Proceeding Series of the Brazilian Society of Applied and Computational Mathematics, Vol. 3, N. 1, 2015.
Trabalho apresentado no XXXV CNMAC, Natal-RN, 2014.

Coberturas curtas em espaços de Hamming

Anderson N. Martinhão, **Emerson L. Monte Carmelo**
Departamento de Matemática, UEM,
87020-900, Maringá, PR
E-mail: anderson.martinhao@gmail.com, elmcarmelo@uem.br

Resumo: *Seja $\mathbb{F}_q^3$ o espaço vetorial tridimensional sobre o corpo finito $\mathbb{F}_q$. No espaço métrico induzido pela distância de Hamming, a bola estendida é a união de todas as bolas de raio 1 com centros nos múltiplos escalares de u. O seguinte problema de cobertura é induzido: dizemos que um subconjunto $\mathcal{H}$ de $\mathbb{F}_q^3$ é uma cobertura curta se a união de todas as bolas estendidas com centros nos elementos de $\mathcal{H}$ cobrem todo o espaço. Neste trabalho, algumas condições necessárias e algumas condições suficientes para uma cobertura curta são discutidas. Também determinamos cardinalidade mínima de uma cobertura curta para algumas instâncias de q.*

Palavras-chave: *Códigos, coberturas, distância de Hamming, corpos finitos, ações de grupos.*

1 Introdução

1.1 O problema clássico

Algumas aplicações da teoria de códigos de cobertura são: compressão com distorção, compressão de dados, decodificação de erros, transmissão em redes interconectadas, codificação de voz, telecomunicação via celular e outros, conforme [3]. Conceitos de outras áreas da matemática, como álgebra, combinatória e teoria dos números têm sido aplicados a essa teoria. Para uma visão geral e algumas aplicações de códigos de coberturas veja o livro [3].

O problema de coberturas tem suas origens em 1948, quando Taussky e Todd [11] o introduziram no contexto da teoria de grupos. Com o passar dos anos o problema de coberturas ganhou um contexto mais combinatório e foi estudado dentro da teoria dos códigos, e tem se mostrado um grande desafio. Neste novo contexto, surgiram mais problemas, como por exemplo o problema de encontrar bons sistemas de loteria esportiva (*football pool systems*) enunciado a seguir. Dadas n partidas de futebol a serem realizadas, deve-se determinar o menor número de apostas que devem ser feitas para garantir que exista pelo menos uma aposta que consiga acertar o resultado de pelo menos $n-1$ dessas partidas. Este problema da loteria esportiva vem sendo estudado desde os anos 50 por matemáticos, cientistas da computação e engenheiros. Alguns pesquisadores que estudaram esse problema são Kamps, Van Lint, Hämäläinen, Rankinen, Östergard. Além do Brasil, este sistema de loteria esportiva é comum em países escandinavos, como Suécia e Finlândia.

Seja Q um conjunto finito com q elementos para qualquer inteiro q. Para simplificar a notação utilizaremos $Q = \mathbb{Z}_q$ o anel dos inteiro módulo q. Uma estrutura de espaço métrico é induzida em $\mathbb{Z}_q^n$ quando considerada a *distância de Hamming* que é definida da seguinte maneira: dados u e v em $\mathbb{Z}_q^n$, $d(u,v)$ denota o número de coordenadas em que u e v diferem. Por exemplo, $d(000,102) = 2$, pois estes vetores diferem na primeira e na terceira coordenadas. Um subconjunto $\mathcal{C}$ de $\mathbb{Z}_q^n$ é um *código de cobertura*, ou simplesmente uma *R-cobertura* quando a união das bolas com raio R, com centros nos vetores de $\mathcal{C}$ é todo o espaço. Uma pergunta interessante da teoria é: Qual é a cardinalidade mínima $K_q(n,R)$ de uma R-cobertura em $\mathbb{Z}_q^n$?

Com o passar dos anos, os cálculos revelaram-se extremamente difíceis. Usando várias ferramentas e introduzindo novos conceitos, poucas classes exatas desse problema extremal foram

determinadas até hoje. Até meados da década de 80, esses tipos de problemas foram estudados considerando-se apenas o raio 1. Em [1, 2] Carnielli estendeu o estudo desses números para raios arbitrários R. Em alguns desses casos foram obtidas aproximações para estas classes de valores de $K_q(n, R)$.

É comum também buscar valores computacionalmente. Códigos de cobertura podem ser reformulados em termos de conjuntos dominantes em grafos, que é um problema NP-completo, de acordo com [4]. Uma tabela atualizada desses valores é mantida por Kéri em [5]. Atualmente, devido a grande dificuldade computacional, diversos tipos de coberturas têm sido investigadas na tentativa de fornecer informações.

1.2 Uma variante: Coberturas curtas

Este trabalho concentra-se no estudo de uma nova variante, recentemente introduzida por Monte Carmelo, Nakaoka e Gerônimo em [9]. Para que esse novo problema esteja bem definido é essencial usarmos o corpo $\mathbb{F}_q$, pois utilizaremos a multiplicação de um vetor por escalar, assim o número q é uma potência de primo. Naturalmente quando q for um número primo, usaremos o corpo $\mathbb{F}_q = \mathbb{Z}_q$ (aritmética modular).

Seja $\mathbb{F}_q^n$ o espaço vetorial sobre o corpo finito $\mathbb{F}_q$ e considere a seguinte mudança do ponto de vista "geométrico": cada centro u é trocado pela linha $\{\lambda u \ : \ \lambda \in \mathbb{F}_q\}$. Mais especificamente, dado um vetor $u \in \mathbb{F}_q^n$, a *bola estendida* de *centro* u e *raio* R é definida como sendo a união de todas as bolas de raio R e com centros nos múltiplos escalares de u, isto é,

$$E(u, R) = \bigcup_{\lambda \in \mathbb{F}_q} B(\lambda u, R), \tag{1}$$

onde $B(x, R)$ denota a bola no espaço de Hamming $\mathbb{F}_q^n$ de centro x e raio R. Um subconjunto $\mathcal{H}$ de $\mathbb{F}_q^n$ é uma *R-cobertura curta*, se a união das bolas estendidas centradas nos vetores de $\mathcal{H}$ cobre todo o espaço $\mathbb{F}_q^n$. Analogamente ao problema clássico pode-se definir o seguinte problema extremal: Determinar a cardinalidade mínima de uma R-cobertura curta de $\mathbb{F}_q^n$. Esse número é denotado por $c_q(n, R)$.

Essa nova função está profundamente relacionada com a função clássica. Ainda no trabalho [9] foi provada a seguinte relação entre esses dois tipos de coberturas, a saber, para todos $n > R > 0$,

$$c_q(n, R) + 1 \leq K_q(n, R) \leq (q - 1)c_q(n, R) + 1.$$

Vários resultados da função clássica foram transladados naturalmente para esse novo problema, e em [8], Mendes e outros provaram um resultado de coberturas (clássicas) via coberturas curtas. Foi provado $c_5(10, 7) = 2$ e, a partir desse resultado, pôde-se concluir que $K_5(10, 7) = 9$.

Considere partir de agora o caso particular em que $n = 3$ e $R = 1$. Por isso, denote simplesmente por $c(q)$ o número $c_q(3, 1)$ e a bola estendida $E(u, 1)$ por $E(u)$ para cada $u \in \mathbb{F}_q^3$. Segundo [7] e suas referências, os melhores limites conhecidos são

$$\left\lceil \frac{q+1}{2} \right\rceil \leq c(q) \leq \begin{cases} (q+3)/2, \text{ se } q \equiv 3 \mod 4, \\ (q+5)/2, \text{ se } q \equiv 1 \mod 4, \\ 3(q+4)/4, \text{ se } q \text{ é par.} \end{cases} \tag{2}$$

Resultados de [7] foram obtidos a partir de emparelhamentos em grafos completos com pesos. Devido a dificuldade deste problema, são conhecidos apenas alguns valores para $c(q)$.

q	2	3	4	5	7	8	9
$c(q)$	1	3	3	4	4-5	5-9	5-7

Como pode-se ver, alguns valores pequenos de q ainda estão em aberto.

O principal objetivo deste trabalho é a busca por condições que ajudem a afirmar se um subconjunto $\mathcal{H}$ de $\mathbb{F}_q^3$ é uma cobertura curta ou não. Como consequência seguirá os valores

DOI: 10.5540/03.2015.003.01.0235

exatos para os números $c(q)$ para algumas instâncias de q. Na Seção 2 encontra-se alguns resultados referentes a cardinalidade das bolas estendidas, que são úteis para o decorrer do trabalho. Na Seção 3 são provados os limites inferiores $c(7) \geq 5$, $c(8) \geq 6$ e $c(9) \geq 6$. Na Seção 4 coberturas curtas minimais para $\mathbb{F}_q^3$ são exibidas para alguns casos de q.

A maioria das provas serão omitidas. Para o leitor mais interessado, uma versão completa deste trabalho pode ser encontrado em [6].

2 Preliminares

No manuscrito [6], a fim de obter limitantes inferiores para a função $c(q)$, os autores investigam como as bolas estendidas se intersectam. Às vezes, uma bola estendida cobre boa parte do espaço, por exemplo em $\mathbb{F}_5^3$ temos que $|B(1,1,1)| = 13$, $|E(1,1,1)| = 65$, enquanto que $\mathbb{F}_5^3 = 125$. Além disso, um novo obstáculo surge nesse ponto: no caso clássico temos que as cardinalidade das bolas independem do centro, enquanto que $|E(u)|$ não são independentes do centro u, por exemplo, em $\mathbb{F}_5^3$, $|E((0,0,0))| = |B((0,0,0))| = 13$, enquanto que $|E((1,1,1))| = 65$, veja [9].

A busca de limites inferiores é um problema bastante desafiador. Uma tática já usada para o caso clássico é estudar o comportamento das cardinalidades das bolas estendidas restritas a algum subconjunto particular do espaço $\mathbb{F}_q^n$. De modo natural essa estratégia pode ser usada também no caso de coberturas curtas. Considere o seguinte subconjunto de $\mathbb{F}_q^3$,

$$\mathcal{D}_q = \{(u_1, u_2, u_3) \in \mathbb{F}_q^3 \ : \ u_1, u_2, u_3 \text{ são dois a dois distintos e não nulos}\}.$$

Denote a bola estendida $E(u)$ restrita a $\mathcal{D}_q$ por $\widetilde{E}(u)$. O número $|\widetilde{E}(u)|$ está determinado.

Teorema 1. *[6, Teorema 5] Seja $u = (u_1, u_2, u_3)$ um vetor em $\mathbb{F}_q^3$, denote por $\omega(u)$ o* peso *do vetor u, isto é, $\omega(u)$ é a quantidade de coordenadas não nulas de u e por $\delta(u) = |\{u_1, u_2, u_3\}|$.*

1. *Se $\omega(u) = 1$, então $|\widetilde{E}(u)| = 0$.*
2. *Se $\omega(u) = 2$, então $|\widetilde{E}(u)| = 0$ ou $|\widetilde{E}(u)| = (q-1)(q-3)$, se $\delta(u) = 1$ ou $\delta(u) = 2$ respectivamente.*
3. *Se $\omega(u) = 3$, então $|\widetilde{E}(u)| = 0$ ou $|\widetilde{E}(u)| = (q-1)(2q-6)$ ou $|\widetilde{E}(u)| = (q-1)(3q-11)$, se $\delta(u) = 1$ ou $\delta(u) = 2$ ou $\delta(u) = 3$ respectivamente.*

É um pouco surpreendente que no cálculo de $|\widetilde{E}(u) \cap \widetilde{E}(v)|$, sob a condição $u, v \in \mathcal{D}_q$, o limite inferior dependa consideravelmente da forma aritmética de q, como vemos no próximo resultado.

Teorema 2. *[6, Teorema 1] Dados q uma potência de primo e $u, v \in \mathcal{D}_q$, tem-se*

$$|\widetilde{E}(u) \cap \widetilde{E}(v)| \geq \begin{cases} 2(q-1) & \text{se } q-1 \not\equiv 0 \mod 3, \\ 0 & \text{se } q-1 \equiv 0 \mod 3. \end{cases}$$

Os limites são atingidos, isto é, se $q-1 \not\equiv 0 \mod 3$, existem $u, v \in \mathcal{D}_q$ tais que $|\widetilde{E}(u) \cap \widetilde{E}(v)| = 2(q-1)$, e se $q-1 \equiv 0 \mod 3$, existem $u, v \in \mathcal{D}_q$ tais que $|\widetilde{E}(u) \cap \widetilde{E}(v)| = 0$.

3 Condições necessárias

Algumas condições necessárias para uma cobertura curta com poucos vetores são discutidas agora. Denote as projeções canônicas de $\mathbb{F}_q^3$ em $\mathbb{F}_q$, por $\pi_i(u_1, u_2, u_3) = u_i$, para cada $i \in \{1, 2, 3\}$. O símbolo $*$ representa um elemento arbitrário em $\mathbb{F}_q$.

Teorema 3. *Sejam $q \geq 7$ uma potência de primo e $m = \lceil (q+1)/2 \rceil$. Suponha que $\mathcal{H} = \{h_1, \ldots, h_m\}$ é uma cobertura curta de $\mathbb{F}_q^3$. As seguintes condições seguem:*

1. *Existe um vetor em $\mathcal{H}$ com peso 3.*

2. *Para cada coordenada j, $1 \leq j \leq 3$, existe um vetor $h_k \in \mathcal{H}$ tal que $\pi_j(h_k) = 0$.*

3. *Podemos assumir sem perda de generalidade que $\mathcal{H}$ assume um das formas:*

$$\begin{aligned} \mathcal{H}_1 &= \{(1,1,1),(0,*,*),(*,0,*),(*,*,0),h_5,\ldots,h_m\}, \\ \mathcal{H}_2 &= \{(1,1,1),(0,*,*),(*,0,0),h_4,\ldots,h_m\}. \end{aligned}$$

Ideia da demonstração. A demonstração da primeira parte deste teorema consiste em contar quantos elementos um vetor de peso no máximo 2 pode cobrir. Isso é feito aplicando o Teorema 1. Para provar a segunda parte, considera-se o plano $\Pi_1 = \{(0,u_2,u_3) \ : \ u_2,u_3 \in \mathbb{F}_q\}$ e o seu subconjunto $\mathcal{X}_1 = \{(0,u_2,u_3) \in \Pi_1 \ : \ u_2 \neq u_3 \text{ e } u_2,u_3 \neq 0\}$. A terceira parte é consequência imediata das duas primeiras partes. Ver detalhes em [6, Teorema 18]. □

3.1 Aplicações numéricas

O propósito do restante dessa seção é apresentar condições para se obter limites inferiores para $c(q)$ e também fornecer valores exatos pelo menos para $q \in \{7,8,9\}$. A condição $c(q) > m$ corresponde à afirmação: nenhum dos $\binom{q^3}{m}$ m-subconjuntos $\mathcal{H}$ de $\mathbb{F}_q^3$ satisfazem

$$\bigcup_{h\in\mathcal{H}} E(h) = \mathbb{F}_q^3. \tag{3}$$

Visto que o espaço é muito grande e as bolas estendidas são altamente intersectantes, não é fácil checar (3). A abordagem utilizada analisa essencialmente o comportamento das bolas estendidas restritas a $\mathcal{D}_q$. Mais precisamente, a ideia está descrita brevemente como segue.

Dado q uma potência de primo, suponha por absurdo que existe uma cobertura curta $\mathcal{H} = \{h_1,\ldots,h_m\}$ de $\mathbb{F}_q^3$ com $m = \lceil (q+1)/2 \rceil$ vetores. O Teorema 3 afirma que existem apenas duas possibilidades para $\mathcal{H}$. Visto que $\mathcal{H}$ é uma cobertura curta do subconjunto $\mathcal{D}_q$, a condição $\mathcal{D}_q \subset \cup_{i=1}^m \widetilde{E}(h_i)$ segue. Por outro lado, ao mostrar que

$$\left|\bigcup_{i=1}^m \widetilde{E}(h_i)\right| < (q-1)(q-2)(q-3), \tag{4}$$

tem-se uma contradição: $\mathcal{D}_q$ não está contido em $\cup_{i=1}^m \widetilde{E}(h_i)$, visto que $|\mathcal{D}_q| = (q-1)(q-2)(q-3)$.

Omitiremos algumas demonstrações dessa seção. Faremos com detalhes a demonstração do caso $q = 7$.

Proposição 4. *Obtemos $c(7) \geq 5$.*

Demonstração. Suponha por absurdo que $\mathcal{H} = \{h_1,\ldots,h_4\}$ é uma cobertura curta de $\mathbb{F}_7^3$. O Teorema 3 implica que existem apenas duas possíveis formas para $\mathcal{H}$, a saber:

$$\begin{aligned} \mathcal{H}_1 &= \{(1,1,1),(0,*,*),(*,0,*),(*,*,0)\}, \\ \mathcal{H}_2 &= \{(1,1,1),(0,*,*),(*,0,0),(*,*,*)\}. \end{aligned}$$

Se $\mathcal{H} = \mathcal{H}_1$, segue do Teorema 1, $|\widetilde{E}(h_1)| = 0$ e $|\widetilde{E}(h_i)| \leq 24$ para todo $i \in \{2,3,4\}$. Então $\mathcal{H}_1$ cobre no máximo 72 vetores de $\mathcal{D}_7$.

Se $\mathcal{H} = \mathcal{H}_2$, o Teorema 1 implica que $|\widetilde{E}(h_1)| = 0$, $|\widetilde{E}(h_2)| \leq 24$, $|\widetilde{E}(h_3)| = 0$ e $|\widetilde{E}(h_4)| \leq 60$. Então $\mathcal{H}_2$ cobre no máximo 84 vetores de $\mathcal{D}_7$.

Portanto, com $|\mathcal{D}_7| = 120$, a desigualdade (4) segue, donde $\mathcal{H}$ não pode ser uma cobertura curta de todo o espaço $\mathbb{F}_7^3$. Assim, $c(7) \geq 5$. □

DOI: 10.5540/03.2015.003.01.0235

O argumento para $c(8) > 5$ é o mais intrincado. O espaço de todas as possíveis coberturas curtas de $\mathbb{F}_8^3$ com 5 elementos, corresponde a família de todos os 5-subconjuntos de $\mathbb{F}_8^3$, ou seja, são $\binom{8^3}{5} \simeq 2.8 \times 10^{11}$ candidatos. O Teorema 1 não é suficiente para lidar com todos. Nesse caso aplica-se o Teorema 2.

Proposição 5. *O limite $c(8) \geq 6$ é válido.*

Demonstração. A demonstração pode ser encontrada detalhada em [6, Proposição 21]. □

Proposição 6. *O limite inferior $c(9) \geq 6$ segue.*

Demonstração. Ver [6, Proposição 20]. □

4 Condições suficientes

4.1 Ações de grupos aplicadas a coberturas curtas

Um método de encontrar coberturas curtas é baseado em encontrar conjuntos que são invariantes sob certas ações de grupos.

Dado uma potência de primo q, L_q denota o grupo de todos os operadores lineares não-singulares $\mathbb{F}_q$, isto é,

$$L_q = \{\sigma : \mathbb{F}_q \to \mathbb{F}_q \ : \ \sigma(x) = \lambda x, \text{ para algum } \lambda \in \mathbb{F}_q^*\}.$$

Seja L_q^3 o produto direto $L_q \oplus L_q \oplus L_q$. Como usual, S_3 denota o grupo simétrico de grau 3. Considere o seguinte subgrupo de L_q^3,

$$K = \{(\sigma, \sigma, \sigma) \ : \ \sigma \in L_q\} = \{(u_1, u_2, u_3) \mapsto (\lambda u_1, \lambda u_2, \lambda u_3) \ : \ \lambda \in \mathbb{F}_q^*\}.$$

A ação do produto direto $G = S_3 \times K$ em $\mathbb{F}_q^3$ tem papel fundamental nos resultados, e para $(\varphi, (\sigma, \sigma, \sigma)) \in G$, e $u = (u_1, u_2, u_3) \in \mathbb{F}_q^3$, é dada por,

$$u^{(\varphi,(\sigma,\sigma,\sigma))} = (\lambda u_{\varphi^{-1}(1)}, \lambda u_{\varphi^{-1}(2)}, \lambda u_{\varphi^{-1}(3)}).$$

Ou seja, o vetor u é multiplicado por um escalar não nulo e tem as suas entradas permutadas. O conjunto

$$\mathcal{A}_q = \{(u_1, u_2, u_3) \in \mathbb{F}_q^3 \ : \ u_1, u_2, u_3 \text{ são dois a dois distintos}\}$$

é invariante pela ação do produto direto $S_3 \times K$, e tem duas órbitas, a saber, $\{u \in \mathcal{A}_q \ : \ d(u, 0) = 3\}$ e $\{u \in \mathcal{A}_q \ : \ d(u, 0) = 2\}$.

Um método de encontrar coberturas curtas é descrito em [10, Teorema 1]. Uma adaptação deste método é descrito abaixo.

Teorema 7. *Seja N um subgrupo de S_3 e escolha um subconjunto $\mathcal{L}$ de $\mathbb{F}_q^3$ que é invariante pela ação de N, isto é, $\mathcal{L}^N = \mathcal{L}$. Seja $\mathcal{O}$ a família de todas as órbitas da ação de $N \times K$ sobre $\mathcal{A}_q$. Suponha que cada órbita da ação de $S_3 \times K$ em $\mathcal{A}_q$ contém um elemento u que pode ser escrito como $u = \lambda h + \mu e_j$ para algum $h \in \mathcal{L}$, λ, $\mu \in \mathbb{F}_q$ e $j \in \{1, 2, 3\}$. Então, o conjunto $\mathcal{L} \cup \{(1, 1, 1)\}$ é uma cobertura curta de $\mathbb{F}_q^3$.*

Demonstração. Ver [6, Teorema 22] □

O próximo exemplo mostra uma aplicação do método descrito acima para a construção de uma cobertura curta ótima para o caso $q = 5$.

DOI: 10.5540/03.2015.003.01.0235

Exemplo 8. O teorema acima é otimal para alguns valores de q pequenos. Sabe-se que $c(5) = 4$. O limite superior pode ser provado novamente usando esse método. Escolha $\mathcal{L} = \{(0,2,3),(3,0,2),(2,3,0)\}$. Como $\mathcal{L}$ é invariante pela ação do 3-ciclo $\varphi : (u_1,u_2,u_3) \mapsto (u_2,u_3,u_1)$, considere $N =< \varphi >$ o subgrupo gerado por φ. A ação de $G =< \varphi > \times K$ em $\mathcal{A}_5$ gera cinco órbitas. Visto que o estabilizador de um vetor u é o subgrupo trivial, cada órbita u^G tem doze elementos. Além disso, cada um dos representantes são cobertos por $\mathcal{L}$, como descrito abaixo

$$\begin{array}{ll} (0,1,2) = 3(0,2,3) + 3e_3 & (0,1,3) = 3(0,2,3) + 4e_3 \\ (0,1,4) = 3(0,2,3) & (1,2,3) = 1(0,2,3) + 1e_1 \\ (1,3,2) = 4(0,2,3) + 1e_1, & \end{array}$$

onde $e_1 = (1,0,0)$, $e_2 = (0,1,0)$ e $e_3 = (0,0,1)$. O limite $c(5) \leq 4$ segue do Teorema 7.

4.2 Aplicações numéricas

Os limitantes superiores $c(8) \leq 6$ e $c(9) \leq 6$ são obtidos nessa seção, utilizando o Teorema 7. Mas antes disso, uma forma de representar os elementos de um corpo finito $\mathbb{F}_q$ é discutida.

Denote os elementos não nulos de $\mathbb{F}_q$ como segue: Para todas as potências de primo q, o grupo multiplicativo $\mathbb{F}_q^*$ é cíclico e é isomorfo ao grupo aditivo $\mathbb{Z}_{q-1}$, pelo isomorfismo de $\mathbb{Z}_{q-1}$ em $\mathbb{F}_q^*$, dado por $\overline{x} \mapsto \xi^x$, onde ξ denota um gerador arbitrário de $\mathbb{F}_q^*$. Então, a partir de agora considere $\mathbb{F}_q^* = \{\xi^0, \xi^1, \ldots, \xi^{q-2}\}$. A multiplicação em $\mathbb{F}_q^*$ segue a regra: $\xi^x\xi^y = \xi^{x+y} = \xi^z$, se e somente se, $z = x + y$ em $\mathbb{Z}_{q-1}$.

Exemplo 9. Tem-se que se 2 é um gerador do grupo multiplicativo de $\mathbb{Z}_5^*$, então podemos escrever $\mathbb{Z}_5 = \{0, 1, 2^1, 2^2, 2^3\}$. Os vetores

$$h_1 = (1,1,1),\ h_2 = (0,1,2^2),\ h_3 = (1,2^2,2^2) \text{ e } h_4 = (1,0,0),$$

formam uma cobertura curta de $\mathbb{Z}_5^3$.

De fato, dado $u = (u_1,u_2,u_3)$ em $\mathbb{Z}_5^3$ um vetor arbitrário tem-se. Se u tem alguma coordenada nula, então ele é coberto por $h_2 = (0,1,2^2)$ e $h_4 = (1,0,0)$. Por exemplo, se $u = (0,u_2,u_3)$, como $u_2(0,1,2^2) = (0,u_2,u_2 2^2)$ tem-se $h_2 = (0,1,2^2)$ cobre u. Se u tem pelo menos duas coordenadas iguais, então ele é coberto por $h_1 = (1,1,1)$. Por exemplo se $u = (u_1,u_1,u_3)$, então como $u_1(1,1,1) = (u_1,u_1,u_1)$ segue-se $h_1 = (1,1,1)$ cobre u. Agora, se u tem as três coordenadas não nulas e distintas, então podemos supor sem perda de generalidade que u é da forma $u = (1,u_2,u_3)$. Portanto, basta mostrar que os vetores h_1, h_2, h_3 e h_4 cobrem os vetores

$$(1,2^1,2^2),(1,2^1,2^3),(1,2^2,2^1),(1,2^2,2^3),(1,2^3,2^1),(1,2^3,2^2).$$

Rapidamente pode-se observar que $h_3 = (1,2^2,2^2)$ cobre $(1,2^1,2^2)$, $(1,2^2,2^1)$, $(1,2^2,2^3)$ e $(1,2^3,2^2)$. Como $2^1h_2 = (0,2^1,2^3)$ e $2^3h_2 = (0,2^3,2^1)$ segue que $h_2 = (0,1,2^2)$ cobre $(1,2^1,2^3)$ e $(1,2^3,2^1)$.

Proposição 10. *O limite superior $c(8) \leq 6$ é válido.*

Ideia da demonstração. Seja ξ um gerador do grupo multiplicativo $\mathbb{F}_8^*$ e considere os vetores

$$\begin{array}{lll} h_1 = (1,1,1), & h_2 = (0,0,\xi^1), & h_3 = (1,\xi^1,0), \\ h_4 = (1,\xi^2,\xi^3), & h_5 = (1,\xi^3,\xi^2), & h_6 = (\xi^6,\xi^5,1). \end{array}$$

É possível provar que $\mathcal{H} = \{h_1,\ldots,h_6\}$ é uma cobertura curta de $\mathbb{F}_8^3$, via Teorema 7, conforme [6, Proposição 24]. □

Proposição 11. *Temos $c(9) \leq 6$.*

Ideia da demonstração. Considere ξ um gerador do grupo multiplicativo $\mathbb{F}_9^*$ e os vetores

$$\begin{array}{lll} h_1 = (1,1,1), & h_2 = (1,0,0), & h_3 = (0,1,\xi^4), \\ h_4 = (1,\xi^2,\xi^4), & h_5 = (1,\xi^4,\xi^2), & h_6(1,\xi^6,\xi^6), \end{array}$$

Assim $\mathcal{H} = \{h_1,\ldots,h_6\}$ é uma cobertura curta de $\mathbb{F}_9^3$. Ver detalhes em [6, Proposição 25]. □

5 Conclusão

Concluímos esse trabalho com a seguinte contribuição para o cálculo da função c.

Teorema 12. *São válidos* $c(7) = 5$, $c(8) = 6$ *e* $c(9) = 6$.

Demonstração. É consequência imediata dos resultados anteriores. De fato, o limite inferior $c(7) \geq 5$ segue da Proposição 4, enquanto que o limite superior $c(7) \leq 5$ provém da desigualdade (2). O valor $c(8) = 6$ é uma consequência imediata das Proposições 5 e 10. Obtém-se pelas Proposições 6 e 11 que $c(9) = 6$. □

Referências

[1] W.A. Carnielli, Hyper-rook domain inequalities, *Stud. Appl. Math.*, 82 (1990), no. 1, 59-69.

[2] W.A. Carnielli, On covering and coloring problems for rook domains, *Discrete Math.*, vol. 57 (1985), 9-16.

[3] G. Cohen, I. Honkala, S. Litsyn e A. Lobstein, *Covering Codes*, North-Holland, Amsterdam, (1997).

[4] M. Garey e D. Johnson, *Computers and intractability: a guide to the theory of NP-completeness*, W.H.Freeman and Company, (1979).

[5] G. Kéri, Tables for bound on covering codes, homepage: http://www.sztaki.hu/~keri/ acessado (2014).

[6] A.N. Martinhão e E.L. Monte Carmelo, Intersecting families of extended balls in the Hamming spaces, http://arxiv.org/

[7] A.N. Martinhão e E.L. Monte Carmelo, Short covering codes arising from matchings in weighted graphs, *Math. Comput.*, vol. 82 (2013), 605-616.

[8] C. Mendes, E.L. Monte Carmelo e M. Poggi, Bounds for Short Covering Codes and Reactive Tabu Search. *Discrete Applied Mathematics*, (2009), 522-533.

[9] E.L. Monte Carmelo, I.N. Nakaoka e J.R. Gerônimo, A covering problem on finite spaces and rook domains, *Inter. J. Appl. Math.*, 20 (2007), 875-886.

[10] E.L. Monte Carmelo e I.N. Nakaoka, Short coverings in tridimensional spaces arising from sum-free sets, *European J. Combin.*, 29 (2008), 227–233.

[11] O. Taussky e J. Todd, Covering theorems for groups, *Ann. Soc. Polonaise Math.* 21, (1948), 303-305.

DOI: 10.5540/03.2015.003.01.0235