Universidade Estadual de Maringá

Programa de Pós-Graduação em Matemática

Centro de Ciências Exatas

(Mestrado)

Códigos de Cobertura em Espaços de Hamming

George Arruda Gomm

Orientador: Emerson Luiz do Monte Carmelo

Maringá - Pr

2010

"Que força é esta, eu não sei; tudo o que sei é que existe, e está disponível apenas quando alguém está num estado em que sabe exatamente o que quer, e está totalmente determinado a não desistir até conseguir."

[Alexander Graham Bell]

Aos que amo.

Aos meus pais George e Ione com imenso carinho.

Agradecimentos

Agradeço aos professores do Departamento de Matemática da UEM pelo auxílio no avanço do meu conhecimento, em especial ao professor Emerson Luiz do Monte Carmelo, pela orientação, paciência e dedicação e a professora Valéria Neves Domingos Cavalcanti pela compreensão e força que me deu no momento mais difícil que passei durante o curso.

Agradeço aos professores do Departamento de Matemática da UTFPR em especial ao chefe professor Antônio Amilcar Levandoski, pelo apoio e retaguarda que me deu durante todo tempo em que fiquei afastado de minhas funções para fazer o curso.

Resumo

Neste trabalho, abordaremos o problema de encontrar a cardinalidade mínima de um código de cobertura no espaço finito de Hamming. Esta cardinalidade mínima será dada pela função $K_q(n, R)$, e apresentaremos valores exatos e aproximações para algumas classes desta função através da teoria dos códigos de cobertura. Estas construções podem ser feitas através de argumentos combinatórios e em algumas delas são usadas ferramentas algébricas, propriedades de corpos finitos, a teoria aditiva dos números, construções matriciais. Tais construções serão úteis na obtenção de limites superiores. Por outro lado, métodos utilizando s-sobrejetividade e partição de matrizes serão de grande utilidade na obtenção de alguns limites inferiores para algumas classes da função $K_q(n, R)$.

Abstract

In this work, we will approach the issue to find the minimum cardinality of a covering code in the Hamming finite space. This minimum cardinality will be given by the function $K_q(n, R)$, and we will introduce exact values and approximations to some classes of these functions through the covering codes theory. These constructions can be done through combinatory arguments and in some of them we will use algebraic tools using finite fields properties, the numbers addictive theory, constructions using matrixes. These constructions will be very useful to get upper bounds. on the other hand methods using the s-surjective and matrixes partition will be very useful to get some lower bounds to some classes of the function $K_q(n, R)$.

Sumário

Introdução

Como é conhecido a loteria esportiva consiste em apostas em uma relação de treze jogos dados, visando acertar o resultado de todos eles para obter o prêmio máximo, ou acertar pelo menos doze dos treze jogos. Um bom sistema para atingir este objetivo pode ser reduzido a um problema combinatório.

De uma maneira mais geral a descrição de bons sistemas para apostar em loteria esportiva consiste em assumir que n partidas de futebol são jogadas, e desejamos apostar nestas partidas. Cada aposta custa um preço igual. Uma aposta é uma previsão dos vencedores nestas n partidas, e nós aceitamos que o empate é um possível resultado em cada jogo. Portanto uma aposta é um vetor ternário de comprimento n. O problema da loteria esportiva consiste em determinar a seguinte questão:

> Qual o menor número de apostas a serem feitas para garantir pelo menos o segundo prêmio, não importando quais os resultados dos jogos?

Na terminologia a ser descrita um conjunto de apostas é um código ternário de comprimento n e raio no máximo 1. Se os empates não fossem permitidos, nós teríamos um problema correlato restrito a códigos binários. Trabalharemos com uma generalização deste problema ao longo deste trabalho.

Estes sistemas de loteria esportiva têm sido estudados desde os anos 50 por matemáticos, cientistas da computação e engenheiros. Alguns pesquisadores que estudaram este problema são H. J. L. Kamps e J. H. Van Lint, H. O. Hämäläinen , S. Rankinen , P. J. Östergard, etc. Além do Brasil, é comum encontrar este sistema

de loteria esportiva em países escandinavos da Europa, com por exemplo a Suécia e Finlândia.

No entanto este problema inicialmente foi estudado por O. Taussky e J. Todd [21] em um contexto puramente algébrico, gerando uma função $K_q(n)$, cuja descrição será detalhada no capítulo 2.

Na década de 60, mais informações sobre $K_q(n)$ foram desobertas por H. J. Kamps e J. H. Van Lint, J. G. Kalbfleich e R. G. Stanton [10].

A partir da década de 60, os problemas de cobertura ganharam um contexto mais combinatório e foram estudados dentro da teoria dos códigos, onde estas coberturas recebem o nome de *códigos de cobertura*. Neste contexto, surgiram problemas correlatos, como por exemplo, o problema do tabuleiro de xadrez, a saber: dado um tabuleiro de xadrez 8×8, qual é o número mínimo de torres necessárias para cobrir todo tabuleiro?

Estaremos interessados numa extensão a tabuleiros n-dimensionais.

No começo da década de 80, W. A. Carnielli [3] começou a estudar estes problemas de coberturas para raios arbitrários gerando a função $K_q(n, R)$ (descrição a ser detalhada no capítulo 2), generalizando $K_q(n)$, estudada por O. Taussky e J. Todd.

Coloquemos um problema mais geral:

Dado um conjunto finito arbitrário Q, de cardinalidade q, definimos o conjunto Q^n de todas as n-uplas ordenadas, onde todas as coordenadas assumem valores em Q. Queremos obter um subconjunto C de Q^n de menor cardinalidade possível, tal que dado x em Q^n, podemos encontrar um y em C, tal que x e y diferem, entre si, em no máximo R coordenadas, onde $R < n$. A cardinalidade mínima deste subconjunto C será dado por $K_q(n, R)$. A obtenção dos valores exatos de $K_q(n, R)$ é, na maioria das vezes, um problema extremamente difícil e em muitos casos os valores exatos não são conhecidos. Nestes casos foram obtidos limites inferiores e superiores para estes valores de $K_q(n, R)$.

A determinação de valores de $K_q(n, R)$ é o assunto que enfocaremos neste trabalho utilizando a *teoria dos códigos de cobertura*.

No capítulo 1, introduziremos conceitos básicos da *teoria dos códigos corretores de erros* e construiremos algumas classes de códigos utilizadas no desenvolvimento deste trabalho, como os códigos perfeitos, códigos equivalentes, códigos lineares e os códigos MDS.

No capítulo 2, abordamos o conceito de coberturas e as funções $K_q(n, R)$. Neste mesmo capítulo, descrevemos as construções de algumas classes exatas das funções $K_q(n, R)$, bem como construções de algumas classes indutivas de $K_q(n, R)$, com o objetivo de obter coberturas em espaços maiores a partir de coberturas em espaços menores.

No capítulo 3, iniciaremos construções de coberturas via matrizes, um método bastante utilizado até hoje.

No capítulo 4, introduziremos alguns conceitos básicos da teoria aditiva dos números. Particularmente, estamos interessados em informações sobre a cardinalidade do conjunto soma $A + B$, onde A e B são subconjuntos de um grupo abeliano finito G. Em seguida, faremos algumas construções de coberturas, utilizando como ferramenta o teorema de I. Chowla e o de Cauchy-Davemport [17].

No capítulo 5, obteremos alguns limites inferiores de algumas classes das funções $K_q(n, R)$, utilizando a s-sobrejetividade e partição de matrizes. Com isso, obteremos mais algumas classes exatas das funções $K_q(n, R)$.

No capítulo 6, faremos as considerações finais dos resultados descritos neste trabalho, e apresentaremos algumas tabelas de valores da função $K_q(n, R)$, onde indicaremos os valores exatos, alguns limites superiores e inferiores.

Ao longo de todo este trabalho, serão feitas construções combinatórias de coberturas e em alguma delas usaremos ferramentas algébricas, como por exemplo as construções via matrizes, propriedades de corpos finitos e em outras construções,

usaremos ferramentas via partição de matrizes.

Iremos observar que a obtenção de valores exatos, limites superiores e inferiores para $K_q(n, R)$ é um problema extremamente difícil que tem desafiado pesquisadores de várias áreas como matemáticos, engenheiros e profissionais da área de informática desde mais ou menos 1950.

Capítulo 1

Códigos

Para o desenvolvimento da teoria dos *códigos* de cobertura, precisamos introduzir conceitos da *teoria dos códigos corretores de erros*. Por isso, vamos direcionar a exposição priorizando algumas classes de códigos importantes para o desenvolvimento deste trabalho, a saber, códigos perfeitos, códigos equivalentes, códigos lineares e códigos MDS. Os tópicos que serão mencionados neste capítulo são discutidos em [8] e [6]. As demonstrações omitidas podem ser encontradas em [8].

1.1 Conceitos Básicos

Dado um conjunto finito arbitrário Q e $n \in \mathbb{N}$, denote o espaço

$$Q^n = \{(x_1, \ldots, x_n) : \ x_i \in Q, \ i = 1, \ldots, n\}.$$

Um código C é um subconjunto qualquer não vazio de Q^n, isto é, $C \subset Q^n$. O conjunto finito Q é chamado de *alfabeto* e cada elemento $c \in C$ chama-se *palavra-código*.

A fim de tornar precisa a noção intuitiva de proximidade entre duas palavras código, apresentamos a seguir um modo de medir distâncias entre palavras código em Q^n.

Definição 1.1. Dados dois elementos $x = (x_1, \ldots, x_n)$ e $y = (y_1, \ldots, y_n)$ de Q^n, a

distância de Hamming entre x e y é definida como

$$d(x, y) = |\{i : \ x_i \neq y_i, \ 1 \leq i \leq n\}|.$$

Note que em $\{0, 1\}^3$, $d(001, 111) = 2$, pois tais vetores diferem na primeira e segunda coordenadas.

Demonstra-se que a distância de Hamming é uma métrica, assim o espaço Q^n munido da métrica d tem a estrutura de um espaço métrico, chamado de *espaço de Hamming.* Neste espaço, a *bola* de centro c e raio r é denotada por

$$B(c, r) = \{x \in Q^n : \ d(x, c) \leq r\}.$$

Este conjunto é finito e por um simples argumento combinatório, podemos mostrar que $|B(c, r)| = \sum_{i=0}^{r} \binom{n}{i}(q-1)^i$.

Observe que a cardinalidade de $B(c, r)$ depende apenas de n, q e r e a denotaremos por $V_q(n, r)$, isto é, $|B(c, r)| = V_q(n, R)$.

Definição 1.2. Seja C um código em Q^n. A distância mínima de C é o número

$$d = min \ \{d(x, y) \ : \ x, y \in C \text{ e } x \neq y\}.$$

Se não tivermos propriedades especiais em C, note que para calcular a distância mínima d de um código C é necessário calcular $\binom{M}{2}$ distâncias, onde M é o número de palavras do código, o que tem um custo computacional elevado.

O parâmetro d está associado a propriedades estruturais do código C. Como ilustração intuitiva, se d é "grande", então existem bolas centradas em C disjuntas de raios "grandes".

Dado um código C no espaço de Hamming Q^n, podemos encontrar um número R, tal que a união de todas as bolas centradas em cada palavra-código de raio R é o espaço todo. O menor R que satisfaz a condição acima é chamado de *raio de cobertura do código* C. Em outras palavras, o raio de cobertura mede a distância

entre o código e os vetores mais distantes do código. Se todas estas bolas forem disjuntas, temos uma classe importante de códigos com esta propriedade, como veremos a seguir.

Definição 1.3. Um código $C \subseteq Q^n$ de distância mínima d é perfeito, quando exite um R tal que todas as bolas de raio R centradas em cada palavra-código satisfaz

$$\bigcup_{c \in C} B(c, R) = Q^n,$$

e esta união é disjunta.

Exemplo 1.4. Como ilustração, tome $C = \{(000), (111)\}$ em $\{0, 1\}^3$. Observe que $d = 3$ e tome $R = 1$, então:

$B((000), 1) = \{(000), (100), (010), (001)\}$.

$B((111), 1) = \{(111), (110), (011), (101)\}$.

Como $B((000), 1) \bigcup B((111), 1) = Q^3$ e $B((000), 1) \bigcap B((111), 1) = \phi$, C é um código perfeito.

Um código $C \subseteq Q^n$ com M palavras código, distância mínima d e raio de cobertura R é denotado por $(n, M, d)_q R$- código. Se d ou R não são necessários, nós denotamos C por código $(n, M)_q$, $(n, M, d)_q$ ou $(n, M)_q R$.

1.2 Códigos Equivalentes

Definiremos, agora, a noção de equivalência sobre códigos.

Definição 1.5. Dois códigos de comprimento n sobre um alfabeto Q são equivalentes se, e somente se, um deles pode ser obtido do outro mediante uma seqüência de operações do tipo:

(i) Substituição dos símbolos numa dada posição fixa i em todas as palavras do código por meio de uma bijeção f_i de Q.

(ii) Permutação das posições das letras em todas as palavras do código, mediante uma permutação π de $\{1, 2, \ldots, n\}$.

Observação 1.6. (i) Note que, pelo item (i) da definição, estamos efetuando uma aplicação do tipo

$$\begin{aligned} T_f^i : Q^n &\rightarrow Q^n \\ (x_1, \ldots, x_n) &\mapsto (x_1, \ldots, f(x_i), \ldots, x_n), \end{aligned}$$

onde f_i é uma bijeção de Q.

(ii) Uma permutação de $\{1, 2, \ldots, n\}$ é uma aplicação dada por:

$$\begin{aligned} T_\pi : Q^n &\rightarrow Q^n \\ (x_1, \ldots, x_n) &\mapsto (x_{\pi(1)}, \ldots, x_{\pi(n)}) \end{aligned}$$

Observe que as aplicações dos itens (i) e (ii) efetuadas em duas palavras quaisquer do código, a distância de Hamming entre elas é preservada, bem como por uma composição destas aplicações.

Da definição de códigos equivalentes, uma seqüência de operações dadas nos itens (i) e (ii), é efetuar em cada palavra-código uma aplicação do tipo

$$F = T_\pi \circ T_{f_1}^1 \circ \ldots \circ T_{f_n}^n.$$

Podemos, então, definir códigos equivalentes da seguinte forma: Dois códigos C e C' são equivalentes, se existe uma aplicação $F : Q^n \longrightarrow Q^n$, dada por

$$F = T_\pi \circ T_{f_1}^1 \circ \ldots \circ T_{f_n}^n$$

tal que $F(C) = C'$.

Note que quando dois códigos são equivalentes, as distâncias entre suas palavras são preservadas, isto é, $d(x, y) = d(F(x), F(y))$ para todo $x, y \in C$.

Exemplo 1.7. Dado o alfabeto $Q = \{1, 2, 3, 4\}$ e sejam os códigos $C = \{(113), (134), (331), (143), (111)\}$ e $C' = \{(323), (124), (141), (223), (321)\}$. Vamos verificar se C e C' são equivalentes.

Tome as bijeções f_1, f_2 e a permutação π:

$$f_1 : \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}, \quad f_2 : \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \quad \text{e} \quad \pi : \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

Por uma análise simples, tomando $F = T_\pi \circ T^1_{f_1} \circ T^2_{f_2}$, vemos que $F(C) = C'$. Assim C e C' são equivalentes.

1.3 Códigos Lineares

Uma classe de códigos muito utilizada na prática é a classe de códigos lineares e estes códigos são subespaços vetoriais sobre corpos finitos.

Um código $C \subset \mathbb{F}_q^n$ será chamado de *código linear* se for um subespaço vetorial de $\mathbb{F}_q^n$.

Seja k a dimensão de C sobre $\mathbb{F}_q$, denotada por $dim_{\mathbb{F}_q} C$, e seja $v_1, v_2, \ldots, v_k$ uma de suas bases, portanto cada elemento de C se escreve de modo único sob a forma $v = \lambda_1 v_1 + \ldots + \lambda_k v_k$ com $\lambda_i \in \mathbb{F}_q$ para todo $i = 1, 2, \ldots, n$. Segue daí que $|C| = q^k$ e conseqüentemente temos que $dim_{\mathbb{F}_q} C = k = log_q q^k = log_q |C|$.

Definição 1.8. Sejam $C \subset \mathbb{F}_q^n$ um código linear e $c = (c_1, \ldots, c_n) \in C$ uma palavra de C. Definimos o *peso* de c, denotado por $w(c)$, pelo número $w(c) = |\{c_i \ : c_i \neq 0\}|$, e definimos o *peso do código* C, denotado por $w(C)$, pelo número

$$w(C) = min\{w(x) \ : \ x \in C - \{0\}\}.$$

Enunciaremos, agora, a proposição que relaciona a distância mínima de um código linear com o seu peso.

Proposição 1.9. *Seja $C \subset \mathbb{F}_q^n$ um código linear de distância mínima d. Então, temos que:*

(i) Para todo $x, y \in \mathbb{F}_q^n$, temos $d(x, y) = w(x - y)$.

(ii) $d = w(C)$.

Note que, se C é um código linear de cardinalidade M, podemos calcular a distância mínima a partir de $M - 1$ cálculos de distâncias ao invés de $\binom{M}{2}$, o que induz um custo computacional mais barato. Acabamos de comentar uma vantagem de se trabalhar com códigos lineares.

Aproveitando os recursos intrínsecos de espaços vetoriais, a construção de códigos lineares pode ser obtida via transformações lineares, isto é, podemos representar estes códigos como imagem ou núcleo de transformações lineares, como veremos nos exemplos a seguir.

Exemplo 1.10. Como ilustração, seja C um código linear que é subespaço vetorial de $\mathbb{F}_2^5$ dado por

$$C = \{(00000), (01011), (10110), (11101)\}.$$

Como $|C| = 4$, a dimensão de C é 2. Escolhendo (10110) e (01011) como base, tal código pode ser escrito com imagem da transformação linear

$$\begin{aligned} T : \mathbb{F}_2^2 &\rightarrow \mathbb{F}_2^5 \\ (x_1, x_2) &\mapsto (x_1, x_2, x_1, x_1 + x_2, x_2) \end{aligned}$$

Exemplo 1.11. Considere o corpo finito com três elementos $\mathbb{F}_3 = \{0, 1, 2\}$ e seja $C \subset \mathbb{F}_3^4$ o código gerado pelos vetores $v_1 = (1011)$ e $v_2 = (0112)$. Este código C pode ser representado como núcleo de uma transformação linear $S : \mathbb{F}_3^4 \longrightarrow \mathbb{F}_3^2$. Tome os vetores $v_3 = (0010)$ e $v_4 = (0001)$ linearmente independentes entre si que não pertencem ao subespaço gerado por v_1 e v_2 e defina $S(0010) = (10)$, $S(0001) = (01)$, $S(1011) = (00)$ e $S(0112) = (00)$. Assim C é o núcleo da transformação linear $S(x_1, x_2, x_3, x_4) = (2x_1 + 2x_2 + x_3, 2x_1 + x_2 + x_4)$.

Definição 1.12. Sejam $\mathbb{F}_q$ um corpo finito com q elementos e $C \subset \mathbb{F}_q^n$ um código linear de dimensão k. Seja $\beta = \{v_1, \ldots, v_k\}$ uma base ordenada de C e considere a

matriz G cujas linhas são os vetores $v_i = (v_{i1}, \ldots, v_{in})$ com $i = 1, 2, \ldots, k$, isto é,

$$G = \begin{pmatrix} v_1 \\ \vdots \\ v_k \end{pmatrix} = \begin{pmatrix} v_{11} & \ldots & v_{1n} \\ v_{21} & \ldots & v_{2n} \\ \vdots & & \vdots \\ v_{k1} & \ldots & v_{kn} \end{pmatrix}.$$

Dizemos que G é a *matriz geradora* de C em relação à base β.

Assim C coincide com a imagem da seguinte transformação linear

$$\begin{aligned} T : \mathbb{F}_q^k &\rightarrow \mathbb{F}_q^n \\ x &\mapsto xG \end{aligned}$$

Se $x = (x_1, \ldots, x_k)$, então $T(x) = xG = x_1v_1 + \ldots + x_kv_k$.

A matriz G não é unicamente determinada por C, pois ela depende da base escolhida β. Efetuando operações elementares sobre as linhas da matriz geradora de um código C, obtemos uma outra matriz, que é a matriz geradora do mesmo código C, dada em relação a uma outra base de C.

A definição a seguir irá nos permitir construir códigos lineares com mais facilidade.

Definição 1.13. Diremos que uma matriz geradora de um código C está na *forma padrão*, se tivermos $G = (Id_k|A)$, onde Id_k é a matriz identidade $k \times k$ e A uma matriz de ordem $k \times (n - k)$.

Se não for possível obter a matriz geradora na forma padrão de um código linear, podemos permutar duas colunas e multiplicar uma coluna por um escalar não nulo (se necessário) afim de se obter uma matriz G' na forma padrão. Note que esta matriz G' é a matriz, na forma padrão, de um código C' equivalente a C. Logo, se G é a matriz geradora de um código C, sempre é possível obter uma matriz geradora G' de um código C', equivalente a C na forma padrão.

Sejam $u = (u_1, \ldots, u_n)$ e $v = (v_1, v_2, \ldots, v_n)$ elementos de $\mathbb{F}_q^n$, definimos o produto interno de u por

$$\langle u, v \rangle = u_1 v_1 + \ldots u_n v_n.$$

Esta operação possui as propriedades usuais de produto interno, ou seja, é simétrica $\langle u, v \rangle = \langle v, u \rangle$ e bilinear, isto é, linear em ambas as variáveis u e v.

Vale destacar que não estamos incluindo a propriedade $\langle u, u \rangle = 0$, se e somente se $u = 0$, pois esta propriedade não é válida em espaços vetoriais finitos. Como ilustração o vetor $u = (1, 1) \in \mathbb{F}_2^2$ é tal que $\langle u, u \rangle = 0$.

Naturalmente, o conceito de produto interno induz a um novo código, denotado por $C^\perp$, definido por:

$$C^\perp = \{v \in \mathbb{F}_q^n \ \ \langle v, u \rangle = 0 \ \text{ para todo } u \in C\}.$$

Este é o *código dual* de C.

Observe que, apesar das definições serem análogas, o código $C^\perp$ não pode ser visto como o complemento ortogonal do código C.

Lema 1.14. *Se $C \subset \mathbb{F}_q^n$ é um código linear de dimensão k com matriz geradora G, então:*

(i) $C^\perp$ é um subespaço vetorial de $\mathbb{F}_q^n$.

(ii) $x \in C^\perp$, se e somente se, $Gx^t = 0$.

(iii) $\dim C^\perp = n - k$.

Se a matriz geradora de C estiver em sua forma padrão, isto é, $G = (Id_k|A)$, então:

(iv) $H = (-A^t|Id_{n-k})$, é a matriz geradora de $C^\perp$.

A próxima proposição, nos dirá como se relaciona a dualidade com a equivalência de códigos lineares.

Proposição 1.15. *Sejam C e D, dois códigos lineares em $\mathbb{F}_q^n$. Se C e D são equivalentes, então $C^\perp$ e $D^\perp$ também são equivalentes.*

Lema 1.16. *Sejam C e $C^\perp$ códigos lineares de $\mathbb{F}_q^n$, e sejam G e H, respectivamente, as matrizes geradoras de C e $C^\perp$. Então:*

(i) $GH^t = 0$.

(ii) $(C^\perp)^\perp = C$.

(iii) $Hv^t = 0$, *se e somente se,* $v \in C$.

Note que o Lema 1.16 é importante para verificarmos se um vetor pertence ou não a um código C, utilizando a matriz geradora H de $C^\perp$. A matriz geradora H de $C^\perp$ é chamada *matriz teste de paridade* de C.

Para verificar se um vetor $v \in \mathbb{F}_q^n$ pertence ou não a um código C com matriz geradora G, é preciso verificar se o sistema de n equações $xG = v$ tem solução, onde $x = (x_1, \ldots, x_k)$ denota o vetor das k variáveis. Este sistema pode ter um alto custo computacional.

No entanto, trabalhando com a matriz teste de paridade H, a solução pode ser encontrada bem mais rapidamente. É só verificar se é nulo o vetor Hv^t.

A matriz teste de paridade de um código linear contém de maneira bastante simples informações sobre o valor do peso d do código. Vimos que se C é um código linear de distância mínima d, então $d = w(C)$, onde $w(C)$ é o peso do código C. Veremos isso nos dois teoremas enunciados a seguir:

Teorema 1.17. *Seja H a matriz teste de paridade de um código C. Temos que $w(C) \geq s$, se e somente se, quaisquer $s-1$ colunas de H são linearmente independentes.*

Demonstração: Suponhamos, inicialmente, que cada conjunto de $s-1$ colunas de H é linearmente independente. Seja $c = (c_1, \ldots, c_n)$, uma palavra não nula de C

e sejam $h^1, h^2, \ldots, h^n$ as colunas de H. Como $Hc^t = 0$, temos que

$$0 = Hc^t = \sum_{i=1}^{n} c_i h^i.$$

Visto que $w(c)$ é o número de componentes não nulas de c, segue que $w(c) \geq s$, pois caso contrário, se $w(c) \leq s-1$, teríamos uma combinação linear nula de t colunas de H, com $1 \leq t \leq s-1$, o que é uma contradição.

Reciprocamente, suponhamos que $w(C) \geq s$. Suponhamos, por absurdo, que exista em H um conjunto de $s-1$ colunas linearmente dependente, digamos $h^{i_1}, h^{i_2}, \ldots, h^{i_{s-1}}$. Logo existem elementos $c_{i_1}, \ldots, c_{i_{s-1}}$ no corpo, não todos nulos, tais que

$$c_{i_1} h^{i_1} + \ldots + c_{i_{s-1}} h^{i_{s-1}} = 0.$$

Portanto, existe um vetor $c \in C$ com no máximo $s-1$ componentes não nulas, logo $w(c) \leq s-1 < s$, o que é um absurdo. ■

Teorema 1.18. *Seja H, a matriz teste de paridade de um código C. Temos que $w(C) = s$ se, e somente se, quaisquer $s-1$ colunas de H são linearmente independentes e existem s colunas de H linearmente dependentes.*

Demonstração: De fato, suponhamos que $w(C) = s$, logo todo conjunto de $s-1$ colunas de H é linearmente independente, pelo teorema anterior. Por outro lado, existem s colunas de H linearmente dependentes, pois caso contrário, pelo teorema anterior, teríamos que $w(C) \geq s+1$, uma contradição.

Reciprocamente, suponhamos que todo conjunto de $s-1$ colunas de H é linearmente independente e existem s colunas linearmente dependente. Logo, pelo teorema anterior, temos que $w(C) \geq s$. Mas se $w(C) \geq s+1$, então todo conjunto com s colunas de H é linearmente independente, uma contradição. Logo $w(C) = s$.

■

O corolário a seguir, nos fornecerá uma relação entre os parâmetros de um código linear.

Corolário 1.19. *(**Cota de Singleton**) Os parâmetros (n, k, d) de um código linear satisfaz a desigualdade $d \leq n - k + 1$.*

Demonstração: Se H é a matriz teste de paridade deste código, então H tem posto $n-k$, logo tem no máximo $n-k$ colunas linearmente independentes. Portanto, pelo teorema anterior, vem que quaiquer $d-1$ colunas são linearmente independentes, logo $d-1 \leq n-k$. Daí $d \leq n-k+1$. ■

1.4 Classes de Códigos

1.4.1 Códigos de Hamming

Uma classe importante de códigos lineares é a classe dos códigos de Hamming, conforme construção abaixo.

Definição 1.20. Um código de Hamming sobre $\mathbb{F}_q$ é um código de ordem m, com matriz teste de paridade H_m de ordem $m \times n$, cujas colunas são todas as m-uplas de $\mathbb{F}_q$, duas a duas linearmente independentes, com a primeira coordenada não nula igual a 1. Temos, portanto, que o comprimento de um código de Hamming é $n = \frac{q^m-1}{q-1}$, sua dimensão é $k = n - m$ e sua distância mínima d é 3, pois é fácil encontrar três colunas linearmente dependentes em H_m.

Por argumentos simples, demonstra-se que todo código de Hamming é perfeito. Ver demonstração em [6, capítulo 11]

Exemplo 1.21. Um código de Hamming para $q = 2$ e $m = 3$ é um código sobre $\mathbb{F}_2^7$, cuja matriz teste de paridade pode ser dada por

$$H_3 = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

Note que este código tem dimensão 4.

1.4.2 Códigos MDS

Seja C um q-código de cardinalidade q^m com $m < n$. Pelo Corolário 1.19, sua distância mínima não pode ser maior do que $n - m + 1$. Vimos isso quando C é um q-código linear com $m = k = \dim C$. Veremos, agora, que esta propriedade vale para qualquer q-código com q^m palavras e comprimento n. A referência para os assuntos discutidos nesta seção é [20].

Teorema 1.22. *Seja C um q-código com q^m palavras e comprimento n, então sua distância mínima d satisfaz $d \leq r + 1$, onde $r = n - m$.*

Demonstração: Escolhendo quaiquer m posições, existem q^m possíveis designações de símbolos para estas posições. Se há duas palavras-código, dentre as q^m, que concordam nestas m posições, então $d \leq r$. Se quaisquer duas palavras-código não concordam em todas as m posições, algumas concordarão em no máximo $m - 1$ posições. Desta forma, temos que $d \leq n - m + 1 = r + 1$. ∎

Daremos ênfase, agora, a uma classe de códigos em $\mathbb{Z}_q^n$ com q^m palavras (com $m < n$), onde sua distância mínima é $d = n - m + 1$, estes códigos são chamados de *códigos MDS (máxima distância separável).*

Definição 1.23. Seja C um q-código em $\mathbb{Z}_q^n$ com q^m palavras e comprimento n. Dizemos que C é um q-código MDS se sua distância mínima d é dada por

$$d = n - m + 1.$$

Exemplo 1.24. Seja $C \subset \mathbb{Z}_3^4$, um 3-código formada pelas seguintes palavras:

$$\begin{array}{lll} (0,0,0,2) & (0,1,1,1) & (0,2,2,0) \\ (1,0,1,0) & (1,1,2,2) & (1,2,0,1) \\ (2,0,2,1) & (2,1,0,0) & (2,2,1,2) \end{array}.$$

Observe que C é um código formado por 9 palavras, logo $m = 2$ e $n = 4$, portanto $d \leq 4 - 2 + 1 = 3$. Mas observe que não existe duas palavras quaisquer de C cuja distância seja menor do que 3, logo $d \geq 3$, donde concluímos que $d = 3 = 4 - 2 + 1$, logo C é um 3-código MDS de distância mínima 3.

Observe que, no exemplo anterior, escolhendo 2 coordenadas quaisquer, é possível obter os 9 vetores de $\mathbb{Z}_3^2$, vistos como projeções dos vetores de C.

Tal propriedade é válida para todo código MDS, conforme a proposição que enunciaremos a seguir.

Proposição 1.25. *Seja C um código MDS com q^m palavras em $\mathbb{Z}_q^n$. Então m coordenadas das palavras-código podem ser consideradas como posições de informação, e as as $r = n - m$ restantes como posições redundantes. Ou seja, com m posições de uma palavra-código é possível recuperar as $r = m - n$ restantes.*

Demonstração: De fato, existem q^m vetores em um alfabeto de cardinalidade q em m posições fixadas. Como $d = r + 1$, duas quaisquer palavras-códigos x e y não podem coincidir em todas estas m coordenadas, caso contrário $d(x, y) \leq r$, contrariando a hipótese. Assim, cada uma das q^m associações possíveis ocorrem exatamente uma única vez em cada palavra-código. ■

Construção de alguns Códigos MDS

Veremos, agora, como construir alguns códigos MDS, segundo os valores de m e r.

Caso 1 : Se $m = 1$, temos um q-código MDS com cardinalidade q e distância mínima $d = r + 1$. Este código pode ser construído para qualquer r considerando $C = \{\mathbf{a} = (a, \ldots, a) \ : \ a \in \mathbb{F}_q\}$. Neste caso $d = n$.

Caso 2 : Se $r = 1$, um código MDS tem distância mínima $d = 2$ e este código pode ser formado para qualquer m, basta tomar

$$C = \{(x_1, \ldots, x_n) \in \mathbb{Z}_q^n \ : \ x_1 + \ldots + x_n = 0 \ (mod\ q)\}.$$

Note que $|C| = q^{n-1}$.

Observe que um código definido desta forma tem distância mínima 2, basta observar que $m = n - 1$, logo $d \leq 2$. Com um simples argumento mostra-se que $d \geq 2$, portanto C tem distância mínima 2.

Para os próximos casos, consideramos $C \subset \mathbb{F}_q^n$ um código MDS linear. Sabemos que a matriz teste de paridade H na forma padrão de um código linear de dimensão m tem ordem $r \times n$, onde $r = n - m$, é da forma $H = (A|I)$, onde I é a matriz identidade $r \times r$.

Para $m = 1$ ou $r = 1$, a construção é feita da mesma forma que nos casos 1 e 2.

Caso 3 : Para $m = 2$ e $r = q - 1$. As matrizes teste de paridade podem ser contruídas da seguinte forma:

a) A primeira coluna é formada somente do elemento 1.

b) O primeiro elemento da segunda coluna é 1 e os outros são dados por $\xi, \xi^2, \ldots, \xi^{q-2}$, onde ξ é a raiz primitiva do corpo $\mathbb{F}_q$, isto é, o elemento de $\mathbb{F}_q$ que gera todo $\mathbb{F}_q - \{0\}$.

c) As outras colunas são as colunas da matriz identidade $r \times r$.

Daremos, a seguir, alguns exemplos de matrizes teste de paridade de códigos MDS lineares com $m = 2$ e $r = q - 1$. Observe que $d = q$.

Para $q = d = 3$

$$H = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 2 & 0 & 1 \end{pmatrix}$$

Para $q = d = 4$

$$H = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & \xi & 0 & 1 & 0 \\ 1 & \xi^2 & 0 & 0 & 1 \end{pmatrix},$$

onde $\xi^2 + \xi + 1 = 0$. Observe que ξ é a raiz primitiva de $\mathbb{F}_4$.

Para $q = d = 5$

$$H = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 2 & 0 & 1 & 0 & 0 \\ 1 & 3 & 0 & 0 & 1 & 0 \\ 1 & 4 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Caso 4 : Para $m = 3$, códigos MDS lineares com $r = q - 1$ existem , se e somente se, q é uma potência de 2. Se q é potência de 2, uma forma geral para a porção A da

matriz teste de paridade é a primeira coluna de 1's, a segunda coluna formada por $1, \xi, \ldots, \xi^{q-2}$ e a terceira coluna formada por $1, \xi^2, \ldots, \xi^{2(q-2)}$, onde ξ é a raiz primitiva de $\mathbb{F}_q$.

1.4.3 Códigos Reed-Solomon

Um exemplo muito comum de códigos MDS lineares são os códigos Reed-Solomon.

Estes q-códigos são códigos definidos sobre o corpo finito $\mathbb{F}_q$, com $q = p^m$, onde p é primo. Uma maneira simples de definir os códigos *Reed-Solomon* é pela sua representação polinomial: para todo q, os códigos *Reed-Solomon* sobre $\mathbb{F}_q$ de dimensão k, consiste em todos os vetores da forma

$$(f(1), f(\alpha), \ldots, f(\alpha^{q-2})),$$

onde α é a raiz primitiva de $\mathbb{F}_q$, e $f(x) \in \mathbb{F}_q[x]$ percorre todos os polinômios de grau no máximo $k-1$. Para determinar a distância mínima d deste código, tome uma palavra não nula c. Logo existe um polinômio $f(x) \in \mathbb{F}_q[x]$, tal que

$$c = (f(1), f(\alpha), \ldots, f(\alpha^{q-2})).$$

Logo,

$$w(c) = |\{i \in \{0, 1, \ldots, q-2\} : \ f(\alpha^i) \neq 0\}| =$$

$$= n - |\{i \in \{0, 1, \ldots, q-2\} : \ f(\alpha^i) = 0\}| \geq$$

$$\geq n - \text{grau}(f) \geq n - (k-1) = n - k + 1,$$

onde $w(c)$ denota o peso de c, segue daí que $d \geq n - k + 1$. Pelo Corolário 1.19, obtemos que $d = n - k + 1$. Portanto o código Reed-Solomon é um código MDS linear.

Este código tem parâmetros $(n = q - 1, k, d = n - k + 1)_q$.

Se adicionarmos uma coordenada extra contendo $f(0)$, obtemos o código Reed-Solomon estendido com parâmetros $(n = q, k, d = n - k + 1)_q$.

Se for possível estender ainda mais o código Reed-Solomon, obtemos o código Reed-Solomon duplamente estendido com parâmetros $(n = q+1, k, d = n-k+1)_q$.

Capítulo 2

Coberturas

Em 1948, O. Taussky e J. Todd [21] introduziram o seguinte problema no contexto da teoria dos grupos:

> Seja G um grupo abeliano com n geradores independentes $g_1, g_2, \ldots, g_n$, cada um com ordem q e seja S o conjunto de todas as potências destes geradores. Deseja-se encontrar H um subconjunto de G tal que $G = HS$, isto é, tal que todo elemento g de G pode ser escrito na forma $g = hs$, onde h está em H e s em S. Neste caso dizemos que H forma uma cobertura de G.

Mais tarde na década de 60, O. Taussky e J. Todd reformularam este mesmo problema de uma maneira combinatória:

> Dado um conjunto G (grupo abeliano), constituído por q^n vetores de comprimento n e cada uma das coordenadas assumindo precisamente q valores, desejamos determinar um subconjunto H de G com a seguinte propriedade: qualquer vetor de G tem ao menos $n-1$ coordenadas em comum com algum vetor de H, ou seja, dado um vetor g de G, existe um vetor h de H, tal que g e h concordam, ao menos, em $n-1$ coordenadas. A cardinalidade deste subconjunto H será dada por $K_q(n)$.

J. G. Mauldon, S. K. Zaremba e E. Mattioli mostraram que se q é primo e $1 + n(q-1)$ é uma potência de q, ou digamos $1 + n(q-1) = q^r$, então

$$K_q(n) = q^{n-r}.$$

S. K. Zaremba, em 1951, estendeu o resultado acima para toda potência de primo q.

Se a cardinalidade da cobertura H for igual a $\frac{q^n}{1+n(q-1)}$, então nós temos uma 'cobertura perfeita', no sentido de que nenhum elemento de G pode ser escrito de duas maneiras distintas como produto de elementos de H e S. No contexto combinatório, podemos dizer que esta cobertura é perfeita se os conjuntos dos vetores de G que diferem em uma coordenada de cada vetor de H são disjuntos.

Como vimos na introdução, os problemas de cobertura descritos acima, são estudados desde a década de 60 em um contexto combinatório e originaram a *Teoria dos Códigos de Cobertura* no espaço métrico de Hamming Q^n já definido no Capítulo 1.

Estas questões são tratadas neste capítulo de uma forma mais geral e precisaremos de algumas definições discutidas na Seção 2.1.

Nosso objetivo é focado dentro da seguinte questão:

Dados n e R, qual é o menor número de bolas de raio R, que podem ser colocadas de tal forma que todo vetor do espaço pertence a ao menos uma destas bolas?

Na realidade, nós buscamos um código tal que as bolas de raio R centradas em cada palavra-código cubram todo espaço n-dimensional de Hamming, ou mais precisamente, queremos encontrar a cardinalidade mínima de tal código. Esta cardinalidade mínima será dada pela função $K_q(n, R)$ que é uma generalização da função $K_q(n)$, como vimos na introdução.

2.1 Definições Básicas e Propriedades da Função $K_q(n, R)$

Seja $\mathbb{Z}_q^n$, o conjunto de todos os vetores com n componentes onde cada componente assume os valores $0, 1, \ldots, q-1$. Daremos agora a definição de *cobertura*, que será crucial para entendermos a idéia do problema que será tratado neste trabalho. Os assuntos tratados nesta seção são discutidos em [3].

Definição 2.1. Um subconjunto C de $\mathbb{Z}_q^n$ é uma *R-cobertura* de $\mathbb{Z}_q^n$, ou uma *cobertura de raio R* de $\mathbb{Z}_q^n$, se todo vetor de $\mathbb{Z}_q^n$ está a uma distância de no máximo R de algum vetor de C. Em outras palavras, um subconjunto C é uma R-cobertura de $\mathbb{Z}_q^n$ se para todo $x \in \mathbb{Z}_q^n$ existe um vetor $y \in C$ tal que $d(x, y) \leq R$.

Observação 2.2. É importante salientar que um subconjunto C de $\mathbb{Z}_q^n$ não forma uma R-cobertura quando existe um vetor $x \in \mathbb{Z}_q^n$ que não é coberto por C, isto é, se existe $x \in \mathbb{Z}_q^n$ tal que para todo vetor $y \in C$, temos $d(x, y) \geq R + 1$.

Exemplo 2.3. Seja o espaço $\mathbb{Z}_2^4 = \{(a, b, c, d) : \ a, b, c, d \in \mathbb{Z}_2\}$, o subconjunto

$$C = \{(0, 0, 0, 0), (1, 1, 1, 1)\}$$

forma uma 2-cobertura para $\mathbb{Z}_2^4$, basta observar que cada elemento (a, b, c, d) dista no máximo 2 de cada um dos vetores de C. A cobertura C é minimal. De fato, qualquer subconjunto unitário C' de $\mathbb{Z}_2^4$ não forma coberturas de raio 2, basta tomar um elemento (a', b', c', d') com quatro coordenadas diferentes deste vetor, que não será coberto por C'.

Exemplo 2.4. O subconjunto

$$C = \{(0, 0, 0), (1, 1, 1), (2, 2, 2)\}$$

forma uma 2-cobertura para $\mathbb{Z}_3^3$. Note que cada tripla ordenada (a, b, c) dista no máximo 2 de algum vetor em C. Note que qualquer subconjunto C' com menos

de três vetores não forma uma 2-cobertura. De fato, projetando cada vetor de C' na primeira coordenada, podemos encontrar um elemento $x_1 \in \mathbb{Z}_3$ tal que x_1 não aparece na primeira coordenada em cada palavra de C', pois $|C'| < 3$. Repetimos este processo, projetando cada vetor de C' nas segunda e terceira coordenadas. Logo, podemos encontrar um vetor $x = (x_1, x_2, x_3)$ tal que $d(x, C') = 3 > 2$. Portanto, este vetor x não é coberto por C'.

Nosso objetivo é determinar a cardinalidade mínima deste conjunto C, ou seja, dados n e R queremos determinar a quantidade mínima de vetores que são necessários para cobrir o espaço $\mathbb{Z}_q^n$. Esta cardinalidade será dada pela função $K_q(n, R)$.

Definição 2.5. Definimos a função $K_q(n, R)$ como sendo a cardinalidade mínima de um q-código de comprimento n e raio de cobertura R, ou seja

$$K_q(n, R) = min\ \{M :\ \text{existe um } (n, M)_q R - \text{código}\}.$$

Algumas observações importantes devem ser notadas em relação a função $K_q(n, R)$.

Proposição 2.6. *Seja $C = \{x_1, \ldots, x_M\}$ uma R-cobertura mínima para $\mathbb{Z}_q^n$, logo $K_q(n, R) = M$. Então $K_q(n, R) \geq \frac{q^n}{V_q(n,R)}$, onde $V_q(n, R)$ é a cardinalidade da bola de raio R.*

Demonstração: Sendo R o seu raio de cobertura, então temos:

$$|\bigcup_{i=1}^{M} B(x_i, R)| = q^n,$$

mas $\sum_{i=1}^{M} |B(x_i, R)| \geq |\bigcup_{i=1}^{M} B(x_i, R)| = q^n$. Logo, temos que $MV_q(n, R) \geq q^n$, donde vem que

$$K_q(n, R) \geq \frac{q^n}{V_q(n, R)}. \tag{2.1}$$

■

A relação (2.1) é o limite inferior trivial de $K_q(n, R)$.

Proposição 2.7. $K_q(n, R) \leq q^{n-R}$.

Demonstração: Temos que mostrar que existe uma R-cobertura de $\mathbb{Z}_q^n$ com q^{n-R} palavras. Seja C um código, onde em cada palavra de C, fixamos $n - R$ posições. Nestas posições, tomamos todos os q^{n-R} vetores de $\mathbb{Z}_q^{n-R}$ e nas outras R posições colocamos 0 como símbolo, note que $|C| = q^{n-R}$. Dado $x \in \mathbb{Z}_q^n$, observe que $d(x, C) \leq R$. Assim, C é uma R-cobertura de $\mathbb{Z}_q^n$, donde vem que

$$K_q(n, R) \leq q^{n-R}. \tag{2.2}$$

■

A relação (2.2) é o limite superior trivial de $K_q(n, R)$.

Observação 2.8. Trivialmente vemos que $K_q(n, 0) = q^n$ e $K_q(n, n) = 1$, basta observar que se $R = 0$ a bola de raio zero é somente um ponto, logo todos os pontos de $\mathbb{Z}_q^n$ são necessários para cobri-lo. Se $R = n$, dado um vetor de $\mathbb{Z}_q^n$ a distância de todos os outros vetores do espaço a ele nunca será maior do que n, logo somente este vetor cobre todo espaço $\mathbb{Z}_q^n$.

Antes de passarmos a alguns resultados da função $K_q(n, R)$, lembremos da definição de soma direta que será importante para entendermos algumas construções e obtermos alguns resultados desta função em questão.

Se C_1 e C_2 são subconjuntos de $\mathbb{Z}_q^n$ e $\mathbb{Z}_q^m$ respectivamente, denotamos a soma direta dos vetores $x = (x_1, \ldots, x_n) \in C_1$ e $y = (y_1, \ldots, y_m) \in C_2$ como o vetor $(x, y) = (x_1, \ldots, x_n, y_1, \ldots, y_m) \in \mathbb{Z}_q^{n+m}$, e definimos a soma direta dos subconjuntos C_1 com C_2 por:

$C_1 \oplus C_2 = \{(x, y) \in \mathbb{Z}_q^{n+m} : x \in C_1 \text{ e } y \in C_2\}$. Note que esta definição não é a mesma de soma direta entre dois subespaços vetoriais, vista em álgebra linear.

Enunciaremos, agora, um teorema sobre soma direta, o que nos ajudará na demonstração de alguns resultados sobre a função $K_q(n, R)$.

Teorema 2.9. *Sejam $C_1 \subset \mathbb{Z}_q^n$ um código de raio de cobertura R_1 e $C_2 \subset \mathbb{Z}_q^m$ um código de raio de cobertura R_2. Então $C_1 \oplus C_2$ tem raio de cobertura no máximo $R_1 + R_2$. Em particular,*

$$K_q(n_1 + n_2, R_1 + R_2) \leq K_q(n_1, R_1)K_q(n_2, R_2).$$

Demonstração: O resultado sai de forma imediata, pois

$$d((x, y), C_1 \oplus C_2) = d(x, C_1) + d(y, C_2)$$

e como $d(x, C_1) \leq R_1$ e $d(y, C_2) \leq R_2$, concluímos que

$$d((x, y), C_1 \oplus C_2) \leq R_1 + R_2.$$

Projetando $\mathbb{Z}_q^{n_1+n_2}$ nos espaços $\mathbb{Z}_q^{n_1}$ e $\mathbb{Z}_q^{n_2}$, respectivamente, suponhamos que C_1 seja uma R_1-cobertura mínima de $\mathbb{Z}_q^{n_1}$, isto é, $|C_1| = K_q(n_1, R_1)$ e seja C_2 uma R_2-cobertura mínima para $\mathbb{Z}_q^{n_2}$, isto é, $|C_2| = K_q(n_2, R_2)$. É fácil ver que $C_1 \oplus C_2$ é uma $(R_1 + R_2)$-cobertura de $\mathbb{Z}_q^{n_1+n_2}$. De fato,

$$|C_1 \oplus C_2| = |C_1||C_2| = K_q(n_1, R_1)K_q(n_2, R_2).$$

Logo temos o resultado, ou seja, $K_q(n_1 + n_2, R_1 + R_2) \leq K_q(n_1, R_1)K_q(n_2, R_2)$. ■

Daremos, agora, alguns resultados sobre a função $K_q(n, R)$ em alguns lemas.

Observação 2.10. Como aplicação direta deste lema, temos que

$$K_q(n_1 + n_2, R) \leq q^{n_2}K_q(n_1, R),$$

basta ver que $K_q(n_2, 0) = q^{n_2}$. Em particular, se $n_2 = 1$ e $n_1 = n$, temos que $K_q(n + 1, R) \leq qK_q(n, R)$.

Esta observação é importante para obtermos limites superiores para $K_q(n, R)$.

Lema 2.11. *Se* $0 \leq R \leq n$, *então:*

(i) $K_q(n, R+1) \leq K_q(n, R)$.

(ii) $K_q(n, R) \leq K_{q+1}(n, R)$.

Demonstração: (i) Seja C uma R-cobertura mínima para $\mathbb{Z}_q^n$, logo $|C| = K_q(n, R)$. Esta quantidade de vetores cobre $\mathbb{Z}_q^n$ para um raio maior, como por exemplo $R+1$. Logo esta quantidade de vetores forma uma $R+1$-cobertura para $\mathbb{Z}_q^n$, daí o resultado segue.

(ii) Seja C uma R-cobertura mínima de $\mathbb{Z}_{q+1}^n$, ou seja, $|C| = K_{q+1}(n, R)$. Defina a função $f : \mathbb{Z}_{q+1} \longrightarrow \mathbb{Z}_q^n$ por:

$$f(z) = \begin{cases} z, & \text{se} \quad z < q \\ 0, & \text{se} \quad z = q. \end{cases}$$

Vamos dividir esta demonstração em dois casos:

1) Suponha que C não tenha q em nenhuma coordenada em todas as suas palavras-código. Assim C forma uma R-cobertura para $\mathbb{Z}_q^n$ e assim temos o resultado esperado.

2) Suponha, agora, que C possua q em no mínimo uma coordenada de alguma palavra-código de C, assim substituindo q por zero, obtemos um novo código C' dado por $C' = \{(f(a_1), \ldots, f(a_n)); (a_1, \ldots, a_n) \in C\}$, cuja cardinalidade satisfaz $|C'| \leq |C|$. Esta substituição de q por zero faz com que a distância de C' com todos os pontos de $\mathbb{Z}_q^n$ nunca ultrapasse R. Assim C' forma uma R-cobertura para $\mathbb{Z}_q^n$, logo o resultado também segue, ou seja, $K_q(n, R) \leq |C'| \leq |C| = K_{q+1}(n, R)$. ■

2.2 Algumas Classes Exatas de $K_q(n, R)$

Pensemos no problema das torres no tabuleiro de xadrez bi-dimensional, ou seja, $n = 2$. Podemos definir o tabuleiro de xadrez de tamanho $(q \times q)$ ao espaço $\mathbb{Z}_8^2$.

Dada uma torre em uma dada posição (a, b) no tabuleiro, temos que o conjunto de todas as casas as quais esta torre pode se movimentar corresponde ao conjunto de todos os vetores que distam uma unidade desta torre em questão, basta notar que quando a torre se move na direção horizontal a segunda coordenada não se altera, analogamente, se esta torre se move na direção vertical, a primeira coordenada não se altera.

Nosso objetivo é determinar a quantidade mínima necessária de torres que cobre todo tabuleiro. Suponha que estas torres sejam dadas pelo seguinte código $C = \{(a, a) \in \mathbb{Z}_q^2 : a \in \mathbb{Z}_q\}$ e assim, $|C| = q$. Dado $(x, y) \in \mathbb{Z}_q^2$, note que $d((x, y), (x, x)) \leq 1$ e $(x, x) \in C$, logo $d((x, y), C) \leq 1$, e assim $K_q(2, 1) \leq q$.

Seja, então C um código tal que $|C| < q$, mostraremos, agora, que ao menos um vetor $(x, y) \in \mathbb{Z}_q^2$ não é coberto por C. De fato, sempre é possível escolher $(x, y) \in \mathbb{Z}_q^2$, onde $x \neq a$ e $y \neq b$ para todo $(a, b) \in C$, logo $d((x, y), C) = 2$, o que implica que este vetor (x, y) não é coberto por C, daí $K_q(2, 1) \geq q$, logo temos que $K_q(2, 1) = q$.

A idéia desta construção deve-se a J. G. Kalbfleisch e R. G. Stanton [10], temos então a seguinte proposição:

Proposição 2.12. *Se $q \geq 2$, então $K_q(2, 1) = q$.*

Uma generalização da idéia acima foi obtida por W. A. Carnielli [3], que será dada pelo teorema a seguir. A segunda parte da demonstração deste teorema deve-se a W. Chen e I. S. Honkala [5].

Teorema 2.13. *Para todos $q \geq 2$ e $t \geq 1$, temos:*

(i) $K_q(n, n - t) = q$, *se* $n \geq (t - 1)q + 1$.

(ii) $K_q(n, n - t) > q$, *se* $n \leq (t - 1)q$.

Demonstração: (i) Limite inferior: Seja $n \geq (t-1)q+1$ e seja $C \subset \mathbb{Z}_q^n$ um código que contenha menos do que q palavras, então para cada $i = 1, 2, \ldots, n$ podemos

escolher $x_i \in \mathbb{Z}_q$, tal que $c_i \neq x_i$, para todo $c = (c_1, \ldots, c_n) \in C$, então o vetor $x = (x_1, \ldots, x_n) \in \mathbb{Z}_q^n$ satisfaz $d(x, C) = n$, logo este vetor x não é coberto por C e portanto $K_q(n, n-t) \geq q$ para todo $t \geq 1$.

Para o limite superior, escolha $C = \{\mathbf{a}= (a, \ldots, a) : a \in \mathbb{Z}_q\}$. Como $n \geq (t-1)q + 1$, então dado um vetor $x \in \mathbb{Z}_q^n$, pelo *Princípio da Casa dos Pombos*, ao menos um elemento $a \in \mathbb{Z}_q$ aparece ao menos t vezes e $d(x,\mathbf{a}) \leq n - t$, logo $K_q(n, n-t) \leq q$.

(ii) Finalmente, suponha $n \leq (t-1)q$ e $C \subset \mathbb{Z}_q^n$ um código de cobertura que tenha cardinalidade igual a q.

Afirmação: Podemos assumir (a menos de equivalência) que cada elemento de $\mathbb{Z}_q$ aparece em cada uma das primeiras j coordenadas, $0 < j < n$, da seguinte forma: a primeira palavra-código aparece com j 0's nas j primeiras coordenadas, a segunda com j 1's e assim por diante até a q-ésima palavra-código com j $(q-1)$'s e que as outras coordenadas $i > j$, nós podemos encontrar $x_i \in \mathbb{Z}_q$ que não aparece na i-ésima coordenada em qualquer palavra-código.

De fato, se não existisse o índice j satisfazendo as condições desta afirmação, poderíamos encontrar x_i que não aparece na i-ésima coordenada de cada palavra-código para todo $i = 1, 2, \ldots, n$. Assim teríamos

$$d((x_1, \ldots, x_n), C) = n > n - t,$$

o que é um absurdo, porque C é uma $(n-t)$-cobertura por hipótese.

Para todo $i \leq j$, defina $x_i \equiv i (mod\ q)$. Desta forma, temos que

$$d((x_1, \ldots, x_n), C) = (j - \lceil \frac{j}{q} \rceil) + (n-j) = n - \lceil \frac{j}{q} \rceil \geq n - \lceil \frac{n}{q} \rceil \geq n - (t-1) = n - t + 1,$$

logo $x = (x_1, \ldots, x_n)$ não é coberto por C, o que é uma contradição. Por isso $K_q(n, n-t) > q$. ∎

Observação 2.14. Note que se quisermos provar que $K_q(n, R) = K$, temos que provar que $K_q(n, R) \leq K$ (o limite superior é K) e que $K_q(n, R) \geq K$ (o limite

inferior é K). Para provarmos que $K_q(n,R) \leq K$, basta mostrar que existe um $(n,K)_q R$-código. Para provar que $K_q(n,R) \geq K$, temos que mostrar que para todo $(n,K-1)_q$-código C, existe $x \in \mathbb{Z}_q^n$, tal que para todo $c \in C$, temos que $d(x,c) \geq R+1$, isto é, existe um vetor $x \in \mathbb{Z}_q^n$ que não é coberto por C. Na maioria das vezes, esta obtenção do limite inferior não é um problema trivial.

A construção para $K_q(2,1) = q$ foi relativamente simples, isto não ocorre para $K_q(3,1)$, como veremos no teorema a seguir, cuja demonstração deve-se a J. G. Kalbfleisch e R. G. Stanton [10].

Teorema 2.15. $K_q(3,1) = \lceil \frac{q^2}{2} \rceil$.

Demonstração: Limite superior: Escolha $\mathbb{Z}_q = \{1,2,\ldots,q\}$ como nosso alfabeto. Assuma que $Q_1 = \{1,2,\ldots,i\}$ e considere o conjunto

$$C_1 = \{(a,b,c) : \ a,b,c \in Q_1 \text{ e } a+b \equiv c \ (mod\ i)\}.$$

Então todo par ordenado (x,y), com $x,y \in \mathbb{Z}_q$, ocorre (exatamente uma vez) em todas as coordenadas em C_1, caso contrário se existisse (x_1,x_2,x_3) e (x_1,x_2,x_4) em C_1 com $x_3 \neq x_4$, então teríamos $x_1+x_2 \equiv x_3 \ (mod\ i)$ e $x_1+x_2 \equiv x_4 \ (mod\ i)$, o que seria um absurdo, pois a equação $a+b \equiv c \ (mod\ i)$ tem solução única. Por isso qualquer vetor em $\mathbb{Z}_q^3$ com ao menos duas coordenadas em C_1 é coberto.

Similarmente, escolha $Q_2 = \{i+1, i+2, \ldots, q\}$ e construa o conjunto

$$C_2 = \{(a,b,c) : \ a,b,c \in Q_2 \text{ e } a+b \equiv c \ (mod\ q-i)\}.$$

Com o mesmo argumento acima, qualquer vetor em $\mathbb{Z}_q^3$ com ao menos duas coordenadas em Q_2 é coberto, ponha $C = C_1 \cup C_2$. Logo dado $x = (x_1,x_2,x_3) \in \mathbb{Z}_q^3$, então pelo menos duas coordenadas de x estão em Q_1 ou em Q_2, logo pelo Princípio da casa dos pombos, duas coordenadas de x estão em C_1 ou C_2, portanto $d(x,C) = 1$, concluímos, então, que C forma uma 1-cobertura para $\mathbb{Z}_q^3$.

Queremos encontrar um $i \in \mathbb{Z}_q$, tal que $|C|$ seja mínima. Como C_1 e C_2 são disjuntos, temos que $|C| = |C_1| + |C_2|$ e que $|C_1| = i^2$ e $|C_2| = (q-i)^2$, pois vimos que cada par ordenado $(a, b) \in Q_1^2$ aparece exatamente uma vez em $|C_1|$, o mesmo acontecendo em $|C_2|$.

É fácil de ver, então, que $|C| = i^2 + (q-i)^2$, logo $|C|$ é uma função de i. Estamos, então, querendo encontrar o ponto de mínimo desta função. Derivando em relação a i e igualando a zero, obtemos $2i = q$ e é fácil ver que o ponto crítico encontrado é um ponto de mínimo.

Escolhemos, então, $i = \lfloor \frac{q}{2} \rfloor$, se q é ímpar. Para determinar $|C|$, vamos dividir o problema em dois casos:

a) Se q é par, então $i = \frac{q}{2}$ e $|C| = \frac{q^2}{4} + \frac{q^2}{4}$, logo $|C| = \frac{q^2}{2}$.

b) Se q é ímpar, então $i = \frac{q-1}{2}$, então $|C| = \frac{(q-1)^2}{4} + \frac{(q+1)^2}{4} = \frac{q^2+1}{2}$, logo $|C| = \lceil \frac{q^2}{2} \rceil$.

Concluímos, então, que escolhendo $i = \lfloor \frac{q}{2} \rfloor$, obtemos $|C| = \lceil \frac{q^2}{2} \rceil$ que é uma 1-cobertura de $\mathbb{Z}_q^3$, logo $K_q(3, 1) \leq \lceil \frac{q^2}{2} \rceil$.

Limite inferior: Para provarmos que $K_q(3, 1) = \lceil \frac{q^2}{2} \rceil$, temos que provar que qualquer código com cardinalidade menor do que $\lceil \frac{q^2}{2} \rceil$ faz com que algum vetor de $\mathbb{Z}_q^3$ não seja coberto.

Trataremos de dois casos separadamente, quando q é par e ímpar:

a) Seja q par, então $q = 2s$ e suponha que existe uma cobertura de raio 1 H com $\frac{q^2}{2} - 1 = 2s^2 - 1$ vetores, isto é, seus vetores são da forma $h_i = (a_i, b_i, c_i)$, onde $i = 1, 2, \ldots, 2s^2 - 1$. Obteremos a contradição mostrando que existe um vetor (a, b, c) que não é coberto por H.

Escolhemos a uma componente que ocorre com menos freqüência na primeira coordenada dos vetores de H. Nós podemos supor que $a_1 = a_2 = \ldots = a_\alpha = a$, mas $a_i \neq a$, se $i > \alpha$ e $\frac{2s^2-1}{2s} < s$, então $\alpha \leq s - 1$.

Escolha $b \neq b_i$ e $c \neq c_i$, com $i = 1, 2, \ldots, \alpha$, daí (a, b, c) não é coberto por h_i

para $i \leq \alpha$. Suponha que r das componentes $b_1, b_2, \ldots, b_\alpha$ são distintas. Como cada componente ocorre ao menos α vezes (pela escolha de a), estas r componentes aparecem ao menos $r\alpha$ vezes e $r\alpha - \alpha$ destas ocorrências serão os b_i's para $i > \alpha$. Para estes $r\alpha - \alpha$ valores de i, $a \neq a_i$ e $b \neq b_i$, então (a, b, c) não é coberto por h_i. Desta forma (a, b, c) deve ser coberto pelos remanescentes $2s^2 - 1 - r\alpha$ vetores. Mas b pode ser escolhido em $2s - r$ maneiras e c em ao menos $2s - \alpha$ maneiras e assim temos que $(2s - r)(2s - \alpha) \leq 2s^2 - 1 - r\alpha$, donde vem que $2(s - \alpha)(s - r) \leq -1$, o que é um absurdo pois $r \leq \alpha \leq s - 1$.

b) Seja, agora, q ímpar, logo $q = 2s + 1$. Portanto

$$\lceil \frac{q^2}{2} \rceil = \frac{q^2 + 1}{2} = 2s^2 + 2s + 1.$$

Suponha que exista uma cobertura H com os vetores $h_i = (a_i, b_i, c_i)$ com $i = 1, 2, \ldots, 2s^2+2s$. Analogamente ao item a), escolha a a componente menos freqüente na primeira coordenada dos vetores de H e ponha $a_1 = a_2 = \ldots = a_\alpha = a$ e $a_i \neq a$ para $i > \alpha$. Como $\frac{2s^2+2s}{2s+1} < s + 1$, então $\alpha \leq s$. Escolha $b \neq b_i$ e $c \neq c_i$ para $i = 1, 2, \ldots, \alpha$ e suponha que r das componentes $b_1, \ldots, b_\alpha$ são distintas, então estas r componentes aparecem ao menos $r\alpha$ vezes e $r\alpha - \alpha$ destas ocorrências serão os b_i's para $i > \alpha$. Então (a, b, c) deve ser coberto pelos $2s^2 + 2s - r\alpha$ vetores remanescentes, logo b pode ser escolhido de $2s + 1 - r$ vezes e c de $2s + 1 - \alpha$ vezes, logo $(2s+1-r)(2s+1-\alpha) \leq 2s^2+2s-r\alpha$, donde vem que: $(s-\alpha)[2(s-r)+1] \leq r-s-1$, o que é um absurdo, pois a expressão do lado esquerdo da desigualdade é não negativa e a do lado direito é negativa.

Portanto a prova está concluída. ■

Note que a construção de q-códigos para o caso de $K_q(3, 1)$ (tridimensional) foi bem mais complicada em relação à obtenção de $K_q(2, 1)$ (bidimensional).

A partir do Teorema 2.15 fica fácil mostrar que $K_2(4, 1) = 4$. De fato, utilizando este teorema, vemos que $K_2(3, 1) = 2$, logo pela Observação 2.10 visto na seção anterior, temos que $K_2(4, 1) \leq 4$. Utilizando agora o limite inferior trivial (2.1)

vem que $K_2(4,1) \geq 4$, donde concluímos que $K_2(4,1) = 4$. É de se esperar que a obtenção de $K_q(4,1)$ seja um problema bastante difícil. De fato, basta observar na tabela 6.4, que a classe $K_5(4,1)$ não é conhecida.

O próximo resultado é devido a A. C. Lobstein [15].

Teorema 2.16. *$K_2(2R+2, R) = 4$, para todo $R = 0, 1, \ldots$.*

Demonstração: Limite inferior: Assuma que C é um $(2R+2, K)_2$-código com $K < 4$. Como existem menos que quatro palavras-código em C, podemos escolher o par x_1x_2, tal que este par não aparece como as duas primeiras coordenadas em qualquer palavra-código de C. Similarmente, escolha os pares $x_3x_4, \ldots, x_{2R+1}x_{2R+2}$, da mesma forma em que escolhemos x_1x_2. Então, o vetor $x = (x_1, \ldots, x_{2R+2})$ dista ao menos $R+1$ de C. Assim $K_2(2R+2, R) \geq 4$.

Limite superior: Tome o código $C = \{(0,\overline{0}), (0,\overline{1}), (1,\overline{0}), (1,\overline{1})\}$, onde $\overline{0}$ e $\overline{1}$ são, respectivamente, vetores de comprimento $2R+1$ formado somente por 0's e 1's. Note que $|C| = 4$.

Afirmação: Este código tem raio de cobertura igual a R. De fato, dado $x = (x_1, x_2, \ldots, x_{2R+2})$, temos que as duas primeiras coordenadas de x são cobertas por C, então projetemos o vetor x a cada par $x_{2i+1}x_{2i+2}$ de coordenadas consecutivas, com $i = 1, 2, \ldots, R$. Projetando cada palavra de C aos respectivos pares de coordenadas correspondentes a x, temos que cada par de projeções de x dista no máximo 1 das projeções correspondentes em C. Como temos R projeções distintas, vem que $d(x, C) \leq R$, o que implica que C tem raio de cobertura igual a R, logo $K_2(2R+2, R) \leq 4$. Portanto, temos o resultado. ■

Enunciaremos, agora, um teorema importante que envolve o alfabeto $\mathbb{F}_q$, quando q é primo ou potência de um primo. Neste caso, temos que o espaço de Hamming $\mathbb{F}_q^n$ em questão é um espaço vetorial, pois $\mathbb{F}_q$ é um corpo finito.

Nosso objetivo é determinar sobre que condições podemos determinar uma 1-cobertura perfeita para este espaço (não esquecendo que esta cobertura perfeita

é um código perfeito). Este resultado será dado pelo Teorema de Zaremba. A demonstração deste teorema deve-se a S. K. Zaremba, utilizando a teoria dos grupos, mas daremos aqui uma demonstração mais simplificada feita por G. Losey [16].

Teorema 2.17. *Se q é um primo ou uma potência de um primo e $1+n(q-1)$ é igual a q^r, para algum r, então existe uma 1-cobertura perfeita H de $\mathbb{F}_q^n$ de cardinalidade q^{n-r}. Logo $K_q(\frac{q^r-1}{q-1}, 1) = q^{n-r}$.*

Demonstração: Seja $\mathbb{F}_q$ um corpo finito com q elementos, logo $\mathbb{F}_q^n$ é um espaço vetorial de dimensão n sobre $\mathbb{F}_q$. Seja $\{e_1, \ldots, e_n\}$ a base canônica de $\mathbb{F}_q^n$.

Seja V um subespaço de dimensão r sobre $\mathbb{F}_q$, então o número de subespaços unidimensionais de V é $m = \frac{q^r-1}{q-1}$. De fato, tome $\mathcal{M}$ como sendo o conjunto maximal formado pelos subespaços unidimensionais possíveis em V e suponha que $|\mathcal{M}| = m$, com

$$\mathcal{M} = \{V_1, \ldots, V_m\},$$

onde V_i são os possíveis subespaços unidimensionais para V. Logo todos estes subespaços são disjuntos se não considerarmos o vetor nulo em cada um destes subespaços. Portanto é fácil ver que $V = \bigcup_{i=1}^{m} V_i$, assim

$$|V| = |V_1| + \ldots + |V_m| + 1,$$

logo $q^r = m(q-1) + 1$, donde vem que $m = \frac{q^r-1}{q-1} = n$.

Sejam v_i um vetor representante de V_i, $1 \leq i \leq n$. Defina a transformação linear $T : \mathbb{F}_q^n \longrightarrow V$ por $T(e_i) = v_i$. É fácil ver que T é sobrejetora. De fato, dado $v \in V$ não nulo, temos que v está em exatamente um subespaço unidimensional de V, logo $v = \lambda_i v_i$ para algum $i = 1, 2, \ldots, n$. Tome, então, $u = \lambda_i e_i \in \mathbb{F}_q^n$ e temos que $T(u) = T(\lambda_i e_i) = \lambda_i T(e_i) = \lambda_i v_i = v$, logo T é sobrejetora.

Seja H o núcleo de T, ou seja $H = Ker(T)$, logo pelo teorema do núcleo e da imagem temos que $n = dimH + dimV$, portanto $dimH = n - r$, o que implica que $|H| = q^{n-r}$.

Resta provar que H é uma 1-cobertura perfeita. De fato, seja $x \in \mathbb{F}_q^n$, então $T(x) \in V$, logo $T(x)$ está em algum dos subespaços unidimensionais de V, portanto $T(x) = \lambda v_i$ para algum $\lambda \in \mathbb{F}_q$, $v_i \in V_i$ com $i = 1, \ldots, n$. Logo $T(x - \lambda e_i) = \lambda v_i - \lambda v_i = 0$, então $w = x - \lambda e_i \in H = Ker(T)$. Desta maneira $x = w + \lambda e_i$, o que implica que x difere de w no máximo na i-ésima coordenada, por isso H é uma 1-cobertura de $\mathbb{F}_q^n$ de cardinalidade q^{n-r}. Para mostrar que H é perfeita, basta observar que $|H| = q^{n-r} = \frac{q^n}{q^r} = \frac{q^n}{1+n(q-1)}$, logo H é perfeita e o resultado segue, isto é, $K_q(\frac{q^r-1}{q-1}, 1) = q^{n-r}$. ∎

Exemplo 2.18. Para o caso em que $q = 2$, obtemos que $K_2(2^r - 1, 1) = 2^{2^r - r - 1}$.

O Teorema de Zaremba pode ser generalizado para raios arbitrários.

2.3 Classes Induzidas

Enunciaremos, a seguir, dois resultados obtidos por W. A. Carnielli [3], em que obteremos o limite superior para classes de cobertura em espaços maiores a partir de classes em espaços menores conhecidas.

Teorema 2.19. *Para todos $n, r, q \geq 1$ e p, k, tais que $0 \leq p < r$ e $0 < k \leq n$, vale a seguinte desigualdade:*

$K_q(nr, kr + (n-k)p) \leq K_a(n, k)$, *onde* $a = K_q(r, p)$.

Demonstração: Temos que provar que $K_a(n, k)$ vetores forma uma $(kr+(n-k)p)$-cobertura para $\mathbb{Z}_q^{nr}$.

Considere um vetor

$x = (x_1, \ldots, x_r, x_{r+1}, \ldots, x_{2r}, x_{2r+1}, \ldots, x_{(n-1)r}, x_{(n-1)r+1}, \ldots, x_{nr}) \in \mathbb{Z}_q^{nr}$.

Podemos considerar x como um vetor do tipo $x = (Y_0, Y_1, \ldots, Y_{n-1})$, onde $Y_i = (x_{ir+1}, \ldots, x_{(i+1)r})$, com $i = 0, 1, \ldots, n-1$.

Seja $a = K_q(r, p)$ a cardinalidade mínima de uma p-cobertura de $\mathbb{Z}_q^r$ dada por um conjunto H_1, então para todo $Y_i \in \mathbb{Z}_q^r$, existe um $Z_j \in H_1$, tal que Y_i e Z_j discordam

em no máximo p coordenadas. Agora, considere $K_a(n,k)$ a cardinalidade mínima de uma k-cobertura de $\mathbb{Z}_a^n$ dada por um conjunto H_2, onde os símbolos são os elementos de H_1. Então, dado um vetor $Z = (Z_0, Z_1, \ldots, Z_{n-1}) \in \mathbb{Z}_a^n$, existe um vetor $W \in H_2$, tal que W e Z discordam em no máximo k coordenadas. Assim W e Z discordam em no máximo kr coordenadas. Agora, levando em consideração as $n-k$ coordenadas em que eles concordam, não esquecendo que estas coordenadas são elementos de H_1, temos que, nestas coordenadas, eles discordam em no máximo $(n-k)p$ coordenadas. Logo W e x discordam em no máximo $kr + (n-k)p$ coordenadas, o que podemos concluir que $K_a(n,k)$ vetores formam uma $(kr+(n-k)p)$-cobertura para $\mathbb{Z}_q^{nr}$, logo o resultado segue, isto é, $K_q(nr, kr + (n-k)p) \leq K_a(n,k)$, onde $a = K_q(r,p)$. ■

Exemplo 2.20. Sejam $n = 3$, $r = 3$, $q = 3$ e $k = 2$. O Teorema 2.19 nos fornece que $K_3(9,7) \leq K_5(3,2) = 5$, melhorando o limite superior trivial que é dado por $K_3(9,7) \leq 9$.

Exemplo 2.21. Sejam $r = 3$, $n = 4$, $k = p = 1$ e $q = 2$. Uma aplicação direta do Teorema 2.19, mostra que $K_2(12,6) \leq K_2(4,1)$. Já vimos que $K_2(4,1) = 4$, logo $K_2(12,6) \leq 4$. Podemos observar que a obtenção do limite superior de $K_2(12,6)$, usando o Teorema 2.19 não é boa, pois utilizando o Teorema 2.13, obtemos que $K_2(12,6) = 2$.

Veremos agora, como encontrar um vetor na cobertura, dado um vetor em $\mathbb{Z}_2^{12}$, satisfazendo as condições do Teorema 2.19

Seja o vetor $x = (000, 111, 010, 001) \in \mathbb{Z}_2^{12}$. Pelo Teorema 2.15, vem que $K_2(3,1) = 2$. Podemos supor que $H_1 = \{000, 111\}$(não esquecendo que este código em questão é um código perfeito), assim $a = K_2(3,1) = 2$. Fazendo $H_1 = \{\overline{0}, \overline{1}\}$, onde $\overline{0} = (000)$ e $\overline{1} = (111)$, então o vetor x pode ser visto como o vetor

$$Y = (000, 111, 000, 000),$$

que pode ser visto como o vetor $Z = (\overline{0}, \overline{1}, \overline{0}, \overline{0}) \in \mathbb{Z}_2^4$.

Seja H_2 uma 1-cobertura para $\mathbb{Z}_2^4$ que contenha o vetor $(\overline{0},\overline{0},\overline{0},\overline{0})$, logo H_2 pode ser dada por

$H_2 = \{(\overline{0},\overline{0},\overline{0},\overline{0}),(\overline{0},\overline{0},\overline{0},\overline{1}),(\overline{1},\overline{1},\overline{1},\overline{0}),(\overline{1},\overline{1},\overline{1},\overline{1})\}$, pois $K_2(4,1) = 4$. Para este vetor Z dado existe um vetor $W = (\overline{0},\overline{0},\overline{0},\overline{0}) \in H_2$, tal que W e Z diferem em no máximo uma coordenada, assim vemos que W e x diferem em cinco coordenadas (o que satisfaz as condições do Teorema 2.19).

O próximo teorema está relacionado com a existência de um d-código MDS. Como vimos no capítulo anterior um d-código MDS em $\mathbb{Z}_q^n$ é definido como um subconjunto G de $\mathbb{Z}_q^n$ com exatamente q^m vetores, onde $d = n - m + 1$, tal que a distância $d(x,y)$ entre x e y é tal que $d(x,y) \geq d$ para todo $x, y \in G$.

Para facilitar as demonstrações, trabalharemos com um $(d+1)$-código MDS.

Teorema 2.22. *Se existe um $(d+1)$-código MDS em $\mathbb{Z}_q^n$, então para todo $r \geq 1$, a seguinte desigualdade segue: $K_{qr}(n,d) \leq q^{n-d}K_r(n,d)$.*

Demonstração: Notemos primeiro que no $(d+1)$-código MDS $G \subset \mathbb{Z}_q^n$, qualquer escolha de $n-d$ coordenadas (dos n lugares possíveis) apresenta todos os q^{n-d} vetores de $\mathbb{Z}_q^{n-d}$, pois caso contrário, se dois vetores de G concordam em $n-d$ coordenadas, a distância entre eles seria igual a $d < d+1$ o que seria um absurdo.

Seja $X = (a_1,\ldots,a_n)$ um vetor de $\mathbb{Z}_{qr}^n$, logo como cada $a_i \in \mathbb{Z}_{qr}$ com $i = 1,2,\ldots,n$, podemos escrever $a_i = rb_i + c_i$, onde $b_i \in \mathbb{Z}_q$ e $c_i \in \mathbb{Z}_r$. Podemos considerar os vetores $X_1 = (b_1,\ldots,b_n)$ em $\mathbb{Z}_q^n$ e $X_2 = (c_1,\ldots,c_n)$ em $\mathbb{Z}_r^n$, temos então que $X = rX_1 + X_2$.

Se um conjunto H é uma d-cobertura mínima de $\mathbb{Z}_r^n$, isto é, $|H| = K_r(n,d)$ e G é um $(d+1)$-código MDS de $\mathbb{Z}_q^n$, afirmamos que o conjunto

$$rG + H = \{rZ_1 + Z_2 \ : Z_1 \in G \text{ e } Z_2 \in H\}$$

é uma d-cobertura para $\mathbb{Z}_{qr}^n$. De fato, dado $X \in \mathbb{Z}_{qr}^n$, temos que $X = rX_1 + X_2$, onde $X_1 \in \mathbb{Z}_q^n$ e $X_2 \in \mathbb{Z}_r^n$, então como H é uma d-cobertura de $\mathbb{Z}_r^n$, temos que existe

um vetor $Z_2 \in H$, tal que Z_2 e X_2 discordam em no máximo d coordenadas e como G é um $(d+1)$-código MDS, existe um vetor $Z_1 \in G$, tal que Z_1 e X_1 discordam em no máximo d coordenadas. Observemos que, pelo fato de G ser um $(d+1)$-código MDS, podemos escolher Z_1, tal que Z_1 discorda com X_1 nas mesmas coordenadas em que Z_2 discorda com X_2, isto é sempre possível.

Logo $Z = rZ_1 + Z_2$ discorda com $X = rX_1 + X_2$ em no máximo d coordenadas. Daí $rG+H$ forma uma d-cobertura para $\mathbb{Z}_{qr}^n$ e como $|rG+H| = q^{n-d}K_r(n,d)$, temos que o resultado segue, logo $K_{qr}(n,d) \leq q^{n-d}K_r(n,d)$. ■

Exemplo 2.23. Ilustraremos a construção acima para o caso em que $q = 3$, $r = 2$ e $n = 3$ e seja G um código MDS de $\mathbb{Z}_3^3$ para $m = 2$ dado abaixo:

$$G = \{(000), (012), (021), (102), (111), (120), (201), (210), (222)\}.$$

É fácil ver que sua distância mínima é 2, logo $d = 1$.

Seja $H = \{(000), (111)\}$ uma 1-cobertura mínima para $\mathbb{Z}_2^3$ (vimos, no Exemplo 1.4, que esta é uma 1-cobertura mínima perfeita). Pelo Teorema 2.22, o conjunto

$$2G + H = \{2Z_1 + Z_2 \ : \text{onde } Z_1 \in G \text{ e } Z_2 \in H\}$$

forma uma 1-cobertura para $\mathbb{Z}_6^3$.

Dado um vetor $Y = (450) \in \mathbb{Z}_6^3$, queremos encontrar um vetor da cobertura que satisfaz as condições do teorema.

Logo, considere a associação $4 = 2.2 + 0$, $5 = 2.2 + 1$ e $0 = 2.0 + 0$.

Em termos vetoriais $(450) = 2(220) + (010)$.

Para o vetor (010), podemos tomar o vetor $X_2 = (000) \in H$ e para o vetor (220), podemos tomar o vetor $X_1 = (210) \in G$. Observemos que escolhemos
$(210) \in G$, pois é na segunda coordenada que (010) difere de $(000) \in H$, logo o vetor X procurado é $X = 2(210) + (000) = (420)$ que discorda de Y somente em uma coordenada.

Da mesma forma que no exemplo anterior, aplicando o teorema substituindo os valores de n, r e q obtemos $K_6(3,1) \leq 3^2 K_2(3,1) = 18$, observemos que este teorema neste exemplo melhora o limite superior trivial. De fato, sabemos que $K_6(2,1) = 6$, logo $K_6(3,1) \leq 36$ (portanto o Teorema 2.22 melhora este limite superior). Note que neste teorema, obtemos uma outra forma de obter o limite superior de $K_6(3,1)$, e vimos que pelo Teorema 2.15, $K_6(3,1) = 18$.

Recordando alguns casos de existência de $(d+1)$-códigos MDS na subseção 1.4.2 e como conseqüência do Teorema 2.22, obteremos alguns limites particulares para $K_{qr}(n,d)$, dado pelo corolário a seguir.

Corolário 2.24. *Valem as propriedades:*

a) $K_{qr}(n,1) \leq q^{n-1} K_r(n,1)$*, para um 2-código MDS.*

b) $K_{qr}(n,n-2) \leq q^2 K_r(n,n-2)$*, se existe um* $(n-1)$*-código MDS, para todo* $2 \leq n \leq q+1$*, onde* q *é primo ou potência de primo.*

A demonstração do Corolário 2.24 segue diretamente do Teorema 2.22

Apresentaremos, a seguir, a demonstração de um caso particular do Teorema 2.22, que se refere ao caso de existência de códigos MDS de distância mínima 2, cujo resultado é devido a R. G. Stanton, J. D. Horton e J. G. Kalbfleisch, e redescoberto por A. Blokhuis e C. W. Lam [2]. Faremos esta demonstração para $r = t$, e t exercendo o papel de q no Teorema 2.22.

Teorema 2.25. *Para todo* $q \geq 2$ *e* $t \geq 1$*, temos* $K_{tq}(n,1) \leq t^{n-1} K_q(n,1)$.

Demonstração: Seja C um código sobre o alfabeto $Q = \{0,1,\ldots,q-1\}$ que atinge o limite $K_q(n,1)$. Defina o código

$$C' = \{(c_1 t + b_1, c_2 t + b_2, \ldots, c_n t + b_n) : (c_1, c_2, \ldots, c_n) \in C$$

$$0 \leq b_i < t \text{ para todo } i = 1,2,\ldots,n \text{ com } b_1 + b_2 + \ldots + b_n = 0 \ (mod\ t)\}.$$

C' é um código sobre o alfabeto $\{0, 1, \ldots, tq-1\}$ e note que os vetores $(b_1, b_2, \ldots, b_n)$, tais que $b_1 + b_2 + \ldots + b_n = 0 \ (mod \ t)$ formam um código MDS de distância mínima 2, logo o número de vetores deste código é t^{n-1}. Assim $|C'| = t^{n-1}K_q(n, 1)$. **Afirmação**: C' é um código de cobertura 1.

Usando o mesmo argumento do Teorema 2.22, obtemos o resultado. ■

Exemplo 2.26. Sabendo que $K_6(3, 1) = 18$, a Observação 2.10 nos fornece que $K_6(4, 1) \leq 108$. Aplicando o Teorema 2.25, obtemos que $K_6(4, 1) \leq 72$, melhorando este limite superior.

Capítulo 3

Coberturas usando matrizes

Vamos relembrar o que é uma R-cobertura no espaço de Hamming. Vimos que H é uma R-cobertura de $\mathbb{Z}_q^n$ se para todo $x \in \mathbb{Z}_q^n$, existe $y \in H$ tal que x e y diferem em no máximo R coordenadas. Neste caso, podemos escrever o vetor x da seguinte forma:

$$x = y + \sum_{i=1}^{m} a_i e_{k_i},$$

onde $m \leq R$, $a_i \in \mathbb{Z}_q^n$ e e_{k_i} são vetores canônicos de $\mathbb{Z}_q^n$. Observe que estamos escrevendo o vetor x como soma de um vetor $y \in H$ com uma combinação linear de no máximo R colunas da matriz identidade $I_{n\times n}$.

O método de cobertura usando matrizes é uma generalização das coberturas clássicas, no seguinte sentido: além do vetor $y \in H$ e dos vetores canônicos da matriz identidade, permitimos outros vetores de $\mathbb{Z}_q^n$ na combinação linear que gera x. Isto ficará mais claro quando enunciarmos a definição do método de cobertura usando matrizes.

As coberturas usando matrizes foram desenvolvidas inicialmente por A. Blokhuis e C. W. H. Lam [2] para o caso em que $R = 1$, que é uma sistematização de alguns resultados anteriores de H. J. L. Kamps e J. H. van Lint . A generalização deste método, para R arbitrário, foi apresentada por J. H. van Lint Jr. e independentemente por W. A. Carnielli [4].

3.1 O Método das Matrizes

Definição 3.1. Suponha que $A = (I_r|M)$ uma matriz de ordem $r \times n$, onde I_r é a matriz identidade de ordem $r \times r$. Um conjunto $S \subset \mathbb{Z}_q^r$ é uma *m-cobertura de* $\mathbb{Z}_q^r$ *usando a matriz* A, se para todo $x \in \mathbb{Z}_q^r$, x pode ser escrito como soma de um elemento de S e uma $\mathbb{Z}_q$-combinação linear de no máximo m colunas de A, isto é, dado $x \in \mathbb{Z}_q^r$, nós podemos encontrar uma palavra $y \in \mathbb{Z}_q^n$ de peso no máximo m e um elemento $s \in S$, tal que $x = s + Ay$.

Exemplo 3.2. O conjunto $S = \{(0,0),(1,1)\}$ não é uma 1-cobertura de $\mathbb{Z}_3^2$, pois o vetor $(2,2)$ não é coberto por S. No entanto, S é uma 1-cobertura usando a matriz

$$A = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}.$$

De fato, observe que todo vetor de $\mathbb{Z}_3^2$, com exceção do vetor $(2,2)$ é 1-coberto por S. Logo, podemos escrever o vetor $(2,2)$ da seguinte maneira:

$$(2,2) = (0,0) + 2(1,1).$$

Portanto S é uma 1-cobertura de $\mathbb{Z}_3^2$ usando a matriz A.

Enunciaremos a seguir o teorema mais importante desta seção que será dado com o fim de obter os limites induzidos para coberturas em espaços de dimensões maiores. A demonstração do teorema a seguir deve-se a A. Blokhuis e C. W. Lam [2].

Teorema 3.3. *Se S é uma m-cobertura de $\mathbb{Z}_q^r$ usando a matriz $A = (I_r|M)$, então o código $C = \{x \in \mathbb{Z}_q^n : Ax \in S\}$ tem cardinalidade $|S|q^{n-r}$ e forma uma m-cobertura para $\mathbb{Z}_q^n$. Como conseqüência, $K_q(n,m) \leq |S|q^{n-r}$.*

Demonstração: Suponha que $z \in \mathbb{Z}_q^n$, então $Az \in \mathbb{Z}_q^r$ e como S é uma m-cobertura de $\mathbb{Z}_q^r$ usando A, existe um $y \in \mathbb{Z}_q^n$ de peso no máximo m e um $s \in S$,

tal que $Az = s + Ay$, logo $A(z - y) \in S$ e por isso $z - y \in C$ e é fácil ver que $d(z, z - y) \leq m$. Mostraremos, agora, que $|C| = |S|q^{n-r}$.

De fato, denotemos uma n-upla de $\mathbb{Z}_q^n$ por $(u; v)^T$, onde u representa as primeiras r componentes e v as últimas $n - r$ componentes. Desta forma

$$A(u; v)^T = (I|M)(u; v)^T = u + Mv \in \mathbb{Z}_q^r.$$

Para cada $s \in S$, nós podemos escolher v arbitrariamente e escolher u a ser $s - Mv$ para obter $(u; v)^T \in S$, isto é, $(s - Mv; v)^T \in S$. Existem q^{n-r} escolhas para v e $|S|$ escolhas para s, logo $|C| = |S|q^{n-r}$. ∎

Podemos observar facilmente, utilizando o Exemplo 3.2, que $K_3(3, 1) \leq 6$.

O próximo teorema é baseado na existência de códigos MDS e sua demonstração deve-se a W. A. Carnielli [4].

Teorema 3.4. *Sejam $q \geq 1$, $r \geq 1$ e $n \geq d$. Se L é um $(d+1)$-código MDS de $\mathbb{Z}_q^n$, então existe um conjunto S tal que $|S| = K_r(n, d)$ e S é uma $(d + 1)$-cobertura de $\mathbb{Z}_{qr}^n$ usando uma matriz A de ordem $n \times (n + q^{n-d} - 1)$.*

Demonstração: Seja cada vetor $x \in \mathbb{Z}_{qr}^n$ escrito da forma $x = x_1 + rx_2$, onde $x_1 \in \mathbb{Z}_r^n$ e $x_2 \in \mathbb{Z}_q^n$, isto é possível pois cada coordenada a, tal que $0 \leq a < qr$, podemos escrever $a = b + rc$, onde $0 \leq b < r$ e $0 \leq c < q$. Seja S uma d-cobertura mínima para $\mathbb{Z}_r^n$, isto é, $|S| = K_r(n, d)$ e A uma matriz de ordem $n \times (n + q^{n-d} - 1)$ dada por $A = (I|M)$, onde I é a matriz identidade de ordem $n \times n$ e M é a matriz cujas colunas são todos os vetores não nulos de L. Logo para $x = x_1 + rx_2$ existe um vetor $y_1 \in S$, onde y_1 discorda com x_1 em no máximo d coordenadas e é possível escolher $y_2 \in L$, onde y_2 discorda de x_2 em no máximo d coordenadas (não esquecendo que $y_2 \in L$ deve ser escolhido nas mesmas coordenadas em que y_1 discorda com x_1). Então se $y = y_1 + ry_2$, então y difere de x em no máximo d coordenadas. Logo $x = y + \sum_{k=1}^{d} a_{i_k} e_{i_k}$, donde vem que $x = y_1 + ry_2 + \sum_{k=1}^{d} a_{i_k} e_{i_k}$, onde $y_1 \in S$, y_2 e e_{i_k} são colunas da matriz A. Logo S é uma $(d + 1)$-cobertura de $\mathbb{Z}_{qr}^n$ usando a matriz A. ∎

Exemplo 3.5. Podemos tomar como exemplo o conjunto

$$S = \{(0000), (1000), (0111), (1111)\}$$

que é uma 2-cobertura de $\mathbb{Z}_4^4$ usando a matriz

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

Note que os últimos sete vetores à direita e o vetor nulo formam um 2-código MDS em $\mathbb{Z}_2^4$. Observe também que S é uma 1-cobertura mínima de $\mathbb{Z}_2^4$, logo pelo Teorema 3.3, S forma uma 2-cobertura de $\mathbb{Z}_4^4$ usando a matriz A.

Como aplicação dos Teoremas 3.3 e 3.4, temos o seguinte corolário:

Corolário 3.6. *Se $q \geq 1$, $r \geq 1$, $n \geq d$ e existe um $(d+1)$-código MDS em $\mathbb{Z}_q^n$, então*

$$K_{qr}(n+k, d+1) \leq K_r(n,d)(qr)^k,$$

onde $k = q^{n-d} - 1$.

Demonstração: Pelo Teorema 3.4, existe um conjunto S tal que $|S| = K_r(n,d)$ e S é uma $(d+1)$-cobertura de $\mathbb{Z}_{qr}^{n+k}$ usando a matriz $A = (I|M)$ de ordem

$$n \times (n + q^{n-d} - 1),$$

logo pelo Teorema 3.3, temos que

$$K_{qr}(n+k, d+1) \leq |S|(qr)^k = K_r(n,d)(qr)^k.$$

■

Como conseqüência deste corolário, podemos aplicá-lo em alguns casos de códigos MDS, vistos no capítulo 1.

(a) Sabemos que existe 2-código MDS em $\mathbb{Z}_q^n$ para todo n,q com $q \geq 2$, logo $K_{qr}(n+a, 2) \leq K_r(n,1)(qr)^a$, onde $a = q^{n-1} - 1$.

(b) Para todo n,q com q primo ou potência de primo e $2 \leq n \leq q+1$, existe um $(n-1)$-código MDS em $\mathbb{Z}_q^n$, logo $K_{qr}(n+b, n-1) \leq K_r(n, n-2)(qr)^b$, onde $b = q^2 - 1$.

Exemplo 3.7. (a) Para $n = 4$, $q = 3$ e $r = 3$, temos que $K_9(30, 2) \leq K_3(4, 1)9^{26}$, mas pelo Teorema de Zaremba 2.17, vem que $K_3(4, 1) = 9$, logo

$$K_9(30, 2) \leq 3^{54}.$$

(b) Para $n = 4$, $q = 3$ e $r = 2$, temos que $K_6(12, 3) \leq K_2(4, 2)6^8$. Mas

$$K_2(4, 2) = 2,$$

pelo Teorema 2.13, logo $K_6(12, 3) \leq 2.6^8$.

3.2 Limites Induzidos

Veremos, agora, alguns teoremas envolvendo coberturas usando matrizes. Estes teoremas derivam do Teorema 3.3 e melhoram alguns limites superiores triviais. Os dois próximos teoremas que veremos a seguir devem-se a A. Blokhuis e C. W. H. Lam. [2]

Teorema 3.8. *Se p é um número primo e $n = t[\frac{p^{r-1}-1}{p-1}] + 1$ para inteiros $p \geq t > 0$ e $r > 1$, então $K_p(n, 1) \leq (p - t + 1)p^{n-r}$.*

Demonstração: Seja $S = \{s_j = (0, \ldots, 0, j) \in \mathbb{Z}_p^r : 0 \leq j \leq p - t\}$. Desta forma $|S| = p - t - 1$ e para construir a matriz A começamos dos $\frac{p^{r-1}-1}{p-1}$ vetores não nulos projetivos em $\mathbb{Z}_p^{r-1}$, cuja primeira componente não nula é 1, isto é, basta fazer a contagem $p^{r-2} + p^{r-3} + \ldots + 1 = \frac{p^{r-1}-1}{p-1}$.

Para cada um destes vetores em $\mathbb{Z}_p^{r-1}$, digamos x, nós construiremos t colunas de A denotadas por $(x; i)^T$, onde $0 \leq i \leq t - 1$, desta forma temos $t(\frac{p^{r-1}-1}{p-1})$ colunas de A e para a última coluna de A, tomamos $e_r = (0, 0, \ldots, 1)$ e permutando as colunas de A observamos que $A = (I|M)$, onde I é a matriz identidade $r \times r$.

Afirmação: S é uma 1-cobertura de $\mathbb{Z}_p^r$ usando a matriz A.

De fato, seja $(x;y)^T \in \mathbb{Z}_p^r$, onde $x \in \mathbb{Z}_p^{r-1}$ e $y \in \mathbb{Z}_p$. Se x é o vetor nulo, então $(x;y)^T = s_0 + ye_r$, onde $s_0 \in S$ e e_r^T é uma coluna de A. Se $x \neq 0$, então, como p é primo, $\mathbb{Z}_p$ é corpo, logo existe $\beta \neq 0$, tal que βx tem 1 na primeira coordenada não nula. Pelo Princípio da Casa dos Pombos a equação $\beta^{-1}i + j = y(mod\ p)$ tem uma solução, onde $0 \leq i \leq t-1$ e $0 \leq j \leq p-t$.

Desta forma $(x;y)^T = (0;j)^T + (x;\beta^{-1}i)^T = (0;j)^T + \beta^{-1}(\beta x;i)^T$, onde $s_j = (0;j)^T \in S$ e $(\beta x;i)^T$ é uma coluna de A, logo temos o resultado

$$K_p(n,1) \leq |S|p^{n-r} = (p-t+1)p^{n-r}.$$

■

Exemplo 3.9. No caso $p = 5$, usando um código de Hamming, ver Exemplo 1.20 e o Teorema 2.17, obtemos que $K_5(6,1) = 5^4$. Desta forma, quando $i > 0$, temos o limite $K_5(6+i,1) \leq 5^{4+i}$, logo para $i = 25$ vem que $K_5(31,1) \leq 5^{29}$ e com $t = 5$ e $r = 3$, obtemos pelo Teorema 3.8, que $K_5(31,1) \leq 5^{28}$, melhorando este limite.

Teorema 3.10. *Se p é primo, então $K_p(np+1,1) \leq K_p(n,1)p^{n(p-1)}$.*

Demonstração: Seja W uma 1-cobertura de $\mathbb{Z}_p^n$. Construiremos um conjunto $S \subset \mathbb{Z}_p^{n+1}$ e uma matriz A de ordem $(n+1) \times (np+1)$, tal que $|S| = |W|$, onde $S = \{(x;0) : x \in W\}$ e a matriz A é dada por:

$$A = \begin{pmatrix} I_n & I_n & 2I_n & \dots & (p-1)I_n & 0 \\ 0\dots0 & 1\dots1 & 1\dots1 & 1\dots1 & 1\dots1 & 1 \end{pmatrix}$$

Afirmação: S 1-cobre $\mathbb{Z}_p^{n+1}$ usando a matriz A.

De fato, seja $(v;y) \in \mathbb{Z}_p^{n+1}$, onde $v \in \mathbb{Z}_p^n$ e $y \in \mathbb{Z}_p$. Analisemos os seguintes casos:

Caso 1: Se $y = 0$, $(v;0)$ é 1-coberto por S.

Caso 2: Se $y = 1$, temos que: $(v;1) = (v;0) + (0;1)$. Como W é uma 1-cobertura de $\mathbb{Z}_p^n$, existe $x \in W$, tal que $v = x + \alpha e$, onde $\alpha \in \mathbb{Z}_p$ e e é um vetor canônico

conveniente, logo: $(v;1) = (x;0) + (\alpha e;0) + (0;1)$, ou seja: $(v;1) = (x;0) + (\alpha e;1)$, onde $(x;0) \in S$ e $(\alpha e;1)$ é uma coluna de A, portanto S 1-cobre $(v;1)$ usando a matriz A.

Caso 3: Se $y \neq 0$ e $y \neq 1$. Temos então que: $(v;y) = (v;0) + (0;y)$, como W é uma 1-cobertura de $\mathbb{Z}_p^n$, pelo mesmo raciocínio utilizado no segundo caso, temos que $v = x + \alpha e$, daí vem que: $(v;y) = (x;0) + (\alpha e;y)$. Como p é primo, então $\mathbb{Z}_p$ é um corpo, logo como $y \neq 0$ existe y^{-1}, assim temos que: $(v;y) = (x;0) + y(\alpha y^{-1} e;1)$, onde $(x;0) \in S$ e $(\alpha y^{-1} e;1)$ é uma coluna de A. ■

Exemplo 3.11. Usando o fato que $K_3(3,1) = 5$, o Teorema 3.10 nos fornece que $K_3(10,1) \leq 5.3^6$, melhorando o limite superior $K_3(10,1) \leq 6.3^6$ obtido usando o fato que $K_3(9,1) \leq 2.3^6$.

Os próximos resultados que veremos a seguir foram obtidos por W. A. Carnielli [3].

Teorema 3.12. *Seja* $n = 1 + t[1 + q + K_q(3,1) + \ldots + K_q(r-1,1)]$, *para quaisquer* $q \geq 2$, $t \leq q$ *e* $r \geq 3$. *Então* $K_q(n,2) \leq (q - t + 1)q^{n-r}$.

Demonstração: Nosso objetivo é determinar um conjunto S de vetores de $\mathbb{Z}_q^r$ e uma matriz A de ordem $r \times n$ e mostrar que S é uma 2-cobertura de $\mathbb{Z}_q^r$ usando a matriz A. Seja, então o conjunto S dado por $S = \{(0,0,\ldots,z) : 0 \leq z \leq q - t\}$ de vetores em $\mathbb{Z}_{q-t+1}^r$ e seja A a matriz de ordem $r \times n$ formada pelas seguintes submatrizes $\begin{bmatrix} 0 & 0 & \ldots & 0 & \Gamma(k,q) & * & \ldots & * & x_k \end{bmatrix}^T$ de ordem $r \times tK_q(k,1)$, onde $\Gamma(k,q)$ denota um conjunto de vetores que forma uma 1-cobertura mínima de $\mathbb{Z}_q^k$, assim $|\Gamma(k,q)| = K_q(k,1)$. Logo esta submatriz é dada pela coleção de todos os vetores da forma $(0,\ldots,0,v_1,\ldots,v_k,x_k)$ para $x_k \in \{0,1,\ldots,t-1\}$ e $(v_1,\ldots,v_k) \in \Gamma(k,q)$ contendo o vetor canônico $e_1 = (1,0,\ldots,0)$ de comprimento k (isto é sempre possível adicionando um vetor conveniente a esta cobertura). Desta forma A tem ordem $r \times [1 + t(1 + K_q(2,1) + \ldots + K_q(r-1,1))]$. Resta agora mostrar que S é uma 2-cobertura de $\mathbb{Z}_q^r$ usando a matriz A.

De fato, é fácil ver que para qualquer $0 \leq y \leq q-1$, existem i, j, onde $0 \leq i \leq q-t$ e $0 \leq j \leq t-1$, tais que $i + j = y$.

Dado $(x; y)^T \in \mathbb{Z}_q^r$, com $x \in \mathbb{Z}_q^{r-1}$ e $y \in \mathbb{Z}_q$, nós temos que

$$(x; y)^T = (0; i)^T + (x; j)^T.$$

Pela construção de A, está claro que existe uma coluna de A da forma $(v; j)^T$, tal que x e v discordam em no máximo uma coordenada, logo $x = v + \alpha e$, com $\alpha \in \mathbb{Z}_q$ e e é um vetor canônico conveniente de $\mathbb{Z}_q^{r-1}$, logo

$$(x; y)^T = (0, i)^T + (v + \alpha e; j)^T = (0; i)^T + (v; j)^T + \alpha(e; 0)^T,$$

onde $(0; i) \in S$ e $(v; j)$ e $(e; 0)$ são colunas de A. Assim concluímos que S é uma 2-cobertura de $\mathbb{Z}_q^r$ usando a matriz A, daí temos que $K_q(n, 2) \leq (q - t + 1)q^{n-r}$. ■

Uma construção similar pode ser feita considerando a seguinte matriz $r \times n$, onde $n = t|\Gamma(r-1, q)| + (r-1)$ e o mesmo conjunto S definido no teorema anterior. Assim teríamos a matriz A da forma

$$A = \begin{pmatrix} \Gamma(r-1, q) & I_{(r-1)\times(r-1)} \\ x & 0 \end{pmatrix}$$

Aqui $I_{(r-1)\times(r-1)}$ denota a matriz identidade de ordem $r-1$ e $\Gamma(r-1, q)$ denota um conjunto de vetores que forma uma 1-cobertura mínima para $\mathbb{Z}_q^{r-1}$ contendo o vetor nulo. Então A é composta de colunas da forma $(v; x)^T$ para $v \in \Gamma(r-1, q)$, $x \in \{0, 1, \ldots, t-1\}$ e vetores $(w; 0)^T$, onde w é um vetor coluna de $I_{(r-1)\times(r-1)}$. Desta forma, temos o seguinte teorema:

Teorema 3.13. *Seja $n = tK_q(r-1, 1) + (r-1)$ para quaisquer $q \geq 2$, $t \leq q$ e $r \geq 3$, então $K_q(n, 2) \leq (q - t + 1)q^{n-r}$.*

Demonstração: Utilizando o mesmo raciocínio do Teorema 3.12, concluímos que S é uma 2-cobertura de $\mathbb{Z}_q^r$ usando a matriz A. ■

Teorema 3.14. *Se q é primo ou potência de um primo e*

$$n = 1 + (q + K_q(3,1) + \ldots + K_q(r-1,1)),$$

então $K_q(n,1) \leq [1 + (q-1)(r-1)]q^{n-r}$.

Demonstração: Note que, como q é primo ou potência de primo, estamos trabalhando no espaço de Hamming $\mathbb{F}_q^n$, onde $\mathbb{F}_q$ é um corpo. Considere S o conjunto de todos os $1 + (q-1)(r-1)$ vetores em $\mathbb{F}_q^r$ da forma

$$S = \begin{pmatrix} 0 & 0 & 0 & \ldots & 0 & 0 & 0 & \ldots & 0 & \ldots & 0 & \ldots & 0 \\ 0 & 1 & 0 & \ldots & 0 & 2 & 0 & \ldots & 0 & \ldots & q-1 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 & 0 & 2 & \ldots & 0 & \ldots & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 1 & 0 & 0 & \ldots & 2 & \ldots & 0 & \ldots & q-1 \end{pmatrix}$$

Observe que o conjunto S é o conjunto de todos os vetores coluna desta matriz

Agora, tome a matriz A da seguinte forma

$$A = \begin{pmatrix} 0 & 0 & 0 & \ldots & 1 & 0 \\ 0 & 0 & 0 & \ldots & \Gamma(r-1,q) & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 1 & \ldots & * & 0 \\ 0 & 1 & \Gamma(3,q) & \ldots & * & 0 \\ 1 & \Gamma(2,q) & * & \ldots & * & 0 \\ 0 & * & * & \ldots & * & 1 \end{pmatrix}$$

onde cada símbolo $\Gamma(i,q)$ denota uma 1-cobertura de $\mathbb{F}_q^i$ que contém o vetor nulo de $\mathbb{F}_q^i$ (isto sempre é possível pela equivalência de códigos), não esquecendo que $|\Gamma(i,q)| = K_q(i,1)$.

Então A é uma matriz de ordem $r \times n$. Resta provar que S é uma 1-cobertura de $\mathbb{F}_q^r$ usando a matriz A.

Para isto, considere um vetor arbitrário $w \in \mathbb{Z}_q^r$, tal que $w = (0, 0, \ldots, 0, a_1, \ldots, a_i)$ com as $r - i$ primeiras coordenadas iguais a zero. Note que se $i = 0$ ou $i = 1$, w é coberto por S.

Se $2 \leq i \leq r$, seja β tal que $\beta a_1 = 1$ (que é sempre possível, pois $\mathbb{F}_q$ é corpo). Então o vetor $\beta w = (0, 0, \ldots, 0, 1, \beta a_2, \ldots, \beta a_i)$ é 1-coberto por um vetor do conjunto

$$\begin{bmatrix} 0 & 0 & \ldots & 0 & 1 & \Gamma(i-1,q) & * & * & \ldots & * \end{bmatrix}^T$$

em A.

Daí $\beta w = \lambda e + v$, para algum λ conveniente em $\mathbb{F}_q$ e algum vetor canônico conveniente e em $\mathbb{F}_q^r$. Logo $w = (\beta^{-1}\lambda)e + \beta^{-1}v$, onde $(\beta^{-1}\lambda)e \in S$ e v é uma coluna de A. Logo o resultado segue, isto é, $K_q(n,1) \leq |S|q^{n-r}$ e o teorema vale. ■

Exemplo 3.15. Para $r = 7$ e $q = 2$ o Teorema 3.14 nos fornece que

$$K_2(27, 1) \leq 7.2^{20}.$$

Usando o fato de que $K_2(15, 1) = 2^{11}$ (pelo Teorema 2.17), obtemos o seguinte limite superior $K_2(27, 1) \leq 2^{23}$, notemos que este teorema melhora este limite.

O último caso nesta seção é uma aplicação que se leva em conta somente a cardinalidade dos parâmetros:

Teorema 3.16. *Para todo $n, q \geq 2$, se $q(n-2-j) < n-2$, então $K_q(n, j) \leq (q-1)q$.*

Demonstração: Basta provar que existe uma j-cobertura de $\mathbb{Z}_q^{n-1}$ consistindo de $q-1$ vetores usando uma matriz de ordem $(n-1) \times n$.

De fato, considere o subconjunto S de $\mathbb{Z}_q^{n-1}$, dado por $S = \{(a, a, \ldots, a) \in \mathbb{Z}_q^{n-1}\}$, logo $0 \leq a \leq q-2$, e a matriz $A = (I; M)$, onde I é a matriz identidade de ordem $(n-1) \times (n-1)$ e M é a matriz coluna $(n-1) \times 1$ cujas entradas são todas iguais a 1. Agora, tome um vetor $v \in \mathbb{Z}_q^{n-1}$, vamos dividir em dois casos:

Caso 1: Suponha que $v = (x_1, \ldots, x_{n-1})$ tenha ao menos $n-1-j$ coordenadas iguais a a, para algum a, com $0 \leq a \leq q-2$. Neste caso, v é coberto por S e podemos escrever:

$v = (a, a, \ldots, a) + \sum_{i=1}^{j} a_{t_i} e_{t_i}$, onde os vetores $(a, a, \ldots, a) \in S$ e e_{t_i} são colunas de A.

Caso 2: Caso contrário, se $v = (x_1, \ldots, x_{n-1})$ tem no máximo $n-2-j$ coordenadas iguais a a, com $0 \leq a \leq q-2$, neste caso defina os conjuntos

$$A = \{i : x_i = q-1\} \quad \text{e} \quad B = \{i : x_i \neq q-1\}.$$

Logo temos que $|A| + |B| = n-1$, mas $|B| \leq (n-2-j)(q-1)$, portanto

$$|A| = (n-1) - |B| \geq (n-1) - (n-2-j)(q-1),$$

mas por hipótese temos que $q(n-2-j) \leq n-3$, logo $q(n-2-j)+2 \leq n-1$, donde vem que $|A| \geq q(n-2-j)+2-(n-2-j)(q-1) = n-2-j+2 = n-j$, o que implica que existe ao menos $n-j$ coordenadas com o valor $q-1$, logo é fácil ver que $d(v, (q-1, q-1, \ldots, q-1)) \leq j$. Portanto, podemos escrever:

$v = (0, 0, \ldots, 0) + (q-1)(1, 1, \ldots, 1) + \sum_{i=1}^{j-1} a_{t_i} e_{t_i}$,

onde $(0, 0, \ldots, 0) \in S$ e os vetores $(1, 1, \ldots, 1)$ e e_{t_i} são colunas de A.

Podemos concluir, então que S é uma j-cobertura de $\mathbb{Z}_q^{n-1}$ usando a matriz A, logo o resultado segue. ■

Exemplo 3.17. No caso onde $q = 3$, $j = 3$ e $n = 6$. Estes parâmetros satisfazem as condições do Teorema 3.16, logo aplicando o teorema, obtemos $K_3(6, 3) \leq 6$. Este teorema melhora o limite superior trivial $K_3(6, 3) \leq 27$, pois $K_3(4, 3) = 3$.

Capítulo 4

Coberturas usando a teoria aditiva dos números

Os próximos teoremas que enunciaremos a seguir, necessitam de algum conhecimento da teoria aditiva dos números como, por exemplo, o Teorema de Cauchy-Davemport. Logo apresentamos uma breve introdução de adição em grupos até chegarmos nos teoremas em questão. Os assuntos das duas seções a seguir são discutidos na referência [17]. Posteriormente, tais resultados serão aplicados à construção de coberturas.

4.1 Adição em Grupos

Seja G um grupo abeliano e sejam A e B subconjuntos finitos de G, denotamos

$$A + B = \{g \in G \ : \ g = a + b, \text{ onde } a \in A \text{ e } b \in B\}.$$

Para $g \in G$, seja $r_{A,B}(g)$ o número de representações de g como soma de um elemento de A com um elemento de B, isto é,

$$r_{A,B}(g) = |\{(a, b) \ : a + b = g, \text{ onde } a \in A \text{ e } b \in B\}|.$$

O problema para adição de conjuntos $A + B$ é encontrar o limite inferior para $|A + B|$ em termos de $|A|$ e $|B|$. Esta questão é fácil de ser respondida para grupos

finitos, quando $|A| + |B|$ é grande. Apresentaremos dois lemas que nos garantirão este resultado.

Lema 4.1. *Seja G um grupo abeliano finito e sejam $A, B \subseteq G$ tais que*

$$|A| + |B| \geq |G| + t,$$

então $r_{A,B}(g) \geq t$ para todo $g \in G$.

Demonstração: Para $g \in G$, seja $g - B = \{g - b : b \in B\}$. Como

$$|G| \geq |A \cup (g - B)| = |A| + |g - B| - |A \cap (g - B)| = |A| + |B| - |A \cap (g - B)|,$$

segue que $|A \cap (g - B)| \geq |A| + |B| - |G| \geq |G| + t - |G| = t$.

Logo existem, no mínimo, t elementos distintos $a_1, \ldots, a_t \in A$ e t elementos distintos $b_1, \ldots, b_t \in B$, tais que $a_i = g - b_i$, com $i = 1, 2, \ldots, t$. Isto implica que $g = a_i + b_i$, com $i = 1, 2, \ldots, t$. Desta forma $r_{A,B}(g) \geq t$. ∎

Lema 4.2. *Seja G um grupo abeliano finito e sejam A e B subconjuntos de G tais que $|A| + |B| > |G|$. Então $A + B = G$.*

Demonstração: Aplicando o Lema 4.1 com $t = 1$, nós vemos que $r_{A,B}(g) \geq 1$ para todo G. Isto completa a prova, pois para todo $g \in G$ existem $a \in A$ e $b \in B$ tais que $g = a + b$, logo $A + B = G$. ∎

Segue do Lema 4.1 que para estudar o problema para a adição de conjuntos é suficiente examinar os casos onde $|A| + |B| \leq |G|$.

Uma ferramenta fundamental para provar muitos resultados da teoria aditiva dos números é a transformada-e de pares ordenados (A, B) de subconjuntos não vazios de um grupo abeliano G dado abaixo.

Definição 4.3. Seja $e \in G$, a *transformada-e do par ordenado* (A, B) de subconjuntos de G é o par $(A(e), B(e))$ de subconjuntos de G definidos por

$$A(e) := A \cup (B + e)$$

$$B(e) := B \cap (A - e).$$

O próximo lema que anunciaremos a seguir nos fornecerá as propriedades da transformada-e.

Lema 4.4. *Sejam A e B subconjuntos não vazios de um grupo abeliano G e seja $e \in G$. Seja $(A(e), B(e)$ a transformada-e do par ordenado (A, B). Então:*

(i) $A(e) + B(e) \subseteq A + B$.

(ii) $A(e) - A = e + (B - B(e))$.

(iii) $|A(e)| + |B(e)| = |A| + |B|$, *se A e B são subconjuntos finitos e se $e \in A$ e $0 \in B$, então $e \in A(e)$ e $0 \in B$.*

Demonstração: Ver em [17] ■

4.2 Teorema de Cauchy-Davemport

O Teorema de Cauchy-Davemport, que é o que nos interessa, é um caso particular do Teorema de I. Chowla, o qual enunciaremos abaixo.

Teorema 4.5. ***(I. Chowla)*** *Seja $m \geq 2$ e sejam A e B subconjuntos não vazios de $\mathbb{Z}/m\mathbb{Z}$. Se $0 \in B$ e $mdc(b, m) = 1$ para todo $b \in B$ não nulo, então*

$$|A + B| \geq \ min\{m, |A| + |B| - 1\}.$$

Demonstração: Como nós já vimos, o resultado é verdadeiro se $|A| + |B| > m$. Logo, podemos assumir que $|A| + |B| \leq m$, então

$$min\{m, |A| + |B| - 1\} = |A| + |B| - 1 \leq m - 1.$$

O teorema é válido se $|A| = 1$ ou $|B| = 1$, pois $|A + B| = |A| + |B| - 1$.

Para $|A| \geq 2$ e $|B| \geq 2$, suponha que o teorema seja falso, então existem $A, B \subset \mathbb{Z}/m\mathbb{Z}$, tais que $|A + B| < |A| + |B| - 1$.

Em particular $A \neq \mathbb{Z}/m\mathbb{Z}$. Escolha o par (A, B) tal que a cardinalidade de B seja mínima. Como $|B| \geq 2$, existe $b^* \in B$ tal que $b^* \neq 0$.

Afirmação: Se $a + b^* \in A$ para todo $a \in A$, então $a + jb^* \in A$ para todo $j = 0, 1, \ldots$.

De fato, se $j = 0$ ou $j = 1$, a afirmação é assegurada. Suponha que $a+(j-1)b^* \in A$ para todo $a \in A$, logo $a + jb^* = a + (j - 1)b^* + b^*$ e pela hipótese de indução temos que $a + jb^* \in A$ para todo $j = 0, 1, \ldots$.

Como $\text{mdc}(b^*, m) = 1$, isto implica que :

$$\mathbb{Z}/m\mathbb{Z} = \{a + jb^* : j = 0, 1, \ldots, m - 1\} \subseteq A \subseteq \mathbb{Z}/m\mathbb{Z}.$$

Logo $A = \mathbb{Z}/m\mathbb{Z}$, o que é um absurdo.

Portanto, existe um elemento $e \in A$ tal que $e+b^* \notin A$. Aplicando a transformada-e no par (A, B), pelo lema anterior nós temos que $A(e) + B(e) \subseteq A + B$, e então:

$$|A(e) + B(e)| \leq |A + B| < |A| + |B| - 1 = |A(e)| + |B(e)| - 1.$$

Como $e \in A$ e $0 \in B$, segue que $0 \in B(e) \subseteq B$ e $\text{mdc}(b, m) = 1$ para todo $b \in B(e)-\{0\}$. Como $e+b^* \notin A$, temos que $b^* \notin A-e$ e então $b^* \notin B \cap (A-e) = B(e)$. Portanto $|B(e)| < |B|$, o que contradiz a minimalidade de B, o que conclui a prova.

■

Teorema 4.6. ***(Cauchy-Davemport)*** *Seja p um número primo e A e B subconjuntos não vazios de $\mathbb{Z}/p\mathbb{Z}$, então*

$$|A + B| \geq min\{p, |A| + |B| - 1\}.$$

Demonstração: Seja $b_0 \in B$ e $B' = B - b_0$, então $|B'| = |B|$ e $|A + B'| = |A + B|$. Como $0 \in B'$ e $\text{mdc}(b, p) = 1$ para todo $b \in B'$ não nulo, aplicando o teorema

anterior, temos que $|A+B| = |A+B'| \geq min\{p, |A|+|B'|-1\} = min\{p, |A|+|B|-1\}$.

■

4.3 Coberturas via a Teoria Aditiva dos Números

Enunciaremos agora o próximo teorema envolvendo coberturas usando matrizes, onde o Teorema de Cauchy-Davemport é muito útil em sua demonstração. O próximo resultado deve-se a I. Honkala [9].

Teorema 4.7. *Se q é um número primo, então $K_q(tn+1, R) \leq sq^{(t-1)n}K_q(n, R)$, onde $s = max\ \{1, q-(t-1)R\}$.*

Demonstração: Sejam $a_1 = 0$ e $a_2, \ldots, a_t$ quaisquer elementos de $\mathbb{Z}_q - \{0\}$ e denote por $M = \{a_1, \ldots, a_t\}$. Escolhemos a seguinte matriz sobre $\mathbb{Z}_q$ de ordem $(n+1) \times (1+tn)$

$$A = \begin{pmatrix} 1 & a_1 \ldots a_1 & a_2 \ldots a_2 & \ldots & a_t \ldots a_t \\ 0 & I_n & I_n & \ldots & I_n \end{pmatrix}$$

Seja $N \subset \mathbb{Z}_q$ um conjunto arbitrário tal que $|N|$=máx$\{1, q-(t-1)R\}$ e suponha que $C \subset \mathbb{Z}_q^n$ seja uma R-cobertura mínima de $\mathbb{Z}_q^n$. Então definimos

$$S = \{(b, c)\ :\ b \in N \text{ e } c \in C\},$$

logo é fácil de ver que $|C| = K_q(n, R)$ e que $|S| = sK_q(n, R)$.

Afirmação: S é uma R-cobertura de $\mathbb{Z}_q^{n+1}$ usando a matriz A.

De fato, seja $(x; y) \in \mathbb{Z}_q^{n+1}$, onde $x \in \mathbb{Z}_q$ e $y \in \mathbb{Z}_q^n$ um vetor arbitrário, como C é uma R-cobertura de $\mathbb{Z}_q^n$, existe uma palavra $c \in C$ tal que $d(c, y) \leq R$. Denote por $z = y - c$ e suponha que as coordenadas não nulas de z sejam $z(i_1) = \alpha_1$, $z(i_2) = \alpha_2, \ldots, z(i_k) = \alpha_k$. Denote por A_i a i-ésima coluna de A.

Se $k < R$, então para todo $b \in N$, temos que:

$(x; y)^T = (b; c)^T + (x-b)A_1 + \sum_{j=1}^{k} \alpha_j A_{i_j}$, onde $2 \leq i_j \leq n+1$.

Se $k = R$, então pelo Teorema de Cauchy-Davemport, vem que:

$\alpha_1 M + \alpha_2 M + \ldots + \alpha_R M + N = \mathbb{Z}_q$, pois

$|\alpha_1 M+\alpha_2 M+\ldots+\alpha_R M+N| \geq |\alpha_1 M+\alpha_2 M+\ldots+\alpha_R M|+|N|-1$. Aplicando o Teorema de Cauchy-Davemport $R-1$ vezes em $|\alpha_1 M+\alpha_2 M+\ldots+\alpha_R M|$, obtemos que $|\alpha_1 M + \alpha_2 M + \ldots + \alpha_R M| \geq R|M| - (R-1)$, logo

$$|\alpha_1 M+\alpha_2 M+\ldots+\alpha_R M+N| \geq R|M|-(R-1)+|N|-1 \geq Rt+(q-(t-1)R)-R = q.$$

Para cada $j = 1, 2, \ldots, R$, podemos escolher um elemento $b \in N$ e inteiros $k(j)$, onde $1 \leq k(j) \leq t$, tais que $\alpha_1 a_{k(1)} + \alpha_2 a_{k(2)} + \ldots + \alpha_R a_{k(R)} + b = x$, então

$(x; y)^T = (b; c)^T + \sum_{j=1}^{R} \alpha_j A_{i_j}$, onde $1 \leq i_j \leq tn + 1$. Logo S é uma R-cobertura de $\mathbb{Z}_q^{n+1}$ usando a matriz A. Assim o resultado segue, ou seja

$K_q(tn + 1, R) \leq |S|q^{tn+1-(n+1)} = sK_q(n, R)q^{n(t-1)}$. ■

Como conseqüência do Teorema 4.7, enunciaremos dois corolários.

Corolário 4.8. *Se q é primo e $1 \leq t \leq q$, então*

$$K_q(tn + 1, 1) \leq (q - t + 1)q^{(t-1)n} K_q(n, 1).$$

Quando $t = q$, o Corolário 4.8 se reduz ao Teorema 3.10, e quando n é da forma $\frac{q^m-1}{q-1}$, isto é, igual ao comprimento de um q-código de Hamming, então o Corolário 4.8 se reduz ao Teorema 3.8.

Corolário 4.9. *Se q é primo e $R \geq q - 1$, então $K_q(2n + 1, R) \leq q^n K_q(n, R)$.*

Exemplo 4.10. Sendo $n = 11$, $q = 3$ e $R = 2$, o corolário anterior nos fornece que $K_3(23, 2) \leq 3^{11} K_3(11, 2)$. Pela tabela de códigos ternários [11], vemos que $K_3(11, 2) = 729 = 3^6$, logo $K_3(23, 2) \leq 3^{17}$, refinando o limite superior trivial $K_3(23, 2) \leq 3^{21}$.

O próximo teorema, devido a P. R. J. Östergard [18], utiliza um pouco da teoria aditiva dos números em sua demonstração, e melhora alguns limites superiores.

Teorema 4.11. *Se* $0 \leq p \leq q-2$, *então* $K_q(qr-p, qr-r-p-1) \leq q(p+2)$.

Demonstração: Seja o código

$$C' = \bigcup_{a \in \mathbb{Z}_q} C'_a$$

onde $C'_a = \{(a, a, \ldots, a)\}$ é um conjunto formado por todos os a-vetores, isto é, vetores cujas coordenadas são todas iguais a a, de comprimento $qr-p-1$. Nós então podemos formar o código

$$C = \bigcup_{a \in \mathbb{Z}_q} C_a = \bigcup_{a \in \mathbb{Z}_q} C'_a \oplus \{a, a+1, \ldots, a+(p+1)\}.$$

Logo $|C| = q(p+2)$.

Temos que provar que C é uma $(qr-r-p-1)$-cobertura para $\mathbb{Z}_q^{qr-p}$.

Considere um vetor arbitrário $x = (u; v)$, onde $u \in \mathbb{Z}_q^{qr-p-1}$ e $v \in \mathbb{Z}_q$. Vamos dividir em dois casos:

Caso 1: Se $d(u, C') \leq qr-r-p-2$, então $d(x, C) \leq qr-r-p-1$.

Caso 2: Se $d(u, C') \geq qr-r-p-1$, então neste caso existem no mínimo $q-p-1$ vetores de C', tais que $d(u, C'_a) = qr-r-p-1$.

De fato, se existisse no máximo $q-p-2$ elementos C'_a tais que

$$d(u, C'_a) = qr-r-p-1,$$

então

$$\sum_a d(u, C'_a) \geq (q-p-2)(qr-r-p-1)+(p+2)(qr-r-p) = q^2r-qp-qr-q+p+2.$$

Pois os outros $p+2$ vetores restantes distam de C' ao menos $qr-r-p$, mas isto contradiz o fato de que

$$\sum_a d(u, C'_a) = (q-1)(qr-p-1) = q^2r-qp-qr-q+p+1.$$

Pois em cada coordenada, temos 1 acerto e $q-1$ erros. Tomando no mínimo os $q-p-1$ símbolos, tais que $d(u, C'_a) = qr - r - p - 1$, obteremos no mínimo $q-p-1$ conjuntos da forma $\{a, a+1, \ldots, a+(p+1)\}$, onde $a \in \mathbb{Z}_q$ tal que $d(u, C'_a) = qr - r - p - 1$.

Afirmação: O conjunto

$$\bigcup_{a \in \mathbb{Z}_q} \{a, a+1, \ldots, a+(p+1)\} = \mathbb{Z}_q.$$

De fato, este conjunto pode ser dado da forma $A + B$, onde
$A = \{a \in \mathbb{Z}_q : d(u, C'_a) = qr - r - p - 1\}$ e $B = \{0, 1, \ldots, p+1\}$.

Pelo Teorema de Chowla, temos que $|A+B| \geq |A|+|B|-1$. Como $|A| \geq q-p-1$ e $|B| = p+2$, então $|A+B| \geq q-p-1+p+2-1 = q$. Logo $A + B = \mathbb{Z}_q$ e $d(x, C) = qr-r-p-1$. Daí o raio de cobertura de C é no máximo $qr-r-p-1$, pois caso contrário existiria um $x \in \mathbb{Z}_q^{qr-p}$, tal que $d(x, c) \geq qr - r - p$, para todo $c \in C$, o que é um absurdo, pois vimos que existe $c \in C$ tal que $d(x, c) = qr - r - p - 1$. ■

Exemplo 4.12. Seja $q = 5$, $r = 1$ e $p = 1$, então temos o limite superior trivial $K_5(4, 2) \leq 25$. Aplicando o Teorema 4.11, obtemos $K_5(4, 2) \leq 11$, melhorando o limite superior trivial.

Exemplo 4.13. Seja $q = 3$, $p = 0$ e $r = 2$, então temos o limite superior trivial $K_3(6, 3) \leq 27$. Aplicando o Teorema 4.11, obtemos $K_3(6, 3) \leq 6$, melhorando o limite superior trivial.

Capítulo 5

Limites Inferiores e s-Sobrejetividade

5.1 Limites Inferiores

Provamos no capítulo 2 que o limite inferior trivial é dado por $K_q(n,R) \geq \frac{q^n}{V_q(n,R)}$. Vimos que se quisermos provar que $K_q(n,R) \geq M$, temos que mostrar que para qualquer $(n, M-1)_q$-código C, existe $x \in \mathbb{Z}_q^n$ tal que para todo $c \in C$, vem que $d(x,c) \geq R+1$. Na maioria das vezes, é uma tarefa árdua, por isso precisamos de alguns conceitos auxiliares para determinarmos alguns limites inferiores.

Veremos, agora, alguns casos de limites inferiores.

O teorema a seguir deve-se a M. C. Bhandari e C.Durairajan [1].

Teorema 5.1. $K_q(n_1+n_2, R_1+R_2+1) \geq min\{K_q(n_1,R_1), K_q(n_2,R_2)\}$.

Demonstração: Suponha que C seja um código sobre o alfabeto Q, onde $|Q| = q$, comprimento n_1+n_2 e raio de cobertura R_1+R_2+1 e $|C| = M$. Suponha que $M < \min\{K_q(n_1,R_1), K_q(n_2,R_2)\}$, então projetando C nas primeiras n_1 coordenadas, obteremos um código cujo raio de cobertura deve ser maior do que R_1. Analogamente, projetando C nas n_2 últimas coordenadas, obteremos um código cujo raio de cobertura é maior do que R_2, desta forma é fácil ver que o raio de cobertura de C é dado por $R(C) \geq R_1+R_2+2$, o que é uma contradição. ∎

Exemplo 5.2. Como conseqüência a classe $K_3(6n, 4n-1) = 6$ passa a ser determinada. De fato, pelo Teorema 4.11, Östergard mostrou que $K_3(6n, 4n-1) \leq 6$. Por outro lado, como $K_3(6,3) = 6$, ver [6, Exemplo 6.7.5]. Assim, aplicando o Teorema 5.1 recursivamente, vemos que $K_3(6n, 4n-1) \geq 6$, para todo n. Logo temos a igualdade.

Exemplo 5.3. Pela tabela de valores de $K_q(n, R)$ em [11], vem que $K_5(9,6) \geq 8$. Note que aplicando o Teorema 5.1, obtemos $K_5(9,6) \geq min\ \{K_5(5,3), K_5(4,2)\}$. Pelo Teorema 5.25, sabemos que $K_5(5,3) = 9$ (veremos no final deste capítulo) e aplicando a desigualdade de Rodemich (5.2), que veremos a seguir, obtemos que $K_5(4,2) \geq 9$, logo $K_5(9,6) \geq 9$, melhorando este limite inferior. Por um raciocínio análogo, obtemos que $K_5(10,7) \geq 9$, melhorando o limite inferior, pois pela tabela em [11], observamos que $K_5(10,7) \geq 8$.

O próximo teorema deve-se a W. Chen e I. S. Honkala [5].

Teorema 5.4. *Se existe um q-código $C \subset \mathbb{Z}_q^n$ com raio de cobertura R e M palavras-código, então*

$$\lfloor \frac{M}{q} \rfloor V_q(n-1, R) + (M - \lfloor \frac{M}{q} \rfloor) V_q(n-1, R-1) \geq q^{n-1}. \tag{5.1}$$

Demonstração: **Afirmação**: existe um elemento $x \in \mathbb{Z}_q$ que aparece na primeira coordenada em no máximo $\lfloor \frac{M}{q} \rfloor$ palavras-código. De fato, se todo $x \in \mathbb{Z}_q$ aparece na primeira coordenada em no mínimo $\lfloor \frac{M}{q} \rfloor + 1$ palavras-código, logo $M \geq q\lfloor \frac{M}{q} \rfloor + q$.

Se $\frac{M}{q}$ é uma divisão exata, então $M \geq q\frac{M}{q} + q = M + q$, o que é um absurdo.

Se $\frac{M}{q}$ não é uma divisão exata, então $k < \frac{M}{q} < k+1$, onde $k \in \mathbb{N}$ e $\lfloor \frac{M}{q} \rfloor = k$, logo $M \geq qk + q = q(k+1) > M$, o que também é um absurdo. Provamos, então a afirmação.

Como C cobre as q^{n-1} palavras de $\mathbb{Z}_q^n$ que começam por x, cada palavra-código que começa por x cobre $V_q(n-1, R)$ tais palavras e as outras que não começam por

x cobrem somente $V_q(n-1, R-1)$ tais palavras. Por isso

$$\lfloor \frac{M}{q} \rfloor V_q(n-1, R) + (M - \lfloor \frac{M}{q} \rfloor) V_q(n-1, R-1) \geq q^{n-1}.$$

■

Observe que este teorema é útil para obtermos limites inferiores para determinadas classes de $(n, M)_q R$-códigos quando elas não verificam a desigualdade do Teorema 5.4.

Exemplo 5.5. Suponha que exista um $(5, 5)_3 2$-código. Logo $M = n = 5$, $V_3(4, 2) = 33$, $V_3(4, 1) = 9$ e $\lfloor \frac{5}{3} \rfloor = 1$. Substituindo na desigualdade (5.1) do Teorema 5.4, temos que $69 \geq 81$, o que é uma contradição. Logo, concluímos que não existe um $(5, 5)_3 2$-código, donde vem que $K_3(5, 2) \geq 6$, melhorando o limite inferior trivial $K_3(5, 2) \geq 5$.

Para a determinação de alguns resultados na seção a seguir, vamos supor conhecidas as desigualdades de Rodemich [19].

$$K_q(n, n-2) \geq \frac{q^2}{n-1} \tag{5.2}$$

$$K_q(n, 1) \geq \frac{q^{n-1}}{n-1}. \tag{5.3}$$

Nestas desigualdades, a igualdade pode ser atingida se, e somente se, $n-1$ divide q.

É importante observar que as desigualdades de Rodemich (5.2) e (5.3), nem sempre melhoram o limite inferior trivial. Com efeito, utilizando a desigualdade (5.3), obtemos $K_2(8, 1) \geq 19$, em contraste com o limite inferior trivial $K_2(8, 1) \geq 29$.

Para verificar se a desigualdade (5.2) melhora o limite inferior trivial, basta verificar se $q^2 V_q(n, n-2) > q^n(n-1)$. Da mesma forma, para que a desigualdade (5.3) melhore o limite inferior trivial, basta verificar se $n < q + 1$.

5.2 s-Sobrejetividade

Antes de entrarmos na definição de s-sobrejetividade, voltemos ao Exemplo 1.24. Neste exemplo, temos um código MDS com nove palavras (neste caso $m = 2$) de comprimento 4, sobre o alfabeto $\mathbb{Z}_3$ e de distância mínima 3. Pondo, em linhas, todas as palavras deste código, obtemos a matriz

$$\begin{pmatrix} 0 & 0 & 0 & 2 \\ 1 & 0 & 1 & 0 \\ 2 & 0 & 2 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 2 & 2 \\ 2 & 1 & 0 & 0 \\ 0 & 2 & 2 & 0 \\ 1 & 2 & 0 & 1 \\ 2 & 2 & 1 & 2 \end{pmatrix}.$$

Pelo Exemplo 1.24, vimos que escolhendo quaisquer duas posições dentre as quatro possíveis, encontraremos todos os vetores de $\mathbb{Z}_3^2$. Analogamente, analisando esta matriz, podemos observar que a escolha de quaisquer duas colunas distintas e para todo $(x, y) \in \mathbb{Z}_3^2$, existe uma linha desta matriz tal que (x, y) está nesta linha. Dizemos, neste caso, que esta matriz é 2-sobrejetiva. Esta idéia será formalmente estabelecida a seguir.

Definição 5.6. Uma matriz $A = (a_{ij})$ sobre $\mathbb{Z}_q$ é chamada *s-sobrejetiva* , se para todo conjunto formado por s colunas com índices $j_1, j_2, \ldots, j_s$ e para todo vetor $(b_1, b_2, \ldots, b_s) \in \mathbb{Z}_q^s$, existe uma linha i, tal que $a_{ij_t} = b_t$ para todo $t = 1, 2, \ldots, s$.

Denotaremos por $\sigma_q(n, s)$ o número mínimo de linhas de uma matriz s-sobrejetiva sobre $\mathbb{Z}_q$ com n colunas.

Observação 5.7. Um código $C \subset \mathbb{Z}_q^n$ com M palavras é s-sobrejetivo se a matriz obtida pondo suas palavras em cada linha é s-sobrejetiva.

Note que um código MDS com q^m palavras é um caso particular de código m-sobrejetivo.

Pelo Teorema 2.13, $K_q(n, n-2) = q$, se $n \geq q+1$. Vamos enfocar, agora, o caso limítrofe, ou seja, quando $n = q$. Em contraste com a situação anterior, o caso limítrofe ainda continua um problema em aberto, sabe-se somente que algumas instâncias de $K_q(q, q-2)$ são computadas até hoje. Discutiremos o limite superior no teorema a seguir, e o limite inferior será tratado somente na próxima seção.

Teorema 5.8. $K_q(q, q-2) \leq q - 2 + \sigma_2(q, 2)$.

Demonstração: Seja C um código cujas palavras são todas as linhas de uma matriz binária 2-sobrejetiva com q colunas e $\sigma_2(q, 2)$ linhas e todos os vetores $\mathbf{a} = (a, a, \ldots, a)$, onde $a \in \{2, 3, \ldots, q-1\}$. Isto induz um q-código de comprimento q com $q - 2 + \sigma_2(q, 2)$ palavras-código. Mostraremos que este código nos fornece uma cobertura de raio $q-2$. De fato, qualquer vetor de comprimento q que tenha ao menos duas coordenadas binárias é coberto pelas palavras obtidas da matriz 2-sobrejetiva. Por outro lado, se x é um vetor de comprimento q com no máximo uma coordenada binária, então existe um $a \in \{2, 3, \ldots, q-1\}$ que ocorre ao menos duas vezes em x, desta forma $d(x, \mathbf{a}) \leq q - 2$. ■

Veremos mais adiante que o limite superior do Teorema 5.8 é exato para determinados valores de q.

Antes de passarmos ao próximo teorema, voltemos ao Teorema 2.25.

Observação 5.9. Na construção do código C' do Teorema 2.25, nós utilizamos vetores da forma $(b_1, \ldots, b_n)$, onde $0 \leq b_i < t$, para todo i, e $b_1 + \ldots + b_n \equiv 0 \ (mod\ t)$. Observe que este código forma um código MDS sobre $\mathbb{Z}_t^n$ de distância mínima 2 possuindo t^{n-1} palavras. Logo, a matriz formada pondo suas palavras em cada uma de suas linhas, é uma matriz $(n-1)$-sobrejetiva, onde especificamente para este caso $\sigma_t(n, n-1) = t^{n-1}$. Portanto, a idéia do Teorema 2.25 pode ser generalizada pelo teorema a seguir.

Teorema 5.10. *Para todo $q \geq 2$ e $t \geq 1$, então $K_{tq}(n, 1) \leq \sigma_t(n, n-1) K_q(n, 1)$.*

Demonstração: Usando o mesmo raciocínio da demonstração do Teorema 2.25, tomando as palavras $(b_1, \ldots, b_n)$ como linhas de uma matriz $(n-1)$-sobrejetiva de ordem $\sigma_t(n, n-1) \times n$, obtemos o resultado. ■

Corolário 5.11. *Se q é primo ou uma potência de primo, então para todo $t \geq 1$, temos $K_{tq}(q+1, q) = q^{q-1}t^q$.*

Demonstração: Aplicando o Teorema 2.25, temos

$$K_{tq}(q+1, 1) \leq t^q K_q(q+1, 1).$$

Note que podemos usar o Teorema 2.17 em $K_q(q+1, 1)$, logo

$$K_q(q+1, 1) = \frac{q^{q+1}}{1 + (q+1)(q-1)} = \frac{q^{q+1}}{q^2} = q^{q-1}.$$

Assim $K_{tq}(q+1, 1) \leq t^q q^{q-1}$. Utilizando a desigualdade 5.2 de Rodemich, obtemos $K_{tq}(q+1, 1) \geq \frac{(tq)^q}{q} = t^q q^{q-1}$. Logo o resultado segue. ■

O próximo teorema é uma generalização do Teorema 5.10.

Teorema 5.12. *Para todo $q \geq 2$ e $t \geq 1$, temos*

$$K_{tq}(n, R) \leq \sigma_t(n, n-R) K_q(n, R).$$

Demonstração: Este teorema generaliza o Teorema 5.10 para R arbitrário, basta tomar o código C' como no Teorema 2.25, onde os vetores $(b_1, b_2, \ldots, b_n)$, $0 \leq b_i < t$, formam uma matriz $(n-R)$-sobrejetiva com $\sigma_t(n, n-R)$ linhas e n colunas. Logo, obtemos que $|C'| = \sigma_t(n, n-R) K_q(n, R)$. Utilizando o mesmo raciocínio do Teorema 2.25, vemos que C' forma uma cobertura de raio R. ■

Note que este teorema é um caso particular do Teorema 2.22, para o caso onde $\sigma_t(n, n-R) = t^{n-R}$.

Corolário 5.13. *Se q é primo ou uma potência de um primo e $2 \leq n \leq q+1$, então*

$$K_{q(n-1)}(n, n-2) = q^2(n-1).$$

Demonstração: Pela subseção 1.4.3, sabemos que existe um código Reed-Solomon duplamente estendido com parâmetros $(q+1, k, d = n-k+1)_q$. Para $k = 2$, obtemos um código com os seguintes parâmetros $(n, 2, n-1)_q$, para todo $2 \leq n \leq q+1$. O teorema anterior implica que $K_{q(n-1)}(n, n-2) \leq \sigma_q(n, 2)K_{n-1}(n, n-2)$.

Mas, $K_{n-1}(n, n-2) = n-1$, pelo Teorema 2.13, e $\sigma_q(n, 2) = q^2$, pois um código Reed-Solomon é um código MDS, logo o limite superior vale. O limite inferior vem da desigualdade de Rodemich (5.2). ■

Note que $\sigma_q(n, s) \geq q^s$, atingindo a igualdade se, e somente se, existe um código MDS com q^s palavras e distância mínima $d = n - s + 1$. Isto é, uma $q^s \times n$ matriz sobre $\mathbb{Z}_q$ formado pelas palavras de um $(n, q^s, d)_q$ código é s-sobrejetiva se, e somente se, $d \geq n - s + 1$. Basta observar que se existisse duas linhas com a mesma s-upla em s colunas para algum s, isto aconteceria se, e somente se, a distância entre estas linhas fosse no máximo $n - s$. Por exemplo: Se tivéssemos uma matriz $(n-1)$-sobrejetiva, cujas linhas sejam formadas por um código MDS de distância mínima 2, teríamos $\sigma_q(n, n-1) = q^{n-1}$.

5.3 s-Sobrejetividade de raio r $(r > 0)$ e Matriz-Partição

O próximo conceito é uma generalização do conceito de s-sobrejetividade, introduzido por G. Kéri e P. R. J. Östergard [12]. Anteriormente, vimos que um código é apenas s-sobrejetivo se para qualquer s-upla de coordenadas distintas e para qualquer $(x_1, x_2, \ldots, x_s) \in \mathbb{Z}_q^s$, existe uma palavra-código $c = (c_1, c_2, \ldots, c_n)$ tal que $c_{k_i} = x_i$ para todo $i = 1, 2, \ldots, s$, onde $(k_1, k_2, \ldots, k_s)$ é uma s-upla de coordenadas distintas duas a duas. Passemos agora para o conceito de códigos s-sobrejetivo de raio r, com $r > 0$.

Para facilitar a compreensão dos próximos resultados , denotaremos uma palavra-código por um vetor de comprimento n da seguinte forma $c = (c_0, c_1, \ldots, c_{n-1})$.

Definição 5.14. Seja $0 \leq r < s \leq n$. Um q-código $C \subset \mathbb{Z}_q^n$ de comprimento n é chamado *s-sobrejetivo de raio $r > 0$*, se para qualquer s-upla $(k_1, k_2, \ldots, k_s)$ de coordenadas distintas duas a duas e qualquer $(x_1, x_2, \ldots, x_s) \in \mathbb{Z}_q^s$, existe uma palavra-código $c = (c_0, c_1, \ldots, c_{n-1}) \in C$, tal que $|i \in \{1, 2, \ldots, s\} : c_{k_i} = x_i| \geq s - r$.

Vamos denotar por $\sigma_q(n, s, r)$ a cardinalidade mínima de um q-código que é s-sobrejetivo de raio r.

Assim um q-código $C \subset \mathbb{Z}_q^n$ de comprimento n não é s-sobrejetivo de raio r, se existe uma s-upla $(k_1, k_2, \ldots, k_s)$ de coordenadas distintas duas a duas e existe uma s-upla $(x_1, x_2, \ldots, x_s) \in \mathbb{Z}_q^s$, tal que toda palavra-código $c = (c_0, c_1, \ldots, c_{n-1}) \in C$ é tal que $|i \in \{1, 2, \ldots, s\} : c_{k_i} = x_i| \leq s - r - 1$.

Observação 5.15. Notemos que:

(i) O conceito que vimos anteriormente de s-sobrejetividade corresponde ao caso onde $r = 0$, logo é fácil ver que $\sigma_q(n, s) = \sigma_q(n, s, 0)$.

(ii) Se $s = n$, então $\sigma_q(n, n, r) = K_q(n, r)$.

(iii) Um q-código $C \subset \mathbb{Z}_q^n$ com raio de cobertura R é n-sobrejetivo de raio R.

(iv) Claramente, podemos notar que $\sigma_q(n+1, s, r) \geq \sigma_q(n, s, r)$(basta observar que $\sigma_q(n + 1, s, r) \leq q\ \sigma_q(n, s, r)$) e que $\sigma_q(n, r + 1, r) = q$.

O próximo teorema deve-se a A. Brace, D. E. Daykin e D. J. Kleitman, J. H. Spencer, que nos fornecerá alguns valores conhecidos para $\sigma_2(n, 2, 0)$.

Teorema 5.16. *$\sigma_2(n, 2, 0)$ é igual ao menor inteiro M satisfazendo $n \leq \binom{M-1}{\lfloor \frac{M}{2} \rfloor}$.*

Demonstração: As colunas de uma matriz binária $M \times n$ pode ser vista como vetores incidentes de subconjuntos do conjunto $\{1, 2, \ldots, M\}$. Se nós escolhermos como colunas todos os subconjuntos que contém o elemento 1 e exatamente $\lfloor \frac{M}{2} \rfloor - 1$ dos elementos restantes, então a união dos subconjuntos correspondentes a quaisquer

duas colunas contém menos de M elementos e nós verificamos que a matriz resultante é 2-sobrejetiva. Assim o M tomado da forma colocada no teorema, o resultado segue.

■

Alguns resultados para $\sigma_2(n, 2, 0)$ são derivados do Teorema 5.16.

$\sigma_2(2, 2, 0) = \sigma_2(3, 2, 0) = 4$, $\sigma_2(4, 2, 0) = 5$ e $\sigma_2(n, 2, 0) = 6$, se $5 \leq n \leq 10$.

Entraremos agora, em um conceito importante para o desenvolvimento de algumas classes de limites inferiores, que é o nosso principal objetivo neste capítulo.

Todos os resultados obtidos no restante deste capítulo foram desenvolvidos por W. Haas, Jan-Christoph Schlage-Puchta e J. Quirstoff [7].

Definição 5.17. Uma $(q \times n)$-matriz $\mathcal{P} = (P_{ik})$ (com $i \in \mathbb{Z}_q$ e $k \in \mathbb{Z}_n$) sobre os subconjuntos de $\mathbb{Z}_M$ é uma (n, M, q)-matriz partição se todas as colunas de $\mathcal{P}$ *formam uma partição de* $\mathbb{Z}_M$. Se adicionalmente a condição

$$|\bigcap_{k \in \mathbb{Z}_n} P_{i_k k}| \leq 1$$

for verificada para todo $(i_0, i_1, \ldots, i_{n-1}) \in \mathbb{Z}_q^n$, então $\mathcal{P}$ é chamada de *matriz-partição estrita.*

Uma seqüência de s subconjuntos disjuntos dois a dois de colunas distintas duas a duas de $\mathcal{P}$ é chamada de *s-transversal* ou *transversal de comprimento s.*

Exemplo 5.18. Exibiremos um exemplo de matriz-partição para $M = 5$:

$$\mathcal{P} = \begin{pmatrix} \{0,1\} & \{0\} & \{0\} \\ \{2,4\} & \{1,2,3,4\} & \{3,4\} \\ \{3\} & \phi & \{1,2\} \end{pmatrix}.$$

(i) Observe que cada coluna de $\mathcal{P}$ é uma partição de $\mathbb{Z}_5$.

(ii) A seqüência $\{2,4\}$, $\{0\}$ forma uma 2-transversal e a seqüência $\{3\}$, ϕ, $\{1,2\}$ forma uma 3-transversal.

O próximo teorema apresenta uma conexão entre a matriz-partição e a função $\sigma_q(n, s, r)$.

Teorema 5.19. *Se $2 \leq s \leq n$, então as seguintes afirmações são equivalentes:*

(i) Toda (n, M, q)-matriz partição tem uma s-transversal.

(ii) Toda (n, M, q)-matriz partição estrita tem uma s-transversal.

(iii) $\sigma_q(n, s, s-2) > M$.

Demonstração: $(i) \implies (ii)$ Esta implicação é trivial, pois basta ver que se toda (n, M, q)-matriz partição tem uma s-transversal, então uma (n, M, q)-matriz partição estrita (que é um caso particular desta matriz) tem uma s-transversal.

$(ii) \implies (iii)$ Seja $C \subset \mathbb{Z}_q^n$ um código de cardinalidade M. Seja $C = (c_{jk})$, onde $j \in \mathbb{Z}_M$ e $k \in \mathbb{Z}_n$, uma matriz de ordem $M \times n$ obtida de C usando as palavras-código de C como linhas desta matriz em uma ordem arbitrária.

Para $i \in \mathbb{Z}_q$ e $k \in \mathbb{Z}_n$, defina $P_{ik} = \{j \in \mathbb{Z}_M \ : \ c_{jk} = i\}$, então $\mathcal{P} = (P_{ik})$ é uma (n, M, q)-matriz partição estrita, pois caso contrário existiria $k_1, k_2, \ldots, k_n \in \mathbb{Z}_n$, tal que

$$|\bigcap_{l=1}^{n} P_{i_{k_l} k_l}| > 1,$$

onde $P_{i_{k_l} k_l} = \{j \in \mathbb{Z}_M \ : \ c_{jk_l} = i_{k_l}\}$, para algum $(i_0, i_1, \ldots, i_{n-1}) \in \mathbb{Z}_q^n$. Suponha que j_1 , $j_2 \in \mathbb{Z}_M$ satisfaz a condição acima, logo:

$c_{j_1 k_1} = i_{k_1}, c_{j_1 k_2} = i_{k_2}, \ldots, c_{j_1 k_n} = i_{k_n}$ e

$c_{j_2 k_1} = i_{k_1}, c_{j_2 k_2} = i_{k_2}, \ldots, c_{j_2 k_n} = i_{k_n}$.

Assim as palavras c_{j_1} e c_{j_2} seriam iguais, o que seria um absurdo. Então, como $\mathcal{P}$ é uma matriz partição estrita, temos que por hipótese $\mathcal{P}$ tem uma s-transversal $(P_{x_i k_i})$, onde $i \in \{1, 2, \ldots, s\}$. Logo, dado $j \in \mathbb{Z}_M$, a equação $c_{jk_i} = x_i$ é assegurada para no máximo um $i \in \{1, 2, \ldots, s\}$, pois se existisse um $j \in \mathbb{Z}_M$, tal que $c_{jk_i} = x_i$ é assegurada para no mínimo dois valores de $i \in \{1, 2, \ldots, s\}$, então, neste caso, existe no mínimo i_m , $i_n \in \{1, 2, \ldots, s\}$, tal que $P_{x_{i_m} k_{i_m}} \cap P_{x_{i_n} k_{i_n}} \neq \phi$, o que seria

um absurdo. Desta forma C não é s-sobrejetivo de raio $s-2$ o que implica que $\sigma_q(n,s,s-2) > M$.

$(iii) \Longrightarrow (i)$ Seja $\mathcal{P} = (P_{ik})$ uma (n, M, q)-matriz partição. Para todo $j \in \mathbb{Z}_M$ e todo $k \in \mathbb{Z}_n$, existe exatamente um $i \in \mathbb{Z}_q$, tal que $c_{jk} = i$, com $j \in P_{ik}$, pois $\mathcal{P}$ é matriz partição. Então $C = \{(c_{j0}, \ldots, c_{j,n-1}) \in \mathbb{Z}_q^n \ : \ j \in \mathbb{Z}_M\}$ é um código de cardinalidade M e que por hipótese não é s-sobrejetivo de raio $s-2$. Logo, existe uma s-upla $(k_1, \ldots, k_s)$ de coordenadas distintas duas a duas e uma s-upla $(x_1, \ldots, x_s) \in \mathbb{Z}_q^s$, tal que para todo $j \in \mathbb{Z}_M$ a equação $c_{jk_i} = x_i$ é assegurada para no máximo um $i \in \{1, 2, \ldots, s\}$. Consequentemente $(P_{x_i k_i})$ com $i \in \{1, 2, \ldots, s\}$ é uma s-transversal. E o teorema está provado. ■

5.4 Limites Inferiores via s-sobrejetividade generalizada e Matrizes-Partição

O próximo teorema refina alguns limites inferiores de $K_q(n, R)$.

Teorema 5.20. *Se $r < s$, então*

$$\sigma_{q+1}(n+1, s+1, r+1) \geq min\{2(q+1), \sigma_q(n,s,r)+1\}.$$

Especialmente, se $s = n$, temos $K_{q+1}(n+1, R+1) \geq min\{2(q+1), K_q(n,R)+1\}$.

Demonstração: No caso de $s - r = 1$, o teorema segue, pois $\sigma_q(n, r+1, r) = q$, logo $\sigma_{q+1}(n+1, r+2, r+1) = q+1$.

Assuma que $s - r \geq 2$. Seja $C \subset \mathbb{Z}_{q+1}^{n+1}$ um código de cardinalidade igual a $\min\{2q+1, \sigma_q(n,s,r)\}$. Para $i \in \mathbb{Z}_{n+1}$ e $z \in \mathbb{Z}_{q+1}$, definimos o conjunto

$$C_{iz} = \{(y_0, \ldots, y_n) \in C \ : \ y_i = z\}$$

e defina a função $f : \mathbb{Z}_{q+1} \longrightarrow \mathbb{Z}_q$ por:

$$f(z) = \begin{cases} z & \text{se,} \quad z < q \\ 0 & \text{se,} \quad z = q. \end{cases}$$

Afirmação: Existe um $z \in \mathbb{Z}_{q+1}$ tal que $|C_{nz}| \leq 1$. De fato, se todo $z \in \mathbb{Z}_{q+1}$ é tal que $|C_{nz}| > 1$, então todo $z \in \mathbb{Z}_{q+1}$ aparece em cada palavra de C na enésima coordenada no mínimo duas vezes, logo $|C| \geq 2(q+1)$, o que é um absurdo.

Sem perda de generalidade, seja $z = q$ e que $(q, q, \ldots, q) \in C$ (isto é possível, usando equivalência de códigos).

Ponha $C' = \{(f(y_0), \ldots, f(y_{n-1})) \in \mathbb{Z}_q^n \ : \ (y_0, \ldots, y_n) \in C - (q, q, \ldots, q)\}$.

Como $|C'| < |C| \leq \sigma_q(n, s, r)$, C' não é s-sobrejetivo de raio r. Logo existe uma s-upla $k = (k_1, \ldots, k_s)$ de coordenadas distintas duas a duas e uma s-upla $x \in \mathbb{Z}_q^s$ tal que para todo $c \in C'$, a equação $c_{k_i} = x_i$ é assegurada para menos de $s - r$ coordenadas.

Ponha $\overline{x} = (x, q) \in \mathbb{Z}_{q+1}^{s+1}$ e $\overline{k} = (k, n)$, uma $(s+1)$-upla de coordenadas distintas duas a duas. Então para todo $\overline{c} \in C$ a equação $\overline{c}_{k_i} = \overline{x}_i$ também é assegurada para menos de $s - r$ coordenadas. Desta forma C não é $(s+1)$-sobrejetivo de raio $r+1$, assim o resultado segue. ■

Exemplo 5.21. Pela tabela de valores de $K_q(n, R)$ em [11], vem que $K_7(5, 3) \geq 13$. Aplicando o Teorema 5.20, obtemos $K_7(5, 3) \geq min\ \{14,\ K_6(4, 2)+1\}$. Utilizando a desigualdade (5.2), vem que $K_6(4, 2) \geq 13$, logo $K_7(5, 3) \geq 14$, refinando este limite inferior. Da mesma forma para $K_7(9, 6)$, obtemos que

$$K_7(9, 6) \geq min\ \{14,\ K_6(8, 5) + 1\}.$$

Pela tabela de valores de $K_q(n, R)$ em [11], vem que $K_6(8, 5) \geq 15$ e $K_7(9, 6) \geq 13$, logo obtemos que $K_7(9, 6) \geq 14$, refinando este limite inferior. Note que o mesmo raciocínio poderia ser usado para avaliar $K_6(6, 4)$, mas neste caso, o uso do Corolário 5.26 seria mais conveniente.

O próximo resultado melhora o limite de Rodemich 5.2 se $5 \leq n < q \leq 2n - 4$.

Teorema 5.22. $K_q(n, n-2) \geq 3q - 2n + 2$.

Demonstração: Seja $\mathcal{P} = (P_{ik})$ uma $(n, 3q - 2n + 1, q)$-matriz partição. Pelo Teorema 5.19 é suficiente provar que $\mathcal{P}$ tem uma n-transversal.

Escolha uma transversal τ de comprimento máximo (digamos t) constituindo de conjuntos com cardinalidade menor ou igual a 1. Se $t = n$, o resultado segue. Seja então $t < n$.

Sem perda de generalidade, suponha que os subconjuntos de τ estão nas t primeiras colunas de $\mathcal{P}$. Seja p o número de conjuntos de cardinalidade 1 em τ. Considere a coluna $k \in \mathbb{Z}_n - \mathbb{Z}_t$ e seja a o número de conjuntos de cardinalidade 1 nesta coluna.

Afirmação: A maximalidade de τ implica que não há conjunto vazio nesta coluna (coluna k) e $a \leq p$.

De fato, se houvesse um conjunto vazio na coluna k, este seria disjunto aos conjuntos de τ, contradizendo a maximalidade de τ, e se $a > p$, então existem conjuntos unitários na coluna k disjuntos aos conjuntos de τ, contradizendo a maximalidade de τ.

Portanto o número de conjuntos com cardinalidade maior ou igual a 3 na coluna k é no máximo $(3q - 2n + 1 - a) - 2(q - a) = q - 2n + a + 1 \leq q - 2n + p + 1$. Basta observar que as a primeiras colunas contribuem com um elemento e as $q - a$ restantes com, no mínimo, dois elementos. Sendo x o número de conjuntos com cardinalidade maior ou igual a 3, temos que $a + 2(q - a) + x \leq 3q - 2n + 1$, logo $x \leq 3q - 2n + 1 - a - 2(q - a) \leq q - 2n + p + 1$.

Recursivamente, definimos uma seqüência (τ_s) com $s \in \{t, \ldots, n\}$ de s-transversais constituindo de conjuntos de cardinalidade menor ou igual 2 somente. Seja $\tau_t = \tau$ e assuma que τ_{s_0} já está definida para um $t \leq s_0 < n$.

Então o número de conjuntos de uma coluna não usada em τ_{s_0}, que não são disjuntos a todos os conjuntos de τ_{s_0} é no máximo $p + 2(s_0 - t)$.

Portanto o número de conjuntos de cardinalidade 2 nesta coluna, que são dis-

juntos a todos os conjuntos de τ_{s_0} é ao menos

$$q-(q-2n+p+1)-(p+2(s_0-t))=2n-2p-1-2s_0+2t=2(n-s_0)+2(t-p)-1.$$

Não esquecendo que $t-p\geq 0$ e $n-s_0\geq 1$. Assim vem que

$$q-(q-2n+p+1)-(p+2(s_0-t))\geq 2(n-s_0)-1\geq 1.$$

Note que existe no mínimo um conjunto nesta coluna de cardinalidade 2 que são disjuntos a todos os conjuntos de τ_{s_0}. Escolha tal conjunto e adicione a τ_{s_0} para obter τ_{s_0+1}, ainda constituindo de conjuntos com cardinalidade menor ou igual a 2. Fazemos este procedimento para cada $t\leq s_0<n$ até obter τ_n, que é a n-transversal desejada. ■

Observe que a desigualdade de Rodemich implica que $K_{3n}(2n+1,2n-1)\geq \frac{9n}{2}$, enquanto este teorema melhora esta desigualdade para $K_{3n}(2n+1,2n-1)\geq 5n$.

O próximo resultado refina limite de Rodemich sob certas condições.

Teorema 5.23. *Seja $p\in\mathbb{Z}_{n-1}$, tal que $q\equiv p$ (mod $n-1$). Então*

$$K_q(n,n-2)\geq \frac{q^2-p^2}{n-1}+p.$$

Demonstração: Considere uma (n,M,q)-matriz partição $\mathcal{P}$, onde não admite uma n-transversal. Pelo Teorema 5.19 (com $s=n$) é suficiente provar que M pode ser limitado inferiormente por $\frac{q^2-p^2}{n-1}+p$.

Definiremos a noção de uma s-transversal minimal em $\mathcal{P}$, recursivamente por:

1) Uma 0-transversal é minimal.

2) Uma s-transversal $\tau_s=(P_{x_ik_i})$, com $i\in\{1,2,\ldots,s\}$ e $s\geq 1$ é minimal, se contém uma $(s-1)$-transversal minimal e se entre todas as s-transversais com esta propriedade, temos que

$$l(\tau_s)=|\bigcup_{i=1}^{s}P_{x_ik_i}|=\sum_{i=1}^{s}|P_{x_ik_i}|$$

é minimal.

Seja t o maior inteiro tal que existe uma t-transversal minimal $\tau_t = (P_{x_i k_i})_{i\in\{1,2,\ldots,t\}}$ em $\mathcal{P}$. Observe que temos que $1 \leq t \leq n-1$, já que não existe uma n-transversal em $\mathcal{P}$.

Para todo $s \in \{1, 2, \ldots, t\}$, seja $A_s = P_{x_s k_s}$ e podemos assumir que $\tau_t = (A_1, \ldots, A_t)$ é ordenado de tal forma que $\tau_s = (A_1, \ldots, A_s)$ é uma s-transversal minimal.

Mais ainda, para todo $s \in \{1, \ldots, t\}$, seja $l_s = |A_s|$ e $L_s = l(\tau_s) = l_1 + \ldots + l_s$ e também $L_0 = 0$. Como $t \leq n-1$, existe uma coluna $k \in \mathbb{Z}_n$ de $\mathcal{P}$ que não é usada em τ_t. Sem perda de generalidade, suponha que $|P_{0k}| \leq |P_{1k}| \leq \ldots \leq |P_{q-1,k}|$.

Agora, seja u o maior inteiro menor do que t, com $L_u < q$. Temos que $u \leq t-1$ ($u \leq n-2$), já que caso contrário, se $u = t$, ao menos um conjunto da coluna k é disjunto a $A_1 \cup \ldots \cup A_t$, logo τ_t podia podia ser estendida a uma $(t+1)$-transversal, contradizendo a maximalidade de t.

Agora, alegamos que $q - L_u$ conjuntos da coluna k tem cardinalidade maior ou igual a $q - L_u$. Caso contrário, haveria, no mínimo, $L_u + 1$ conjuntos na coluna k com cardinalidade menor do que $q - L_u$, que nós poderíamos estender a transversal τ_u por algum conjunto da coluna k a uma transversal τ' com $l(\tau') < q \leq L_{u+1} = l(\tau_{u+1})$, contradizendo a minimalidade de τ_{u+1}.

Analogamente, para cada $s \in \mathbb{Z}_u$, existem ao menos $q - L_s$ conjuntos na coluna k, com cardinalidade $\geq l_{s+1}$, caso contrário τ_{s+1} não seria minimal.

Temos então, que $|P_{ik}| \geq q - L_u$, se $i \geq L_u$ e $|P_{ik}| \geq l_{s+1}$, se $i \geq L_s$ e $s \in \mathbb{Z}_u$.

Desta forma, nós obtemos

$$M = |\bigcup_{i=0}^{q-1} P_{ik}| = \sum_{s=0}^{u-1} \sum_{L_s \leq i < L_{s+1}} |P_{ik}| + \sum_{L_u \leq i < q} |P_{ik}| \geq \sum_{s=0}^{u-1} l_{s+1}^2 + (q - L_u)^2.$$

A razão destes quadrados é que na primeira parcela da soma, estamos somando l_{s+1} termos iguais a l_{s+1} e na segunda parcela da soma, estamos somando $q - L_u$

termos iguais a $q - L_u$.

O lado direito da desigualdade acima é uma soma de $u+1$ inteiros, onde a soma destes inteiros é q. Vemos que esta soma é uma função convexa, e é mínima se $u+1$ é máximo, ou seja, se $u + 1 = n - 1$, e as distâncias mútuas entre os inteiros são mínimas. Logo, temos a soma de $n - 1$ inteiros e como p é o resto da divisão de q por $n - 1$, por hipótese, temos $n - 1 - p$ inteiros iguais a $\lfloor \frac{q}{n-1} \rfloor$ e p inteiros iguais a $\lceil \frac{q}{n-1} \rceil$. Desta forma, temos que $M \geq (n - 1 - p)\lfloor \frac{q}{n-1} \rfloor^2 + p\lceil \frac{q}{n-1} \rceil^2$.

Se $\lfloor \frac{q}{n-1} \rfloor = r$, então $\lceil \frac{q}{n-1} \rceil = r+1$ e, por isso, é fácil ver que $r = \frac{q-p}{n-1}$. Substituindo no lado direito da desigualdade acima, obtemos $M \geq (n-1)r^2 + 2pr + p = \frac{q^2-p^2}{n-1} + p$.

■

Note que o limite de Rodemich corresponde ao caso onde $p = 0$ e este teorema melhora o limite de Rodemich, basta observar que $\frac{q^2}{n-1} - \frac{p^2}{n-1} + p > \frac{q^2}{n-1}$, quando $p > 0$.

Exemplo 5.24. Para avaliar $K_{12}(6, 4)$ observemos que $K_{12}(6, 4) \geq 29$, pela tabela em [11]. Aplicando o Teorema 5.23, temos que encontrar $p \equiv 12$ $(mod\ 5)$. Então $p = 2$, portanto $K_{12}(6, 4) \geq 30$, refinando este limite inferior. Utilizamos o mesmo raciocínio para avaliar $K_{13}(6, 4)$, observando que $K_{13}(6, 4) \geq 34$ (por [11]), obtemos que $K_{13}(6, 4) \geq 35$.

A aplicação de matrizes partição e suas transversais é também muito útil para obter limites inferiores específicos. O próximo teorema junto com o Teorema 5.20 nos conduzem a seis novos valores exatos de $K_q(q, q - 2)$ para $q \leq 10$.

Teorema 5.25. $K_5(5, 3) = 9$.

Demonstração: O limite superior vem do Teorema 5.8.

Para o limite inferior, temos que provar que toda $(5, 8, 5)$-matriz partição $\mathcal{P}$ tem uma 5-transversal, considerando vários casos. Podemos assumir que $\mathcal{P}$ não contém

o conjunto vazio, já que caso contrário o limite $K_5(4,2) \geq 9$, dado por (5.2) nos conduz a uma 5-transversal, pelo Teorema 5.19, o que é um absurdo.

Seja t o comprimento maximal de uma transversal τ, constituindo de conjuntos de cardinalidade 1. Claramente $t \geq 2$, já que cada coluna de $\mathcal{P}$ contém no mínimo dois conjuntos de cardinalidade 1.

Se $t \geq 4$, o resultado segue, pois se $t = 5$ temos o resultado. Se $t = 4$, como os conjuntos unitários da coluna 5 já foram usados na transversal, então existem conjuntos nesta coluna de cardinalidade maior ou igual a 2, que são disjuntos aos conjuntos usados na transversal. Daí obtemos a 5-transversal desejada. Resta-nos considerar os casos onde $t = 2$ e $t = 3$.

Seja $t = 2$, por causa da maximalidade de τ, toda coluna de $\mathcal{P}$ consiste de três conjuntos de cardinalidade 2 e os mesmos conjuntos de cardinalidade 1, digamos $\{6\}$ e $\{7\}$. Sem perda de generalidade, seja $P_{3k} = \{6\}$ e $P_{4k} = \{7\}$, para $k \in \mathbb{Z}_5$. Deletando as linhas 3 e 4, obtemos uma (5,6,3)-matriz partição. Sabendo que $\sigma_3(5,3,1) = 7 > 6$ (ver em Kéri, Östergard [13]) e pelo Teorema 5.19, temos que a (5,6,3)-matriz partição admite uma 3-transversal e desta forma $\mathcal{P}$ tem uma 5-transversal.

Seja $t = 3$, para $k \in \mathbb{Z}_5$ e $x \in \mathbb{Z}_8$, defina:

$$s_k(x) = \begin{cases} 1, & \text{se} \quad \{x\} \quad \text{ocorre na coluna } k \\ 0, & \text{caso contrário.} \end{cases}$$

e $s(x) = \sum_{k=0}^{4} s_k(x)$.

Sem perda de generalidade, sejam k_5, k_6, $k_7 \in \mathbb{Z}_5$ colunas distintas, tais que $s_{k_5}(5) = s_{k_6}(6) = s_{k_7}(7) = 1$ e

$$s(7) \geq s(6) \geq s(5). \tag{5.4}$$

Sejam $\{k', k''\} = \mathbb{Z}_5 - \{k_5, k_6, k_7\}$ e $s_k = s_k(5) + s_k(6) + s_k(7)$, para todo $k \in \mathbb{Z}_5$.

Claramente s_{k_5}, s_{k_6} e $s_{k_7} \geq 1$. A maximalidade de τ implica que $s_{k'}$, $s_{k''} \geq 2$.

Agora, vamos provar a seguinte afirmação auxiliar:

$s(7) \geq 4$, $s(6) \geq 3$, se existe uma coluna $l \in \mathbb{Z}_5$, tal que $s_l = 1$, então $s(6) \geq 4$.

Primeiro, assuma que existe um l com $s_l = 1$, claramente $l \in \{k_5, k_6, k_7\}$.

Seja $l = k_a$, isto é $s_l(a) = 1$ e $\{a', a''\} = \{5, 6, 7\} - \{a\}$. Como cada coluna de $\mathcal{P}$ contém ao menos dois conjuntos de cardinalidade 1, existe $x \in \mathbb{Z}_8 - \{5, 6, 7\}$ tal que $s_l(x) = 1$.

Seja $\{l', l''\} = \{k_5, k_6, k_7\} - \{l\}$, a maximilidade de τ implica que $s_{k'}(a) = s_{k''}(a) = 0$ e, por isso, $s_{k'}(a') = s_{k''}(a'') = s_{k''}(a') = s_{k'}(a'') = 1$, logo esta maximilidade também implica que $s_{l'}(a') = s_{l''}(a'') = s_{l'}(a'') = s_{l''}(a') = 1$ e $s_{l'}(a) = s_{l''}(a) = 0$. Conseqüentemente, $s(a) = 1$ e $s(a') = s(a'') = 4$.

Finalmente, se $a = 5$ e $\{a', a''\} = \{6, 7\}$, segue por (5.4) que $s(6)$, $s(7) \geq 4$.

Agora, assuma que não existe l, com $s_l = 1$. Então

$$s(5) + s(6) + s(7) = \sum_{k=0}^{4} s_k \geq 5.2 = 10$$

e por (5.4), temos que $s(7) \geq 4$ e $s(6) \geq 3$, finalizando a prova da afirmação auxiliar.

Sem perda de generalidade, sejam 6, $7 \in P_{3k} \cup P_{4k}$, para todo $k \in \mathbb{Z}_5$. Delete as linhas 3 e 4 de $\mathcal{P}$ e adicione, se necessário, alguns elementos de $\mathbb{Z}_6$ para obter uma (5,6,3)-matriz partição $\mathcal{P}'$. Vimos que esta matriz admite uma 3-transversal, digamos P'_{02}, P'_{03} e P'_{04}. Sem perda de generalidade, seja $5 \notin P'_{03} \cup P'_{04}$ e $s_0(7) = 1$ (pela afirmação auxiliar). Se $s_1(6) = 1$ ou $s_0(6) = s_1(7) = 1$, então $\{7\}$, $\{6\}$, P_{02}, P_{03} e P_{04} é a 5-transversal desejada.

Se $s_1(6) = s_0(6) = 0$, então a afirmação auxiliar implica que $s_2(6) = 1$, já que $s(6) \geq 3$ e $s_1(5) = 1$, já que $s_1 \geq 2$, então $\{7\}$, $\{5\}$, $\{6\}$, P_{03} e P_{04} é a 5-transversal desejada.

Se $s_1(6) = s_1(7) = 0$, então $s_1(5) = s_2(6) = 1$ (pela afirmação auxiliar), assim $\{7\}$, $\{5\}$, $\{6\}$, P_{03} e P_{04} é a 5-transversal desejada. ∎

Corolário 5.26. *$K_q(q, q-2) = q - 2 + \sigma_2(q, 2, 0)$, se $q \leq 10$.*

Demonstração: O limite superior vem do Teorema 5.8 e o limite inferior é uma aplicação do Teorema 5.25 e o Teorema 5.20. ■

Capítulo 6

Considerações Finais

Vimos, ao longo de todo este trabalho, construções de $(n, M)_q R$-códigos para obter valores ou limites para a função $K_q(n, R)$. Foram feitas construções combinatórias e, em alguma delas, foram usadas ferramentas algébricas, como por exemplo as construções via matrizes, propriedades de corpos finitos e a teoria aditiva dos números. Em algumas construções, utilizamos, como ferramenta a partição de matrizes. Pudemos observar que a obtenção destes valores e limites é um problema extremamente difícil e que tem desafiado pesquisadores de várias áreas, como matemáticos, engenheiros e profissionais da área de informática, desde mais ou menos 1950. Também pudemos observar que, em muitas classes da função $K_q(n, R)$, os seus valores ainda não são conhecidos e o que foram obtidos até agora foram os limites inferiores e superiores para estas classes. Portanto existem muitos problemas em aberto. Logo, ainda há muita pesquisa a se fazer. Nosso objetivo, ao longo deste trabalho, foi apresentar o problema e algumas destas construções.

Daremos, agora, um panorama geral das construções mais importantes desenvolvidas neste trabalho, como algumas classes exatas obtidas. Destaquemos algumas delas:

a) $K_q(2, 1) = q$, para todo $q \geq 2$. (Proposição 2.12.)

b) $K_q(3, 1) = \lceil \frac{q^2}{2} \rceil$, para todo $q \geq 2$. (Teorema 2.15.)

c) $K_2(2R+2, R) = 4$. Para todo $R = 0, 1, \ldots$. (Teorema 2.16.)

d) $K_q(\frac{q^r-1}{q-1}, 1) = q^{n-r}$, se q é primo ou potência de primo. (Teorema 2.17). Para o caso particular, onde $q = 2$, vem que $K_2(2^r - 1, 1) = 2^{2^r-r-1}$, para todo $r \geq 3$.

e) $K_{tq}(q+1, 1) = q^{q-1}t^q$, para todo $t \geq 1$ e q uma potência de primo. (Corolário 5.11.)

f) $K_2(n, R) = 2$, quando $R < n \leq 2R + 1$. (Teorema 2.13.)

g) $K_{q(n-1)}(n, n-2) = q^2(n-1)$, se q é uma potência de primo e $2 \leq n \leq q+1$. (Corolário 5.13).

h) $K_3(6n, 4n-1) = 6$, para todo $n = 1, 2, \ldots$.(Exemplo 5.2.)

i) $K_q(q, q-2) = q - 2 + \sigma_2(q, 2, 0)$, se $q \leq 10$. (Corolário 5.26.)

6.1 Tabelas de Valores da Função $K_q(n, R)$

Apresentaremos aqui, algumas tabelas de valores de $K_q(n, R)$ para pequenos valores de q e R. Iremos observar que algumas classes de valores de $K_q(n, R)$ não são conhecidos, nestes casos indicaremos limites superiores e inferiores obtidos neste trabalho e em outros, indicaremos nas referências. Note que para $n = 2$ e $n = 3$, os valores são imediatamente determinados pela Proposição 2.12, pelo Teorema 2.15 e Teorema 2.13.

Tabela 6.1: Limites em $K_2(n, R)$

n	$R = 1$	$R = 2$	$R = 3$
1	1		
2	2	1	
3	2	2	1
4	4^b	2^a	2^a
5	7^c	2^a	2^a
6	12^d	4^b	2^a
7	16^e	7	4
8	32^d	12	4^b
9	62	16	7
10	107-120	24-30	12

Tabela 6.2: Limites em $K_3(n, R)$

n	$R = 1$	$R = 2$	$R = 3$
1	1		
2	3	1	
3	5	3	1
4	9^e	3^a	3^a
5	27^f	8	3^a
6	71-73	15-17	6^g
7	156-186	26-34	11-12
8	402-486	54-81	14-27

Tabela 6.3: Limites em $K_4(n, R)$

n	$R = 1$	$R = 2$	$R = 3$
1			
2	4	1	
3	8	4	1
4	24^d	7^h	4^a
5	64^e	$k16i$	4^a
6	$228 - 256l$	32-52	$k11 - 14$
7	762-992	84-128	$19 - 32i$
8	2731-3456	240-352	$44 - 96i$

Tabela 6.4: Limites em $K_5(n, R)$

n	$R = 1$	$R = 2$	$R = 3$
1	1		
2	5	1	
3	13	5	1
4	46-51	$k11$	5^a
5	160-184	$22 - 35i$	9^j
6	625^e	$71 - 125i$	$16 - 25i$
7	$2722 - 3125l$	222-525	38-125

Tabela 6.5: Algumas referências para as tabelas 6.1, 6.2, 6.3 e 6.4

a	Teorema 2.13
b	Teorema 2.16
c	[21]
d	[10]
e	Teorema 2.17
f	[14]
g	Exemplo 5.2
h	Corolário 5.26
i	[18]
j	Teorema 5.25
k	[7]
l	Observação 2.10

Bibliografia

[1] BHANDARI, M. C., DURAIRAJAN, C., *A Note on Bounds for q-ary Covering Codes*. IEEE Transactions on Information Theory, vol. 42, NO. 5 (1996), 1640-1642.

[2] BLOKHUIS A., LAM, C. W. H., *More Covering by Rook Domains*. Journal of Combinatorial Theory, Series A 36, (1984) 240-244.

[3] CARNIELLI, W. A., *On Covering and Coloring Problems for Rook Domains*. Discrete Mathematics 57 (1985) 9-16.

[4] CARNIELLI, W. A., *Hyper-rook Domain Inequalities*. Studies in Applied Mathematics 82 (1990), 59-69.

[5] CHEN, W., HONKALA, I. S., *Lower Bounds for q-ary Covering Codes*. IEEE Transaction on Information Theory, vol. 36, NO. 3 (1990), 664-671.

[6] COHEN, G., HONKALA, I., LITSYN, S., LOBSTEIN, A., *Covering Codes*. North-Holland Matematical Library.

[7] HAAS, W., SCHLAGE-PUCHTA, J., QUISTORFF, J., *Lower Bounds on Covering Codes via Particion Matrices*. Journal of Combinatorial Theory, Series A 116 (2009) 478-484.

[8] HEFEZ, A., VILLELA, M. L. T., *Códigos Corretores de Erros*. Instituto de Matemática Pura e Aplicada-IMPA, Série de Computação e Matemática (2002).

[9] HONKALA, I., *On Lengthening of Covering Codes*. Discrete Mathematics 106/107 (1992) 291-295.

[10] KALBFLEISCH, J. G., STANTON, R. G., *A Combinatorial Problem in Matching*. J. London Math. Soc. 44 (1969), 60-64.

[11] KÉRI, G., *Tables for Covering Codes*, http://www.sztaki.hu/ keri/codes/, acessado (2010).

[12] KÉRI, G., ÖSTERGARD, P. R. J., *On the Covering Radius of Small Codes*. Studia Sci. Math. Hungar. 40 (2003) 243-256.

[13] KÉRI, G., ÖSTERGARD, P. R. J., *Further Results on the Covering Radius of Small Codes*. Discret Math. 307 (2007) 69-77.

[14] KAMPS, H. J. L., LINT, J. H. van, *A Covering Problem*. Combinatorial Theory and its Applications, vol. II, pp. 679-685, in: Colloquia Mathematica Societatis János Bolyai, Ser. 4, 1970.

[15] LOBSTEIN, A. C., *Contribution au codage Comninatoire: Ordres Addifits, Rayon de Recourvrement*. Thése, Télécom Paris, France (1985), 163.

[16] LOSEY G., *Note of a Theorem of Zaremba*. Journal of Combinatorial Theory 6 (1969), 208-209.

[17] NATHANSON, M. B., *Additive Number Theory: Inverse Problems and the Geometry of Sumsets*. New York, Springer-Verlag (1996).

[18] ÖSTERGARD, P. R. J., *Upper Bounds for q-ary Covering Codes*. IEEE Transaction on Information Theory (1991) VOL.37, NO. 3, 660-664.

[19] RODEMICH, E. R., *Covering by Rook Domains*. J. Combinatorial Th., Ser. A, vol. 9 (1970), 117-128.

[20] SINGLETON, R. C., *Maximum Distance Q-Nary codes*. IEEE Trans. Inf. Theory IT 10 (1964), 116-118.

[21] TAUSSKY, O., TODD, J., *Covering Theorems for Groups*, Ann. Polon. Math., 21 (1948), 303-305.

Livros Grátis

(http://www.livrosgratis.com.br)

Milhares de Livros para Download:

Baixar livros de Literatura
Baixar livros de Literatura de Cordel
Baixar livros de Literatura Infantil
Baixar livros de Matemática
Baixar livros de Medicina
Baixar livros de Medicina Veterinária
Baixar livros de Meio Ambiente
Baixar livros de Meteorologia
Baixar Monografias e TCC
Baixar livros Multidisciplinar
Baixar livros de Música
Baixar livros de Psicologia
Baixar livros de Química
Baixar livros de Saúde Coletiva
Baixar livros de Serviço Social
Baixar livros de Sociologia
Baixar livros de Teologia
Baixar livros de Trabalho
Baixar livros de Turismo