Loterias Esportivas e Códigos

Marcelo Firer

Novembro de 2000

Quando de seu lançamento na década de 70, a Loteria Esportiva despertava o imaginário coletivo com contos de fada sobre o enriquecimento instantâneo de personagens até então anônimos e histórias de terror sobre o esfacelamento da vida social e afetiva destes mesmos protagonistas.

Embora um tanto decadente, os prêmios oferecidos pelo Loteria Esportiva ainda são vultosos o suficiente para muitos exercícios de imaginação e sonhos de fazer os treze pontos. Vou logo advertindo o leitor que este artigo não deve ajuda-lo a ganhar na loteria, mesmo porque nele, faço uma simplificação não admitida pelo mundo da bola: ignoro resultados, ignoro os times e juízes; olhamos os jogos como simples pontos indistinguiveis, sem paixão, sem favoritismos. Mais ainda, as estratégias encontradas aplicam-se a loterias imaginárias.

Vamos tentar olhar a Loteria Esportiva e outras possíveis loterias baseadas no mesmo princípio, sob o prisma da Teoria de Códigos Corretores de Erros. Utilizando apenas os conceitos básicos da teoria, vamos buscar estratégias para otimizar o jogo na loteria esportiva. Apesar destas estratégias não poderem ser úteis para se ganahr na Loteria Esportiva (aquela da Caixa Econômica Federal), podemos oferecer um lucro de outra natureza: um primeiro contato com códigos corretores de erros, uma teoria fértil, com muitas ramificações em matemática e diversas aplicações em engenharia.

1 Para que Códigos?

Em inúmeras situações, não podemos transmitir informações *in natura*, do modo como são geradas e compreendidas, devido ao canal de transmissão. O processo de projeção de um filme no cinema, por exemplo, preserva a natureza da imagem, pois o projetor nada mais faz que iluminar e amplificar (através de facho de luz e das lentes) a informação contida na película,

imagens gravadas no celulóide. Se porventura o projetor estiver quebrado, podemos ver o filme colocando a película contra um facho de luz, pois a informação contida na obra está contida na película em sua forma natural, na forma de imagens. Este mesmo filme pode ser armazenado em uma fita magnética (vídeo), de uma forma codificada: Não adianta colocarmos a película do vídeo sob um facho de luz, pois precisamos de algum aparelho que decodifique seu sinal. Algo semelhante ocorre em transmissões via satélite, comunicação digital e muitos outros canais, de uso cada vez mais intenso. Um dos principais problemas existente na transmissão de informação codificada (não confundir com criptografada) é a existência de interferências de diversas naturezas que causam erros de transmissão: a informação recebida não é a informação transmitida.

Os Códigos Corretores de Erro foram criados na década de 40 por Claude Shanon para tratar com os problemas acarretados pelas interferências (ruídos) dos canais de transmissão: como detectar a existência de erros e como corrigi-los.

Começemos então com o trabalho propriamente dito, estudando a principal família de códigos

2 Códigos Corretores de Erro

Vamos apresentar alguns conceitos realmente básicos da Teoria de Códigos Corretores de Erros. Ao leitor que se interessar pelo assunto e quiser aprender algo mais, recomendamos o livro de L.F. Voloch ([Vo]), uma introdução simples e bastante suscinta ao tema. Se depois disto o leitor quiser se aprofundar no assunto, a referência inevitável é o livro enciclopédico de MacWilliams e Sloane ([MS]), que contém tudo o que vamos apresentar aqui (e quase tudo relacionado a esta teoria).

O conhecimento necessário para compreender os conceitos deste trabalho é bastante elementar (para quem já viu alguma vez na vida): as operações aritméticas nos corpos finitos $\mathbb{F}_q$ e rudimentos de álgebra linear sobre estes corpos. Como os conceitos que vamos usar de álgebra linear são bastante elementares, tudo o que foi visto em um curso regular de álgebra linear (sobre os reais ou complexos) aplica-se também quando estudamos espaços vetoriais sobre corpos finitos. Mais ainda, quase todas as demonstrações que encontramos em um livro didático qualquer de álgebra linear podem ser generalizadas apenas trocando os termos "$\mathbb{R}$ ou $\mathbb{C}$" por "K um corpo qualquer".

No entanto, caso você sinta-se inseguro com estas definições (e para

evitar que precise buscar alguma bibliografia auxiliar), pense em $\mathbb{F}_q$ como o conjunto dos símbolos $\left\{\overline{0}, \overline{1}, ..., \overline{q-1}\right\}$ com duas operações, a soma e o produto. Para somarmos $\overline{x}$ e $\overline{y}$, fazemos a soma usual $x+y$, dividimos esta pelo primo q e obtemos um resto inteiro r entre 0 e $q-1$. Dizemos então que $\overline{r} = \overline{x} + \overline{y}$. O produto $\overline{x} \cdot \overline{y}$ é definido de modo similar: fazemos o produto usual $x \cdot y$, dividimos por q, obtemos um resto r e definimos $\overline{r} = \overline{x} + \overline{y}$. Para sanar qualquer dúvida, vamos apresentar as tabelas com a soma e o produto em $\mathbb{F}_2$ e $\mathbb{F}_3$, os únicos casos que vamos realmente considerar neste trabalho.

$\mathbb{F}_2$;

$+$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$

$\cdot$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$

$\mathbb{F}_3$;

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$

Conhecendo as operações, fica fácil pensarmos em espaços vetoriais sobre corpos finitos: pense $\mathbb{F}_q^n$ como o conjunto das enuplas $(\overline{x}_1, ..., \overline{x}_n)$ com cada coordenada $\overline{x}_i \in \mathbb{F}_q$. Estes são os vetores de $\mathbb{F}_q^n$. Soma-se dois vetores somando-se as coordenadas duas a duas

$$(\overline{x}_1, ..., \overline{x}_n) + (\overline{y}_1, ..., \overline{y}_n) = (\overline{x}_1 + \overline{y}_1, ..., \overline{x}_n + \overline{y}_n),$$

e multiplica-se um vetor $(\overline{x}_1, ..., \overline{x}_n)$ por um escalar $\overline{\lambda} \in \mathbb{F}_q$ multiplicando-se cada uma das coordenadas

$$\overline{\lambda}\,(\overline{x}_1, ..., \overline{x}_n) = \left(\overline{\lambda} \cdot \overline{x}_1, ..., \overline{\lambda} \cdot \overline{x}_n\right).$$

Podemos com isto começar a falar dos códigos propriamente ditos. Suponha que nosso canal de transmissão possa transmitir exatamente q sinais distintos. Vamos chamar este conjunto de sinais de *alfabeto*, cada sinal sendo uma *letra* do alfabeto. Frequentemente $q = 2$ e vamos sempre assumir que q seja primo.

Vamos denotar por $\mathbb{F}_q$ o corpo finito com q-elementos, de modo que temos uma identificação bijetora entre nosso alfabeto e o corpo dado. Se considerarmos o espaço vetorial $\mathbb{F}_q^n$, podemos construir um *vocabulário* com até q^n palavras: a cada elemento $x = (x_1, x_2, ..., x_n) \in \mathbb{F}_q^n$ pode ser atribuido

um significado, e temos um código: buscamos o elemento $x \in \mathbb{F}_q^n$ que expressa o significado desejado (codificação), transmitimos a informação (as coordenadas de x) e aquele que a recebe (pessoa ou equipamento) olha na tabela de significados para dar sentido à mensagem (decodificação).

No entanto, todo canal de comunicação possui algum tipo de ruído que causa erros na transmissão, de modo que o sinal transmitido $x = (x_1, x_2, ..., x_n)$ e o sinal recebido $y = (y_1, y_2, ..., y_n)$ não são necessariamente iguais.

Se todos os elementos de $\mathbb{F}_q^n$ forem palavras do meu código, não poderemos nem ao menos detectar a existência de erros (não se esqueça, estamos tratando de linguagens sem semântica). Para tratarmos deste tipo de problema necessitamos introduzir mecanismos de controle, o que, no nosso caso, é feito pelos códigos linares.

Um $[n, d; q]$-*código linear* é um subespaço vetorial d-dimensional $\mathcal{C}$ de $\mathbb{F}_q^n$ (com $d \leq n$). As palavras do nosso código são os q^d elementos de $\mathcal{C}$. Temos diversos modos de descrever o sub-espaço $\mathcal{C}$. Podemos descrevê-lo exibindo uma base ou como o núcleo de uma transformação linear : $\mathbb{F}_q^n \to \mathbb{F}_q^{n-d}$. Tal transformação é representada por uma matriz $H = (h_{ij})_{(n-d)\times n}$, que neste contexto é chamada de *matriz de controle de paridade*: um elemento $x \in \mathbb{F}_q^n$ pertence a $\mathcal{C}$ se e somente se

$$Hx^T = \begin{pmatrix} h_{11} & h_{12} & ... & h_{1n} \\ \vdots & \vdots & \vdots & \vdots \\ h_{(n-d)1} & h_{(n-d)2} & ... & h_{(n-d)n} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Assumimos que $d < n$ e observamos que de imediato, temos um modo (falível mas razoável) para detectar erros. Ao recebermos uma palavra $y = (y_1, ..., y_n)$ basta fazer o produto Hy^T e temos certeza de haver algum erro se tivermos $Hy^T \neq 0$. Observamos também que temos de imediato um custo para esta capacidade de detecção de erros, pois ao invés de transmitirmos apenas as d-coordenadas de um ponto (relativa a uma base de $\mathcal{C}$), temos que transmitir n, de modo que temos $n - d$ *coordenadas de controle*. Este é o embate natural entre interesses opostos na teoria de códigos: o aumento na capacidade de detectar e corrigir erros versus o aumento de custo, representado pela *taxa de informação* n/d.

Já conseguimos tocar na questão de detecção de erro, mas para falarmos sobre correção precisamos saber "o quanto " uma informação está errada. Para isto, consideramos a *norma de Hamming* em $\mathbb{F}_q^n$, $|x|_H$ = número de coordenadas não nulas de x. Como toda norma, esta define uma distância:

$d_H(x,y) = |x-y|_H$. Temos então que se transmitirmos a palavra x e recebermos a palavra y, a distância de Hamming $d_H(x,y)$ é exatamente o número de erros que ocorreu no processo de transmissão.

A distância de Hamming admite um fenômeno extremamente interessante para o desenvolvimento de uma teoria de códigos: subespaços distintos podem ter distâncias distintas entre seus pontos. Consideremos por exemplo o espaço $\mathbb{F}_2^4$. Os conjuntos

$$\begin{aligned} V_1 &= \{(0,0,0,0),(1,0,0,0)\}, \quad V_2 = \{(0,0,0,0),(1,1,0,0)\}, \\ & V_3 = \{(0,0,0,0),(1,1,1,0)\}, \quad V_4 = \{(0,0,0,0),(1,1,1,1)\}, \end{aligned}$$

são todos subespaços unidimensionais, mas os vetores de cada um destes subespaços estão a distância distinta um do outro, variando em ordem crescente de 1 a 4.

Este fenômeno é quantificado pelo conceito de *distância mínima* ou *peso* de um código $\mathcal{C}$, definido como $W(\mathcal{C}) = \min\{d_H(x,y) \,|x,y \in \mathcal{C}\}$. Sendo $\mathcal{C}$ subespaço vetorial, temos que $x-y \in \mathcal{C}$ sempre que $x,y \in \mathcal{C}$, de modo que $W(\mathcal{C}) = \min\{|x|_H \,|x \in \mathcal{C}\}$.

A capacidade de detecção e correção de um código está intimamente relacionada à distância mínima do código. Estamos supondo que a pertubação de nosso canal é gaussiana, ou seja, a cada letra transmitida tenho a mesma probabilidade de ter algum erro e ésta é menor que $1/2$ (do contrário, minha linha de transmissão não é confiável, para usarmos um eufemismo). Como cada palavra de meu código tem n letras (a dimensão do espaço ambiente $\mathbb{F}_q^n$), estamos querendo dizer que a probabilidade de recebermos exatamente $m+1$ letras erradas é menor que a de recebermos m letras erradas.

Se considerarmos

$$e = \left[\frac{W(\mathcal{C})-1}{2}\right] = \text{a parte inteira de } \frac{W(\mathcal{C})-1}{2},$$

temos que, dado um ponto qualquer $z \in \mathbb{F}_q^n$, existe no máximo um ponto $x \in \mathcal{C}$ com $d_H(x,z) \leq e$. De fato, suponha que existam $x,y \in \mathcal{C}$ com $d_H(x,z) \leq e$ e $d_H(y,z) \leq e$. Temos então, pela desigualdade triangular que

$$\begin{aligned} d_H(x,y) &\leq d_H(x,z) + d_H(z,x) \\ &\leq e+e \\ &= W(\mathcal{C})-1 \end{aligned}$$

contradizendo a minimalidade de $W(\mathcal{C})$.

Vamos então supor que estamos trabalhando com um $[n,d;q]$-código e que este tenha distância mínima $W = W(\mathcal{C})$. Transmitimos uma mensagem,

digamos $x = (x_1, x_2, ..., x_n)$ e recebemos uma mensagem, eventualmente errada, digamos $y = (y_1, y_2, ..., y_n)$. Vamos supor que o número de erros seja menor que W. Temos então que o número de de erros, ou seja, o número de coordenadas erradas é dado por

$$d_H(x, y) = |x - y|_H .$$

Vamos supor, como hipótese adicional, que o numero de erros é menor que e, ou seja,

$$d_H(x, y) \leq e = \left[\frac{W(\mathcal{C}) - 1}{2}\right].$$

Temos então que podemos recuperar o ponto originalmente transmitido x: este é o ponto de $\mathcal{C}$ mais próximo da mensagem recebida y, o único ponto de $\mathcal{C}$ cuja distância a y é menor ou igual a e.

Vamos tentar descrever a situação geometricamente. Dado um ponto $x \in \mathbb{F}_q^n$ e $r \geq 0$ (na realidade, basta considerarmos r natural), a bola (fechada) de centro x e raio r é o conjunto

$$B_r(x) = \left\{y \in \mathbb{F}_q^n \,|\, d_H(x, y) \leq r\right\}.$$

Obviamente, para qualquer $x \in \mathbb{F}_q^n$, $B_0(x) = \{x\}$ e $B_n(x) = \mathbb{F}_q^n$. Ao tomarmos $e = \left[\frac{W(\mathcal{C})-1}{2}\right]$, temos que a família $\{B_e(x) \,|\, x \in \mathcal{C}\}$ das bolas em $\mathbb{F}_q^n$, centradas em pontos de $\mathcal{C}$ e de raio e são todas disjuntas. Assim, se a mensagem recebida y contiver no máximo e erros, temos que y pertence a uma destas bolas, $B_e(x)$, e corrigimos o erro de transmissão substituindo y por x, o centro da bola que o contém.

Se x for a mensagem transmitida e a mensagem recebida y tiver mais do que e erros, podem ocorrer duas situações: ou y não pertence a qualquer uma das bolas da família $\{B_e(x) \,|\, x \in \mathcal{C}\}$ ou então $y \in B_e(z)$, com $z \neq x$. No primeiro caso não sabemos (ao menos no ponto em que nos encontramos) como proceder; no segundo caso, interpretaremos a mensagem de modo errado, atribuindo o valor equivocado z. No entanto, sob condições razoáveis (em que o erro é considerado aleatório), a probabilidade de ocorrermos neste tipo de equívoco é relativamente pequena, e sob o ponto de vista de aplicações práticas, pode-se ajustar os parâmetros envolvidos (n, d, q e e) de modo a se conviver com os erros incorrigíveis sem grandes prejuízos à aolicação.

Vamos considerar dois exemplos.

Exemplo: Consideremos $q = 2, n = 4$ e $d = 1$. Vamos considerar o melhor

$[4,1;2]$ código possível, o código

$$\mathcal{C}_1 = \{(0,0,0,0),(1,1,1,1)\}.$$

Obtemos então que $W(\mathcal{C}_1) = 4$ e $e = \left[\frac{4-1}{2}\right] = 1$. Temos então as bolas

$$\begin{aligned} B_1((0,0,0,0)) &= \{(0,0,0,0),(1,0,0,0),(0,1,0,0),(0,0,1,0),(0,0,0,1)\} \\ B_1((1,1,1,1)) &= \{(1,1,1,1),(0,1,1,1),(1,0,1,1),(1,1,0,1),(1,1,1,0)\} \end{aligned}$$

Observe que ambas as bolas são disjuntas e contém, cada uma delas 5 pontos de $\mathbb{F}_2^4$. Temos então que $6 = 2^4 - 2\cdot 5$ pontos para os quais não são cobertos por qualquer uma das bolas, pontos para os quais não sabemos decidir o que fazer. □

Exemplo: Consideremos agora $q = 2, n = 3$ e $d = a$. Vamos considerar o melhor $[3,1;2]$ código possível, o código

$$\mathcal{C}_2 = \{(0,0,0),(1,1,1)\}.$$

Novamente obtemos que $W(\mathcal{C}_2) = 3$ e $e = \left[\frac{3-1}{2}\right] = 1$ e temos as bolas disjuntas

$$\begin{aligned} B_1((0,0,0)) &= \{(0,0,0),(1,0,0),(0,1,0),(0,0,1)\} \\ B_1((1,1,1)) &= \{(1,1,1),(0,1,1),(1,0,1),(1,1,0)\} \end{aligned}$$

Temos agora que cada uma das bolas contém 4 pontos e $B_1((0,0,0)) \cup B_1((1,1,1)) = \mathbb{F}_2^3$. Em outras palavras, podemos escrever o espaço ambiente $\mathbb{F}_2^3$ como união disjunta de bolas centradas em pontos do código. Esta situação, sob o ponto de vista de códigos, é ideal pois não importa qual a mensagem recebida y, sabemos sempre o que fazer com ela: se necessário, trocamos y pelo centro da única bola (desta família) que o contém. É por este motivo, que códigos com esta propriedade são ditos *códigos perfeitos.* □

3 Loteria Esportiva

Todos conhecem a loteria esportiva, em que temos treze jogos, cada jogo com três opções: vitória do time da casa (coluna 1), empata (coluna do meio) ou vitória do visitante (coluna 2). Podemos renomear os possíveis resultados atribuindo o valor 0 à coluna 1, o valor 1 à coluna do meio e o valor 2 à

coluna 2. Temos com isto que o resultado da loteria pode ser representado por um vetor $(x_1, x_2, ..., x_{13})$, com $x_i \in \{0, 1, 2\}$, para todo $i = 1, 2, ..., 13$. Além disto, cada vetor da forma $(x_1, x_2, ..., x_{13})$ representa um possível resultado da loteria. Em outras palavras, estamos identificando os resultados da loteria esportiva com o espaço $\mathbb{F}_3^{13}$. Vamos supor que o jogo feito seja $x = (x_1, x_2, ..., x_{13})$ e o resultado apurado $y = (y_1, y_2, ..., y_{13})$. Como saber quantos pontos fizemos? É simples, basta calcularmos a distância $d_H(x, y) = |x - y|_H$, que mede exatamente quantas coordenadas dos dois vetores são distintas, ou seja, quantos jogos erramos. O número de pontos, óbviamente, é $13 - d_H(x, y)$.

Se fizermos uma aposta x e o resultado for y, fazermos 13 pontos quer dizer que $x = y$, ou seja, $d(x, y) = 0$. Como podemos interpretar uma aposta que faz doze pontos? Ora, doze pontos equivale a termos a $d_H(x, y)$ - a distância entre a aposta e o resultado - igual a 1. Em outras palavras, se o resultado cair numa bola fechada de raio 1 da aposta - $B_1(x)$ - então podemos garantir que fizemos ao menos doze pontos (treze se o resultado for o centro da bola). De modo similar, fazer ao menos $13 - n$ pontos significa o resultado apurado cair numa bola de raio n centrada na aposta feita.

Como podemos ter certeza de acertar todos os 13 pontos? A única possibilidade que nos dá a certeza de fazermos treze pontos é apostarmos 13 jogos triplos, fazendo o absurdo de 3^{13} apostas. E para fazermos no mínimo 12 pontos? Uma possibilidade é fazermos 3^{12} apostas: jogamos triplo em todos os jogos a não ser em uma delas, um jogo simples. No entanto, é possível buscar estratégias para garantir este mesmo resultado com um número significativamente menor de apostas e é isto que faremos abaixo.

É fácil contarmos o número de pontos em uma bola fechada. Vamos examinar as bolas centradas na origem, isto é, no ponto $0 = (0, 0, ..., 0)$. Não perdemos qualquer generalidade pois podemos sempre transladar as bolas à origem, ou seja, para qualquer $x \in \mathbb{F}_3^{13}$ e qualquer positivo $r \geq 0$, temos que $y \in B_r(x)$ se e somente se $y - x \in B_r(0)$.

A bola unitária de $\mathbb{F}_3^{13}$ centrada em 0 é o conjunto dos pontos que tem no máximo uma coordenada não nula. É fácil contá-los: Um ponto tem treze coordnadas, cada uma delas com duas possibilidades distintas de 0, o que dá $13 \cdot 2 = 26$ possibilidades. Somando-se a esta o próprio x temos $27 = 3^3$ vetores na bola unitária.

Para a bola de raio 2, devemos adicionar, aos 27 vetores já encontrados, aqueles que distam exatamente 2, ou seja, aqueles que tem exatamente duas coordenadas não nulas. Para escolhermos as coordenadas temos $()132 = \frac{13!}{11!2!}$. Para cada uma destas duas coordenadas temos 2 possibilidades de elas

serem não nulas o que perfaz $4 = 2^2$ possibilidades. Temos então $2^2()132$ vetores que distam exatamente 2 da origem. Obtemos com isto que $B_2(0)$ tem $1+2()131+2^2()132 = 1+26+312 = 339$ vetores. É fácil continuarmos computando e mostrar que uma bola de raio $0 \leq n \leq 13$ tem exatamente $\sum_{i=0}^{n} 2^i()13i$ elementos.

Podemos examinar o número de elementos de cada bola na tabela abaixo ($\sharp(B_r(x))$ é o número de elementos da bola e centro x e raio r):

r	0	1	2	3	4	5
$\sharp(B_r(x))$	1	27	339	2.627	14.067	55.251
Fatores de 3	3^0	3^3	3×113	2.627	$3^3 \times 521$	$3^2 \times 6139$

r	6	7	8	9
$\sharp(B_r(x))$	165.080	384.720	714.200	1.080.300
Fatores de 3	165.080	3×128.240	714.200	3×360.100

r	10	11	12	13
$\sharp(B_r(x))$	1.373.100	1.532.900	1.586.100	1.594.300
Fatores de 3	3×457.700	1.532.900	3×528.700	3^{13}

Observe que apenas em três casos, a quantidade de elementos de uma bola é potência de 3. Um dos casos é quando o raio é 13, e este não nos acrescenta qualquer informação, apenas significa que se jogarmos treze jogos triplos, então com certeza acertaremos faremos treze pontos. O outro caso, que também não acrescenta qualquer informação, é quando o raio é zero: significa apenas que, se fizermos $3^{13} = 1.594.300$ jogos simples, cobriremos todas as possibilidades e, com certeza, faremos treze pontos. O único caso interessante é do raio ser 1, quando a bola possui exatamente $3^3 = 27$ elementos.

É óbvio que podemos particionar $\mathbb{F}_3^{13}$ em 3^{10} conjuntos disjuntos, cada um deles com 3^3 elementos, isto não é suficiente: queremos particionar $\mathbb{F}_3^{13}$ em $3^{10} = 59049$ bolas disjuntas, cada uma delas de raio um. Observe que $\sharp(B_r(x))$ ser divisor de 3^{13} é uma condição necessária para podermos recobri $\mathbb{F}_3^{13}$ com bolas disjuntas de raio r, ou seja, para encontrarmos um código perfeito. Quando esta condição não for satisfeita, qualquer recobrimento por bolas de mesmo raio necessáriamente recobrirá algum ponto ao menos duas vezes. Isto significa que estamos, em um certo sentido, disperdiçando apostas, ou seja, estamos concorrendo a 12 ou 11 pontos em mais de um cartão.

Para a infelicidade dos apostadores, não é possível construir um código perfeito (não trivial) em $\mathbb{F}_3^{13}$ (veja [MS, Teorema 33, cap. 6.10]). Podemos no

entanto nos perguntar quais variações da loteria esportiva admitem códigos perfeitos. É isto o que faremos na próxima seção.

4 Loterias com Códigos Perfeitos

O que entendemos por variação de loteria esportiva? É simples, temos um conjunto de n jogos, cada um dos jogos com q possíveis resultados distintos e um grande prêmio para quem acerta os n resultados, um prêmio menor para quem acerta $n-1$ resultados e, assim por diante, até $n-k>0$ resultados.

Podemos considerar por exemplo, uma loteria de futebol com n jogos e $q=3$ resultados (vitória empate ou derrota do time da casa). Vamos nos restringir ao caso em que $n=11$, essencialmente o único caso de loteria de futebol no qual podemos, através da teoria de códigos, podemos encontrar um código perfeito que nos garantirá ao menos $9=n-2$ pontos com 3^6 apostas. Em outras palavras, vamos construir um código perfeito de dimensão $d=6$ sobre $\mathbb{F}_3^{11}$ que corrige $e=2$ erros.

Este código é chamado de *Código de Golay* $\mathcal{G}_{11}$ e sua construção envolve diversas etapas. Vamos antes de tudo particionar os naturais não nulos e menores que 11 em dois conjuntos:

$$\begin{aligned}\mathcal{Q} &= \{1,3,4,5,9\} = \left\{\text{resíduos quadrados módulo } 11\right\}\\ \mathcal{N} &= \{2,6,7,8,10\} = \left\{\text{não-resíduos quadrado módulo } 11\right\}\end{aligned}$$

ou seja, nos números que são congruos ou não (módulo 11) a um número quadrado. Identificamos ainda $\mathbb{F}_{11}$ com o corpo de Galois $GF(11)$ das raízes n-ésimas da identidade do modo natural, via a função exponencial, ou seja, a cada $x\neq 0$ associamos $e^{ix\frac{2\pi}{11}}$. Ao nos restringirmos apenas aos elementos de $\mathbb{F}_{11}$, obtemos um isomorfismo de corpos. Em outras palavras, estamos considerando o conjunto das raízes n-ésimas da unidade

$$GF(11) = \left\{\alpha^k | \alpha = e^{i\frac{2\pi}{11}}, k=0,1,...,10\right\}.$$

Se considerarmos os polinômios

$$q(x) = \prod_{r\in\mathcal{Q}}(x-\alpha^r) \quad \text{e} \quad n(x) = \prod_{n\in\mathcal{N}}(x-\alpha^n)$$

temos que $x^{11}-1$, o polinômio mínimo de α, pode ser decomposto como

$$x^{11}-1 = (x-1)\,q(x)\,n(x).$$

Se consideramos o anel de polinômios $\mathbb{F}_3[x]$, e denotarmos por I o ideal gerado por $x^{11}-1$, temos o anel quociente $A = \mathbb{F}_3[x] / \left(x^{11}-1\right) = \mathbb{F}_3[x] / I$. Se considerarmos em A os ideais cíclicos $\mathcal{I}_q$ gerado por $q(x)$ e $\mathcal{I}_n$ gerado por $n(x)$, é fácil ver que a mudança de coordenada induzida por $x \mapsto x^2$ permuta os ideais $\mathcal{I}_q$ e $\mathcal{I}_n$, de modo que, cada um deles tem dimensão $\frac{1}{2}(n+1) = 6$.

Sendo um anel, se considerarmos a operação usual de soma em A, $p(x) I + q(x) I = (p+q)(x) I$, e a restrição do produto aos polinômios constantes, $(\lambda I)(p(x) I) = \lambda p(x) I$, vemos que A é um espaço vetorial sobre $\mathbb{F}_3$ e qualquer ideal, em particular os ideais $\mathcal{I}_q$ e $\mathcal{I}_n$, são sub-espaços vetoriais. É possível demonstrar que $\mathcal{I}_q$ é um $[11, 6; 3]$-código com distância mínima $W(\mathcal{I}_q) = 5$. Em particular, como dois elementos de $\mathcal{I}_q$ distam um do outro ao menos 5, temos que duas bolas distintas, centradas em elementos de $\mathcal{I}_q$ e de raio 2 são disjuntas. Seguindo um raciocínio análogo ao feito na seção 3, obtemos que a bola de raio 2 centrada em um ponto, digamos a origem 0, possui um elemento que dista 0 da origem, o próprio centro, $22 = 2()111$ elementos que distam 1, aqueles que tem exatamente uma coordenada não nula, e $220 = 2^2()112$ elementos a distância exatamente 2, aqueles que tem precisamente duas coordenadas não nulas. No total, temos que cada uma destas bolas tem $1 + 22 + 220 = 243 = 3^5$ elementos. Como $\mathcal{I}_q$ possui 3^6 elementos, temos que a união destas bolas disjuntas contém $3^5 3^6 = 3^{11}$ elementos, ou seja, estas recobrem todo o anel A. Em outras palavras, $\mathcal{I}_q$ é um código perfeito em A.

Um raciocínio análogo pode ser feito de forma a obter outros códigos de Golay.

Se considerarmos, por exemplo o ideal gerado por $x^3 + x + 1$ no anel $\mathbb{F}_2[x] / \left(x^7 + 1\right)$, obtemos um $[7, 4; 2]$-código perfeito com distância mínima 3. Este código pode naturalmente ser identificado com um código em $\mathbb{F}_2^{11}$. Neste caso, vamos ser explícitos. Basta considerarmos o subespaço de $\mathbb{F}_2^{11}$ gerado pelos elementos

$$\{(1,1,1,0,0,0,1), (0,0,0,1,1,1,0), (1,0,0,1,0,0,1), (1,1,0,1,0,1,0)\}.$$

Neste caso, como o código é relativamente pequeno (somente 16 elementos), podemos exibir explicitamente todos os seus elementos e ao leitor basta constatar que todos, com excessão do vetor nulo, tem ao menos 3 coordenadas não nulas. Apresentamos os vetores do código como aqueles que tem as coordenadas dadas pelas colunas da matriz abaixo:

$$\begin{pmatrix} 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Observe que este código, construído em um espaço vetorial sobre o corpo $\mathbb{F}_2$ não se presta a uma loteria de futebol ou xadrez, jogos que admitem o empate, mas apenas a jogos como basquete ou voleibol, que admitem apenas dois resultados possíveis, vitória ou derrota do time da casa.

Para estas loterias, existe uma classe de códigos perfeitos, bem mais simples de serem descritos, chamados de *Códigos de Hamming*. Para cada inteiro $r \geq 0$, existem exatamente 2^r naturais que podem ser escrito, no sistema binário, como números com no máximo r dígitos. Escrevemos uma matriz $r \times (2^r - 1)$ (que denotamos por H_r) em que a n-ésima coluna é a representação binária de n. Obtemos que H_r é uma matriz de posto r. De fato, as r colunas associadas às potencias $2^0, 2^1, ..., 2^{r-1}$ formam a matriz identidade. Podemos assim concluir que as r linhas de H_r são linearmente independentes e geram portanto um sub-espaço $\mathcal{C}_r$ de dimensão r. Se considerarmos o complemento ortogonal de $\mathcal{C}_r^{\perp}$, obtemos um subespaço vetorial de dimensão $2^r - 1 - r$, um $[2^r - 1, 2^r - 1 - r; 2]$-código $\mathcal{C}_r^{\perp}$. É possível mostrar que $\mathcal{C}_r^{\perp}$ tem distância mínima $W\left(\mathcal{C}_r^{\perp}\right) = 3$. Obtemos então que as bolas unitárias de $\mathbb{F}_2^{2^r-1}$ centradas em $\mathcal{C}_r^{\perp}$ são disjuntas. Em cada uma destas 2^{2^r-1-r} bolas temos exatamente 2^r elementos, perfazendo na união um total de $2^{2^r-1} = 2^{2^r-1-r}2^r$ elementos. Como $\mathbb{F}_2^{2^r-1}$ tem $(2)^{2^r-1}$ elementos, concluímos que $\mathcal{C}_r^{\perp}$ é um $[2^r - 1, 2^r - 1 - r; 2]$-código perfeito que corrige um erro.

Em resumo, em uma loteria esportiva de basquete com $n = 2^r - 1$ jogos, podemos fazer $n-1$ pontos com 2^{2^r-1-r} apostas, economizando 2^{r-1} apostas em relação ao palpite usual: jogar duplo em todas as colunas exceto uma delas.

Exemplo: Para $r = 3$ temos por exemplo a matriz

1 2 3 4 5 6 7

$$\mathcal{H}_r^{\perp} = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

e o código de Hamming $\mathcal{C}_r^{\perp}$ é gerado pelas linhas da matriz

$$\mathcal{H}_r = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

Neste caso, podemos ter certeza de acertar 6 dos setes jogos da loteria, fazendo 2^4 jogos, ao invés de 2^6 jogos no palpite usual. □

References

[MS] MacWilliams, F.J. and Sloane, N.J.A. - *The Theory of Error-Correcting Codes* - North-Holland, 1992.

[Vo] Voloch, J.F. - *Códigos Corretores de Erros* - 16° Colóquio Brasileiro de Matemática, CNPq, 1987.