*

$$\frac{81-2t}{5}$$

células dessa cobertura.

Demonstração. Considere-se a seguinte situação

a	x	b
y	c	d
e	f	z

Pela Proposição 1 tem-se

$$\begin{aligned} y+d+e+z &\leq 6x-(27-t) \\ x+b+f+z &\leq 6y-(27-t) \\ x+a+c+y &\leq 6z-(27-t)\,. \end{aligned}$$

Adicionando estas três desigualdades, obtém-se

$$(x+y+z)+t \leq 6(x+y+z)-3\,(27-t)\,,$$

de onde resulta facilmente a observação feita no enunciado. □

4. Breve visita ao Paraíso

Os três resultados da secção anterior permitem diminuir drasticamente o conjunto de hipóteses a considerar, por forma a que seja tratável computacionalmente o problema de mostrar a impossibilidade de existência soluções com menos de 26 chaves.

Suponhamos então que temos uma cobertura C com 25, ou menos, chaves. Das proposições da secção anterior resulta que:

- O antagonista de uma pilha com x chaves tem no máximo $6x-2$ chaves, enquanto que nas outras pilhas da mesma linha e nas da mesma coluna dessa pilha estão pelo menos $27-7x$ chaves.
- Cada linha, cada coluna e cada diagonal generalizada de pilhas tem pelo menos 7 chaves.

Em particular tem-se:

0	a
b	≤ -2

com $a + b \geq 27$,

1	a
b	≤ 4

com $a + b \geq 20$,

2	a
b	≤ 10

com $a + b \geq 13$,

de onde se conclui imediatamente que todas as pilhas devem conter pelo menos um elemento de C. Mais ainda, se uma pilha tem apenas uma única chave, então tem-se, a menos das simetrias óbvias, a situação seguinte:

1	a	b
c	1	1
d	1	1

Mas daqui resulta que $a + c \leq 2$ e $b + d \leq 2$. Isto implicaria $|C| \leq 9$, o que é manifestamente insuficiente.

Assim se conclui que cada pilha têm necessariamente pelo menos duas chaves. Portanto é agora fácil de ver que se tem, a menos de simetria,

2	a	b
c	d	e
f	g	2

com $a, b, c, d, e, f, g \geq 2$, e

$$\begin{aligned} a+b+c+e &\geq 13 \\ b+e+f+g &\geq 13 \\ a+c+d &\leq 8 \\ d+e+g &\leq 8. \end{aligned}$$

Mas, usando o minorante acima obtido para as diagonais generalizadas, obtém-se $d \geq 3$, $e+g \geq 5$ e $a+c \geq 5$, o que, juntamente com as duas últimas desiguladades, permite concluir que

$$d = 3, \quad e + g = 5, \quad a + c = 5, \quad \text{e portanto} \quad b + f = 8.$$

Agora não é difícil concluir o resultado seguinte.

Proposição 4 *Se houver uma cobertura com* 25 *chaves para o totobola com* 5 *jogos, o número de células das pilhas numa qualquer direcção é*

3	2	3
2	5	2
3	2	3

a menos de permutações de linhas ou colunas.

Demonstração. Deixada como exercício (fácil) para o leitor. □

5. Um resultado subtil

Kamps e Lint provaram o seguinte resultado, que desempenha um papel não trivial na eliminação de um grande número casos que, de outra forma, teriam de ser considerados.

Proposição 5 *Se uma cobertura C tiver uma pilha que tem dois planos sem nenhuma célula e outro com duas células dessa cobertura, então $|C| \geq 27$.*

Demonstração. Suponhamos, então, que se tem uma tal cobertura

0	0	2
a_1	b_1	c_1
a_2	b_2	c_2

a_3	b_3	c_3
e_1	e_3	d_1
e_2	e_4	d_2

a_4	b_4	c_4
e_5	e_7	d_3
e_6	e_8	d_4

onde cada símbolo literal representa o número de chaves do respectivo plano. Usando o facto de que cada plano tem 9 células e que uma chave exterior a esse plano cobre no máximo uma dessas células, enquanto que duas interiores deixam pelo menos uma a descoberto, deduz-se que $\sum_{i=1}^{4} a_i \geq 7$, $\sum_{i=1}^{4} b_i \geq 7$ e $\sum_{i=1}^{4} c_i \geq 1$.

Faça-se $\sum_{i=1}^{4} (a_i + b_i) + \sum_{i=1}^{8} e_i = 14 + x$, $\sum_{i=1}^{4} (c_i + d_i) = 1 + y$. Tem-se que $\sum_{i=1}^{8} e_i \leq x$, $\sum_{i=1}^{4} d_i \leq y$. Seja agora E o conjunto constituído pelas células dos planos marcados com algum e_i na figura anterior. O número de células cobertas em E, pela cobertura que está a ser considerada, é igual a

$$7 \sum_{i=1}^{8} e_i + 2 \sum_{i=1}^{4} (a_i + b_i + d_i) = 5 \sum_{i=1}^{8} e_i + 2 \left(\sum_{i=1}^{4} (a_i + b_i) + \sum_{i=1}^{8} e_i + \sum_{i=1}^{4} d_i \right),$$

que é portanto menor ou igual a $2y + 28 + 7x$. Conclui-se assim que

$$2y + 28 + 7x \geq 8 \times 9 = 72.$$

Portanto, $7(x + y) \geq 44 + 5y$. Mas como uma linha ou coluna de planos, ou seja uma pilha, tem pelo menos 7 células da cobertura, resulta que $y \geq 4$, e portanto $x + y \geq 10$. Conclui-se assim que o número de células da cobertura, que é igual a $17 + x + y$, é pelo menos 27. □

6. Descida ao Purgatório

A Proposição 4 permite supor, sem perda de generalidade, que se tem

	2	3	3
2			
3			
3			

5			
2			
2			

2			
3			
3			

Há dois casos a considerar: $|A_{11}| = 0$ ou $|A_{11}| = 1$.

Primeiro, o segundo caso

De $|A_{11}| = 1$, resulta imediatamente e sem perda de generalidade que $|A_{12}| = |A_{21}| = 0, |A_{13}| = |A_{31}| = 1$. Como o plano A_{21} tem de ser coberto por 9 chaves «externas», conclui-se facilmente que o plano C_{21} tem pelo menos 3 chaves, uma vez que, pela Proposição 5, o plano B_{21} não tem mais do que uma chave. Mas como a segunda linha de planos de C não pode ter mais do que 3 chaves, resulta

	2	3	3
2	1	0	1
3	0		
3	1		

5			
2	1		
2			

2			
3	3	0	0
3			

Da Proposição 4 resulta que a única coluna de C que pode eventualmente ter 5 chaves é a primeira, e portanto a segunda e terceira colunas de C têm no máximo 3 chaves. Mas então, de $|C_{22}| = |C_{23}| = 0$ e como a segunda linha de B tem necessariamente um 0, deduz-se que na segunda linha de A tem de haver um 2 e um 3, o que contradiz o facto dessa linha ter 3 elementos.

Por último, o primeiro caso

Agora, se $|A_{11}| = 0$, pela Proposição 5, tem-se então

	2	3	3
2	0	1	1
3	1		
3	1		

5			
2			
2			

2			
3			
3			

Como $|C_{11}| \leq 1$, tem-se $|B_{11}| \geq 4$, o que conduz aos dois subcasos seguintes:

O primeiro subcaso: $|B_{11}| = 4$

Nesta situação, tem-se, sem qualquer perda de generalidade

	2	3	3
2	0	1	1
3	1		
3	1		

	5	2	2
5	4	1	0
2			
2			

2	1	ε	δ
3			
3			

com $\varepsilon = 0, \delta = 1$, ou vice-versa. Indiferentemente daquele que seja igual a 0, o facto de o plano correpondente ter de ser coberto por 9 chaves exteriores implica que a correspondente coluna de C tem de ter pelo menos 5 células, o que contradiz a Proposição 5.

O segundo, e último, subcaso: $|B_{11}| = 5$

Estamos pois reduzidos a mostrar que esta situação não é possível. Neste caso tem-se que $|B_{12}| = |B_{13}| = 0$, de onde se deduz facilmente que $|C_{12}| = |C_{13}| = 1$.

	2	3	3
2	0	1	1
3	1		
3	1		

	5	2	2
5	5	0	0
2	0	1	1
2	0	1	1

2	0	1	1
3			
3			

Observe-se, agora, que tanto C_{12} como C_{13} necessitam de 4 chaves exteriores de modo a que fiquem cobertas as suas células. Tal implica pelo menos mais duas chaves nas colunas correspondentes. Portanto, tem-se

	2	3	3
2	0	1	1
3			
3			

	5	2	2
5	5	0	0
2	0	1	1
2	0	1	1

	2	3	3
2	0	1	1
3	1		
3	1		

Este é o caso mais delicado de analisar, e implica uma descida de nível.

7. A descida ao Inferno

Para lidar com este último caso, designem-se as 9 posições de cada plano por $a, b, c, d, e, f, g, h, i$ numa ordem que será dada pela suposta cobertura com 25 chaves, de um modo que passamos a especificar. Comece-se por observar

e	a	d
i	f	h
g	c	b

Figura 1: Uma possível atribuição de nomes às células de um plano (não necessariamente pela ordem certa)

que, na situação em análise, o plano A_{11} é exactamente coberto por 9 chaves exteriores a ele, e portanto não pode haver duas dessas chaves que estejam localizadas na mesma posição relativa, no seu próprio plano. Chamemos *crítico* a um plano nestas condições. Assim, faz sentido determinar a, b, c, d como sendo as posições onde estão localizadas as chaves em A_{12}, A_{13}, A_{21}, A_{23}, respectivamente, e sejam e, f, g, h, i as posições onde estão localizadas as cinco chaves de B_{11}, numa qualquer ordem. Esquematicamente, temos, para já:

0	a	b
c		
d		

$\begin{smallmatrix} efg \\ hi \end{smallmatrix}$		
0	0	0
0	1	1
0	1	1

0	1	1
1		
1		

Usando agora o facto de B_{12} e B_{21} serem ambos críticos, conclui-se que a chave em B_{22} tem que estar na posição b ou d. Procedendo do mesmo modo para os outros planos de B com uma só célula, conclui-se que

0	a	b
c		
d		

$\begin{smallmatrix} efg \\ hi \end{smallmatrix}$		
0	0	0
0	$b \vee d$	$a \vee d$
0	$b \vee c$	$a \vee c$

0	1	1
1		
1		

Por simetria, pode-se supor, sem perder generalidade, que a chave de B_{22} está em b. Mas então tem-se, novamente usando o facto dos vários planos de B com valor 0 serem críticos:

0	a	b
c		
d		

$\begin{smallmatrix} efg \\ hi \end{smallmatrix}$		
0	0	0
0	b	d
0	c	a

0	1	1
1		
1		

Mas o plano A_{12} também é crítico no sentido de os seus pontos serem cobertos uma e uma só vez, seja pela sua única chave, que cobre 5 pontos, seja pelos pontos exteriores. Resulta que b não pode pertencer à vizinhaça (no sentido de Hamming) de a. Por outro lado, os planos de B com uma só chave também são críticos (*porquê?*), e por conseguinte tanto c como d também não pertencem à vizinhança da a. Portanto, ou c ou d pertencem à vizinhança de b. Mas de B resulta que nenhuma destas situações é possível. Fica assim concluída a demonstração de que não há uma cobertura com 25 chaves para o totobola com 5 jogos.

8. Em conclusão

Para quê todo este «trabalho» para provar que uma aposta com 25 chaves não pode garantir quatro resultados certos? ... E ainda temos que proceder a um processo (potencialmente) ainda mais mais complexo, para eliminar a hipótese da existência de uma aposta com 26 chaves nas mesma condicões! Porque não usar um computador que rapidamente teste todas essas apostas eliminando, sem esforço, a possibilidade de existir uma solução de tamanho menor que 27?

O número de possíveis chaves é, para este caso de 5 jogos, 3^5, pelo que o número de possíveis apostas de 25 ou 26 chaves é

$$\binom{3^5}{25} + \binom{3^5}{26} \approx 2^{116}.$$

Ora mesmo que tomemos computadores mais rápidos do que hoje já conseguimos construir, e suponhamos que a geração e teste de cada chave se pode fazer numa só instrução do CPU (o que é uma suposição muito, muito optimista), e que conseguimos um milhão de computadores para resolver este problema, mesmo assim necessitamos de 100 vezes a estimativa actual do tempo que decorreu desde o *Big-Bang*, para garantir que a aposta tem que ter comprimento 27.

Mas, argumentarão alguns, o engenho humano é indomitável e no futuro computadores muito mais rápidos poderão fazer os mais complicados cálculos num abrir e fechar de olhos. Pois assim será, mas existem limites termodinâmicos insuperáveis com que esses cálculos esbarrariam. Como consequência da Segunda Lei da Termodinâmica, há um mínimo de energia necessária para mudar o estado de cada bit. Para mudar um estado de um simples bit, um sistema ideal, consome uma energia correspondente a kT, em que T é a temperatura absoluta do sistema e k a chamada constante de Boltzman.

Como $k = 1{,}38 \times 10^{-61}$ erg/K, mesmo que coloquemos o nosso computador à temperatura média do Universo, 3,2K, gastamos $4{,}4 \times 10^{-16}$ erg de cada vez que temos que «apagar» um bit. A energia irradiada total média do Sol é de $1{,}21 \times 10^{41}$ erg/ano, ou seja o suficiente para alimentar $2{,}7 \times 10^{56}$ mudanças de um bit. Portanto, nesse computador ideal gastaríamos toda a energia do Sol para «contar» de 0 a 2^{188}. Mesmo que construamos uma esfera de Dyson à volta do Sol, e com ela captemos toda a sua energia durante 32 anos, o que iria dificultar significativamente a vida no nosso planeta, não teríamos energia para contar para lá de 2^{220}. Esta não é uma limitação que dependa da evolução tecnológica, é uma limitação termodinâmica incontornável[2].

Para o problema do totobola com 6 jogos, é conhecida uma solução com 73 chaves, mas não se sabe se há alguma com 71 ou 72 [LMT09]. Para testar automáticamente estas hipóteses, ter-se-ia que percorrer

$$\binom{3^6}{71} + \binom{3^6}{72} \approx 2^{335}$$

chaves, que como é claro, pelo que se disse antes, está para lá da mais delirante das expectativas de tratabilidade computacional, seja qual for a velocidade dos computadores futuros.

O raciocínio aqui apresentado, para o caso dos 5 jogos, à luz destas limitações, deve servir de exemplo de como o poder da dedução é a única arma que dispomos para problemas como este, em que a explosão combinatória se manifesta de forma tão exuberante, mesmo para o caso de uma dimensão tão aparentemente inocente como 6.

Referências

[KL67] H. J. L. Kamps, J. H. van Lint, *The Football Pool Problem for* 5 *Matches*, Journal of Combinatorial Theory **3** (1967) 315–325.

[LMT09] J. Linderoth, F. Margot, G. Thain, *Improving Bounds on the Football Pool Problem via Symmetry Reduction and High-Throughput Computing*, INFORMS Journal on Computing 21 (2009), 445-457.

[MR09] A. Machiavelo, R. Reis, *O Problema do Totobola*, Boletim da SPM **61** (2009) 39–45.

[Sch96] Bruce Schneier, *Applied Cryptography*, John Wiley & Sons, 1996.

[2]Esta ideia de estabelecer uma comparação entre limites termodinâmicos da computação e a energia disponível do Sol é de Bruce Schneier [Sch96].