UNIVERSIDADE FEDERAL DO PARANÁ

Welington Santos

Códigos MDS na Métrica de Niederreiter-Rosenbloom-Tsfasman e em Métricas Poset

Curitiba, 2015.

UNIVERSIDADE FEDERAL DO PARANÁ

Welington Santos

Códigos MDS na Métrica de Niederreiter-Rosenbloom-Tsfasman e em Métricas Poset

Dissertação apresentada ao Programa de Pós-Graduação em Matemática da Universidade Federal do Paraná, como requisito parcial à obtenção do grau de Mestre em Matemática.

Orientador: Prof. Dr. Marcelo Muniz Silva Alves.

Curitiba

Julho de 2015

S237c Santos, Welington
Códigos MDS na métrica de Niederreiter-Rosenbloom-Tsfasman e em métricas Poset/ Welington Santos. – Curitiba, 2015.
98 f. : il. color. ; 30 cm.

Dissertação - Universidade Federal do Paraná, Setor de Ciências Exatas, Programa de Pós-graduação em Matemática, 2015.

Orientador: Marcelo Muniz Silva Alves .
Bibliografia: p. 97-98.

1. Teoria da codificação. 2. Conjuntos ordenados. 3. Métrica. 4. Pesos e medidas. I. Universidade Federal do Paraná. II.Alves, Marcelo Muniz Silva. III. Título.

CDD: 511.33

TERMO DE APROVAÇÃO

"CÓDIGOS MDS NA MÉTRICA DE NIEDERREITER-ROSENBLOOM-TSFASMAN E EM MÉTRICAS POSET"

por

Welington Santos

Dissertação aprovada como requisito parcial para obtenção do grau de

Mestre no Programa de Pós-Graduação em Matemática,

pela Comissão Examinadora composta por:

Orientador: _____

Prof. Dr. Marcelo Muniz Silva Alves
Dep. de Matemática – UFPR

_____

Prof. Dr. Marcelo Firer
UniCamp

_____

Prof. Dr. Giuliano Gadioli la Guardia
UEPG

_____

Profa. Dra. Patrícia Massae Kitani
UTFPR

Curitiba, 17 de julho de 2015.

Ministério da Educação
Universidade Federal do Paraná
Setor de Ciências Exatas/Departamento de Matemática
Programa de Pós-Graduação em Matemática - PPGM

ATA DA 67ª DEFESA DE DISSERTAÇÃO DE MESTRADO

Aos dezessete dias do mês de fevereiro de 2015, no Anfiteatro B, bloco das PCs, foi instalada pelo Professor Marcelo Muniz Silva Alves, a Banca Examinadora para a sexagésima sétima Defesa de Dissertação de Mestrado em Matemática. Estiveram presentes ao Ato, professores, alunos e visitantes.

A banca examinadora, homologada pelo Colegiado do Programa de Pós-Graduação em Matemática, ficou constituída pelos professores: Prof. Dr. Marcelo Firer, da Universidade Estadual de Campinas, Prof. Dr. Giuliano Gadioli la Guardia, da Universidade Estadual de Ponta Grossa, e Profa. Dra. Patrícia Massae Kitani, da Universidade Tecnológica Federal do Paraná, Prof. Dr. Edson Ribeiro Álvares do Programa de Pós-Graduação em Matemática da Universidade Federal do Paraná e o Prof. Dr. Marcelo Muniz Silva Alves, orientador da dissertação, a quem coube a presidência dos trabalhos.

Às quinze e trinta horas, a banca iniciou seus trabalhos, convidando a candidata **WELINGTON SANTOS** a fazer a apresentação do tema da dissertação intitulada "CÓDIGOS MDS NA MÉTRICA DE NIEDERREITER-ROSENBLOOM-TSFASMAN E EM MÉTRICAS POSET". Encerrada a apresentação, iniciou-se a fase de arguição pelos membros participantes. Após a arguição, a banca com pelo menos 03 (três) membros, reuniu-se para apreciação do desempenho do pós-graduando.

A banca considerou que o pós-graduando fez uma apresentação com a necessária concisão. A Dissertação apresenta contribuição à área de estudos e não foram registrados problemas fundamentais de estrutura e redação, resultando em plena e satisfatória compreensão dos objetivos pretendidos.

Tendo em vista a dissertação e a arguição, os membros presentes da banca decidiram pela sua aprovação.

Curitiba, 17 de julho de 2015.

Prof. Dr. Marcelo Muniz Silva Alves
Presidente

Prof. Dr. Marcelo Firer
Titular

Prof. Dr. Giuliano Gadioli la Guardia
Titular

Profa. Dra. Patrícia Massae Kitani
Titular

Agradecimentos

Agradeço primeiramente aos meus pais Antônio e Silmara, ao meu irmão Almir que acreditaram, apoiaram e me ajudaram durante todos os anos de minha vida.

Ao Programa de Pós-Graduação em Matemática da UFPR pela oportunidade e formação de qualidade propiciada.

Expresso também meus agradecimentos ao professor Marcelo Muniz, pela paciência e dedicação que teve durante todo este período com minha pessoa.

Aos professores do departamento de matemática da UEPG por me incentivarem a seguir a carreira acadêmica em especial os professores Giuliano Gadioli La Guardia, Luciane Grossi e Rita Amaral Vieira.

À todos os meus amigos de gradução os quais sempre estarão presentes em coração pelos bons momentos que passamos e passaremos juntos.

À Coordenação de Aperfeiçoamento de Pessoal de Nível Superior, pelo apoio financeiro.

" It's only in the mysterious equation of love that any logic or reasons can be found."

John Nash

Resumo

Neste trabalho, desenvolvemos a teoria de códigos corretores de erros, a fim de estudar os conceitos de códigos MDS no espaço das matrizes com relação a ρ-métrica e de códigos MDS em métricas poset quaisquer, seguindo as exposições existentes em trabalhos de Kim e Hyun e de Skriganov. Para tanto, introduzimos alguns conceitos e ferramentas de álgebra e da teoria clássica de códigos corretores de erro. Por fim, apresentamos uma construção explícita de um família de códigos MDS na ρ-métrica.

Palavras-chave: Códigos MDS; Poset; ρ-métrica; Ditribuição de pesos.

Abstract

In this work, we developed the Coding theory in order to study the concepts of MDS codes in the space of matrices with respect to ρ-metric and MDS codes in any poset metrics following the existing exibitions in papers by Kim and Hyun and by Skriganov. To this end, we introduce some concepts and tools of algebra and of classical theory of error-correcting codes. Finally we present an explicit construction of a family of MDS codes in the ρ-metric.

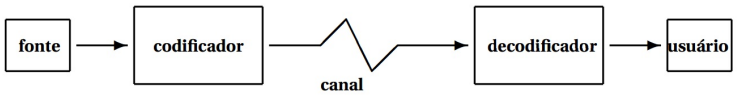
Keywords: MDS Codes; Poset; ρ-metric; Weight Distribution.

Sumário

Introdução

A Teoria de Códigos Corretores de Erro e, de maneira geral, a Teoria da Informação originou-se no trabalho *A Mathematical Theory of Communication* [13] de Claudie Shannon publicado em 1948. O trabalho de Shannon nos dá uma medida precisa do teor das informações na saída de um transmissor aleatório em termos de sua entropia. A teoria de códigos corretores de erro possui várias aplicações, pois a mesma intervém todas as vezes que queremos transmitir uma mensagem que está sujeita a interferências, acarretando em erros na mensagem a ser lida posteriormente. Exemplos de aplicações são as transmissões via satélites e o armazenamento de dados em CD's e DVD's.

Um sistema de comunicação utilizado para transmissão da informação segue o modelo abaixo:



Uma *fonte* é o conjunto das possíveis mensagens a serem enviadas por um *codificador*, que é um dispositivo que transforma a fonte em um sinal, para que possa ser enviada por um *canal* para o dispositivo *decodificador*, que transforma o sinal em uma mensagem para o *usuário*.

Um canal de comunicação pode apresentar uma série de imperfeições como ruídos, distorções, interferências, etc. Como consequência, a função do decodificador pode ser resumida como sendo habilidade de apresentar em sua saída a melhor estimativa da informação ou mensagem que foi transmitida.

Um código corretor de erros é um modo organizado de se introduzir dados a uma informação que se queira transmitir, de forma que ao se receber tal informação se consiga detectar e corrigir possíveis erros (frutos das imperfeições do canal de comunicação). Na prática, a classe de códigos mais utilizada é a dos códigos lineares. Neste caso, o código de canal será

um subespaço vetorial de $\mathbb{F}_q^n$ onde o alfabeto $\mathbb{F}_q$ possui a estrutura de corpo finito.

Dados um corpo finito $\mathbb{F}_q$ e um código linear $C \subseteq \mathbb{F}_q^n$ de dimensão k, onde $1 \leqslant k < n$, pode-se definir uma distância entre as palavras código de C, em geral, utiliza-se a métrica de Hamming. Para um código C, define-se a distância mínima do código C como sendo a menor distância entre duas palavras quaisquer do código. Um problema clássico na teoria de códigos lineares é tentar encontrar um código linear C de dimensão k com maior distância mínima d possível.

O problema de determinar d foi generalizado para o problema de encontrar $d(H)$ por Niederreiter [8], [9], abaixo enunciado:

Sejam $n_1, n_2, \ldots, n_s$ inteiros positivos e $H = \left\{h_{(i,j)} : 1 \leqslant i \leqslant s, 1 \leqslant j \leqslant n_i\right\}$ o sistema de $n_1 + n_2 + \cdots + n_s$ vetores em $\mathbb{F}_q^m$ particionado em s conjuntos ordenados de cardinalidades $n_1, n_2, \ldots, n_s$ respectivamente, ou seja,

$$H = \left\{h_{1,1}, \ldots, h_{1,n_1}, h_{2,1}, \ldots, h_{2,n_2}, \ldots, h_{s,1}, \ldots, h_{s,n_s} \in \mathbb{F}_q^m\right\}.$$

Defina $d(H) = \min \sum_{i=1}^{s} d_i$, onde este mínimo é extendido sobre todos os inteiros $d_1, \ldots, d_s$ tal que $0 \leqslant d_i \leqslant n_i$ $(1 \leqslant i \leqslant s)$ e $\sum_{i=1}^{s} d_i$ é positivo e para o qual o conjunto de vetores $h_{(i,j)}, 1 \leqslant i \leqslant s, 1 \leqslant j \leqslant d_i$, é linearmente dependente.

Se não existem tais inteiros $d_1, \ldots, d_s$, ou seja, os vetores $h_{(i,j)}$ são linearmente independentes e $n_1 + n_2 + \cdots + n_s \leqslant m$, então definimos $d(H)$ como sendo $n_1 + n_2 + \cdots + n_s + 1$.

O problema de Niederreiter foi generalizado por Brualdi et al. [1] introduzindo o conceito de métricas poset, também chamadas de $\mathbb{P}$-métricas, onde $\mathbb{P}$ é um conjunto parcialmente ordenado. O conceito do problema acima, sendo considerado para uma $\mathbb{P}$-métrica qualquer, de fato, é uma generalização, pois o problema clássico da métrica Hamming é equivalente ao problema para a $\mathbb{P}$-métrica onde, o poset $\mathbb{P}$ é do tipo anticadeia.

Em [10], Rosenbloom e Tsfasman introduzem uma nova métrica em um espaço linear sobre um corpo finito $\mathbb{F}_q$, chamada de ρ-métrica ou métrica de Rosenbloom-Tsfasman. A ρ-métrica é definida no espaço linear $Mat_{n,s}(\mathbb{F}_q)$ das matrizes com n-linhas e s-colunas sobre $\mathbb{F}_q$.

A ρ-métrica é aplicada em problemas onde um remetente transmite mensagens, cada uma sendo uma s-upla formada de n-uplas de símbolos q-ários, transmitidos por n canais em paralelo. Existe interferência da seguinte natureza: algumas vezes, partes dos canais falham, iniciando pelo m-ésimo deles, o grau de interferência é medido pelo número total de símbolos q-ários enviados pelo primeiro dos canais que não falha "sobre" a mensagem. Deste modo teremos

que distância mínima de um código no sentido da ρ-métrica caracteriza a sua estabilidade em tal interferência.

Em [2] e [14] Dougherty e Skriganov introduzem o conceito de um Código de *Maximum Distance Separable* (MDS) na ρ-métrica. Também em [14] Skriganov estabelece relações entre códigos MDS na ρ-métrica e Distribuições Ótimas no cubo unitário, além de ser feito o estudo sobre o enumerador de peso de um código MDS na ρ-métrica e de uma distribuição ótima.

A ρ-métrica é um tipo especial de métrica poset. Sendo assim, em [5], Kim e Hyun generalizam o conceito de código MDS para uma $\mathbb{P}$-métrica qualquer e fazem o estudo do enumerador de peso de um $\mathbb{P}$-código MDS qualquer.

Neste trabalho, estamos interessados em desenvolver a teoria de códigos MDS para a ρ-métrica, assim como para $\mathbb{P}$-métricas quaiquer seguindo as exposições encontradas em [5], [10] e [14].

O texto está organizado da seguinte forma:

No Capítulo 1, apresentamos o estudo sobre corpos finitos e de extensões de corpos finitos. Além disso, realizamos o estudo de propriedades polinomiais referentes a raízes de polinômios, raízes da unidade e polinômios ciclôtomicos definidos sobre um corpo finito $\mathbb{F}_q$.

O Capítulo 2, consiste nos conceitos necessários para o entendimento da Teoria de Códigos, como os conceitos de Código linear, dual de um código linear, Métrica de Hamming, distância mínima de um código e definimos códigos MDS. Neste mesmo capítulo, estudamos algumas desigualdades envolvendo a distância mínima do código, definimos o polinômio enumerador de peso de um código linear e, por fim, se faz um estudo sobre códigos cíclicos.

No Capítulo 3, apresentamos o conceito de ρ-métrica no espaço das matrizes sobre um alfabeto finito qualquer $\mathcal{A}$, assim como os conceitos de código MDS na ρ-métrica e Código Uniformemente Distribuído. Mostramos que estas duas últimas definições são equivalentes. Apresentamos o conceito de Distribuição Ótima no cubo unitário e obtemos uma relação biunívoca entre Códigos MDS na ρ-métrica e Distribuições Ótimas no cubo unitário (quando consideramos que nosso alfabeto $\mathcal{A}$ possui a estrutura de corpo). Também no caso em que $\mathcal{A}$ possui a estrutura de corpo, mostramos uma expressão para o enumerador de peso de uma Distribuição Ótima e, consequentemente, para um Código MDS na ρ-métrica. Por fim, exibimos uma construção explícita de uma família de códigos MDS na ρ-métrica, além de argumentarmos sobre a existência de códigos sobre $\mathbb{Z}_q$.

No Capítulo 4, apresentamos um estudo sobre espaços poset e códigos MDS sobre

estes espaços. Obtemos uma expressão para o enumerador de peso de um $\mathbb{P}$-código MDS, onde $\mathbb{P}$ é um poset qualquer. Por fim, argumentamos sobre a existência de códigos posets MDS.

Capítulo 1

Corpos Finitos e Propriedades Polinomiais

1.1 Caracterização de Corpos finitos

Seja $\mathbb{F}$ um corpo. Um subconjunto $\mathbb{K}$ de $\mathbb{F}$ que é um corpo com as operações de $\mathbb{F}$ é chamado de *subcorpo* de $\mathbb{F}$. Neste contexto, $\mathbb{F}$ é chamado uma *extensão* de $\mathbb{K}$. Se $\mathbb{K} \neq \mathbb{F}$, dizemos que $\mathbb{K}$ é um *subcorpo próprio* de $\mathbb{F}$. Um corpo que não contém subcorpos próprios é chamado de *Corpo Primo*.

Definição 1.1 *Seja $\mathbb{L}$ uma extensão do corpo $\mathbb{K}$. Se $\mathbb{L}$ considerado como um espaço vetorial sobre $\mathbb{K}$ possui $\dim < \infty$ então $\mathbb{L}$ é chamado de extensão finita de $\mathbb{K}$. A dimensão de $\mathbb{L}$ é chamada de grau de $\mathbb{L}$ em $\mathbb{K}$ e a denotamos por $\dim \mathbb{L} = [\mathbb{L} : \mathbb{K}]$.*

Exemplo 1.2 *Considere o corpo $\mathbb{Q}$ e sua extensão $\mathbb{Q}(\sqrt{2})$. Quando consideramos $\mathbb{Q}(\sqrt{2})$ como espaço vetorial sobre $\mathbb{Q}$ temos $\left\{1, \sqrt{2}\right\}$ como base, logo*

$$\dim \mathbb{Q}(\sqrt{2}) = [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2.$$

Definição 1.3 *Seja $\mathbb{K}$ um subcorpo de um corpo $\mathbb{F}$ e $\theta \in \mathbb{F}$. Se existe um polinômio não trivial f em $\mathbb{K}[x]$ tal que $f(\theta) = 0$, então θ é dito um Elemento algébrico sobre $\mathbb{K}$. Uma extensão $\mathbb{L}$ de $\mathbb{K}$ é dita Extensão Algébrica de $\mathbb{K}$ se todo elemento de $\mathbb{L}$ é algébrico sobre $\mathbb{K}$.*

Teorema 1.4 *Toda extensão finita de $\mathbb{K}$ é uma extensão algébrica.*

Demonstração. Seja $\mathbb{L}$ um extensão finita de $\mathbb{K}$ e seja $[\mathbb{L} : \mathbb{K}] = m$. Para $\theta \in \mathbb{L}$ os $m + 1$ elementos $1, \theta, \ldots, \theta^m$ são linearmente dependentes sobre $\mathbb{K}$ (devido a definição de grau de extensão finita). Então temos que

$$a_0 + a_1\theta + \cdots + a_m\theta^m = 0$$

com $a_i \in \mathbb{K}$ não todos nulos. Isto mostra que θ é algébrico sobre $\mathbb{K}$. □

Definição 1.5 *Se $\theta \in \mathbb{F}$ é algébrico sobre $\mathbb{K}$, então o polinômio mômico $g \in \mathbb{K}[x]$ gerador do ideal $J = \{f \in \mathbb{K}[x] : f(\theta) = 0\}$ de $\mathbb{K}[x]$ é chamado de Polinômio Minimal de θ sobre $\mathbb{K}$.*

Dizemos que θ é algébrico de grau n sobre $\mathbb{K}$, se seu polinômio minimal sobre $\mathbb{K}$ tem grau n.

Proposição 1.6 *Se $\theta \in \mathbb{F}$ é algébrico sobre $\mathbb{K}$, então o seu polinômio minimal $g \in \mathbb{K}[x]$ é um polinômio irredutível sobre $\mathbb{K}$.*

Demonstração. Suponha que $g = h_1 h_2$ onde $h_1, h_2 \in \mathbb{K}[x]$ com $1 \leqslant \deg(h_i) \leqslant \deg(g)$, $i = 1, 2..$ Então, segue que $0 = g(\theta) = h_1(\theta)h_2(\theta)$ implicando que h_1 ou h_2 pertence a J e assim este é divisível por g, o que é impossível. □

Definição 1.7 *Seja $\mathbb{K}$ um subcorpo de um corpo $\mathbb{F}$ e M qualquer subconjunto de $\mathbb{F}$. Então o corpo $\mathbb{K}(M)$ é definido como a interseção de todos os subcorpos de $\mathbb{F}$ contendo ambos $\mathbb{K}$ e M e é chamado a extensão de $\mathbb{K}$ obtida por Adjacência dos elementos de M. Para $M = \{\theta_1, \ldots, \theta_n\}$ finito escrevemos $\mathbb{K}(M) = \mathbb{K}(\theta_1, \ldots, \theta_n)$. Se M é formado por apenas um elemento $\theta \in \mathbb{F}$ então $L = \mathbb{K}(\theta)$ é dita extensão simples de $\mathbb{K}$.*

Teorema 1.8 *Seja $\theta \in \mathbb{F}$ algébrico de grau n sobre $\mathbb{K}$ e seja g o polinômio minimal de θ sobre $\mathbb{K}$. Então:*

i) $\mathbb{K}(\theta)$ *é isomorfo a* $\mathbb{K}[x]/\langle g \rangle$*;*

ii) $[\mathbb{K}(\theta) : \mathbb{K}] = n$ *e* $\{1, \theta, \ldots, \theta^{n-1}\}$ *é uma base de* $\mathbb{K}(\theta)$ *sobre* $\mathbb{K}$*;*

iii) Todo $\alpha \in \mathbb{K}(\theta)$ *é algébrico sobre* $\mathbb{K}$ *e seu grau é divisor de* n*.*

Demonstração. Ver [7]. □

Teorema 1.9 *Se $\mathbb{L}$ é uma extensão finita do corpo $\mathbb{K}$ e $\mathbb{T}$ é uma extensão finita do corpo $\mathbb{L}$. Então $\mathbb{T}$ é uma extensão finita do corpo $\mathbb{K}$ com*

$$[\mathbb{T} : \mathbb{K}] = [\mathbb{T} : \mathbb{L}]\,[\mathbb{L} : \mathbb{K}]\,.$$

Demonstração. Ver [7]. □

Teorema 1.10 *Se $\mathbb{F}$ é um corpo finito contendo um subcorpo $\mathbb{K}$ com q elementos. Então $\mathbb{F}$ possui q^m elementos onde $m = [\mathbb{F} : \mathbb{K}]$.*

Demonstração. Considere $\mathbb{F}$ como um espaço vetorial sobre $\mathbb{K}$. Como $\mathbb{F}$ é finito, este possui dimensão finita sobre $\mathbb{K}$. Se $[\mathbb{F} : \mathbb{K}] = m$ então, $\mathbb{F}$ possui uma base com m elementos, digamos, $b_1, \ldots, b_m$. Logo todo elemento de $\mathbb{F}$ pode ser representado de maneira única como $a_1b_1 + \cdots + a_mb_m$ onde, $a_1, \ldots, a_m \in \mathbb{K}$. Como cada a_i pode assumir q valores distintos, $\mathbb{F}$ possui exatamente q^m elementos. □

Definição 1.11 *Se* $\mathbf{R}$ *é um anel arbitrário e existe* $n \in \mathbb{Z}^+$ *tal que* $n.r = 0$ *para todo* $r \in \mathbf{R}$*, então o menor inteiro positivo para o qual isto ocorre é chamado de característica de* $\mathbf{R}$*.* $\mathbf{R}$ *é dito de característica zero se não existe tal inteiro.*

Teorema 1.12 *Um anel* $\mathbf{R} \neq \{0\}$ *de característica positiva com identidade e sem divisores de zero possui característica prima.*

Demonstração. Como $\mathbf{R}$ possui elementos não nulos então $\mathbf{R}$ possui característica $n \geqslant 2$. Se n não é primo podemos escrever $n = km$ com $k, m \in \mathbb{Z}$, $1<k, m<n$. Então, $0 = ne = (km)e = (ke)(me)$, onde $e \in \mathbf{R}$ é a identidade. Assim $(ke) = 0$ ou $(me) = 0$ pois $\mathbf{R}$ não possui divisores de zero. Daí, segue que $kr = (ke)r = 0$ para todo $r \in \mathbf{R}$ ou, $mr = (me)r = 0$ para todo $r \in \mathbf{R}$. Contradizendo a definição de n. □

Corolário 1.13 *Um corpo finito* $\mathbb{F}$ *possui característica prima.*

Demonstração. Basta mostrar que todo corpo finito tem característica positiva. Considere então os elementos $e, 2e, 3e, \ldots$. Como $\mathbb{F}$ possui um número finito de elementos, existem $k, m \in \mathbb{Z}^+$ com $1 \leqslant k < m$ tais que $ke = me$, ou seja, $(m - k)e = 0$ e então, $\mathbb{F}$ possui característica positiva. □

Teorema 1.14 *Seja* $\mathbf{R}$ *um anel comutativo com característica prima* p*. Então*

$$(a \pm b)^{p^m} = a^{p^m} \pm b^{p^m}.$$

para $a, b \in \mathbf{R}$ *e* $m \in \mathbb{N}$*.*

Demonstração. Observe que,

$$\left(\begin{array}{c} p \\ i \end{array} \right) = \frac{p(p-1)\ldots(p-i+1)}{i(i-1)\ldots 1} \equiv 0 \; mod(p).$$

para todo $i \in \mathbb{Z}$ com $1 < i < p$, então

$$(a+b)^p = a^p + \left(\begin{array}{c} p \\ 1 \end{array} \right) a^{p-1}b + \cdots + \left(\begin{array}{c} p \\ p-1 \end{array} \right) ab^{p-1} + b^p = a^p + b^p.$$

Agora aplicando indução em m temos o resultado $(a+b)^{p^m} = a^{p^m} + b^{p^m}$. Para a outra igualdade basta notar que $a^{p^m} = ((a-b))+b)^{p^m} = (a-b)^{p^m} + b^{p^m}$ e o Teorema é válido. □

Lema 1.15 *Todo corpo $\mathbb{K}$ de ordem p é isomorfo a $\mathbb{Z}_p$.*

Demonstração. Seja $\mathbb{K}$ um corpo de ordem p e 1 a sua unidade. Observe que $\mathbb{K}$ sendo finito tem característica finita, que só pode ser p. Defina $\phi : \mathbb{Z}_p \longrightarrow \mathbb{K}$ por $\phi(m) = m * 1$ (ou seja, somamos m vezes a unidade em $\mathbb{K}$). Se $m * 1 = n * 1$ então $m = n$ pois $-p < m - n < p$. Logo os p elementos $0, 1, 2 * 1, \ldots, (p-1) * 1$ são elementos distintos de $\mathbb{K}$, e portanto, ϕ é uma bijeção. Como ϕ preserva as operações temos que ϕ é um isomorfismo e o Lema é válido.

□

Teorema 1.16 *Seja $\mathbb{F}$ um corpo finito, então $\mathbb{F}$ possui p^n elementos, onde o primo p é a característica de $\mathbb{F}$ e n é o grau de $\mathbb{F}$ sobre este subcorpo.*

Demonstração. Se $\mathbb{F}$ é um corpo finito, pelo Corolário 1.13 sua característica é prima, mais ainda, o subcorpo primo $\mathbb{K}$ de $\mathbb{F}$ é isomorfo a $\mathbb{Z}_p$ pelo Lema 1.15 e então, contém p elementos. Daí, pelo Lema 1.10, $\mathbb{F}$ possui p^n elementos onde $n := [\mathbb{F} : \mathbb{F}_p]$. □

Lema 1.17 *Se $\mathbb{F}$ é um corpo finito com q elementos, então todo $a \in \mathbb{F}$ satisfaz $a^q = a$.*

Demonstração. A identidade $a^q = a$ é trivial se $a = 0$. Por outro lado, é fácil ver que os elementos não nulos de $\mathbb{F}$ formam um grupo de ordem $(q-1)$ em relação à multiplicação, então pelo Teorema de Lagrange, $a^{q-1} = 1$ para todo $a \in \mathbb{F}$ com $a \neq 0$ ou seja, $a^q = a$. □

Definição 1.18 *Seja $f \in \mathbb{K}[x]$ de grau positivo e $\mathbb{F}$ uma extensão de $\mathbb{K}$. Então f é dito fatorável em $\mathbb{F}$ se pode ser escrito como o produto de fatores lineares em $\mathbb{F}[x]$, isto é, existem $\alpha_1, \ldots, \alpha_m \in \mathbb{F}$ tais que,*

$$f(x) = a(x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_m)$$

onde a é o coeficiente lider de f. O corpo $\mathbb{F}$ é um Corpo de Decomposição de f sobre $\mathbb{K}$ se f é fatorável em $\mathbb{F}$ e se, além disso temos $\mathbb{F} = \mathbb{K}(\alpha_1, \ldots, \alpha_m)$.

Lema 1.19 *Se $\mathbb{F}$ é um corpo finito com q elementos e $\mathbb{K}$ é um subcorpo de $\mathbb{F}$, então o polinômio $x^q - x$ em $\mathbb{K}[x]$ decompõe em $\mathbb{F}[x]$ como,*

$$x^q - x = \prod_{a \in \mathbb{K}} (x-a)$$

e $\mathbb{F}$ é um corpo de decomposição de $x^q - x$ sobre $\mathbb{K}$.

Demonstração. O polinômio $x^q - x$ de grau q possui q raízes em $\mathbb{F}$ pelo Lema 1.17 e sabemos quais são estas raízes (todos os elementos de $\mathbb{F}$). Então o polinômio dado decompõe-se em $\mathbb{F}$ na maneira indicada, e este não pode ser fatorado em qualquer corpo menor. □

Lema 1.20 *Um elemento $b \in \mathbb{F}_q$ é uma raiz múltipla de $f \in \mathbb{F}_q[x]$ se, e somente se, este é raiz de f e f'.*

Demonstração. Ver [7]. □

Teorema 1.21 *Dado um corpo $\mathbb{K}$ e um polinômio $f(x) \in \mathbb{K}[x]$ não constante, existe um corpo de decomposição de $f(x)$ que é único a menos de isomorfismos.*

Demonstração. Ver [11]. □

Teorema 1.22 *(Existência e unicidade de corpos finitos). Para cada primo p e todo inteiro positivo n existe um corpo finito com p^n elementos e qualquer corpo finito com $q = p^n$ elementos é isomorfo ao corpo de decomposição de $x^q - x$ sobre $\mathbb{F}_p$.*

Demonstração.
EXISTÊNCIA: Para $q = p^n$ considere $x^q - x \in \mathbb{F}_p[x]$, e seja $\mathbb{F}$ seu corpo de decomposição sobre $\mathbb{F}_p$. Este polinômio possui q raízes distintas em $\mathbb{F}$ pois, sua derivada é $qx^{q-1} - 1 = -1$ em $\mathbb{F}_q[x]$ e então pelo Lema 1.20 não podemos ter raízes múltiplas. Seja $S := \{a \in \mathbb{F} : a^q - a = 0\}$ então S é um subcorpo de $\mathbb{F}$ pois,

i) $0, 1 \in S$;

ii) Se $a, b \in S$ então pelo Teorema 1.14 temos que $(a-b)^q = a^q - b^q = a - b$ e assim, $(a-b) \in S$;

iii) Para $a, b \in S$ com $b \neq 0$ temos, $(ab^{-1})^q = a^q(b^{-1})^q = ab^{-1}$ e então $ab^{-1} \in S$.

Porém $x^q - x$ pode ser decomposto em S pois S contém todas as raízes de $x^q - x$. Então $\mathbb{F} = S$ e como S possui q elementos temos que $\mathbb{F}$ é um corpo finito com q elementos.
UNICIDADE: Seja $\mathbb{F}$ um corpo finito com $q = p^n$ elementos. Então $\mathbb{F}$ possui característica p pelo Teorema 1.16 e então contém $\mathbb{F}_q$ como subcorpo. Isto mostra pelo Lema 1.19 que $\mathbb{F}$ é corpo de decomposição de $x^q - x$ sobre $\mathbb{F}_p$ e então o resultado segue da unicidade dos corpos de decomposição. □

Teorema 1.23 *Seja $\mathbb{F}_q$ um corpo finito com $q = p^n$ elementos, então todo subcorpo de $\mathbb{F}_q$ possui ordem p^m onde m é um divisor positivo de n. Consequentemente, se m é um divisor positivo de n, então existe exatamente um subcorpo de $\mathbb{F}_q$ com p^m elementos.*

Demonstração. Um subcorpo $\mathbb{K}$ de $\mathbb{F}$ possui ordem p^m para algum $m \leqslant n$. O Lema 1.10 mostra que $q = p^n$ deve ser uma potência de p^m e então necessariamente m é divisor de n.
Consequentemente, se m é um divisor positivo de n então $p^m - 1$ divide $p^n - 1$ assim, $x^{p^m-1} - 1$ divide $x^{p^n-1} - 1$ em $\mathbb{F}_p[x]$. Logo toda raiz de $x^{p^m} - x$ é uma raiz de $x^{p^n} - x = x^q - x$ e então pertence a $\mathbb{F}_q[x]$. Isto mostra que $\mathbb{F}_q$ deve conter como subcorpo um corpo de decomposição de $x^{p^m} - x$ em $\mathbb{F}_p$. Pelo Teorema 1.22 este subcorpo possui ordem p^m. Se houvessem dois subcorpos distintos de ordem p^m em $\mathbb{F}_q$, eles teriam juntos mais que p^m raízes de $x^{p^m} - x$ em $\mathbb{F}_q$ o que é uma contradição. □

Para um corpo finito $\mathbb{F}_q$ denotamos por $\mathbb{F}_q^*$ o grupo multiplicativo dos elementos não nulos de $\mathbb{F}_q$.

Teorema 1.24 *Para todo corpo finito $\mathbb{F}_q$ o grupo multiplicativo $\mathbb{F}_q^*$ de elementos não nulos de $\mathbb{F}_q$ é cíclico.*

Demonstração. Assuma que $q \geqslant 3$. Considere $h = p_1^{r_1} p_2^{r_2} \dots p_m^{r_m}$ a fatoração prima da ordem $h = (q-1)$ do grupo $\mathbb{F}_q^*$. Para cada i, $1 \leqslant i \leqslant m$, o polinômio $x^{\frac{h}{p_i}} - 1$ possui no máximo $\frac{h}{p_i}$ raízes em $\mathbb{F}_q$. Como $\frac{h}{p_i} < h$, existem elementos não nulos em $\mathbb{F}_q$ que não são raízes deste polinômio. Seja a_i um destes elementos. Defina $b_i = a_i^{\frac{h}{p_i^{r_i}}}$. Temos que $b_i^{p_i^{r_i}} = 1$, então a ordem de b_i é um divisor de $p_i^{r_i}$ e mais ainda é da forma $p_i^{s_i}$ com $0 \leqslant s_i \leqslant r_i$. Por outro lado,

$$b_i^{p_i^{r_i-1}} = a_i^{\frac{h}{p_i}} \neq 1.$$

e então a ordem de b_i é $p_i^{r_i}$.

Mostraremos agora que $b = b_1 b_2 \dots b_m$ possui ordem h. Para tanto suponha que a ordem de b é um divisor próprio de h e é portanto, um divisor de, no mínimo, um dos m inteiros $\frac{h}{p_i}$ onde, $1 \leqslant i \leqslant m$, digamos $\frac{h}{p_1}$. Então temos,

$$1 = b^{\frac{h}{p_1}} = b_1^{\frac{h}{p_1}} b_2^{\frac{h}{p_1}} \dots b_m^{\frac{h}{p_1}}$$

Agora, se $2 \leqslant i \leqslant m$, então $p_i^{r_i}$ divide $\frac{h}{p_1}$ e então $b_i^{\frac{h}{p_1}} = 1$. Portanto, $b_1^{\frac{h}{p_1}} = 1$ e isto implica que a ordem de b_1 divide $\frac{h}{p_1}$ o que é impossível pois, a ordem de b_1 é $p_1^{r_1}$. Então $\mathbb{F}_q^*$ é um grupo cíclico com gerador b. □

Definição 1.25 *Um gerador do grupo cíclico $\mathbb{F}_q^*$ é chamado de um elemento primitivo de $\mathbb{F}_q$.*

Teorema 1.26 *Seja $\mathbb{F}_q$ um corpo finito e $\mathbb{F}_r$ uma extensão de $\mathbb{F}_q$. Então $\mathbb{F}_r$ é uma extensão algebrica simples de $\mathbb{F}_q$ e todo elemento primitivo de $\mathbb{F}_r$ pode servir como um elemento primitivo de $\mathbb{F}_r$ sobre $\mathbb{F}_q$.*

Demonstração. Seja θ um elemento primitivo de $\mathbb{F}_r$. Claramente $\mathbb{F}_q(\theta) \subseteq \mathbb{F}_r$, por outro lado, $\mathbb{F}_q(\theta)$ contém 0 e todas as potências de θ e então todos os elementos de $\mathbb{F}_r$ ou seja, $\mathbb{F}_r = \mathbb{F}_q(\theta)$.
□

Teorema 1.27 *Para todo corpo finito $\mathbb{F}_q$ e todo inteiro positivo n existe um polinômio irredutível em $\mathbb{F}_q[x]$ de grau n.*

Demonstração. Seja $\mathbb{F}_r$ a extensão do corpo $\mathbb{F}_q$ de ordem q^n então $[\mathbb{F}_r : \mathbb{F}_q] = n$ e pelo Teorema 1.26 temos que, $\mathbb{F}_r = \mathbb{F}_q(\theta)$ para algum $\theta \in \mathbb{F}_r$. Então o polinômio minimal de θ sobre $\mathbb{F}_q$ é um polinômio irredutível em $\mathbb{F}_q[x]$ de grau n. □

1.2 Raízes de polinômios irredutíveis

Lema 1.28 *Seja $f \in \mathbb{F}_q[x]$ um polinômio irredutível sobre o corpo $\mathbb{F}_q$ e seja α uma raiz de f em uma extensão do corpo $\mathbb{F}_q$. Então para algum polinômio $h \in \mathbb{F}_q[x]$ temos $h(\alpha) = 0$ se, e somente se, f divide h.*

Demonstração. Seja a o coeficiênte lider de f e defina $g(x) = a^{-1}f(x)$. Deste modo g é mônico, irredutível em $\mathbb{F}_q[x]$ com $g(\alpha) = 0$ e então este é o minimal de α em $\mathbb{F}_q$. □

Lema 1.29 *Seja $f \in \mathbb{F}_q[x]$ um polinômio irredutível sobre $\mathbb{F}_q$ de grau m. Então $f(x)$ divide $x^{q^n} - x$ se, e somente se, m divide n.*

Demonstração.
$\Rightarrow$) Suponha que $f(x)$ divide $x^{q^n} - x$. Seja α uma raiz de f no corpo de decomposição de f em $\mathbb{F}_q$. Então $\alpha^{q^n} = \alpha$, e então $\alpha \in \mathbb{F}_{q^n}$. Isto mostra que, $\mathbb{F}_q(\alpha)$ é um subcorpo de $\mathbb{F}_{q^n}$. Como $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = m$ e $[\mathbb{F}_{q^n} : \mathbb{F}_q] = n$, o Teorema 1.9 mostra que m divide n pois

$$\begin{aligned} m &= [\mathbb{F}_q(\alpha) : \mathbb{F}_q] \\ &= [\mathbb{F}_q(\alpha) : \mathbb{F}_{q^n}][\mathbb{F}_{q^n} : \mathbb{F}_q] \\ &= [\mathbb{F}_q(\alpha) : \mathbb{F}_{q^n}]n \end{aligned}$$

$\Leftarrow$) Se m divide n então o Teorema 1.23 implica que $\mathbb{F}_{q^n}$ contém $\mathbb{F}_{q^m}$ como um subcorpo. Seja α uma raiz de f no corpo de decomposição de f sobre $\mathbb{F}_q$. Então $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = m$ e $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}$. Logo temos que $\alpha \in \mathbb{F}_{q^n}$ e então $\alpha^{q^n} = \alpha$ assim α é raiz de $x^{q^n} - x \in \mathbb{F}_q[x]$ e pelo Lema 1.28 segue que $f(x)$ divide $x^{q^n} - x$. □

Teorema 1.30 *Se f é um polinômio irredutível em $\mathbb{F}_q[x]$ de grau m, então f possui uma raiz α em $\mathbb{F}_{q^m}$. Mais ainda, todas as raízes de f são simples e são dadas pelos m elementos $\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}}$ de $\mathbb{F}_{q^m}$.*

Demonstração. Seja α uma raiz de f no corpo de decomposição de f sobre $\mathbb{F}_q$. Assim temos $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = m$ donde, $\mathbb{F}_{q^m} = \mathbb{F}_q(\alpha)$ e em particular $\alpha \in \mathbb{F}_{q^m}$. Vamos mostrar que se $\beta \in \mathbb{F}_{q^m}$ é uma raiz de f então β^q também é uma raiz. Escreva,

$$f(x) = a_m x^m + \cdots + a_1 x + a_0 \quad com \quad a_i \in \mathbb{F}_q \; para \; 0 \leqslant i \leqslant m.$$

Então pelo Lema 1.17 e pelo Teorema 1.14

$$\begin{aligned} f(\beta^q) &= a_m \beta^{qm} + \ldots + a_1 \beta^q + a_0 \\ &= a_m^q \beta^{qm} + \cdots + a_1^q \beta^q + a_0 \\ &= (a_m \beta^m + \cdots + a_1 \beta + a_0)^q \\ &= f(\beta)^q \\ &= 0. \end{aligned}$$

Mais ainda, os elementos $\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}}$ são raízes de f. Basta mostrar que elas são distintas. Para tanto suponha por absurdo que $\alpha^{q^j} = \alpha^{q^k}$ para inteiros j, k com $0 \leqslant j < k \leqslant m-1$. Daí,

$$\alpha^{q^{(m-k+j)}} = \alpha^{q^m} = \alpha.$$

Então pelo Lema 1.28 $f(x)$ divide $x^{q^{(m-k+j)}} - x$ e pelo Lema 1.29 m divide $(m-k+j)$. Porém, $0 < m - k + j < m$, uma contradição. □

Corolário 1.31 *Seja f um polinômio irredutível em $\mathbb{F}_q[x]$ de grau m. Então, o corpo de decomposição de f sobre $\mathbb{F}_q$ é dado por $\mathbb{F}_{q^m}$.*

Demonstração. O Teorema 1.30 mostra que f decompõe-se em $\mathbb{F}_{q^m}$. Além disso,

$$\mathbb{F}_q(\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}}) = \mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}$$

para uma raiz α de f em $\mathbb{F}_{q^m}$, onde a segunda identidade seque do Teorema 1.30. □

O Corolário 1.31 nos diz que quaisquer dois polinômios irredutíveis em $\mathbb{F}_q[x]$ de mesmo grau possuem corpos de decomposição isomorfos.

Definição 1.32 *Seja $\mathbb{F}_{q^m}$ uma extensão de $\mathbb{F}_q$ e seja $\alpha \in \mathbb{F}_{q^m}$. Os elementos $\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}}$ são chamados de conjugados de α com respeito a $\mathbb{F}_q$.*

Teorema 1.33 *O conjugado de $\alpha \in \mathbb{F}_q^*$ com respeito a qualquer subcorpo de $\mathbb{F}_q$ possui a mesma ordem no grupo $\mathbb{F}_q^*$.*

Demonstração. Como $\mathbb{F}_q^*$ é um grupo ciclico o teorema segue da Proposição 4.68 (Apêndice) e do fato de todas potências da característica de $\mathbb{F}_q$ serem co-primas com a ordem $(q-1)$ de $\mathbb{F}_q^*$.
□

Corolário 1.34 *Se α é um elemento primitivo de $\mathbb{F}_q$, então são assim todos os seus conjugados com respeito a qualquer subcorpo de $\mathbb{F}_q^*$.*

Teorema 1.35 *Os automorfismos distintos de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$ são todas as funções $\sigma_0, \sigma_1, \ldots, \sigma_{m-1}$ definidas por $\sigma_j(\alpha) = \alpha^{q^j}$ para $\alpha \in \mathbb{F}_{q^m}$ e $0 \leqslant j \leqslant m-1$.*

Demonstração. Para cada σ_j e todos $\alpha, \beta \in \mathbb{F}_{q^m}$ temos, $\sigma_j(\alpha\beta) = \sigma_j(\alpha)\sigma_j(\beta)$ e também pelo Teorema 1.14 $\sigma_j(\alpha+\beta) = \sigma_j(\alpha) + \sigma_j(\beta)$. Então σ_j é um endomorfismo de $\mathbb{F}_{q^m}$. Além disso, $\sigma_j(\alpha) = 0$ se, e somente se, $\alpha = 0$. Então σ_j é injetora e como $\mathbb{F}_{q^m}$ é finito temos que σ_j é um automorfismo. Ainda pelo Lema 1.17 temos $\alpha_j(a) = a$ para todo $a \in \mathbb{F}_q$ e então cada σ_j é um automorfismo de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$. As funções $\sigma_0, \sigma_1, \ldots, \sigma_{m-1}$ são distintas pois possuem valores distintos para um elemento primitivo de $\mathbb{F}_{q^m}$.

Agora suponha que σ é um automorfismo arbitrário de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$. Seja β um elemento primitivo de $\mathbb{F}_{q^m}$ e seja

$$f(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_0 \in \mathbb{F}_q[x]$$

o seu polinômio minimal sobre $\mathbb{F}_q$. Então,

$$\begin{aligned} 0 &= \sigma(\beta^m + a_{m-1}\beta^{m-1} + \cdots + a_0) \\ &= \sigma(\beta)^m + a_{m-1}\sigma(\beta)^{m-1} + \cdots + a_0. \end{aligned}$$

Daí, $\sigma(\beta)$ é um raiz de f em $\mathbb{F}_{q^m}$ e pelo Teorema 1.30 temos $\sigma(\beta) = \beta^{q^j}$ para algum j $0 \leqslant j \leqslant m-1$. Como σ é um homomorfismo temos $\sigma(\alpha) = \alpha^{q^j}$ para $\alpha \in \mathbb{F}_{q^m}$. □

Note que pelo Teorema 1.35 os conjugados de $\alpha \in \mathbb{F}_{q^m}$ com respeito à $\mathbb{F}_q$ são dados pela aplicação de todos os automorfismos de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$ no elemento α.

1.3 Raízes da Unidade e Polinômios Ciclotômicos

Definição 1.36 *Seja n um inteiro posítivo. O corpo de decomposição de $x^n - 1$ sobre $\mathbb{K}$ é chamado de n-ésimo Corpo Ciclotômico sobre $\mathbb{K}$ e será denotado por $\mathbb{K}^{(n)}$. As raízes de $x^n - 1$ em $\mathbb{K}^{(n)}$ são chamadas de raízes n-ésimas da unidade sobre $\mathbb{K}$. O conjunto de todas as raízes n-ésimas da unidade será denotado por $E^{(n)}$.*

Teorema 1.37 *Seja n um inteiro positivo e $\mathbb{K}$ um corpo de característica p, então,*

i) Se p não divide n, então $E^{(n)}$ é um grupo cíclico de ordem n com respeito à multiplicação em $\mathbb{K}^{(n)}$;

ii) Se $n = mp^e$, onde m é um inteiro não divisível por p, então $\mathbb{K}^{(n)} = \mathbb{K}^{(m)}\mathbb{E}^{(n)} = \mathbb{E}^{(m)}$ e as raízes de $x^n - 1$ em $\mathbb{K}^{(n)}$ são os m elementos de $\mathbb{E}^{(m)}$, onde cada um tem multiplicidade p^e.

Demonstração.

i) Para $n \geqslant 2$, $x^n - 1$ e sua derivada nx^{n-1} não possuem raízes em comum pois, nx^{n-1} possui apenas zero como raiz. E pelo Lema 1.20 $x^n - 1$ não possui raízes repetidas o que mostra que $E^{(n)}$ possui n elementos. Agora se $\alpha, \beta \in E^{(n)}$ então $(\alpha\beta^{-1})^n = \alpha^n(\beta^n)^{-1} = 1$ então $\alpha\beta^{-1} \in E^{(n)}$ isto mostra que $E^{(n)}$ é um grupo multiplicativo.

   Seja $n = p_1^{e_1}p_2^{e_2}\dots p_t^{e_t}$ a fatoração prima de n. Então pelo argumento do Teorema 1.24 temos que para cada i, $1 \leqslant i \leqslant t$, existe $\alpha_i \in E^{(n)}$ que não é raiz do polinômio $x^{\frac{n}{p_i}} - 1$ e que $\beta_t = \alpha_t^{\frac{n}{p^{e_t}}}$ possui ordem $p_t^{e_t}$ e que $E^{(n)}$ é um grupo cíclico com gerador $\beta = \beta_1 \dots \beta_t$.

ii) Temos que $x^n - 1 = x^{mp^e} - 1 = (x^m - 1)^{p^e}$.

□

Definição 1.38 *Seja $\mathbb{K}$ um corpo com característica p, n um inteiro positivo que não é divisível por p. Então um gerador do grupo cíclico $E^{(n)}$ é chamado de raiz n-ésima primitiva da unidade sobre $\mathbb{K}$.*

Definição 1.39 *Seja $\mathbb{K}$ um corpo de característica p, n um inteiro posítivo que não é divisível por p e α uma raiz n-ésima primitiva da unidade sobre $\mathbb{K}$. Então o polinômio*

$$Q_n(x) = \prod_{s=1}^{n}(x - \alpha^s)$$

onde o produto se estende a todo $s = 0, 1, \dots, n$ tais que $mdc(s, n) = 1$, é chamado de n-ésimo polinômio ciclotômico sobre $\mathbb{K}$.

Teorema 1.40 *Seja $\mathbb{K}$ um corpo de característica p e n um inteiro positivo que não é divisível por p, então*

i) $x^n - 1 = \prod_{d|n} Q_d(x)$;

ii) Os coeficientes de $Q_n(x)$ estão no subcorpo primo de $\mathbb{K}$.

Demonstração.

i) Cada raiz n-ésima da unidade sobre $\mathbb{K}$ é uma raiz d-ésima primitíva da unidade sobre $\mathbb{K}$ para um divisor d de n.

De fato, se α é uma raiz n-ésima primitiva da unidade sobre $\mathbb{K}$ e α^s é uma raiz n-ésima arbitrária da unidade sobre $\mathbb{K}$ então tome $d = \frac{n}{mdc(s,n)}$, isto é, d é a ordem de α^s em $E^{(n)}$. A fórmula em $i)$ é obtida pela coleção de fatores para os quais $(x - \alpha^s)$, onde, α^s é uma raiz d-ésima primitiva da unidade sobre $\mathbb{K}$.

ii) Note que $Q_n(x)$ é um polinômio mônico. Para $n = 1$ temos $Q_1 = x - 1$ e o resultado é válido. Agora seja $n > 1$ e suponha que a proposição seja válida para Q_d com $1 \leqslant d \leqslant n$. Então por $i)$

$$Q_n(x) = \frac{x^n - 1}{f(x)} \text{ onde } f(x) = \prod_{d|n} Q_d(x).$$

A hipótese de indução implica que $f(x)$ é um polinômio com coeficientes no subcorpo primo de $\mathbb{K}$ ou em $\mathbb{Z}$ no caso em que a característica de $\mathbb{K}$ é zero.

□

Chamaremos de função de Euler a função ϕ definida por,

$$\phi(x) = |\{n \in \mathbb{N} : n < x \text{ e } mdc(n, x) = 1\}|.$$

Teorema 1.41 *O corpo ciclotômico $\mathbb{K}^{(n)}$ é uma extensão simples de $\mathbb{K}$. Além disso,*

i) Se $\mathbb{K} = \mathbb{Q}$, então o polinômio ciclotômico Q_n é irredutível sobre $\mathbb{K}$ e $[\mathbb{K}^{(n)} : \mathbb{K}] = \phi(n)$;

ii) Se $\mathbb{K} = \mathbb{F}_q$ com $mdc(q, n) = 1$, então, Q_n fatora-se em $\phi(n)/d$ polinômios mônicos distintos irredutíveis em $\mathbb{K}[x]$ de mesmo grau d, onde d é o menor inteiro positivo tal que $q^d \equiv 1\ mod(n)$. $\mathbb{K}^{(n)}$ é um corpo de decomposição de qualquer um dos fatores irredutíveis sobre $\mathbb{K}$ e $[\mathbb{K}^{(n)} : \mathbb{K}] = d$.

Demonstração. Se existe uma raiz n-ésima primitiva α da unidade sobre $\mathbb{K}$ é claro que $\mathbb{K}^{(n)} = \mathbb{K}(\alpha)$. Além disso temos a situação descrita no Teorema 1.37 então $\mathbb{K}^{(n)} = \mathbb{K}^{(m)}$ e o resultado segue novamente. Basta então provar $ii)$.

Seja α uma raiz n-ésima primitiva da unidade sobre $\mathbb{F}_q$. Então $\alpha \in \mathbb{F}_{q^k}$ se, e somente se, $\alpha^k = \alpha$ ou seja, $q^k \equiv 1\ mod(n)$ e o menor inteiro para o qual isto é válido é $k = d$ e então $\alpha \in \mathbb{F}_{q^d}$. Porém não existe subcorpo próprio de $\mathbb{F}_{q^d}$ então o polinômio minimal de α sobre $\mathbb{F}_q$ possui grau d e como α era qualquer raiz de Q_n o que prova o resultado. □

Teorema 1.42 *O corpo finito $\mathbb{F}_q$ é o $(q-1)$-ésimo corpo ciclotômico sobre qualquer um dos seus subcorpos.*

Demonstração. O polinômio $x^{q-1}-1$ decompõe-se em $\mathbb{F}_q$ pois suas raízes são exatamente todos os elementos não nulos de $\mathbb{F}_q$. Obviamente, o polinômio não pode se decompor em qualquer subcorpo próprio de $\mathbb{F}_q$ e então o corpo de decomposição de $x^{q-1} - 1$ sobre qualquer um de seus subcorpos é $\mathbb{F}_q$. □

Lema 1.43 *Se d é um divisor de um inteiro positivo n com $1 < d < n$ então Q_n divide $\frac{x^n-1}{x^d-1}$.*

Demonstração. Pelo Teorema 1.40 sabemos que $Q_n(x)$ divide $x^n - 1 = (x^d - 1)\frac{(x^n-1)}{(x^d-1)}$ e como d é um divisor próprio de n, os polinômios $Q_n(x)$ e $x^d - 1$ não possuem raízes em comum. Então $mdc(Q_n(x), x^d - 1) = 1$ e o lema é válido. □

Capítulo 2

Teoria Algébrica dos Códigos

Neste capítulo apresentaremos a teoria clássica de códigos lineares, introduziremos o conceito de código MDS e também apresentaremos um estudo sobre códigos cíclicos. Seguiremos como referências principais [3] e [7].

2.1 Códigos lineares

Definição 2.1 *Seja H uma matriz $(n-k)\times n$ de posto $(n-k)$ com entradas em $\mathbb{F}_q$. O conjunto C de todos os vetores $c \in \mathbb{F}_q^n$ tais que $Hc^T = 0$ é chamado de $[n,k]$-código linear sobre $\mathbb{F}_q$; n é dito o comprimento e k a dimensão do código. Os elementos de C são chamados de palavras código (vetores código), a matriz H é chamada de matriz de paridade de C. Pode-se provar que todo código C possui um código equivalente com matriz de paridade H da forma $(A\ I_{n-k})$. Se $q = 2$, C é um código binário.*

Exemplo 2.2 *Seja $q = 2$ e $(a_1, \ldots, a_k)$ uma mensagem dada, então o sistema de codificação definido por f,*

$$\begin{aligned} f : \mathbb{F}_2^k &\longrightarrow \mathbb{F}_2^{k+1} \\ (a_1, \ldots, a_k) &\longmapsto (b_1, \ldots, b_{k+1}) \end{aligned}$$

onde, $b_i = a_i$ para $i = 1, \ldots, k$ e

$$b_{k+1} = \begin{cases} 0 & se \quad \sum_{i=1}^{k} a_i = 0, \\ 1 & se \quad \sum_{i=1}^{k} a_i = 1 \end{cases}$$

é tal que a soma $\sum_{i=1}^{k+1} b_i$ *de qualquer palavra código* $(b_1, \ldots, b_{k+1})$ *recebida é zero. Se a soma das coordenadas de uma palavra recebida é 1, então o receptor sabe que ocorreu um erro de transmissão. Seja* $n = k + 1$*, então este é um* $[n, n-1]$*-código linear binário com matriz de paridade* $H = [11 \ldots 1]$*. Este código é conhecido como Código Verificador de Paridade.*

Definição 2.3 *A matriz* $(k \times n)$ $G = [I_k \quad -A^T]$ *é chamada de matriz geradora canônica do* $[n, k]$*-código linear com matriz de paridade* $H = [A \ \ I_{n-k}]$.

Para $Hc^T = 0$ e $c = aG$ segue-se que H e G estão relacionadas por

$$GH^T = 0 \tag{2.1}$$

O código C é igual ao espaço linha da matriz geradora canônica G.

Uma matriz geradora G de C pode ser utilizada para a decodificação, no sentido de que uma palavra código $c \in C$ é decodificada por $c = aG \in C$.

Definição 2.4 *Se* c *é uma palavra código e* y *é uma palavra recebida após a transmissão através de um canal, então* $e = y - c = (e_1, e_2, \ldots, e_n)$ *é chamado de "palavra erro"ou "vetor erro".*

Definição 2.5 *Sejam* x, y *dois vetores em* $\mathbb{F}_q^n$*. Então:*

i) A distância de Hamming $d(x, y)$ *entre* x *e* y *é o número de coordenadas em que* x *e* y *diferem, isto é,*

$$d(x, y) = |\{x_i \neq y_i \quad i = 1, 2, \ldots, n\}| .$$

ii) O peso (de Hamming) $w(x)$ *de* x *é o número de coordenadas não nulas de* x *(ou seja* $d(x, 0)$*).*

Proposição 2.6 *A distância de Hamming é uma métrica em* $\mathbb{F}_q^n$*, isto é, para todos* $x, y, z \in \mathbb{F}_q^n$ *temos:*

i) $d(x, y) = 0$ *se, e somente se,* $x = y$*;*

ii) $d(x, y) = d(y, x)$*;*

iii) $d(x, z) \leqslant d(x, y) + d(y, z)$.

Definição 2.7 *Dado um elemento $y \in \mathbb{F}_q^n$ e um inteiro $r \geqslant 0$ definimos a bola e a esfera de centro em y e raio r como sendo, respectivamente, os conjuntos:*

$$B(y,r) := \left\{x \in \mathbb{F}_q^n : d(y,x) \leqslant r\right\},$$

$$S(y,r) := \left\{x \in \mathbb{F}_q^n : d(y,x) = r\right\}.$$

Definição 2.8 *Para todo $t \in \mathbb{N}$, um código $C \subseteq \mathbb{F}_q^n$ é chamado "t-corretor de erros"se para cada $y \in \mathbb{F}_q^n$ existe no máximo um $c \in C$ tal que $d(y,c) \leqslant t$.*

Definição 2.9 *O número*

$$d(C) = \min d(u,v) = \min w(c)$$

onde, $u, v \in C$, $u \neq v$, $c \neq 0$ é chamado de distância mínima do código linear C.

Teorema 2.10 *Seja C um código linear cuja distância mínima é $d(C) \geqslant 2t+1$ então C pode corrigir até t erros.*

Demonstração. Ver [7]. □

Lema 2.11 *Um código linear C cuja uma matriz de paridade é H possui distância mínima $d(C) \geqslant t+1$ se, e somente se, qualquer conjunto de t colunas de H é linearmente independente.*

Demonstração. Ver [7]. □

2.2 Decodificação de Códigos Lineares

Seja C um $[n,k]$-código linear sobre $\mathbb{F}_q$. O espaço vetorial $\mathbb{F}_q^n/C$ consiste em todos as classes laterais $a + C = \{a + c : c \in C\}$ com $a \in \mathbb{F}_q^n$. Cada classe lateral contém q^k elementos de $\mathbb{F}_q^n$ e podemos escrever

$$\mathbb{F}_q^n = (a^{(0)} + C) \cup (a^{(1)} + C) \cup \cdots \cup (a^{(s)} + C)$$

onde, $a^{(0)} = 0$, $s = q^{n-k} - 1$ e a união é disjunta. Agora um vetor y recebido deve estar em uma das classes, digamos em $a^{(i)} + C$. Se uma palavra código c foi transmitida então o erro é dado por $e = y - c = a^{(i)} + z \in a^{(i)} + C$ para $z \in C$. Devido este fato vamos construir um esquema de decodificação. Mas antes precisamos da seguinte definição.

Definição 2.12 *Seja $C \subseteq \mathbb{F}_q^n$ um $[n,k]$-código linear e seja $\mathbb{F}_q^n/C$ o espaço quociente. Um elemento de peso mínimo em uma classe $a+C$ é chamado de líder da classe $a+C$. Se vários vetores em $a+C$ possuem peso mínimo, nós escolhemos um deles como líder da classe.*

Sejam $a^{(1)}, \ldots, a^{(s)}$ os líderes de classes diferentes de C e sejam $c^{(1)}, \ldots, c^{(q^k)}$ todas as palavras código em C. Então se uma palavra $y = a^{(i)} + c^{(j)}$ é recebida, o decodificador decide que o erro "e"é o líder de classe $a^{(i)}$ correspondente e decodifica y como a palavra código $x = y - e = c^{(j)}$.

Definição 2.13 *Seja H a matriz de paridade de um $[n,k]$-código linear C. Então o vetor $S(y) = Hy^T$ de comprimento $(n-k)$ é chamado de síndrome de y.*

Teorema 2.14 *Para $z, y \in \mathbb{F}_q^n$, temos:*

i) $S(y) = 0$ *se, e somente se,* $y \in C$*;*

ii) $S(y) = S(z)$ *se, e somente se,* $y + C = z + C$.

Demonstração.

i) $0 = S(y) = Hy^T \iff y \in C$;

ii) Note que, $S(y) = S(z) \iff Hy^T = Hz^T \iff H(y-z)^T = 0 \iff y - z \in C \iff y + C = z + C$.

□

Agora para corrigir os erros em y, calcula-se $S(y)$ e daí encontra-se o líder de classe, digamos e com síndrome igual a de y. Então decodifica-se y como $x = y - e$ e x será a palavra código com distância mínima para y.

Teorema 2.15 *Em um $[n,k]$-código linear binário com matriz de paridade H, a síndrome é a soma das colunas de H que correspondem às posições onde os erros ocorreram.*

Demonstração. Seja $y \in \mathbb{F}_2^n$ o vetor recebido, $y = x + e, x \in C$ então $S(y) = He^T$. Sejam $i_1, i_2, \ldots, i_t$ as coordenadas erro em "e", digamos, $e = (0, \ldots, 1_{i_1}, \ldots, 0, 1_{i_t}, \ldots, 0, 0)$ então temos $S(y) = h_{i_1} + h_{i_2} + \cdots + h_{i_t}$ onde h_i denota a i-ésima coluna de H. □

Um código binário C_m de comprimento $n = 2^m - 1$ onde $m \geqslant 2$ com uma matriz de paridade H de dimensões $m \times (2^m - 1)$ é chamado código binário de Hamming se as colunas de H são as representações binárias de $1, 2, \ldots, 2^m - 1$.

Lema 2.16 *C_m é um código de dimensão $2^m - m - 1$, 1-corretor de erro.*

Demonstração. Pela definição da matriz de paridade H de C_m temos que o posto de H é m. Também quaisquer duas colunas são linearmente idependentes. Como H contém a soma de quaisquer duas colunas então pelo Lema 2.11 temos que $d(C) \geqslant 3$ e $d(C) = 3$. Então, C_m é um código 1-corretor de erro. □

Exemplo 2.17 *Considerando o $[7, 4]$-Código de Hamming C_3 com matriz de paridade:*

$$H = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

Se, a sindrome de uma palavra recebida y é, digamos, $S(y) = (1, 0, 1)^T$, então sabemos que ocorreu um erro na quinta posição, pois 101 é a representação binária de 5.

Teorema 2.18 *(Limitante de Singleton). Se C é um $[n, k]$-código linear definido sobre $\mathbb{F}_q$ então temos*

$$|C| \leqslant q^{n-d(C)+1}.$$

Demonstração. Primeiro observe que para $C \subseteq \mathbb{F}_q^n$ temos que $|C| \leqslant q^n$ já que para cada entrada de um vetor $x \in C$ existem no máximo q valores a serem escolhidos.

Seja $d(C)$ a distância mínima de C. Se removermos todas as $(d(C) - 1)$ primeiras coordenadas de cada vetor de C temos que os vetores resultantes são todos distintos, já que para todas as palavras código a menor distância entre elas é $d(C)$. Então obtemos um Código C' de mesma cardinalidade que $|C|$ porém agora cada vetor de C' possui comprimento igual a $n - (d(C) - 1) = n - d(C) + 1$ donde $|C'| \leqslant q^{n-d(C)+1}$ provando o resultado. □

Da desigualdade de Singleton segue que, para um $[n, k]$-código linear C sobre $\mathbb{F}_q$ com $|C| = q^k$ temos, que $d(C) \leqslant n - k + 1$. Chamaremos de códigos MDS aos códigos tais que $d(C) = n - k + 1$.

Teorema 2.19 *(Limitante de Hamming). Seja C um código t-corretor de erro sobre $\mathbb{F}_q$ de comprimento n com $|C|$ palavras código. Então,*

$$|C| \left[1 + \binom{n}{1}(q-1) + \cdots + \binom{n}{t}(q-1)^t \right] \leqslant q^n.$$

Demonstração. Seja $\alpha \in \mathbb{F}_q^n$ então $\alpha = (x_1, x_2, \ldots, x_n)$. Agora, se $w(\alpha) = m \geqslant n$ temos $d(\alpha, 0) = m$, ou seja, α possui m-coordenadas não nulas e $(n-m)$-coordenadas fixas $(= 0)$. Logo temos $(q-1)^m$ opções para as outras coordenadas não fixas, portanto, existem $\begin{pmatrix} n \\ m \end{pmatrix} (q-1)^m$ vetores em $\mathbb{F}_q^n$ com peso m. Como translação preserva distância de Hamming, e $S(\beta, m) = \beta + S(0, m)$, segue que cada esfera possui o mesmo número de elementos, e que cada bola de raio t possui

$$\sum_{m=0}^{t} \begin{pmatrix} n \\ m \end{pmatrix} (q-1)^m$$

vetores de $\mathbb{F}_q^n$. Portanto, como as bolas de raio t e centro em uma palavra código são todas disjuntas (já que C é t-corretor de erro) temos

$$|C| \left(\sum_{m=0}^{t} \begin{pmatrix} n \\ m \end{pmatrix} (q-1)^m \right) \leqslant q^n.$$

□

Teorema 2.20 *(Limitante de Plotkin). Para um $[n, k]$-código linear C sobre $\mathbb{F}_q$ de distância mínima $d(C)$ temos,*

$$d(C) \leqslant \frac{nq^{k-1}(q-1)}{q^k - 1}.$$

Demonstração. Seja $1 \leqslant i \leqslant n$ tal que C contém uma palavra código com a i-ésima coordenada não nula e seja D o subespaço de C formado por todas as palavras código com a i-ésima componente nula. Em C/D estão os q elementos correspondentes a q escolhas para a i-ésima coordenada de uma palavra código

$$C/D := \{c + d : d \in D\}$$

então, $\frac{|C|}{|D|} = q$ dai, $|D| = \frac{|C|}{q} = \frac{q^k}{q} = q^{k-1}$. Continuando este processo para cada componente, a soma dos pesos das palavras código é menor ou igual a $nq^{k-1}(q-1)$, a distância mínima $d(C)$ do código é o peso mínimo não nulo e, mais ainda, deve satisfazer a desigualdade do teorema pois, o número total de palavras código de peso diferente de zero é $q^k - 1$. □

Teorema 2.21 *(Teorema de Gilbert-Varshamov). Existe um $[n, k]$-código linear sobre $\mathbb{F}_q$ com distância mínima maior ou igual a d sempre que,*

$$q^{n-k} > \sum_{i=0}^{d-2} \begin{pmatrix} n-1 \\ i \end{pmatrix} (q-1)^i$$

Demonstração. Provaremos este teorema construindo uma $(n-k) \times k$ matriz de paridade H para tal código. Escolha a primeira coluna como qualquer $(n-k)$-upla não nula sobre $\mathbb{F}_q$ e a segunda coluna como qualquer $(n-k)$-upla sobre $\mathbb{F}_q$ que não seja múltiplo escalar da primeira. Em geral suponha que $j-1$ colunas sejam escolhidas de modo que quaisquer $(d-1)$ delas sejam linearmente independentes. Há no máximo,

$$\sum_{i=0}^{d-2} \begin{pmatrix} j-1 \\ i \end{pmatrix} (q-1)^i$$

vetores obtidos pela combinação linear de $(d-2)$ ou menos dessas $(j-1)$ colunas. Se a desigualdade do enunciado vale, então será possível escolher a j-ésima coluna que é linearmente indepedente de qualquer uma das $(j-1)$ colunas anteriores. A construção pode ser realizada até que H possua posto $(n-k)$ e isto resulta em um código que possui distância minima maior ou igual a d pelo Lema 2.11. □

2.3 Códigos Duais

Fazendo uma analogia com o espaço vetorial $\mathbb{R}^n$, podemos considerar em $\mathbb{F}_q^n$ um produto interno dado pela mesma fórmula usada em $\mathbb{R}^n$, ou seja,

$$x.y = x_1y_1 + \cdots + x_ny_n \text{ para } x, y \in \mathbb{F}_q^n.$$

Este produto interno é uma forma bilinear não-degenerada, e faz sentido então considerarmos o código dual de um código linear C que será definido por,

Definição 2.22 *Seja C um $[n,k]$-código linear sobre $\mathbb{F}_q$. Então seu código dual $C^\perp$ é definido como,*

$$C^\perp := \left\{ u \in \mathbb{F}_q^n : u.v = 0 \textit{ para todo } v \in C \right\}.$$

Lema 2.23 *Se $C \subseteq \mathbb{F}_q^n$ é um código linear, 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, $Gx^T = 0$.

Demonstração.

i) Dados $u, v \in C^\perp$ e $t \in \mathbb{F}_q$ temos, que para todo $x \in C$,

$$(u+tv).x = u.x + t(v.x) = 0$$

e, portanto $u + tv \in C^\perp$ provando que $C^\perp$ é subespaço de $\mathbb{F}_q^n$.

ii) $x \in C^{\perp}$ se, e somente se, x é ortogonal a todo elemento de C se, e somente se, x é ortogonal a todo elemento de uma base de C, o que é equivalente a dizer que $Gx^T = 0$, pois as linhas de G constituem uma base para C.

□

A próxima proposição nos fornecerá relações entre dimensões e matrizes geradoras dos códigos linear C e $C^{\perp}$.

Proposição 2.24 *Seja $C \subseteq \mathbb{F}_q^n$ um código de dimensão k com matriz geradora $G = (I_k \quad A)$ então,*

i) $\dim C^{\perp} = n - k$*;*

ii) $H = (-A \quad I_{n-k})$ *é a matriz geradora de* $C^{\perp}$.

Demonstração.

i) Pelo Lema 2.23 $x \in C^{\perp}$ se, e somente se, $Gx^T = 0$. Isto equivale a

$$\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_k \end{pmatrix} = -A \begin{pmatrix} x_{k+1} \\ x_{k+2} \\ \vdots \\ x_n \end{pmatrix}$$

portanto, $C^{\perp}$ possui q^{n-k} elementos, que são as escolhas arbitrárias para $x_{k+1}, \ldots, x_n$. Logo, $C^{\perp}$ possui dimensão $(n-k)$.

ii) É evidente que as linhas de H são L.I, portanto, geram um subespaço vetorial cuja dimensão é $n-k$. Como as linhas de H são ortogonais às linhas de G, temos que o espaço gerado pelas linhas de H está contido em $C^{\perp}$. Como estes subespaços tem mesma dimensão, eles coincidem, provando assim que $H = (-A^T \quad I_{n-k})$ é uma matriz geradora de $C^{\perp}$.

□

Exemplo 2.25 *É importante observar que um código C e seu dual $C^{\perp}$ não são disjuntos, em geral, e podem inclusive coincidir. Por exemplo considerando-se o Código C sobre $\mathbb{F}_2$ com matriz geradora*

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

chamado de código de Hamming estendido de comprimento 8*. Pode-se provar que* $C = C^{\perp}$.

2.4 Caracteres e Identidade de MacWilliams

Aqui falaremos um pouco sobre caracteres, os quais serão utilizados em demonstrações de resultados apresentados no Capítulo 4 e também para a demonstração de uma das igualdades mais importantes quando se trata de teoria de códigos conhecida como Identidade de MacWilliams.

Definição 2.26 *Seja* G *um grupo abeliano finito, um caractere* λ *em* G *é um homomorfismo de* G *no grupo multiplicativo* $U(\mathbb{C})$ *dos números complexos de valor absoluto* 1*, ou seja, é uma função* $\lambda : G \longrightarrow U(\mathbb{C})$ *tal que* $\lambda(g_1 g_2) = \lambda(g_1)\lambda(g_2), \quad \forall g_1, g_2 \in G$.

Note que $[\lambda(g)]^{|G|} = \lambda(g^{|G|}) = \lambda(1_G) = 1 \ \forall g \in G$ onde 1_G indica a unidade do grupo G. Então os valores de λ são exatamente as $|G|$-ésimas raízes da unidade. Note também que, $\lambda(g)\lambda(g^{-1}) = \lambda(1_G) = 1$ e daí, $\lambda(g^{-1}) = \overline{\lambda(g)}$. Podemos também definir o produto de caracteres $\lambda_1, \ldots, \lambda_n$ de G por, $(\lambda_1 \ldots \lambda_n)(g) = \lambda_1(g) \ldots \lambda_n(g) \ \forall g \in G$.

Teorema 2.27 *Se* λ *é um caractere não trivial de* $\mathbb{F}_q$ *então,*

$$\sum_{a \in \mathbb{F}_q} \lambda(a) = 0.$$

Demonstração. Como λ é não trivial, existe $c \in \mathbb{F}_q$ tal que $\lambda(c) \neq 1$. Assim temos,

$$\lambda(c) \sum_{a \in \mathbb{F}_q} \lambda(a) = \sum_{a \in \mathbb{F}_q} \lambda(ac) = \sum_{a \in \mathbb{F}_q} \lambda(a).$$

Pois, a percorre todo $\mathbb{F}_q$ e assim ac também percorrerá, logo temos

$$(\lambda(c) - 1) \sum_{a \in \mathbb{F}_q} \lambda(a) = 0 \Longleftrightarrow \sum_{a \in \mathbb{F}_q} \lambda(a) = 0.$$

□

Lema 2.28 *Seja* λ *um caractere não trivial aditivo de* $\mathbb{F}_q$ *e* $a \in \mathbb{F}_q$ *fixo então,*

$$\sum_{b \in \mathbb{F}_q} \lambda(ab) = \begin{cases} q & se \quad a = 0 \\ 0 & se \quad a \neq 0 \end{cases}.$$

Demonstração. Se $a = 0$ então,

$$\lambda(ab) = \lambda(0b) = \lambda(0) = 1, \ \forall b \in \mathbb{F}_q.$$

Logo,

$$\sum_{b \in \mathbb{F}_q} \lambda(ab) = \sum_{b \in \mathbb{F}_q} 1 = q, \text{ pois } |\mathbb{F}_q| = q.$$

Agora, se $a \neq 0$, temos que,

$$\sum_{b \in \mathbb{F}_q} \lambda(ab) = \sum_{ab = c \in \mathbb{F}_q} \lambda(c) = 0.$$

Pois ab percorre todos os elementos de $\mathbb{F}_q$ já que b percorre e $a \neq 0$. □

Lema 2.29 *Seja λ um caractere aditivo não trivial de $\mathbb{F}_q$. Então para qualquer código linear C sobre $\mathbb{F}_q$ vale:*

$$\sum_{v \in C} \lambda(u.v) = \begin{cases} 0 & se \quad u \notin C^{\perp}, \\ |C| & se \quad u \in C^{\perp}. \end{cases}$$

Demonstração. Se $u \in C^{\perp}$ então $\lambda(u.v) = \lambda(0) = 1$ e daí,

$$\sum_{v \in C} \lambda(u.v) = \sum_{v \in C} \lambda(0) = \sum_{v \in C} 1 = |C|.$$

Suponha agora que, $u \notin C^{\perp}$. Daí pelo Teorema 2.27 e pela igualdade

$$\sum_{v \in C} \lambda(u.v) = \sum_{a \in \mathbb{F}_q} \sum_{u.v = a \in \mathbb{F}_q} \lambda(a) = 0.$$

□

Para uma função $f : \mathbb{F}_q^n \to \mathbb{C}$ iremos definir a Transformada de *Fourier* $\hat{f}$ de f como sendo,

$$\hat{f}(u) = \sum_{v \in \mathbb{F}_q^n} \lambda(u.v) f(v).$$

Onde, λ é um caractere aditivo não trivial de $\mathbb{F}_q$.

Lema 2.30 *(soma discreta de Poisson). Seja C um código linear de tamanho "n"sobre o corpo $\mathbb{F}_q$ e f uma função definida em $\mathbb{F}_q^n$ então*

$$\sum_{u \in C^{\perp}} f(u) = \frac{1}{|C|} \sum_{u \in C} \hat{f}(u).$$

Demonstração. Segue das definições que

$$\begin{aligned}\sum_{u\in C}\hat{f}(u) &= \sum_{u\in C}\sum_{v\in\mathbb{F}_q^n}\lambda(u.v)f(v)\\ &= \sum_{v\in\mathbb{F}_q^n}f(v)\sum_{u\in C}\lambda(u.v)\\ &= |C|\sum_{u\in C^\perp}f(u).\end{aligned}$$

pois, pelo Lema 2.29 temos que

$$\sum_{u\in C}\lambda(uv)=\begin{cases}0 & se \quad v\notin C^\perp,\\ |C| & se \quad v\in C^\perp.\end{cases}$$

□

Definição 2.31 *Seja A_i o número de palavras código $c \in C$ com peso i ($0 \leqslant i \leqslant n$). Então o polinômio*

$$A(x,y)=\sum_{i=0}^{n}A_i x^i y^{n-i}.$$

em "x"e "y"sobre o corpo dos números complexos é chamado de ***polinômio enumerador de peso*** *de C.*

Definição 2.32 *Seja λ um caractere aditivo não trivial de $\mathbb{F}_q$ e seja $u.v$ o produto interno de $u, v \in \mathbb{F}_q^n$. Definimos para cada $v \in \mathbb{F}_q^n$ fixo a função $\lambda_v : \mathbb{F}_q^n \longrightarrow \mathbb{C}$ por*

$$\lambda_v(u)=\lambda(v.u),\ \forall u\in\mathbb{F}_q^n.$$

Se V é um espaço vetorial sobre $\mathbb{C}$ e f é uma função de $\mathbb{F}_q^n$ em V, então definimos a função $g_f : \mathbb{F}_q^n \longrightarrow V$ por,

$$g_f(u)=\sum_{v\in\mathbb{F}_q^n}\lambda_v(u)f(v)\ para\ u\in\mathbb{F}_q^n. \tag{2.2}$$

Lema 2.33 *Seja E um subespaço de $\mathbb{F}_q^n$, $E^\perp$ seu dual, $f : \mathbb{F}_q^n \longrightarrow V$ uma função no espaço vetorial V sobre $\mathbb{C}$ e λ um caractere aditivo não trivial de $\mathbb{F}_q$. Então,*

$$\sum_{u\in E}g_f(u)=|E|\sum_{v\in E^\perp}f(v). \tag{2.3}$$

Demonstração.

$$\sum_{u\in E}g_f(u) = \sum_{u\in E}\sum_{v\in\mathbb{F}_q^n}\lambda_v(u)f(v)$$

$$\begin{aligned} &= \sum_{v\in\mathbb{F}_q^n}\sum_{u\in E}\lambda(v.u)f(v) \\ &= |E|\sum_{v\in E^\perp} f(v) + \sum_{v\notin E^\perp}\sum_{\alpha\in\mathbb{F}_q}\sum_{u\in E; u.v=\alpha}\lambda(\alpha)f(v). \end{aligned}$$

Para $v \notin E^\perp$ fixo, $u \in E \longmapsto v.u$ é um funcional linear não trivial em E donde é sobrejetor e existem $\frac{|E|}{q}$ elementos na pré-imagem de cada c de $\mathbb{F}_q$, então,

$$\begin{aligned} \sum_{u\in E} g_f(u) &= |E|\sum_{v\in E^\perp} f(v) + \frac{|E|}{q}\sum_{v\notin E^\perp} f(v)\sum_{\alpha\in\mathbb{F}_q}\lambda(\alpha) \\ &= |E|\sum_{v\in E^\perp} f(v). \end{aligned}$$

Onde, na ultima igualdade foi utilizado o Teorema 2.27. □

Teorema 2.34 *(Identidade de MacWilliams). Seja C um $[n,k]$-código linear sobre $\mathbb{F}_q$ e $C^\perp$ seu código dual. Se $A(x,y)$ é o polinômio enumerador de peso de C e $A^\perp(x,y)$ é o polinômio enumerador de peso de $C^\perp$, então*

$$A^\perp(x,y) = q^{-k}A(y-x, y+(q-1)x) \tag{2.4}$$

Demonstração. Seja $f : \mathbb{F}_q^n \longrightarrow \mathbb{C}[x,y]$ dada por, $f(v) = x^{w(v)}y^{n-w(v)}$. Então o polinômio enumerador de peso de $C^\perp$ é

$$A^\perp(x,y) = \sum_{v\in C^\perp} f(v)$$

Seja g_f como em (2.2) e para cada $a \in \mathbb{F}_q$ defina,

$$|a| = \begin{cases} 1 & se \quad a \neq 0 \\ 0 & se \quad a = 0 \end{cases}. \tag{2.5}$$

Para $u = (u_1, u_2, \ldots, u_n) \in \mathbb{F}_q^n$ temos,

$$\begin{aligned} g_f(u) &= \sum_{v\in\mathbb{F}_q^n}\lambda(v.u)x^{w(v)}y^{n-w(v)} \\ &= \sum_{v_1,\ldots,v_n\in\mathbb{F}_q}\lambda(v_1u_1+\cdots+v_nu_n)x^{|v_1|+\cdots+|v_n|}y^{(1-|v_1|)+\cdots+(1-|v_n|)} \\ &= \sum_{v_1,\ldots,v_n\in\mathbb{F}_q}\left[\prod_{i=1}^{n}\lambda(v_iu_i)x^{|v_i|}y^{(1-|v_i|)}\right] \\ &= \prod_{i=1}^{n}\left[\sum_{v\in\mathbb{F}_q}\lambda(vu_i)x^{|v|}y^{(1-|v|)}\right] \end{aligned}$$

para $u_i = 0$ temos $\lambda(u_i v) = \lambda(0) = 1$, então o fator correspondente no produto é $(q-1)x + y$. Para $u_i \neq 0$ o fator correspondente é,

$$y + x \sum_{v \in \mathbb{F}_q^*} \lambda(v) = y - x.$$

Além disso,

$$g_f(u) = (y-x)^{w(u)}(y + (q-1)x)^{n-w(u)}.$$

Do Lema 2.33 implica que

$$|C|\, A^{\perp}(x,y) = |C| \sum_{v \in C^{\perp}} f(v) = \sum_{u \in C} g_f(u) = A(y-x, y+(q-1)x).$$

Finalmente, $|C| = q^k$ por hipótese, concluindo a prova. □

Corolário 2.35 *Sejam $x = z$ e $y = 1$ em $A(x,y)$ e $A^{\perp}(x,y)$ e denote os polinômios enumeradores por $A(z)$ e $A^{\perp}(z)$, respectivamente. A identidade de Macwilliams pode ser escrita da forma*

$$A^{\perp}(z) = q^{-k}(1 + (q-1)z)^n A\left(\frac{1-z}{1+(q-1)z}\right) \tag{2.6}$$

Demonstração. Temos que o polinômio enumerador $A(x,y)$ aplicado em $x = z$ e $y = 1$ vale, $A(z) = A(z,1) = \sum_{i=0}^{n} A_i z^i$ e $A^{\perp}(z) = A^{\perp}(z,1) = q^{-k}A(1-z, 1+(q-1)z)$. Mas

$$\begin{aligned} A(1-z, 1+(q-1)z) &= \sum_{i=0}^{n} A_i (1-z)^i (1+(q-1)z)^{n-i} \\ &= \sum_{i=0}^{n} A_i \left[\frac{(1-z)}{1+(q-1)z}\right]^i (1+(q-1)z)^n \\ &= [1+(q-1)z]^n \sum_{i=0}^{n} A_i \left[\frac{1-z}{1+(q-1)z}\right]^i \\ &= [1+(q-1)]^n\, A\left(\frac{1-z}{1+(q-1)z}, 1\right). \end{aligned}$$

Provando que,

$$A^{\perp}(z) = q^{-k}(1+(q-1)z)^n A\left(\frac{1-z}{1+(q-1)z}\right).$$

□

2.5 Códigos Cíclicos

Vimos que os códigos lineares podem ter suas palavras código descritas utilizando apenas algumas ferramentas importantes como a matriz geradora e a matriz de paridade. Códigos

cíclicos são uma subclasse dos códigos lineares a qual veremos que requerem menos informação para se poder descrever todas as palavras de código.

Definição 2.36 *Um $[n, k]$-código linear C sobre $\mathbb{F}_q$ é chamado cíclico se sempre que a palavra código $(a_0, a_1, \ldots, a_{n-1}) \in C$ tivermos $(a_{n-1}, a_0, \ldots, a_{n-2}) \in C$.*

Note que um código linear C será um código cíclico se, para a permutação π de $\{0, 1, \ldots, n-1\}$ definida por

$$\pi(i) = \begin{cases} i-1 & i \geqslant 1 \\ n-1 & i = 0 \end{cases} \tag{2.7}$$

e para $T_\pi : \mathbb{F}_q^n \mapsto \mathbb{F}_q^n$ definida por

$$T_\pi(c_0, \ldots, c_{n-1}) = (c_{n-1}, c_0, c_1, \ldots, c_{n-2})$$

tivermos

$$T_\pi(c) \in C \; \forall c \in C, \; ou \; seja, \; T_\pi(C) \subseteq C.$$

Definição 2.37 *Defina $\mathbf{R}_n$ como sendo o anel das classes em $\mathbb{F}_q[x]$ módulo $x^n - 1$. Isto é,*

$$\mathbf{R}_n = \mathbb{F}_q[x]_{(x^n-1)} = \mathbb{F}_q[x]/(x^n - 1).$$

Um elemento de $\mathbf{R}_n$ é, portanto, um conjunto da forma

$$[f(x)] = \{f(x) + g(x)(x^n - 1); \quad g(x) \in \mathbb{F}_q[x]\}.$$

Este anel é um espaço vetorial com as seguintes operações:
adição: $[f_1(x)] + [f_2(x)] = [f_1(x) + f_2(x)]$;
multiplicação por escalar: Para todo $\lambda \in \mathbb{F}_q, \; \lambda[f(x)] = [\lambda f(x)]$.

Este espaço vetorial possui $\{1, [x], \ldots, [x^{n-1}]\}$ como base e além disso é isomorfo à $\mathbb{F}_q^n$ com isomorfismo dado por

$$\begin{aligned} \varphi : \mathbb{F}_q^n &\longrightarrow \mathbf{R}_n \\ (a_0, \ldots, a_{n-1}) &\longmapsto [a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}]. \end{aligned}$$

Definição 2.38 *Um subconjunto $I \neq \emptyset$ de um anel $(\mathbf{R}, +, *)$ é um ideal de $\mathbf{R}$ se forem válidas,*

i) Para todo $a, b \in I$ temos que $a + b \in I$;

ii) Para todo $a \in I$ e para todo $c \in \mathbf{R}$ temos que $c * a \in I$.

Sendo $\mathbf{R}$ um anel qualquer, escreveremos $I(r)$ para o ideal de $\mathbf{R}$ gerado por um elemento qualquer $r \in \mathbf{R}$.

Proposição 2.39 *Um ideal de $\mathbb{F}_q[x]$ é da forma $I(f(x))$ onde $f(x) \in \mathbb{F}_q[x]$.*

Demonstração. Seja I um ideal de $\mathbb{F}_q[x]$. Se $I = \{0\}$ tome $f(x) = 0$ e temos $I = (f(x))$. Suponha agora que $I \neq 0$. Seja $f(x) \neq 0$ em I tal que, $f(x)$ seja de menor grau possível. Vamos provar que $I = (f(x))$. De fato, como $f(x) \in I$ temos $I(f(x)) \subseteq I$. Seja agora $g(x) \in I$, pelo algoritmo da divisão de Euclides existem $q(x), r(x)$ com $r(x) = 0$ ou $\deg(r(x)) < \deg(f(x))$ tais que,

$$g(x) = f(x)q(x) + r(x).$$

Como

$$f(x)g(x) \in I$$

segue que

$$r(x) = g(x) - f(x)g(x) \in I.$$

Se $r(x) \neq 0$ teríamos um elemento $r(x) \in I$ de grau menor que o grau de $f(x)$ o que não é possível, portanto, $r(x) = 0$ e $g(x) = f(x)q(x) \in I(f(x))$. □

Proposição 2.40 *Todo ideal de $\mathbb{F}_q[x]/p(x)$ é da forma $I([f(x)])$ onde $f(x)$ é divisor de $p(x)$.*

Demonstração. Seja I um ideal de $\mathbb{F}_q[x]/p(x)$. Considere o conjunto

$$J := \{g(x) \in \mathbb{F}_q[x];\ [g(x)] \in I\}.$$

Vamos provar que J é um ideal de $\mathbb{F}_q[x]$. De fato, se $g_1(x), g_2(x) \in J$, então $[g_1(x)], [g_2(x)]$ estão em I e, portanto,

$$[g_1(x) + g_2(x)] = [g_1(x)] + [g_2(x)] \in I$$

e consequentemente $g_1(x) + g_2(x) \in J$. Por outro lado, se $g(x) \in J$ e $h(x) \in \mathbb{F}_q[x]$, temos que $[g(x)] \in I$, e portanto,

$$[g(x)h(x)] = [g(x)][h(x)] \in I$$

logo, $g(x)h(x) \in J$. Sendo $J \neq \{0\}$, pois $p(x) \in J$ temos que existe $f(x) \in \mathbb{F}_q[x] - \{0\}$ tal que $J = I(f(x))$. Segue que $p(x)$ é múltiplo de $f(x)$, ou seja, $f(x)$ é divisor de $p(x)$. Note que,

$$I = \{[g(x)] : g(x) \in J\}$$

e como $J = I(f(x))$

$$I := \{[h(x)][f(x)]; [h(x)] \in \mathbb{F}_q[x]/p(x)\} = I([f(x)]).$$

□

Note que a ação de T_π em $\mathbb{F}_q^n$ traduz-se, por meio de φ na multiplicação por $[x]$ em $\mathbf{R}_n$. Com efeito, tomando-se $c = (c_0, \ldots, c_{n-1}) \in C$ temos $T_\pi(c) = (c_{n-1}, \ldots, c_{n-2})$ e assim,

$$\begin{aligned} \varphi(T_\pi(c)) &= \left[c_{n-1} + c_0 x + \cdots + c_{n-2}x^{n-2}\right] \\ &= [x]\left[c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}\right] \\ &= [x]\,\varphi(c). \end{aligned}$$

Lema 2.41 *Seja V um subespaço vetorial de $\mathbf{R}_n$. Então, V é um ideal de $\mathbf{R}_n$ se, e somente se, V é fechado pela multiplicação por $[x]$.*

Demonstração. Suponha que V é um ideal em $\mathbf{R}_n$. Da definição, segue que $[x][f(x)] \in V$ para todo $[f(x)] \in V$.

Reciprocamente, suponha que V seja fechado pela multiplicação por $[x]$. É suficiente mostrar que $[g(x)][f(x)] \in V\ \forall [g(x)] \in \mathbf{R}_n$ pois é claro que $a[f(x)] \in V\ \forall a \in \mathbb{F}_q$. Como, por hipótese

$$[xf(x)] = [x][f(x)] \in V$$

então,

$$[x^2 f(x)] = [x][xf(x)] \in V.$$

Por indução em m obtemos

$$[x^m f(x)] = [x^m][f(x)] \in V.$$

Agora se

$$[g(x)] = [a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}]$$

temos que,

$$[g(x)][f(x)] = a_0[f(x)] + a_1[x][f(x)] + \cdots + a_{n-1}[x^{n-1}][f(x)] \in V.$$

□

O Lema 2.41 e os argumentos do parágrafo anterior nos dão a demonstração de uma caracterização importante dos códigos cíclicos a qual é descrita pelo seguinte teorema.

Teorema 2.42 *Um código linear C é cíclico se, e somente se, $\varphi(C)$ é um ideal de $\mathbb{F}_q[x]/(x^n - 1)$.*

Definição 2.43 *Seja C um código cíclico onde $\varphi(C) = I([g(x)])$ então $g(x)$ é chamado de polinômio gerador de C e $h(x) = \frac{x^n-1}{g(x)}$ é chamado de polinômio de paridade de C.*

Teorema 2.44 *Seja $I = I([g(x)])$, onde $g(x)$ é um divisor de $x^n - 1$ de grau "s". Temos que $\{[g(x)], [xg(x)], \ldots, [x^{n-s-1}g(x)]\}$ é uma base de I como espaço vetorial sobre $\mathbb{F}_q$.*

Demonstração. O conjunto é linearmente independente.

De fato, se

$$a_0[g(x)] + a_1[xg(x)] + \cdots + a_{n-s-1}[x^{n-s-1}g(x)] = [0]$$

então

$$[g(x)][a_0 + a_1x + \cdots + a_{n-s-1}x^{n-s-1}] = [0]$$

e, portanto, para algum $d(x) \in \mathbb{F}_q[x]$ temos,

$$g(x)(a_0 + a_1x + \cdots + a_{n-s-1}x^{n-s-1}) = d(x)(x^n - 1).$$

Daí, segue que

$$a_0 + a_1x + \cdots + a_{n-s-1}x^{n-s-1} = d(x)h(x).$$

Como o grau de $h(x)$ é $(n - s)$, devemos ter $a_0 + a_1x + \cdots + a_{n-s-1}x^{n-s-1} = 0$ e consequentemente $a_0 = a_1 = \cdots = a_{n-s-1}$.

Os elementos $[g(x)], [xg(x)], \ldots, [x^{n-s-1}g(x)]$ geram I.

De fato, se $[f(x)] \in I$, temos que

$$f(x) \equiv g(x)d(x)\ mod(x^n - 1).$$

Pelo algoritmo da divisão de Euclides, temos que, $d(x) = c(x)h(x) + r(x)$ com,

$$r(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{n-s-1}x^{n-s-1}$$

logo,

$$f(x) \equiv d(x)g(x) \equiv c(x)h(x)g(x) + r(x)g(x)\ mod(x^n - 1)$$

e, portanto,

$$f(x) \equiv c(x)(x^n - 1) + r(x)g(x) \equiv r(x)g(x)\ mod(x^n - 1).$$

Consequentemente,

$$[f(x)] = a_0[g(x)] + a_1[xg(x)] + \cdots + a_{n-s-1}[x^{n-s-1}g(x)].$$

□

Corolário 2.45 *Dado um código cíclico C, existe $v \in C$ tal que $C = \langle v \rangle$.*

Demonstração. Seja $I = \varphi(C)$. Logo, I é gerado como $\mathbb{F}_q$-espaço vetorial pelas classes $[g(x)]$, $[xg(x)]$,..., $[x^{n-s-1}g(x)]$, onde $g(x)$ é um divisor de $x^n - 1$ que possui grau s. Portanto, escolhendo

$$v = \varphi^{-1}([g(x)])$$

temos que C é gerado por

$$v, T_\pi(v), \ldots, T_\pi^{n-s-1}(v)$$

e portanto, $C = \langle v \rangle$. □

Corolário 2.46 *Seja $g(x) = g_0 + g_1x + \ldots + g_sx^s$ um divisor de $x^n - 1$ de grau "s". Se $I = I([g(x)])$ então,*

$$dim_{\mathbb{F}_q} I = n - s,$$

e o código $C = \varphi^{-1}(I)$ tem matriz geradora,

$$\begin{bmatrix} \varphi^{-1}([g(x)]) \\ \varphi^{-1}([xg(x)]) \\ \varphi^{-1}([x^2g(x)]) \\ \vdots \\ \varphi^{-1}([x^{n-s-1}g(x)]) \end{bmatrix} = \begin{bmatrix} g_0 & g_1 & \ldots & g_s & 0 & 0 & \ldots & 0 \\ 0 & g_0 & g_1 & \ldots & g_s & 0 & \ldots & 0 \\ 0 & 0 & g_0 & g_1 & \ldots & g_s & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ldots & \vdots & \ldots & \vdots \\ 0 & 0 & 0 & \ldots & g_0 & g_1 & \ldots & g_s \end{bmatrix}.$$

Exemplo 2.47 *Em $\mathbb{F}_2^7[x]$ consideremos, $x^7 - 1 = (x+1)(x^3+x+1)(x^3+x^2+1)$. Então $g(x) = x^3 + x^2 + 1$ gera um $[7,4]$-código cíclico com polinômio de paridade dado por $h(x) = \frac{x^7-1}{g(x)} = x^4 + x^3 + x^2 + 1$. A matriz geradora e a matriz de paridade deste código são dadas respectivamente por,*

$$G = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} \quad H = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 \end{bmatrix}.$$

2.6 Códigos Cíclicos Definidos por Anulamento

Seja $\mathbb{F}_q$ corpo finito, n inteiro tal que $mdc(q,n) = 1$, e seja C um código cíclico com polinômio gerador $g(x)$. Seja $\mathbb{F}_p$ uma extensão de $\mathbb{F}_q$ na qual $x^n - 1$ se decompõe em fatores lineares mônicos distintos e sejam $\alpha_1, \ldots, \alpha_r$ as raízes de $g(x)$ em $\mathbb{F}_p$ que são, portanto, duas a duas distintas.

Proposição 2.48 *Nas condições acima, temos:*

$$\varphi(C) = I([g(x)]) = \{[f(x)] \in \mathbf{R}_n : f(\alpha_1) = \cdots = f(\alpha_r) = 0\}.$$

Demonstração. Como $[f(x)] \in I([g(x)])$ se, e somente se, existe $h(x) \in \mathbb{F}_q[x]$ satisfazendo $[f(x)] = [g(x)][h(x)]$, isto equivale a dizer que existe $d(x) \in \mathbb{F}_q[x]$ tal que $f(x) = d(x)g(x)$, o que por sua vez equivale a condição $f(\alpha_i) = 0,\ \forall i = 1, \ldots, r$. □

Para um polinômio dado

$$f(x) = \sum_{j=0}^{n-1} a_j x^j \in \mathbb{F}_q[x],$$

temos que $[f(x)]$ é elemento de $I([g(x)])$ se, e somente se,

$$f(\alpha_i) = \sum_{j=0}^{n-1} a_j \alpha_i^j = 0,\ \forall i = 1, 2, \ldots, r.$$

Pode-se, então, descrever o código cíclico C definido pelo polinômio $g(x)$ como sendo o conjunto dos elementos $a = (a_0, a_1, \ldots, a_{n-1}) \in \mathbb{F}_q^n$ tais que,

$$a_0 + a_1\alpha_i + a_2\alpha_i^2 + \cdots + a_{n-1}\alpha_i^{n-1} = 0 \; para \; i = 1, \ldots, r.$$

Ou seja é o conjunto dos elementos $a = (a_0, a_1, \ldots, a_{n-1}) \in \mathbb{F}_q^n$ tais que

$$\mathcal{H}a^T = 0,$$

onde $\mathcal{H}$ é a seguinte matriz com entradas em $\mathbb{F}_p$:

$$\mathcal{H} = \begin{bmatrix} \alpha_1^0 & \alpha_1^1 & \ldots & \alpha_1^{n-1} \\ \alpha_2^0 & \alpha_2^1 & \ldots & \alpha_2^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_r^0 & \alpha_r^1 & \ldots & \alpha_r^{n-1} \end{bmatrix}.$$

Este fato pode ser resumido como o seguinte teorema

Teorema 2.49 *Seja $C \subseteq \mathbb{F}_q[x]/(x^n - 1)$ um código cíclico gerado pelo polinômio $g(x)$ e sejam $\alpha_1, \ldots, \alpha_{n-k}$ suas raízes em uma extensão $\mathbb{F}_r$ de $\mathbb{F}_q$. Então $f \in \mathbb{F}_q[x]/(x^n - 1)$ é um polinômio código se, e somente se, o vetor $(f_0, \ldots, f_{n-1})$ dos coeficientes de f está no núcleo da matriz*

$$\mathcal{H} = \begin{bmatrix} 1 & \alpha_1^1 & \ldots & \alpha_1^{n-1} \\ 1 & \alpha_2^1 & \ldots & \alpha_2^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_{n-k}^1 & \ldots & \alpha_{n-k}^{n-1} \end{bmatrix}.$$

Por exemplo, seja α uma raiz primitiva da unidade em $\mathbb{F}_{q^m}$ e seja $g(x)$ o polinômio minimal de α sobre $\mathbb{F}_q$ então, o código cíclico gerado por $g(x)$ possui a matriz $\mathcal{H}$ dada por

$$\mathcal{H} = \begin{bmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{n-1} \end{bmatrix}.$$

No próximo resultado, veremos que, construindo códigos cíclicos com um conjunto de raízes n-ésimas da unidade, temos uma cota inferior para a sua distância mínima. Escreveremos $m_{\gamma^r}(x)$ para representar o polinômio minimal de γ^r.

Teorema 2.50 *(Bose-Chaudhuri-Hocquenghem). Seja $\mathbb{F}_q$ um corpo e n um inteiro maior que 1 co-primo com q. Seja $\mathbb{F}_{q^m}$ um corpo onde $x^n - 1$ se decompõe em fatores lineares, e seja $\gamma \in \mathbb{F}_{q^m}$ uma raiz n-ésima primitiva da unidade. Seja C o código cíclico com polinômio gerador*

$$g(x) = mmc\left\{m_{\gamma^a}(x), \dots, m_{\gamma^{a+\delta-2}}(x)\right\},$$

com $a \geqslant 0$ e $\delta \leqslant n$. Então, a distância mínima de C é maior ou igual a δ e a sua dimensão é maior ou igual a $n - m(\delta - 1)$.

Demonstração. Suponhamos que as raízes de $g(x)$ sejam

$$\left\{\gamma^a, \gamma^{a+1}, \dots, \gamma^{a+\delta-2}\right\} \cup \left\{\beta_1, \dots, \beta_s\right\},$$

logo, a matriz $\mathcal{H}$ associada ao código cíclico é da forma

$$\mathcal{H} = \begin{bmatrix} \gamma^0 & \gamma^a & \gamma^{2a} & \dots & \gamma^{(n-1)a} \\ \gamma^0 & \gamma^{a+1} & \gamma^{2(a+1)} & \dots & \gamma^{(n-1)(a+1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \gamma^0 & \gamma^{a+\delta-2} & \gamma^{2(a+\delta-2)} & \dots & \gamma^{(n-1)(a+\delta-2)} \\ \beta_1^0 & \beta_1 & \beta_1^2 & \dots & \beta_1^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \beta_s^0 & \beta_s & \beta_s^2 & \dots & \beta_s^{n-1} \end{bmatrix}.$$

Queremos mostrar que quaisquer $\delta - 1$ colunas de $\mathcal{H}$ são linearmente independentes sobre $\mathbb{F}_q$. De fato, considere as $\delta - 1$ colunas de $\mathcal{H}$ iniciadas com $\gamma^{i_1 a}, \dots, \gamma^{i_{\delta-1} a}$, de maneira que $0 \leqslant i_1 < i_2 < \cdots \leqslant n-1$. Estas formam uma matriz que possui o seguinte bloco principal

$$\mathcal{B} = \begin{bmatrix} \gamma^{i_1 a} & \gamma^{i_2 a} & \gamma^{i_3 a} & \dots & \gamma^{i_{\delta-1} a} \\ \gamma^{i_1 (a+1)} & \gamma^{i_2 (a+1)} & \gamma^{i_3 (a+1)} & \dots & \gamma^{i_{\delta-1} (a+1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \gamma^{i_1 (a+\delta-2)} & \gamma^{i_2 (a+\delta-2)} & \gamma^{i_3 (a+\delta-2)} & \dots & \gamma^{i_{\delta-1} (a+\delta-2)} \end{bmatrix}.$$

Como

$$\det \mathcal{B} = \gamma^{a(i_1+\ldots+i_{\delta-1})} \det \begin{bmatrix} 1 & 1 & 1 & \ldots & 1 \\ \gamma^{i_1} & \gamma^{i_2} & \gamma^{i_3} & \ldots & \gamma^{i_{\delta-1}} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \gamma^{i_1(\delta-2)} & \gamma^{i_2(\delta-2)} & \gamma^{i_3(\delta-2)} & \ldots & \gamma^{i_{\delta-1}(\delta-2)} \end{bmatrix}$$

temos que $\det \mathcal{B} \neq 0$, pois o último determinante acima é de Vandermonde, com $\gamma^{i_j} \neq \gamma^{i_l}$ se $j \neq l$, por ser γ uma raiz n-ésima da unidade. Portanto, quaisquer $\delta - 1$ colunas de $\mathcal{H}$ são linearmente independente sobre $\mathbb{F}_q$, e o que, pelo Lema 2.11, permite concluir que a distância minima do código é pelo menos δ.

O código C identifica-se com o ideal formado pelas classes $[f(x)]$ de polinômios em $\mathbf{R}_n$ tais que

$$f(\gamma^a) = f(\gamma^{a+1}) = \cdots = f(\gamma^{a+\delta-2}) = 0,$$

não precisando de nos preocuparmos em exigir que $f(\beta_i) = 0$ para $i = 1, \ldots, s$, pois estas equações são automaticamente satisfeitas. Portanto, os elementos de C são vetores c tais que $Hc^T = 0$, onde

$$H = \begin{bmatrix} \gamma^0 & \gamma^a & \gamma^{2a} & \ldots & \gamma^{(n-1)a} \\ \gamma^0 & \gamma^{a+1} & \gamma^{2(a+1)} & \ldots & \gamma^{(n-1)(a+1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \gamma^0 & \gamma^{a+\delta-2} & \gamma^{2(a+\delta-2)} & \ldots & \gamma^{(n-1)(a+\delta-2)} \end{bmatrix}$$

Escrevendo os elementos de $\mathbb{F}_{q^m}$ como vetores colunas de comprimento m com elementos em $\mathbb{F}_q$, obtemos uma matriz H', de ordem $m(\delta-1) \times n$, com coeficientes em $\mathbb{F}_q$, tal que $H'c^T = 0$. Portanto, a dimensão do espaço gerado pelas colunas de H' é maior ou igual a $m(\delta - 1)$ e consequentemente, $\dim C \geqslant n - m(\delta - 1)$. □

Os códigos cíclicos definidos como no Teorema 2.50 são chamados de *códigos BCH*. O número δ do teorema é chamado de *peso estimado* do código *BCH*.

Sejam $\mathbb{F}_p$ um corpo e $\mathbb{F}_q$ um extensão com uma raiz n-ésima primitiva da unidade $\gamma \in \mathbb{F}_p$. Defina

$$C_{\mathbb{F}_q}(n, \delta) = \left\{ (a_0, \ldots, a_{n-1}) \in \mathbb{F}_q^n; \sum_{i=0}^{n-1} a_i \gamma^{ij} = 0,\ j = 1, \ldots, \delta - 1 \right\}.$$

Ou seja, o código *BCH* definido pelo polinômio gerador

$$g(x) = mmc \left\{ m_{\gamma^a}(x), \ldots, m_{\gamma^{a+\delta-2}}(x) \right\}.$$

O fato de $\delta \leqslant \delta'$ implica em $C_{\mathbb{F}_q}(n, \delta') \subseteq C_{\mathbb{F}_q}(n, \delta)$. Temos que os códigos *BCH* são encaixados uns nos outros.

Teorema 2.51 *Temos que,* $(a_0, \ldots, a_{n-1}) \in C_{\mathbb{F}_q}(n, \delta)$ *se, e somente se,*

$$\sum_{j=0}^{n-1} a_j \gamma^{j(\delta-1)} \frac{x^{\delta-1} - \gamma^{-j(\delta-1)}}{x - \gamma^{-j}} = 0.$$

Demonstração. Por definição, segue que $(a_0, a_1, \ldots, a_{n-1}) \in C_{\mathbb{F}_q}(n, \delta)$ se, e somente se,

$$\sum_{i=1}^{\delta-1} \left(\sum_{j=0}^{n-1} a_j \gamma^{ij} \right) x^i = 0.$$

Reescrevendo a identidade acima, obtemos

$$\begin{aligned} 0 &= \sum_{i=1}^{\delta-1} \left(\sum_{j=0}^{n-1} a_j \gamma^{ij} \right) x^i \\ &= \sum_{j=0}^{n-1} a_j \gamma^{j(\delta-1)} \sum_{i=0}^{\delta-2} \gamma^{-j(\delta-2-i)} x^i \\ &= \sum_{j=0}^{n-1} a_j \gamma^{j(\delta-1)} \frac{x^{\delta-1} - \gamma^{-j(\delta-1)}}{x - \gamma^{-j}}. \end{aligned}$$

□

Uma subclasse especial de códigos *BCH* são os códigos *Reed-Solomon* o quais estão definidos abaixo.

Definição 2.52 *(Reed-Solomon). Um código Reed-Solomon é um código cíclico BCH de comprimento* $n = q - 1$*, com polinômio gerador*

$$g(x) = (x - \alpha^{a+1})(x - \alpha^{a+2}) \ldots (x - \alpha^{a+\delta-1}),$$

com $a \geqslant 0$ *e* $2 \leqslant \delta \leqslant q - 1$*, onde* α *é um elemento primitivo de* $\mathbb{F}_q$*.*

Da definição de código de Reed-Solomon temos de imediato que

i) Se α é um elemento primitivo de $\mathbb{F}_q$, então o polinômio $x^{q-1} - 1 \in \mathbb{F}_q$ tem a seguinte fatoração:

$$x^{q-1} - 1 = (x - 1)(x - \alpha)(x - \alpha^2) \ldots (x - \alpha^{q-2}).$$

Portanto, $g(x)$ é divisor de $x^{q-1} - 1$ e $g(x)$ é, de fato, o polinômio gerador de um código cíclico;

ii) Como $\deg(g(x)) = \delta - 1$ então a dimensão de C é

$$dim(C) = n - (\delta - 1) = q - \delta.$$

Em particular,

$$1 \leqslant dim(C) \leqslant q - 2;$$

iii) Não existe códigos *Reed-Solomon* binários pois, $2 \leqslant \delta \leqslant q - 1$ então $q \geqslant 3$.

Proposição 2.53 *Seja C um código Reed-Solomon, com polinômio gerador*

$$g(x) = (x - \alpha^{a+1})(x - \alpha^{a+2}) \dots (x - \alpha^{a+\delta-1}).$$

Então,

$$C := \left\{ c(x) \in \mathbf{R}_{q-1} : c(\alpha^i) = 0 \textit{ para } i = a+1, \dots, a+\delta-1 \right\}.$$

Demonstração. Temos que $c(x) \in C$ se, e só se, $c(x) = a(x)g(x)$ para algum $a(x) \in \mathbb{F}_q[x]$. Portanto, as raízes de $g(x)$ são também raízes de qualquer polinômio código.

Seja agora $c(x) \in \mathbf{R}_{q-1}$ tal que, $c(\alpha^i) = 0$ para $i = a+1, \dots, a+\delta-1$. Assim $x - \alpha^i$ divide $c(x)$ (em $\mathbb{F}_q[x]$) para $i = a+1, \dots, a+\delta-1$. Como estes α^i são distintos, concluímos que $g(x)$ divide $c(x)$, logo $c(x) \in C$. □

Teorema 2.54 *Seja C um código Reed-Solomon de parâmetros $[q-1, q-\delta]$, então $d(C) \geqslant \delta$.*

Demonstração. Seja $g(x) = (x - \alpha^{a+1})(x - \alpha^{a+2}) \dots (x - \alpha^{a+\delta-1})$ o polinômio gerador de C. Suponhamos por absurdo que, $d(C) = d < \delta$ e seja $c(x) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1} \in C$ com peso $w(c(x)) = d$. Seja $c = (c_0, \dots, c_{n-1}) \in \mathbb{F}_q^n$ o vetor correspondente a $c(x)$. Temos que $c(\alpha_i) = 0$ para qualquer $i = a+1, \dots, a+\delta-1$. Por outro lado,

$$\begin{aligned} c(\alpha^i) &= c_0 + c_1\alpha^i + \ldots + c_{n-1}(\alpha^i)^{n-1} \\ &= (1, \alpha^i, (\alpha^i)^2, \dots, (\alpha^i)^{n-1}).c. \end{aligned}$$

Portanto $\mathcal{H}c = 0$ onde,

$$\mathcal{H} = \begin{bmatrix} 1 & \alpha^{(a+1)^1} & \alpha^{(a+1)^2} & \dots & \alpha^{(a+1)^{n-1}} \\ 1 & \alpha^{(a+2)^1} & \alpha^{(a+2)^2} & \dots & \alpha^{(a+2)^{n-1}} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{(a+\delta-1)^1} & \alpha^{(a+\delta-1)^2} & \dots & \alpha^{(a+\delta-1)^{n-1}} \end{bmatrix}$$

é uma matriz com $\delta - 1$ linhas e n colunas. Sejam $i_1, i_2, \ldots, i_d$ os índices tais que $c_i \neq 0$. Seja $\mathcal{H}'$ a matriz formada pelas colunas $i_1 + 1, i_2 + 1, \ldots, i_d + 1$ de $\mathcal{H}$, então $\mathcal{H}'$ tem $\delta - 1$ linhas e d colunas. A matriz $\mathcal{H}''$ formada pelas d primeiras linhas de $\mathcal{H}'$ é uma matriz quadrada $d \times d$ e

$$\mathcal{H}'' \begin{bmatrix} c_{i_1} \\ c_{i_2} \\ \vdots \\ c_{i_d} \end{bmatrix} = 0.$$

Portanto, $det(\mathcal{H}'') = 0$ pois, $(c_{i_1}, \ldots, c_{i_d})$ é uma solução não nula de um sistema linear homogêneo $\mathcal{H}''x = 0$. Por outro lado, como

$$\mathcal{H}'' = \begin{bmatrix} \alpha^{(a+1)^{i_1}} & \alpha^{(a+1)^{i_2}} & \ldots & \alpha^{(a+1)^{i_d}} \\ \alpha^{(a+2)^{i_1}} & \alpha^{(a+2)^{i_2}} & \ldots & \alpha^{(a+2)^{i_d}} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha^{(a+\delta-1)^{i_1}} & \alpha^{(a+\delta-1)^{i_2}} & \ldots & \alpha^{(a+\delta-1)^{i_d}} \end{bmatrix}$$

temos que,

$$det(\mathcal{H}'') = \prod_{j=1}^{d} \alpha^{(a+1)^{i_j}} det \begin{bmatrix} 1 & 1 & \ldots & 1 \\ \alpha^{i_1} & \alpha^{i_2} & \ldots & \alpha^{i_d} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha^{i_{d-1}} & \alpha^{i_{d-1}} & \ldots & \alpha^{i_{d-1}} \end{bmatrix}$$

o qual é não nulo (uma contradição) logo devemos ter $d \geqslant \delta$. □

Corolário 2.55 *Os códigos Reed-Solomon são códigos MDS.*

Demonstração. Seja C um código de *Reed-Solomon* de parâmetros $[q-1, q-\delta]$. O polinômio gerador $g(x)$ possui $\deg(g(x)) = q-1$ então, $d(C) \geqslant \delta$. Pelo Teorema 2.54 e pela desigualdade de Singleton temos $d(C) \leqslant \delta$ donde, $d(C) = \delta$ e assim C é MDS. □

Exemplo 2.56 *Considere o código de Reed-Solomon C sobre $\mathbb{F}_{16}$ com polinômio gerador $g(x) = \prod_{i=1}^{6}(x - \alpha^i)$ onde α é um elemento primitivo de $\mathbb{F}_{16}$. O código C tem comprimento $n = q-1 = 15$, dimensão $n - \deg(g(x)) = 9$ e o Corolário 2.55 nos dá que C possui distância mínima igual a 7. Para calcular a distância mínima de C pelo Lema 2.11, como um matriz de paridade H para C possui 6 linhas e 15 colunas teriamos que verificar que*

$$\begin{pmatrix} 15 \\ 6 \end{pmatrix} = 5005$$

conjuntos de 6 colunas de H são L.I.

Capítulo 3

Métrica de NRT em Códigos no Espaço de Matrizes e Distribuições Uniformes.

Neste capítulo trataremos de códigos definidos sobre o espaço das matrizes e definiremos uma métrica não Hamming (a ρ-métrica) além do conceito de Distribuições uniformes com intenção de encontrarmos relações destas com códigos MDS na ρ-métrica. Exibiremos uma família de códigos MDS nesta ρ-métrica. Seguiremos como referências principais [2] e [14].

3.1 ρ-métrica

Para um alfabeto finito $\mathcal{A}$, o conjunto de todas as matrizes com *n* linhas e *s* colunas com entradas em $\mathcal{A}$ será denotado por $Mat_{n,s}(\mathcal{A})$. Um código é um subconjunto de $Mat_{n,s}(\mathcal{A})$. Note que como não estamos assumindo operação binárias em $\mathcal{A}$, nosso código não é necessariamente linear.

Considere o caso em que $n = 1$ e tome $\omega, \omega' \in Mat_{1,s}(\mathcal{A})$ com, $\omega = (\alpha_1, \ldots, \alpha_s)$ e $\omega' = (\beta_1, \ldots, \beta_s)$. Definiremos a ρ-métrica, chamada também de **métrica de Niederreiter-Rosenbloom-Tsfasman** ou de **métrica NRT**, entre ω e ω' por,

$$\rho(\omega, \omega') = max\left\{i : \alpha_i \neq \beta_i\right\} \quad e \quad \rho(\omega, \omega') = 0 \quad se \quad \omega = \omega' \tag{3.1}$$

Estenderemos a ρ-métrica para $\Omega, \Omega' \in Mat_{n,s}(\mathcal{A})$. A saber,

$$\rho(\Omega, \Omega') = \sum_{j=1}^{n} \rho(\omega_j, \omega'_j) \tag{3.2}$$

onde ω_j, ω'_j indicam as j-ésimas linhas de Ω e Ω'. Para ω, ω' e x em $Mat_{1,s}(\mathcal{A})$ vale,

$$\begin{aligned}\rho(\omega, \omega') &\leqslant max\{\rho(\omega, x), \rho(x, \omega')\} \\ &\leqslant \rho(\omega, x) + \rho(x, \omega').\end{aligned}$$

Dado um código $C \subseteq Mat_{n,s}(\mathcal{A})$ pode-se então considerar a *ρ-distância mínima do código C* que será dada por,

$$\rho(C) = \min\{\rho(\Omega, \Omega') : \Omega, \Omega' \in C, \Omega \neq \Omega'\}. \tag{3.3}$$

Agora, dado um código $C \subseteq Mat_{n,s}(\mathcal{A})$ e $\Omega' \in C$ uma matriz fixa. O *raio enumerador de peso do código C relativo a Ω'* é o conjunto formado pelos *ns* inteiros não negativos $w_r(\Omega')$ onde

$$w_r(\Omega') := w_r(C; \Omega') = |\{\Omega \in C : \rho(\Omega, \Omega') = r\}|$$

Teorema 3.1 *Seja $\mathcal{A}$ um alfabeto finito com q elementos e seja $C \subseteq Mat_{n,s}(\mathcal{A})$ um código arbitrário. Então*

$$|C| \leqslant q^{ns-\rho(C)+1}.$$

Demonstração. A prova detalhada deste fato pode ser encontrada em [10]. A saber, fazendo todas as $\rho(C) - 1$ primeiras entradas (a partir das colunas) das matrizes de C iguais, temos um novo código C' em $Mat_{n,s}(\mathcal{A})$. Além disso $|C'| = |C|$ pois duas matrizes quaisquer de C não coincidem nas outras posições pois, de outro modo, a distância entre elas seria inferior a $\rho(C)$. Assim $|C| = |C'| \leqslant q^{ns-\rho(C)+1}$. □

Corolário 3.2 *Seja $C \subseteq Mat_{n,s}(\mathcal{A})$ onde $|\mathcal{A}| = q$, um código qualquer com q^k elementos, $0 \leqslant k \leqslant ns$. Então,*

$$\rho(C) \leqslant ns - k + 1.$$

Naturalmente diremos que um código $C \subseteq Mat_{n,s}(\mathcal{A})$ é MDS em relação a ρ-métrica se $\rho(C) = ns - k + 1$.

3.2 Códigos Uniformemente Distribuídos

Ao longo desta seção, $C \subseteq Mat_{n,s}(\mathcal{A})$ indicará um código com q^k elementos. Para um $A = (a_1, \ldots, a_n)$, com $0 \leqslant a_j \leqslant s$, chamaremos o conjunto

$$V_A(\Omega) = \{\Omega' \in Mat_{n,s}(\mathcal{A}) : \rho(\omega_i, \omega'_i) \leqslant a_i, A = (a_1, \ldots, a_n)\}$$

de *Caixa Elementar Centrada em* $\Omega \in Mat_{n,s}(\mathcal{A})$ e ao número

$$Vol(V_A(\Omega)) = \frac{|V_A(\Omega)|}{|Mat_{n,s}(\mathcal{A})|} = \frac{q^{a_1+\cdots+a_n}}{q^{ns}} = q^{a_1+\cdots+a_n-ns}$$

de *Volume da Caixa Elementar Centrada em* $\Omega \in Mat_{n,s}(\mathcal{A})$. Seja F_k a família de caixas elementares com volume q^{-k}. Dizemos que um código C com q^k elementos é **Uniformemente distribuído (UD)** se cada caixa elementar de F_k intercepta o código C em exatamente um ponto.

Teorema 3.3 *Duas matrizes* $\Omega, \Omega' \in Mat_{n,s}(\mathcal{A})$ *pertencem simultaneamente a uma caixa elementar da família* F_k *se, e somente se,* $\rho(\Omega, \Omega') \leqslant ns - k$.

Demonstração. Suponha que $\rho(\Omega, \Omega') \leqslant ns - k$; escolha $V_A(\Omega)$ com $a_i = \rho(\omega_i, \omega_i')$ e teremos que $\Omega' \in V_A(\Omega)$ devido a definição de $V_A(\Omega)$ e a escolha dos a_i's pois $\rho(\Omega, \Omega') = \sum a_i \leqslant ns - k$, e segue que $Vol(V_A(\Omega)) = q^{\sum a_i - ns} \leqslant q^{-k}$ onde as somas são feitas para $i = 1, \ldots n$.

Assuma agora que $\Omega, \Omega' \in V_A(X)$ onde $X \in Mat_{n,s}(\mathcal{A})$ e $A = (a_1, \ldots, a_n)$, $Vol(V_A(X)) = q^{-k}$. Como $Vol(V_A(X)) = q^{-k}$ pela definição de volume de uma caixa elementar temos que $\sum_{i=1}^{n} a_i = ns - k$. Então $\rho(\omega_i, \omega_i') \leqslant max\{\rho(\omega_i, x_i), \rho(x_i, \omega_i')\} \leqslant a_i$ ou seja, $\rho(\Omega, \Omega') \leqslant ns - k$.
□

Lema 3.4 *Sejam* $A = (a_1, \ldots, a_n)$, $B = (b_1, \ldots, b_n)$ *com* $0 \leqslant b_i \leqslant a_i \leqslant s$, $1 \leqslant i \leqslant n$, *e sejam* $\Omega, \Omega' \in Mat_{n,s}(\mathcal{A})$.

i) Duas caixas elementares, $V_A(\Omega)$ *e* $V_A(\Omega')$ *são iguais ou disjuntas.*

ii) Se $\Omega' \in V_A(\Omega)$ *então* $V_B(\Omega') \subseteq V_A(\Omega)$.

iii) $V_A(\Omega)$ *pode ser particionado como a união de caixas elementares com* B *fixo. Em particular,* $Mat_{n,s}(\mathcal{A})$ *pode ser particionado como a união de caixas elementares com* A *fixo para qualquer* $A = (a_1, \ldots, a_n), 0 \leqslant i \leqslant s$.

Demonstração.
i) Considere duas caixas elementares $V_A(\Omega)$ e $V_A(\Omega')$. Assuma que estas não são disjuntas então existe $X \in V_A(\Omega) \cap V_A(\Omega')$ daí,

$$\rho(x_i, \omega_i) \leqslant a_i \quad e \quad \rho(x_i, \omega_i') \leqslant a_i \quad i = 1, \ldots, n.$$

Como $\rho(\omega_i, \omega_i') \leqslant max\{\rho(x_i, \omega_i), \rho(x_i, \omega_i')\}$ temos que $\Omega \in V_A(\Omega')$ e $\Omega' \in V_A(\Omega)$. Agora se $Y \in V_A(\Omega)$ então $\rho(y_i, \omega_i) \leqslant a_i, \forall i$. Como $\rho(\omega_i', \omega_i) \leqslant a_i$ para todo $i = 1, \ldots, n$ pela

desigualdade $\rho(y_i, \omega_i') \leqslant max\{\rho(\omega_i, y_i), \rho(\omega_i, \omega_i')\}$ concluímos que $Y \in V_A(\Omega')$ donde as duas caixas são iguais.

ii) Seja $X \in V_B(\Omega')$ então $\rho(x_i, \omega_i') \leqslant b_i, i = 1, \ldots, n$. Mostraremos que $X \in V_A(\Omega)$. De fato, a Equação (3.1) diz que

$$\rho(x_i, \omega_i) \leqslant max\{\rho(x_i, \omega_i'), \rho(\omega_i, \omega_i'\}$$

portanto, pela definição dos a_i's e dos b_i's vale $\rho(x_i, \omega_i) \leqslant a_i$ para $i = 1, \ldots, n$, implicando que $X \in V_A(\Omega)$. Ou seja, $V_B(\Omega') \subseteq V_A(\Omega)$.

iii) Pelo item *ii)* temos,

$$V_A(\Omega) = \bigcup_{\Omega' \in V_A(\Omega)} V_B(\Omega').$$

Por *i)* podemos escrever esta união como uma união disjunta

$$V_A(\Omega) = \bigcup_{t=1}^{r} V_B(\Omega_t). \tag{3.4}$$

Como $Vol\,(V_A(\Omega)) = q^{\left(\sum_{i=1}^n a_i\right)-ns}$ e cada $V_B(\Omega_t)$ possui volume

$$Vol\,(V_B(\Omega_t)) = q^{\left(\sum_{i=1}^n b_i\right)-ns}$$

existem,

$$\begin{aligned} \frac{Vol\,(V_A(\Omega))}{Vol\,(V_B(\Omega_t))} &= \frac{q^{\left(\sum_{i=1}^n a_i\right)-ns}}{q^{\left(\sum_{i=1}^n b_i\right)-ns}} \\ &= q^{\sum_{i=1}^n a_i - \sum_{i=1}^n b_i} \end{aligned}$$

caixas nesta união. Finalmente, $Mat_{n,s}(\mathcal{A}) = V_I(\Omega)$ onde $I = (s, s, ..., s)$ e Ω é qualquer elemento de $Mat_{n,s}(\mathcal{A})$. Como $a_i \leqslant s$ para todo i , segue como caso particular da partição de V_A em V_B's. □

Exemplo 3.5 *Seja $\mathcal{A} = \{0, 1\}$ e considere o conjunto das matrizes $Mat_{2,2}(\mathcal{A})$ ou seja,*

$$\left\{ \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \right.$$

$$\left. \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \right\}.$$

Considerando $A = (1, 2)$ temos que

$$Mat_{2,2}(\mathcal{A}) = V_A(\Omega) \cup V_A(\Omega')$$

onde

$$\Omega = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \text{ e } \Omega' = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

pois, $V_A(\Omega)$ e $V_A(\Omega')$ são respectivamente os conjuntos

$$\left\{ \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \right\}$$

$$\left\{ \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \right\}$$

Teorema 3.6 *Um código $C \subseteq Mat_{n,s}(\mathcal{A})$ com q^k elementos é MDS com respeito a ρ-métrica se, e somente se, é uniformemente distribuído.*

Demonstração. Seja C um código MDS na ρ-métrica. Então pela definição $\rho(C) = ns - k + 1$, pelo Lema 3.4 $Mat_{n,s}(\mathcal{A})$ pode ser particionado em caixas elementares $V_A(\Omega)$; como todas têm q^{ns-k} pontos e $Mat_{n,s}(\mathcal{A})$ tem q^{ns} pontos, o número de caixas nesta partição é q^k. Portanto cada caixa $V_A(\Omega)$ contém exatamente um ponto de C. Então C é uniformemente distribuído.

Suponha agora que C é um código uniformemente ditribuído, então cada caixa elementar $V_A(\Omega) \in F_k$ contém exatamente um ponto de C. Portanto, pelo Teorema 3.3 para quaisquer dois pontos distintos $X, X' \in C$ temos $\rho(X, X') > ns - k$ donde $\rho(C) \geqslant ns - k + 1$. Por outro lado, $\rho(C) \leqslant ns - k + 1$ pelo Corolário 3.2 e, portanto, C é um código MDS na ρ-métrica. □

3.3 Enumerador de Peso

A partir desta seção consideraremos que o alfabeto $\mathcal{A}$ possui estrutura de corpo finito. Podemos então considerar $\rho(\Omega) = \rho(\Omega, 0)$ para uma matriz $\Omega \in Mat_{n,s}(\mathbb{F}_q)$ onde $0 \in Mat_{n,s}(\mathbb{F}_q)$ denota a matriz nula.

Vamos definir as r-bola e a r-esfera centradas em $0 \in Mat_{n,s}(\mathbb{F}_q)$ com respeito a ρ-métrica como sendo respectivamente os conjuntos,

$$B^{(n,s)}(r) := \{\Omega \in Mat_{n,s}(\mathbb{F}_q) : \rho(\Omega) \leqslant r\}. \tag{3.5}$$

$$S^{(n,s)}(r) := \{\Omega \in Mat_{n,s}(\mathbb{F}_q) : \rho(\Omega) = r\}. \tag{3.6}$$

Se, $n = 1$ tem-se que $B^{(1,s)}(r) = \{\omega = (\alpha_1, \ldots, \alpha_s) \in Mat_{1,s}(\mathbb{F}_q) : \alpha_i = 0,\ \forall i > r\}$ que é um subespaço vetorial de dimensão r. Além disso, para $r = 0$ vale

$$S^{(1,s)}(0) = B^{(1,s)}(0)$$

e para $r \geqslant 1$ temos $S^{(1,s)}(r) = B^{(1,s)}(r) - B^{(1,s)}(r-1)$. Ainda,

$$Mat_{1,s}(\mathbb{F}_q) = \bigcup_{r=0}^{s} S^{(1,s)}(r).$$

Para $R := (r_1, \ldots, r_n)$ com $0 \leqslant r_i \leqslant S$ para $i = 1, \ldots, n$ definiremos os conjuntos, $V_R := \{\Omega : \rho(\omega_i) \leqslant r_i\}$ e $F_R := \{\Omega : \rho(\omega_i) = r_i\}$. Chamaremos cada F_R de **Fragmento**. O próximo resultado segue diretamente das definições de $V_R, F_R, B^{(n,s)}(r)$ e $S^{(n,s)}(r)$.

Lema 3.7 *Cada Bola $B^{(n,s)}$ pode ser escrita como*

$$B^{(n,s)}(r) = \bigcup_{r_1+r_2+\cdots+r_n=r} V_R. \tag{3.7}$$

Do mesmo modo, cada esfera pode ser escrita como

$$S^{(n,s)}(r) = \bigcup_{r_1+r_2+\cdots+r_n=r} F_R \tag{3.8}$$

Lema 3.8 *Seja $C \subseteq Mat_{n,s}(\mathbb{F}_q)$ um código MDS na ρ-métrica com q^k elementos. Sejam $A = (a_1, \ldots, a_n)$ e $\Omega \in C$ então,*

i) $V_A(\Omega)$ contém $q^{a_1+\cdots+a_n-ns+k}$ pontos de C se $a_1 + \cdots + a_n > ns - k$;

ii) $V_A(\Omega)$ contém no máximo um ponto de C se $a_1 + \cdots + a_n \leqslant ns - k$.

Demonstração.

i) Escolhendo inteiros $c_1, \ldots, c_n$, $0 \leqslant c_i \leqslant s$, tais que $c_1 + \cdots + c_n = \sum_{i=1}^{n} a_i - ns + k$ e definindo $b_i = a_i - c_i$ temos $\sum_{i=1}^{n} b_i = ns - k$. Pelo Lema 3.4 temos que $V_A(\Omega)$ é a união disjunta de $q^{c_1+\cdots+c_n}$ caixas elementares com $B = (b_1, \ldots, b_n)$ e estas caixas possuem volume q^{-k} . Como o código é uniformemente distribuído (por ser MDS na ρ-métrica) cada caixa contém exatamente um elemento de C e daí, a união contém $q^{a_1+\cdots+a_n-ns+k}$ pontos de C.

ii) Se $\sum_{i=1}^{n} a_i = ns - k$ temos que $V_A(\Omega)$ possui volume q^{-k} e como C é uniformemente distribuído esta caixa contém exatamente um ponto de C. Agora se $\sum_{i=1}^{n} a_i < ns - k$ a caixa elementar $V_A(\Omega)$ possui volume inferior a q^{-k} e assim está contida em um caixa elementar de volume q^{-k} que por sua vez contém exatamente um ponto de C. Logo $V_A(\Omega)$ contém um ou nenhum ponto de C. □

No Lema 3.8, em nenhum momento da demonstração se fez necessário o fato de $\mathbb{F}_q$ ser um corpo, sendo assim o lema é válido para um alfabeto qualquer.

Um dos objetivos principais deste capítulo é demonstrar o próximo teorema o qual será apenas enunciado nesta seção pois, como veremos, sua demonstração é análoga à do Teorema 3.17 da seção 3.5.

Teorema 3.9 *Seja* $C \subseteq Mat_{n,s}(\mathbb{F}_q)$ *um código uniformemente distribuído então os pesos* $w_r(\Omega)$ *são independentes dos elementos* $\Omega \in C$ *e* $w_r(\Omega) = w_r(0) = w_r$ *são dados por* $w_0(\Omega) = 1$, $w_r(\Omega) = 0$ *se* $0 \leqslant r \leqslant \rho(C) = ns - k + 1$ *e*

$$\begin{aligned} w_r(\Omega) &= \sum_{l=1}^{n} \begin{pmatrix} n \\ l \end{pmatrix} \sigma_s(l,r) \sum_{t=o}^{r-\rho(C)} (-1)^t \begin{pmatrix} l \\ t \end{pmatrix} \left(q^{r-\rho(C)+1-t} - 1\right) \\ &= (q-1) \sum_{l=1}^{n} \begin{pmatrix} n \\ l \end{pmatrix} \sigma_s(l,r) \sum_{t=0}^{r-\rho(C)} (-1)^t \begin{pmatrix} l-1 \\ t \end{pmatrix} q^{r-\rho(C)-t}. \end{aligned}$$

3.4 Distribuições no Cubo Unitário

Trabalharemos com distribuições no cubo unitário pois, como veremos, existe uma relação biúnivoca entre elas e códigos MDS na ρ-métrica no espaço das matrizes, além de que as distribuições no cubo possuem um bom apelo geométrico que pode ser bem explorado de modo que deixem os resultados mais claros.

Seja $U^n = [0,1)^n$ o cubo unitário de dimensão n. Fixe um número primo p e uma potência $q = p^e, e \in \mathbb{N}$. Defina a caixa retangular elementar $\Delta_A^M \subseteq U^n$ por

$$\Delta_A^M = \left[\frac{m_1}{q^{a_1}}, \frac{m_1+1}{q^{a_1}}\right) \cdots \left[\frac{m_n}{q^{a_n}}, \frac{m_n+1}{q^{a_n}}\right), \tag{3.9}$$

onde $A = (a_1, \ldots, a_n)$, $M = (m_1, \ldots, m_n) \in \mathbb{N}_0^n$ e $m_j \in \{0, 1, \ldots, q^{a_j} - 1\}$, $1 \leqslant j \leqslant n$. Aqui escrevemos $\mathbb{N}_0^n$ para o conjunto de vetores em $\mathbb{R}^n$ com coordenadas inteiras não negativas. Observe que $Vol\Delta_A^M = q^{-a_1 - \cdots - a_n}$.

Consideremos agora para $s \in \mathbb{N}_0$ a seguinte coleção especial de caixas retangulares elementares

$$\mathfrak{C}_s(q,n) := \left\{\Delta_A^M : A = (a_1, \ldots, a_n), 0 \leqslant a_j \leqslant s, 1 \leqslant j \leqslant n\right\}. \tag{3.10}$$

Definição 3.10 *Dado um inteiro* $k \in [0,n]$*, um subconjunto* $D \subseteq U^n$ *com* q^k *pontos é dito uma* $[ns,k]_s$*-Distribuição Ótima na base q se qualquer caixa retangular elementar* $\Delta_A^M \in \mathfrak{C}_s(q,n)$ *de volume* q^{-k} *contém exatamente um ponto de* D*.*

Lema 3.11 *Seja* $D \subseteq U^n$ *uma* $[ns,k]_s$*-distribuição ótima na base* q*. Então,*

i) Cada caixa retangular elementar $\Delta_A^M \in \mathfrak{C}_s(q,n)$ *contém exatamente* $q^{k-a_1-\cdots-a_n}$ *pontos de* D *se* $a_1+\cdots+a_n<k$*;*

ii) Cada caixa retangular elementar $\Delta_A^M \in \mathfrak{C}_s(q,n)$ *contém no máximo um ponto de* D *se* $a_1+\cdots+a_n \geqslant k$*.*

Demonstração.

i) Escolha inteiros $c_1,\ldots,c_n$ tais que $c_1+\cdots+c_n = k-a_1-\cdots-a_n$, $0\leqslant c_j\leqslant s, 1\leqslant j\leqslant n$. Seja $b_i = a_i+c_i, 1\leqslant i\leqslant n$, então cada caixa Δ_A^M pode ser escrita como

$$\Delta_A^M = \left[\frac{q^{c_1}m_1}{q^{b_1}}, \frac{q^{c_1}m_1+q^{c_1}}{q^{c_1}}\right)\cdots\left[\frac{q^{c_n}m_n}{q^{b_n}}, \frac{q^{c_n}m_n+q^{c_n}}{q^{c_n}}\right).$$

Então, cada caixa Δ_A^M é a união de $q^{c_1+\cdots+c_n}$ caixas elementares disjuntas $\Delta_B^T \in \mathfrak{C}_s(q,n)$ de volume q^{-k} e pela Definição 3.10 temos que (*i*) é válida.

ii) Como cada caixa retangular elementar $\Delta_A^M \in \mathfrak{C}_s(q,n)$ com $a_1+\cdots+a_n \geqslant k$ está contida em um caixa retangular elementar maior $\Delta_B^T \in \mathfrak{C}_s(q,n)$ de volume q^{-k} temos que *(ii)* também é válida pela Definição 3.10. □

3.5 Códigos e Distribuições

Nesta seção encontraremos uma relação interessante entre distruibuições no cubo unitário e códigos no espaço de matrizes. Para tanto, começaremos considerando a representação q-ária de um ponto $x\in[0,1)$,

$$x=\sum_{i\geqslant 1}\eta_i(x)q^{-i}, \qquad \eta_i(x)\in\{0,1,\ldots,q-1\}. \tag{3.11}$$

Esta representação é única se escolhermos sempre a série finita para os pontos q-ários racionais $x=\frac{m}{q^a}$, $a\in\mathbb{N}$, $m\in\{0,1,\ldots,q^a-1\}$. Denotaremos por $\mathbb{Q}(q^s)$ $s\in\mathbb{N}$, o conjunto de todos os pontos da forma $x=\frac{m}{q^a}\in[0,1)$ com $a\leqslant s$ e $m\in\{0,1,...,q^a-1\}$. Por $\mathbb{Q}^n(q^s)$ para o conjunto de todos os pontos X tais que $X=(x_1,\ldots,x_n)^T\in U^n$ com coordenadas $x_j\in\mathbb{Q}(q^s), 1\leqslant j\leqslant n$.

Para cada $x\in[0,1)$ consideremos a projeção $\tau_s(x)$ de x em $\mathbb{Q}(q^s)$ definida por

$$\tau_s(x)=\sum_{i=1}^{s}\eta_i(x)\,q^{-i}. \tag{3.12}$$

Observe que

$$x-\tau_s(x)=\sum_{i\geqslant s+1}\eta_i(x)\,q^{-i}\in\left[0,q^{-s}\right). \tag{3.13}$$

Do mesmo modo para $X = (x_1, \ldots, x_n)^T \in U^n$ temos a projeção $\tau_s(X)$ de X em $\mathbb{Q}^n(q^s)$ dada por

$$\tau_s(X) = (\tau_s(x_1), \ldots, \tau_s(x_n))^T. \tag{3.14}$$

Sem perda de generalidade vamos trabalhar com $[ns, k]_s$-distribuições que são subconjuntos de $\mathbb{Q}^n(q^s)$. Podemos escrever a representação (3.11) na seguinte forma:

$$x = \sum_{i=1}^{s} \xi_i(x) q^{i-s-1}, \tag{3.15}$$

onde $\xi_i(x) = \eta_{s+1-i}(x)$.

Identificaremos agora os elementos $\xi_i(x)$ com elementos de um corpo finito. Seja $\mathbb{F}_q$ um corpo finito com $q = p^e$ elementos. Fixe uma base $\mathtt{B}$ de $\mathbb{F}_q$ sobre $\mathbb{F}_p$; como $[\mathbb{F}_q : \mathbb{F}_p] = e$ temos que esta base possui e elementos. Digamos, $\mathtt{B} = \{b_1, \ldots, b_e\}$ daí, todo elemento $\mu \in \mathbb{F}_q$ pode ser escrito como $\mu = \mu^{(1)} b_1 + \cdots + \mu^{(e)} b_e$ com $\mu^{(i)} \in \mathbb{F}_p$ e então cada elemento de $\mathbb{F}_q$ é identificado com um elemento de $\mathbb{F}_p^e$ por $\mu = \mu^{(1)} b_1 + \cdots + \mu^{(e)} b_e \longmapsto (\mu^{(1)}, \ldots, \mu^{(e)})$. Com esta escolha teremos a seguinte bijeção entre elementos $\mu \in \mathbb{F}_q$ e os inteiros $m \in \{0, 1, \ldots, q-1\}$:

$$\mu = \left(\mu^{(1)}, \ldots, \mu^{(e)}\right) \rightleftarrows m = \sum_{i=1}^{e} \mu^{(i)} p^{i-1} \in \{0, 1 \ldots, q-1\}. \tag{3.16}$$

Devido a esta bijeção os elementos $\xi_i(x)$ em (3.15) podem ser considerados como elementos de $\mathbb{F}_q$, além disso, cada $x \in \mathbb{Q}(q^s)$ pode ser identificado com a matriz,

$$\omega\langle x \rangle = (\xi_1(x), \ldots, \xi_s(x)) \in Mat_{1,s}(\mathbb{F}_q) \tag{3.17}$$

e os elementos $X \in \mathbb{Q}^n(q^s)$ com,

$$\Omega\langle X \rangle = (\omega\langle x_1 \rangle, \ldots, \omega\langle x_n \rangle)^T \in Mat_{n,s}(\mathbb{F}_q). \tag{3.18}$$

Por estas relações, para cada distribuição $D \subseteq \mathbb{Q}^n(q^s)$ podemos definir o código $C\langle D \rangle \subseteq Mat_{n,s}(\mathbb{F}_q)$ associado a mesma como o conjunto das matrizes correspondentes em (3.18), ou seja,

$$C\langle D \rangle = \{\Omega\langle X \rangle, X \in D\}. \tag{3.19}$$

Se, para cada quaisquer $X = (x_1 \ldots, x_n)^T, Y = (y_1, \ldots, y_n)^T \in \mathbb{Q}^n(q^s)$ e $\alpha, \beta \in \mathbb{F}_q$ definirmos $\alpha X \oplus \beta Y = (\alpha x_1 \oplus \beta y_1, \ldots, \alpha x_n \oplus \beta y_n)^T \in \mathbb{Q}^n(q^s)$ por

$$\xi_i(\alpha x_j \oplus \beta y_j) = \alpha \xi_i(x_j) + \xi_i(y_j), \quad 1 \leqslant i \leqslant s, \quad 1 \leqslant j \leqslant n, \tag{3.20}$$

onde $\xi_i(x) \in \mathbb{F}_q$ são coeficientes da representação (3.15) temos que $\mathbb{Q}^n(q^s)$ possui a estrutura de espaço vetorial sobre $\mathbb{F}_q$ com dimensão ns. Pode-se também transferir a noção de ρ-métrica (3.2) em $Mat_{n,s}(\mathbb{F}_q)$ para $\mathbb{Q}^n(q^s)$ fazendo as seguintes escolhas:

$$\rho(X) = \rho\left(\Omega\langle X\rangle\right) \tag{3.21}$$

para o ρ-peso de um ponto $X \in \mathbb{Q}^n(q^s)$ e

$$\rho(X \ominus X') = \rho\left(\Omega\langle X\rangle - \Omega\langle X'\rangle\right) \tag{3.22}$$

para a ρ-distância entre $X, X' \in \mathbb{Q}^n(q^s)$ onde $\ominus$ denota a subtração com respeito a $\oplus$. Assim podemos considerar a *ρ-distância mínima* de uma distribuição D.

$$\rho(D) = \min\left\{\rho(X \ominus X') : X, X' \in D, X \neq X'\right\}. \tag{3.23}$$

Mais ainda, temos que $\rho(D) = \rho(C\langle D\rangle)$. Faz sentido então estudarmos resultados referentes a ρ-métrica nas distribuições já que os resultados se transferem aos códigos no espaço de matrizes.

Lema 3.12 *As seguintes afirmações são válidas.*

i) Um ponto dado $X \in \mathbb{Q}^n(q^s)$ está em uma caixa elementar $\Delta_A^0 \in \mathfrak{C}_s(q,n)$ de volume q^{-k} se, e somente se, $\rho(X) \leqslant ns - k$;

ii) $X, X' \in \mathbb{Q}^n(q^s)$ estão simultaneamente em uma caixa elementar $\Delta_A^M \in \mathfrak{C}_s(q,n)$ de volume q^{-k} se, e somente se, $\rho(X \ominus X') \leqslant ns - k$.

Demonstração. Note que a Definição (3.15) implica que

$$x = \sum_{i=1}^{s} \xi_i(x) q^{i-s-1} = \sum_{i=1}^{\rho(x)} \xi_i(x) q^{i-s-1} \leqslant (q-1) \sum_{i=1}^{\rho(x)} q^{i-s-1} < q^{\rho(x)-s} \tag{3.24}$$

para todo $x \in \mathbb{Q}(q^s)$. Também tem-se que,

$$x = \sum_{i=1}^{s} \xi_i(x) q^{i-s-1} = \sum_{i=1}^{\rho(x)} \xi_i(x) q^{i-s-1} \geqslant q^{\rho(x)-s-1} \tag{3.25}$$

para $x > 0, x \in \mathbb{Q}(q^s)$.

i) Suponha primeiro que $\rho(X) \leqslant ns - k$. Escrevendo (3.24) para cada uma das coordenadas de $X = (x_1, \ldots, x_n)^T \in \mathbb{Q}^n(q^s)$ temos que $X \in \Delta_{A(X)}^0$, onde $A(X) = (a_1(x_1), \ldots, a_n(x_n))$ com

$a_j(x_j) = s - \rho(x_j), 1 \leqslant j \leqslant n$.

Com efeito,

$$\Delta^0_{A(X)} = \left[0, \frac{1}{q^{s-\rho(x_1)}}\right) \cdots \left[0, \frac{1}{q^{s-\rho(x_n)}}\right) = \left[0, q^{\rho(x_1)-s}\right) \cdots \left[0, q^{\rho(x_n)-s}\right)$$

logo como cada x_j satisfaz $0 \leqslant x_j < q^{\rho(x_j)-s}$ temos que $X \in \Delta^0_{A(X)}$. Além disso observe que

$$a_1(x_1) + \cdots + a_n(x_n) = ns - \rho(X) \geqslant k$$

e $0 \leqslant a_j(x_j) \leqslant s, 1 \leqslant j \leqslant n$. Então existe uma caixa elementar $\Delta^0_A \in \mathfrak{C}_s(q,n)$ de volume q^{-k} tal que $\Delta^0_{A(X)} \subseteq \Delta^0_A$ donde, $X \in \Delta^0_A$.

Suponha agora que $\rho(X) > ns - k$ escrevendo a desigualdade (3.25) para todas as coordenadas não nulas do ponto $X = (x_1, \ldots, x_n)^T \in \mathbb{Q}^n(q^s)$ temos o seguinte: Se X pertence a uma caixa elementar $\Delta^0_A \in \mathfrak{C}_s(q,n)$ com $A = (a_1, \ldots, a_n)$, então $0 \leqslant a_j \leqslant s - \rho(x_j)$ para $x_j > 0$ e $0 \leqslant a_j \leqslant s$ para $x_j = 0, 1 \leqslant j \leqslant n$. Como $\rho(0) = 0$, temos

$$a_1 + \cdots + a_n \leqslant ns - \rho(x_1) - \cdots - \rho(x_n) = ns - \rho(X) < k$$

Então a caixa $\Delta^0_A \in \mathfrak{C}_s(q,n)$ possui volume estritamente maior que q^{-k} e a prova do *i)* esta completa.

ii) Segue do $itemi)$ e do fato que a ρ-distância é invariante por translação. □

Teorema 3.13 *Seja $D \subseteq \mathbb{Q}^n(q^s)$ uma distribuição e $C\langle D\rangle \subseteq Mat_{n,s}(\mathbb{F}_q)$ seu código. Então são equivalentes.*

i) D é uma $[ns,k]_s$-distribuição ótima;

ii) $C\langle D\rangle$ é um $[ns,k]_s$-código MDS com respeito a métrica ρ.

Demonstração.

i) Seja D uma $[ns,k]_s$- distribuição ótima. Então cada caixa elementar $\Delta^M_A \in \mathfrak{C}_s(q,n)$ de volume q^{-k} contém exatamente um ponto de D, e pelo Lema 3.12 (*ii*), a distância $\rho(X \ominus X') > ns - k$ para quaisquer dois pontos distindos $X, X' \in D$. Portanto, $C\langle D\rangle$ é um $[ns,k]_s$-código MDS na ρ-métrica.

ii) Seja $C\langle D\rangle$ um $[ns,k]_s$-código MDS na ρ-métrica. Então $\rho(X \ominus X') > ns - k$ para quaisquer $X, X' \in D$, e pelo Lema 3.12 (*ii*), cada caixa retangular elementar $\Delta^M_A \in \mathfrak{C}_s(q,n)$ de volume q^{-k} contém no máximo um ponto de D. Agora como para $A = (a_1, \ldots, a_n) \in \mathbb{N}^n_0$, tal que, $a_1 + \cdots + a_n = k$ e $0 \leqslant a_j \leqslant s$, $1 \leqslant j \leqslant n$, o número de caixas retangulares elementares

correspondentes $\Delta_A^M \in \mathfrak{C}_s(q,n)$ com $(m_1,\ldots,m_n) \in \mathbb{N}_0^n$ onde $m_j = \{0,1,\ldots,q^{a_j}-1\}$, $1 \leqslant j \leqslant n$, é igual à q^k ou seja, é igual a cardinalidade de D. Portanto, cada uma destas caixas elementares $\Delta_A^M \in \mathfrak{C}_s(q,n)$ de volume q^{-k} contém exatamente um e apenas um ponto de D. Então, D é uma $[ns,k]_s$-distribuição ótima. □

Seja,

$$\mathfrak{S}(r) = \{X \in \mathbb{Q}^n(q^s) : \rho(X) = r\}, \quad 0 \leqslant r \leqslant ns, \tag{3.26}$$

a esfera de raio $r \in \mathbb{N}_0$ na ρ-métrica em $\mathbb{Q}^n(q^s)$. Note que (3.26) equivale à (3.6) quando consideramos $\Omega\langle X\rangle$ com a ρ-métrica em $Mat_{n,s}(\mathbb{F}_q)$. Escrevendo o intervalo $[0,1)$ como união dos seguintes $s+1$ subintervalos

$$[0,1) = \bigcup_{0 \leqslant b \leqslant s} g_b, \tag{3.27}$$

com $g_0 = [0,q^{-s}), g_1 = [q^{-s},q^{-s+1}), \ldots, [q^{-1},1)$, o cubo unitário pode ser escrito como a união das seguintes $(s+1)^n$ caixas disjuntas

$$U^n = \bigcup_B G_B, \quad G_B = \prod_{j=1}^{n} g_{b_j}, \tag{3.28}$$

onde $B = (b_1,\ldots,b_n) \in \mathbb{N}_0^n, 0 \leqslant b_j \leqslant s, 1 \leqslant j \leqslant n$. Chamaremos as caixas G_B de **Fragmentos**.

Como cada g_{b_i} em (3.27) é definido por $g_{b_i} = \left[q^{b_i-1-s}, q^{b_i-s}\right)$ se $b_i \neq 0$ e $g_0 = [0,q^{-s})$ então as esquações (3.24) e (3.25) implicam que $x \in \mathbb{Q}(q^s)$ está em g_{b_i} se, e somente se, $\rho(x) = b_i$. Disto segue que um ponto $X \in \mathbb{Q}^n(q^s)$ esta em um fragmento G_B com $B = (b_1,\ldots,b_n)$ se, e somente se, $\rho(x_i) = b_i$ para $i = 1,\ldots,n$ donde os elementos de G_B são transformados em elementos de F_B quando consideramos as matrizes dos pontos $X \in G_B$.

O próximo lema é um análogo ao Lema 3.7 sendo assim, pelo parágrafo anterior "basta apenas"trocarmos a notação para obter a demonstração do Lema 3.7.

Lema 3.14 *Cada esfera $\mathfrak{S}(r)$ pode ser escrita como a seguinte união de fragmentos,*

$$\mathfrak{S}(r) = \bigcup_{b_1+\cdots+b_n=r} G_B. \tag{3.29}$$

onde $B = (b_1,\ldots,b_n)$

Demonstração. Como para ponto $X = (x_1,\ldots,x_n)^T \in \mathbb{Q}^n(q^s)$ vale que $x_i \in g_{b_i}$ se, e somente se, $\rho(x_i) = b_i$ pelas definições de $\mathfrak{S}(r)$ e G_B temos que $X \in \mathfrak{S}(r)$ se, e somente se, X está em um fragmento G_B com $b_1 + \cdots + b_n = r$. □

Definamos $\mathfrak{S}_l(r) \subseteq \mathfrak{S}(r)$ o subconjunto formado por fragmentos $G_B \subseteq \mathfrak{S}(r)$ tal que B possui l coordenadas não nulas, isto é,

$$\mathfrak{S}_l(r) = \bigcup_{b_1+\cdots+b_n=r} G_B, \quad l \in \mathbb{N}_0, \quad 0 \leqslant l \leqslant n. \tag{3.30}$$

com B possuindo peso de Hamming l. Também definamos

$$\sigma_s(l,r) = \left|\left\{A = (a_1, \ldots, a_l) \in \mathbb{N}^l : a_1 + \cdots + a_l = r, 0 < a_j \leqslant s, 1 \leqslant j \leqslant l\right\}\right|.$$

Lema 3.15 *Para cada $\mathfrak{S}_l(r)$ o número de fragmentos G_B na união (3.30) é igual à* $\begin{pmatrix} n \\ l \end{pmatrix} \sigma_s(l,r)$.

Demonstração. Seja $l = 0$. Então, existe somente um fragmento $G_B = G_0 = [0, q^{-s})^n$ com peso de Hamming de $B = 0$. É claro que G_0 está na união (3.30) somente para $r = 0$. Isto prova o Lema 3.15 para $l = 0$.

Seja agora $l \geqslant 1$. Consideremos uma entre todas as $\begin{pmatrix} n \\ l \end{pmatrix}$ possíveis escolhas de l índices $J = \{j_1, \ldots, j_l\} \subseteq \{1, \ldots, n\}$. Então o número de fragmentos $G_B \subseteq \mathfrak{S}_l(r)$ com B tal que $0 < b_j \leqslant s$ para $j \in J$ e $b_j = 0$ para $j \notin J$ é igual à $\sigma_s(l,r)$. O que prova o Lema pra $l \geqslant 1$. □

Note que,

$$|\mathbb{Q}(q^s) \cap g_i| = \begin{cases} 1 & se \quad i = 0, \\ (q-1)q^{i-1} & se \quad i = 1, \ldots, s. \end{cases} \tag{3.31}$$

Agora, pela definição de cada G_B concluímos que

$$|\mathbb{Q}^n(q^s) \cap G_B| = (q-1)^{\mathfrak{H}(B)} q^{b_1+\cdots+b_n-\mathfrak{H}(B)} \tag{3.32}$$

onde $B = (b_1, \ldots, b_n)$ e $\mathfrak{H}(B)$ indica o peso de Hamming do ponto B. Portanto, pelo Lema 3.15 e por (3.30) temos que

$$|\mathbb{Q}^n(q^s) \cap \mathfrak{S}(r)| = \sum_{l=0}^{n} \begin{pmatrix} n \\ l \end{pmatrix} \sigma_s(l,r)(q-1)^l q^{r-l}. \tag{3.33}$$

Definamos a bola de raio $r \in \mathbb{N}_0$ como sendo o conjuntos dos pontos X de $\mathbb{Q}^n(q^s)$ com $\rho(X)$ menor ou igual que r ou seja,

$$\mathfrak{B}(r) = \{X \in \mathbb{Q}^n(q^s) : \rho(X) \leqslant r\}. \tag{3.34}$$

Observe novamente que a bola $\mathfrak{B}(r) \subseteq \mathbb{Q}^n(q^s)$ equivale a bola $B^{(n,s)}(r) \subseteq Mat_{n,s}(\mathbb{F}_q)$ quando consideramos $\Omega\langle X\rangle$ com a ρ-métrica em $Mat_{n,s}(\mathbb{F}_q)$. É claro que,

$$\mathfrak{B}(r) = \bigcup_{0 \leqslant j \leqslant r} \mathfrak{S}(j). \tag{3.35}$$

Lema 3.16 *Cada bola $\mathfrak{B}(r)$ pode ser escrita como a seguinte união de caixas elementares de $\mathfrak{C}_s(q,n)$:*

$$\mathfrak{B}(r) = \bigcup_{a_1+\cdots+a_n=r} \Delta^0_{A^*}, \tag{3.36}$$

onde $A^* = (a_1^*, \ldots, a_n^*)$ com $a_j^* = s - a_j$, $0 \leqslant a_j \leqslant s$, $1 \leqslant j \leqslant n$.

Demonstração. Seja $X \in \mathfrak{B}(r)$. Escrevendo a inequação (3.24) para todas as coordenadas do ponto X, temos que $X \in \Delta^0_{A(X)}$ com $A(X) = (a_1(x_1), \ldots, a_n(x_n))$, onde $a_j(x_j) = s - \rho(x_j)$, $1 \leqslant j \leqslant n$ e $\rho(x_1) + \cdots + \rho(x_n) = \rho(X) \leqslant r$. Então existe uma caixa elementar $\Delta^0_{A(X)}$ na união (3.36) tal que $X \in \Delta^0_{A(X)} \subseteq \Delta^0_A$.

Seja agora $X \notin \mathfrak{B}(r)$, isto é, $\rho(X) > r$. Escrevendo a inequação (3.25) e utilizando o fato de $\rho(x_i) \leqslant s$ para todo x_i obtemos o seguinte fato: Um ponto X pertence a uma caixa elementar $\Delta^0_{A^*} \in \mathfrak{C}_s(q,n)$, então $\rho(x_j) \leqslant a_j \leqslant s$, $1 \leqslant j \leqslant n$. Portanto, temos $a_1 + \cdots + a_n \geqslant \rho(X) > r$, e então, a caixa elementar $\Delta^0_{A^*}$ não está contida na união (3.36). □

O próximo teorema é o correspondente do Teorema 3.9 o qual se demonstra de maneira análoga.

Teorema 3.17 *Seja $D \subseteq \mathbb{Q}^n(q^s)$ uma $[ns,k]_s$-distribuição ótima e $C = C\langle D\rangle$ o seu $[ns,k]_s$-código MDS correspondente na ρ-métrica. Então os pesos w são independentes dos elementos $\Omega' \in C$ e dos pontos $X' \in D$ e $w_r = w_r(\Omega') = w_r(X')$ são dados por*

$$w_0 = 1, \quad w_r = 0 \tag{3.37}$$

para $0 \leqslant r \leqslant \rho(D) = ns - k + 1$ e

$$\begin{aligned} w_r &= \sum_{l=1}^{n} \binom{n}{l} \sigma_s(l,r) \sum_{t=0}^{r-\rho(D)} (-1)^t \binom{l}{t} (q^{r-\rho(D)+1-t} - 1) \\ &= (q-1) \sum_{l=1}^{n} \binom{n}{l} \sigma_s(l,r) \sum_{t=0}^{r-\rho(D)} (-1)^t \binom{l-1}{t} q^{r-\rho(D)-t} \end{aligned}$$

para, $\rho(D) \leqslant r \leqslant ns$.

Demonstração. Seja D uma distribuição ótima com q^k elementos e X' um ponto fixo. É claro que $w_0(X') = 1$, pois X' é o único ponto com ρ-distância zero para X'. Para $0 < r \leqslant \rho(D) = ns - k + 1$ temos $w_r(X') = 0$ pois do contrário teríamos uma contradição com a distância mínima.

Agora pelo Lema 3.14 sabemos que,

$$\mathfrak{S}(r) = \bigcup_{b_1+\cdots+b_n=r} G_B, \tag{3.38}$$

onde $B = (b_1, \ldots, b_n)$. Considere então um fragmento G_B, com $\mathfrak{H}(B) = l \geqslant 1$. Suponha que $b_j \neq 0$ $(0 < b_j \leqslant s)$ para $j \in J$ e $b_j = 0$ para $j \notin J$, onde $J = \{j_1, \ldots, j_l\} \subseteq \{1, \ldots, n\}$ é um subconjunto de l índices. Agora pela definição de cada fragmento temos que o fragmento G_B pode ser escrito como a seguinte representação em termos de caixas elementares,

$$G_B = \Delta^0_{A_0} - \bigcup_{i \in J} \Delta^0_{A_i}, \tag{3.39}$$

onde $A_0 = (a_1^{(0)}, \ldots, a_n^{(0)})$,

$$a_j^{(0)} = s - b_j, \quad 1 \leqslant j \leqslant n, \tag{3.40}$$

e $A_i = (a_1^{(i)}, \ldots, a_n^{(i)})$ com

$$a_j^{(i)} = \begin{cases} s & se \quad j \notin J, \\ s - b_j & se \quad j \in J \quad e \quad j \neq i, \\ s - b_j + 1 & se \quad j \in J \quad e \quad j = i. \end{cases} \tag{3.41}$$

Assim definidos temos que

$$a_1^{(i)} + \cdots + a_n^{(i)} = ns - b_1 - \cdots - b_n = ns - r. \tag{3.42}$$

Seja $I = \{i_1, \ldots, i_t\} \subseteq J = \{j_1, \ldots, j_l\}$ um subconjunto de t índices. Então,

$$\Delta^0_{A_{i_1}} \cap \ldots \cap \Delta^0_{A_{i_t}} = \Delta^0_{A_I}, \tag{3.43}$$

onde $A_I = (a_1^{(I)}, \ldots, a_n^{(I)})$ com

$$a_j^{(I)} = max\left\{a_j^{(i_1)}, \ldots, a_j^{(i_t)}\right\} = \begin{cases} s - b_j & se \quad j \notin I, \\ s - b_j + 1 & se \quad j \in I. \end{cases} \tag{3.44}$$

Note que,

$$a_1^{(I)} + \cdots + a_n^{(I)} = ns - r + t. \tag{3.45}$$

Agora utilizando o Princípio da Inclusão-Exclusão temos que

$$\begin{aligned} |D \cap G_B| &= \left| D \cap \left(\Delta^0_{A_0} - \bigcup_{i \in J} \Delta^0_{A_i} \right) \right| \\ &= \left| D \cap \Delta^0_{A_0} \right| - \left| D \cap \left(\bigcup_{i \in J} \Delta^0_{A_i} \right) \right| \\ &= \left| D \cap \Delta^0_{A_0} \right| - \sum_{t=1}^{l} \sum_{I \subseteq J; |I| = t} (-1)^t \left| D \cap \Delta^0_{A_I} \right|. \end{aligned}$$

O Lema 3.11 diz que

$$\left|D \cap \Delta_A^0\right| = \begin{cases} q^{k-a_1-\cdots-a_n} & se \quad \sum_{i=1}^{n} a_i < k, \\ 1 & se \quad \sum_{i=1}^{n} a_i \geqslant k. \end{cases} \tag{3.46}$$

onde $A = (a_1, \ldots, a_n)$. Como $\sum_{j=1}^{n} a_j^{(0)} = ns - r$ e por hipótese $r \geqslant ns - k + 1$ segue que $k \geqslant ns - r + 1 > ns - r = \sum_{j=1}^{n} a_j^{(0)}$. Logo,

$$|D \cap \Delta_{A_0}| = q^{k-ns+r}.$$

Para todo $t \leqslant r - ns + k - 1$ a equação (3.42) implica que $a_1^{(i)} + \cdots + a_n^{(i)} < k$ para cada i. Se $t \geqslant r - ns + k$ vale $a_1^{(i)} + \cdots + a_n^{(i)} \geqslant k$ para cada i. Assim,

$$\begin{aligned} |D \cap G_B| &= \left|D \cap \Delta_{A_0}^0\right| - \sum_{t=1}^{l} \sum_{I \subseteq J; |I|=t} (-1)^t \left|D \cap \Delta_{A_I}^0\right| \\ &= \sum_{t=0}^{r-ns+k-1} (-1)^t \binom{l}{t} q^{k-ns+r-t} + \sum_{t=r-ns+k}^{l} (-1)^t \binom{l}{t} \\ &= \sum_{t=0}^{r-\rho(D)} (-1)^t \binom{l}{t} \left(q^{r-\rho(D)+1-t} - 1\right) \\ &= (q-1) \sum_{t=0}^{r-\rho(D)} (-1)^t \binom{l-1}{t} q^{r-\rho(D)-t}. \end{aligned}$$

Agora como $w_r = |C \cap \mathfrak{S}(r)|$ e $\mathfrak{S}(r) = \bigcup_{0 \leqslant l \leqslant n} \mathfrak{S}_l(r)$ temos que

$$\begin{aligned} w_r &= \sum_{l=1}^{n} \sum_{B:\mathfrak{H}(B)=l} |D \cap G_B| \\ &= \sum_{l=1}^{n} \binom{n}{l} \sigma_s(l,r) \sum_{t=0}^{r-\rho(D)} (-1)^t \binom{l}{t} (q^{r-\rho(D)+1-t} - 1) \\ &= (q-1) \sum_{l=1}^{n} \binom{n}{l} \sigma_s(l,r) \sum_{t=0}^{r-\rho(D)} (-1)^t \binom{l-1}{t} q^{r-\rho(D)-t} \end{aligned}$$

pois pelo Lema 3.15 existem $\binom{n}{l} \sigma_s(l,r)$ fragmentos G_B tais que $\mathfrak{H}(B) = l$. □

3.6 Interpolação de Hermite Sobre Corpos Finitos e Construções Explícitas

Nesta seção iremos construir explicitamente uma família de códigos MDS em relação a ρ-métrica no espaço de matrizes, consequentemente pelo que foi discutido na seção anterior teremos uma família de distribuições ótimas. Iniciemos esta seção com alguns conceitos, propriedades e definições.

Seja $\mathbb{F}_q[x]$, onde $q = p^e$ com p primo. Será conveniente escrever

$$f(x) = \sum_{i=0}^{t-1} f_i x^i, \tag{3.47}$$

com coeficientes $f_i \in \mathbb{F}_q$ e $t = \deg(f)+1$. Para um polinômio $f(x)$ dado definimos sua *j-ésima Hiperderivada* $\partial^j f \in \mathbb{F}_q[x]$ por

$$\partial^j f(x) = \sum_{i=0}^{t-1} \begin{pmatrix} i \\ j \end{pmatrix} f_i x^{i-j}, \tag{3.48}$$

onde por definição $\binom{i}{j} = 0$ quando $j > i$. A hiperderivada ∂^j é linear, ou seja, $\partial^j(cf) = c\partial^j(f)$ e $\partial^j(f+g) = \partial^j(f) + \partial^j(g)$ para $c \in \mathbb{F}_q$ e $f, g \in \mathbb{F}_q[x]$. Pela fórmula

$$\partial^n f_1 f_2 \dots f_t = \sum_{n_1,\dots,n_t \geqslant 0} \partial^{n_1} f_1 \partial^{n_2} f_2 \dots \partial^{n_t} f_t$$

onde $n_1 + \dots + n_t = n$ e $f_1, \dots, f_t \in \mathbb{F}[x]$ que pode ser encontrada em [7] Lema 6.47, pode-se provar que

$$\partial^j (x-\beta)^i = \begin{pmatrix} i \\ j \end{pmatrix} (x-\beta)^{i-j} \tag{3.49}$$

para cada $\beta \in \mathbb{F}_q$. Agora, como $B = \left\{(x-\beta)^k; k = 0, \dots, t-1\right\}$ é uma base do subespaço de polinômios com grau até $t-1$, temos que $f(x) = \sum_{j=0}^{t-1} a_j (x-\beta)^j$ e os a_j são únicos; agora por (3.48) e (3.49) temos

$$\begin{aligned} \partial^k f(x) &= \sum_{j=0}^{t-1} a_j \partial^j (x-\beta)^j \\ &= \sum_{j=0}^{t-1} a_j \begin{pmatrix} j \\ k \end{pmatrix} (x-\beta)^{j-k} \end{aligned}$$

assim $\partial^k f(\beta) = 0$ se $k \neq j$ e $\partial^k f(\beta) = a_j$ se $k = j$ provando que

$$f(x) = \sum_{j=0}^{t-1} \partial^j f(\beta)(x-\beta)^j, \tag{3.50}$$

onde $\partial^j f(\beta)$ denota o valor de $\partial^j f(x)$ avaliado em $\beta \in \mathbb{F}_q$. Se $j < p$ a hiperderivada e a *j-ésima* derivada usual $f^{(j)}(x)$ são tais que,

$$\partial^j f(x) = \frac{1}{j!} f^{(j)}(x). \tag{3.51}$$

Agora, vamos adicionar um ponto $*$ a $\mathbb{F}_q$ e consideremos $\mathbb{F}_q \cup \{*\}$ com $q+1$ elementos. Para um polinômio (3.47) escolhemos, por definição,

$$\partial^j f(*) = \begin{cases} f_{t-1-j} & se \quad 0 \leqslant j \leqslant t-1; \\ 0 & se \quad j > t-1. \end{cases} \tag{3.52}$$

Ainda, se definirmos

$$f^V(x) = x^{t-1} f\left(\frac{1}{x}\right) = f_{t-1} + f_{t-2}x + \cdots + f_0 x^{t-1}$$

que chamaremos de polinômio recíproco de $f(x)$, temos que

$$\partial^j f(*) = \partial^j f^V(0).$$

Seja $\mathbb{F}_q^t[x] \subseteq \mathbb{F}_q[x]$ o conjunto de todos os polinômios (3.47) de grau menor ou igual a $t \in \mathbb{N}_0$. Então $\mathbb{F}_q^t[x]$ é um espaço vetorial de dimensão $t+1$ sobre $\mathbb{F}_q$. Consideremos agora o seguinte *problema de interpolação de Hermite*: Encontre um polinômio $f \in \mathbb{F}_q^t[x]$ satisfazendo as seguintes equações

$$\partial^j f(\beta_i) = a_i^{(j)}, \quad j = 0, \ldots, t_i - 1, \quad 1 \leqslant i \leqslant l, \tag{3.53}$$

onde os l elementos distintos $\beta_1, \ldots, \beta_l \in \mathbb{F}_q \cup \{*\}$ que chamaremos de pontos de interpolação são fixos, e os inteiros $t_i \in \mathbb{N}$ são dados, bem como os coeficientes $a_i^{(j)} \in \mathbb{F}_q$.

Proposição 3.18 *O problema de interpolação de Hermite possui as seguintes propriedades*

*i) O problema de interpolação de Hermite (*3.53*) possui uma única solução $f \in \mathbb{F}_q^t[x]$, se $t_1 + \cdots + t_l = t$;*

*ii) O problema de interpolação de Hermite (*3.53*) com coeficientes $a_i^{(j)}$ possui única solução $f \equiv 0$ no espaço $\mathbb{F}_q^t[x]$, se $t_1 + \cdots + t_l > t$.*

Demonstração.

i) Suponha que todos os pontos de interpolação β_i estão em $\mathbb{F}_q$, $1 \leqslant i \leqslant l$ e considere os polinômios

$$r_i(x) = \sum_{j=0}^{t_i - 1} a_i^{(j)} (x - \beta_i)^j, \quad 1 \leqslant i \leqslant l. \tag{3.54}$$

Pelas relações (3.49), (3.50) e (3.54), se as equações valem para f teremos

$$f(x) = \sum_{j=0}^{t_{i-1}} a_i^{(j)}(x-\beta_i)^j + \sum_{j=t_i}^{t} \partial^j f(\beta_i)(x-\beta_i)^j$$

concluímos que as equações em (3.53) são equivalentes as seguintes congruências em $\mathbb{F}_q[x]$:

$$f(x) \equiv r_i(x) \quad mod(x-\beta_i)^{t_i} \quad 1 \leqslant i \leqslant l. \tag{3.55}$$

Em (3.55) os polinômios $(x-\beta_i)^{t_i},\ 1 \leqslant i \leqslant l$ são co-primos. Portanto, o Teorema Chinês dos Restos garante que as congruências em (3.55) possuem uma única solução $f \in \mathbb{F}_q[x]$ módulo $g(x) = \left(\prod_{i=1}^{l}(x-\beta_i)^{t_i}\right)$. Como o grau de $g(x)$ é $t_1 + \cdots + t_l$, existe uma única solução $f \in \mathbb{F}_{q^t}[x]$ se $t = t_1 + \cdots + t_l$;. Agora suponha que um dos pontos de interpolação, digamos, β_l coincide com $*$. Então, utilizando (3.52),

$$f(x) = g(x) + r_l(x), \tag{3.56}$$

onde

$$r_l(x) = \sum_{j=t-t_l}^{t-1} a_l^{(j)} x^j$$

e $g(x)$ é um polinômio de grau menor que $t - t_l$. Substituindo (3.56) nas equações (3.53) temos que o polinômio $g \in \mathbb{F}_q^{t-t_l}[x]$ é solução do seguinte problema de interpolação de Hermite com $l-1$ pontos de interpolação $\beta_1, \ldots, \beta_{l-1} \in \mathbb{F}_q$:

$$\partial^j g(\beta_i) = b_i^{(j)}, \quad j = 0, \ldots, t_i - 1, \quad 1 \leqslant i \leqslant l-1,$$

onde $b_i^{(j)} = a_i^{(j)} - \partial^j r(\beta_i)$ e $t_1 + \cdots + t_{l-1} = t - t_l$. Este problema possui uma única solução pela primeira parte desta demonstração.

ii) Segue de *i)* pois podemos escolher inteiros $t_i' \in \mathbb{N}, t_i' \leqslant t_i$, que satisfazem $t_1' + \cdots + t_l' = t$.

□

Assumiremos agora que $q \geqslant n-1$. Fixados n elementos distintos $\beta_1, \ldots, \beta_n \in \mathbb{F}_q \cup \{*\}$ defina a seguinte transformação linear.

$$\begin{aligned} \Gamma_{n,s} : \mathbb{F}_q[x] &\longrightarrow Mat_{n,s}(\mathbb{F}_q) \\ f(x) &\longmapsto [\partial^{s-1-j} f(\beta_i)]. \end{aligned}$$

Então para cada polinômio $f \in \mathbb{F}_q[x]$ temos a matriz

$$\Gamma_{n,s}(f) = (w_f^{(1)}, \ldots, w_f^{(n)})^T \in Mat_{n,s}(\mathbb{F}_q)$$

consiste em n-linhas da seguinte forma

$$w_f^{(i)} = \left(\partial^{s-1} f(\beta_i), \ldots, \partial f(\beta_i), f(\beta_i)\right) \in Mat_{1,s}(\mathbb{F}_q), \quad 1 \leqslant i \leqslant n. \tag{3.57}$$

Lema 3.19 *Para $t \leqslant ns$ a imagem $\Gamma_{n,s}\left(\mathbb{F}_q^t[x]\right) \subseteq Mat_{n,s}(\mathbb{F}_q)$ do espaço vetorial $\mathbb{F}_q^t[x] \subseteq \mathbb{F}_q[x]$ é um subespaço vetorial de dimensão t.*

Demonstração. Como $\Gamma_{n,s}$ é linear, basta provar que $\Gamma_{n,s} : \mathbb{F}^{ns}[x] \to Mat_{n,s}$ é injetora, pois como $\mathbb{F}^t[x] \subseteq \mathbb{F}^{ns}[x]$, segue que a restrição $\Gamma_{n,s} : \mathbb{F}^t[x] \to Mat_{n,s}$ é injetora e que $\dim(\Gamma_{n,s}(\mathbb{F}^t[x])) = \dim(\mathbb{F}^t[x]) = t$. Com efeito, seja $f \in \mathbb{F}_q^{ns}[x]$ tal que $\Gamma_{n,s}(f) = 0$. Então pela definição de $\Gamma_{n,s}$ concluímos que f é solução do problema homogêneo de Hermite (3.53) com $l = n$, $t = ns$ e $t_1 + \cdots + t_n = s$. Portanto$f \equiv 0$ pela Proposição 3.18. □

Teorema 3.20 *Para cada inteiro $1 \leqslant k \leqslant ns$, o subespaço $\Gamma_{n,s}(\mathbb{F}_q^k[x]) \subseteq Mat_{n,s}(\mathbb{F}_q)$ é um $[ns,k]_s$-código MDS na ρ-métrica.*

Demonstração. Provaremos que, $\rho\left(\Gamma_{n,s} f\right) \geqslant ns - k + 1$ para $f \not\equiv 0$. Com efeito, suponha o contrário, ou seja, que existe $f \not\equiv 0$, $f \in \mathbb{F}_q^{ks}[x]$ tal que, $\rho(\Gamma_{n,s}(f(x))) \leqslant ns - k$. Ou seja,

$$\rho(\Gamma_{n,s} f) = \rho(w_f^{(1)}) + \cdots + \rho(w_f^{(n)}) \leqslant ns - k. \tag{3.58}$$

Daí, concluímos que ao mínimo para um dos índices temos a desigualdade estrita

$$\rho(w_f^{(i)}) < s \tag{3.59}$$

Sem perda de generalidade assumiremos que (3.59) é válida para $i = 1, \ldots, l$ com $l \geqslant 1$ e $\rho(w_f^{(i)}) = s$ para $i = l+1, \ldots, n$. Defina $t_i = s - \rho(w_f^{(i)}) \in \mathbb{N}$. Pela definição de $\Gamma_{n,s}$, (3.57) e (3.59) temos que o polinômio $f \in \mathbb{F}_q^k[x]$ é solução do seguinte problema de interpolação homogêneo de Hermite

$$\partial^j f(\beta_i) = 0, \quad j = 0, \ldots, t_i - 1, \quad 1 \leqslant i \leqslant l.$$

Assim sendo, temos $t_1 + \cdots + t_l = ns - \rho(\Gamma_{n,s} f)$. Portanto , $t_1 + \cdots + t_l \geqslant k$ e pela Proposição 3.18, $f \equiv 0$, que é uma contradição. Donde $\rho(\Gamma_{n,s} f) \geqslant ns - k + 1$ para $f \not\equiv 0$ e portanto, $\Gamma_{n,s}(\mathbb{F}_q^k[x])$ é um $[ns,k]_s$-código MDS. □

Agora com este Teorema temos uma classe abrangente de $[ns,k]_s$-códigos lineares MDS na ρ-métrica para valores quaisquer dos parâmetros n, k e s. Consequentemente temos uma classe de $[ns,k]_s$-distribuições lineares ótimas, bastando apenas introduzir a transformação linear $\gamma_{n,s} : \mathbb{F}_q[x] \to \mathbb{Q}^n(q^s)$ definida por

$$\gamma_{n,s} f = X = (x_1, \ldots, x_n)^T \in \mathbb{Q}^n(q^s), \tag{3.60}$$

onde as coordenadas x_i de X são dadas por

$$x_i = \sum_{j=1}^{s} \partial^{j-1} f(\beta_i) q^{-j}. \tag{3.61}$$

3.7 Projeções de Códigos MDS

Esta seção tem como objetivo mostrar que em certas condições quando se tem dado um código MDS $C \in Mat_{n,s}(\mathcal{A})$ pode-se obter um código MDS $C' \in Mat_{n',s'}(\mathcal{A})$. Seguiremos como referência principal [5].

Diremos que um código $C \subseteq Mat_{n,s}(\mathcal{A})$ é projetado em $Mat_{n',s'}(\mathcal{A})$ com $n' \leqslant n$ e $s' \leqslant s$ quando cada uma das matrizes Ω no código $C \subseteq Mat_{n,s}(\mathcal{A})$ é "transformada"em uma matriz em $Mat_{n',s'}(\mathcal{A})$ formada pelas $1, \ldots, n'$ primeiras linhas e $s - s' + 1, \ldots, s$ últimas colunas de Ω. Assim, se $\Omega \in C$ é escrita na forma de blocos

$$\Omega = \begin{bmatrix} \Omega^{(1)}_{n',s-s'} & \Omega^{(2)}_{n',s'} \\ \Omega^{(3)}_{n-n',s-s'} & \Omega^{(4)}_{n-n',s'} \end{bmatrix}$$

onde $\Omega^{(l)}_{k,j}$ é uma submatriz de ordem $k \times j$, então a projeção de Ω em $Mat_{n',s'}(\mathcal{A})$ é a matriz $\Omega^{(2)}_{n',s'}$.

Exemplo 3.21 *A matriz,*

$$X = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} \in Mat_{3,3}(\mathbb{F}_2)$$

é projetada em $Mat_{3,1}(\mathbb{F}_2)$ e em $Mat_{2,2}(\mathbb{F}_2)$ nas matrizes $A^{(1)}$ e $A^{(2)}$ respectivamente.

$$A^{(1)} = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \qquad A^{(2)} = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}.$$

Denotaremos por π a projeção em $Mat_{n',s'}(\mathcal{A})$, onde $n's' \geqslant k$.

Lema 3.22 *Seja $\mathcal{A}$ um alfabeto com q elementos se C é um código MDS em $Mat_{n,s}(\mathcal{A})$ com q^k elementos, então o código $\pi(C)$ em $Mat_{n',s'}(\mathcal{A})$, onde $s' \leqslant s$, $n' \leqslant n$ e $s'n' \geqslant k$, possui q^k elementos distintos. Isto é, a projeção π restrita a C é injetiva.*

Demonstração. Denotaremos por $\rho_{n,s}$ e $\rho_{n',s'}$ as ρ-métricas em $Mat_{n,s}(\mathcal{A})$ e $Mat_{n',s'}(\mathcal{A})$, respectivamente. Sejam $\Omega, \Omega' \in Mat_{n,s}(\mathcal{A})$ então,

$$\rho_{n,s}(\Omega, \Omega') \quad \leqslant \quad \rho_{n',s'}(\pi(\Omega), \pi(\Omega')) + (s - s')n' + s(n - n')$$

$$= \quad \rho_{n',s'}(\pi(\Omega), \pi(\Omega')) + sn - s'n'.$$

Assuma agora $\Omega, \Omega' \in Mat_{n,s}(\mathcal{A}) \cap C$ tais que $\pi(\Omega) = \pi(\Omega')$. Então,

$$\rho_{n,s}(\Omega, \Omega') \leqslant sn - s'n' \leqslant ns - k.$$

Como C é código MDS temos que $\rho_{n,s}(\Omega, \Omega') = 0$, donde $\Omega = \Omega'$, ou seja, π é injetiva. □

Teorema 3.23 *Seja $C \subseteq Mat_{n,s}(\mathcal{A})$ um código MDS com q^k elementos, suponha que $s' \leqslant s$, $n' \leqslant n$ e que $s'n' \geqslant k$. Então a projeção de C em $Mat_{n',s'}(\mathcal{A})$ também é um código MDS.*

Demonstração. Seja $\Omega \in C$. Pelo Lema 3.22 temos $|\pi(C)| = |C|$. Como C é MDS temos

$$\rho_{n,s}(\Omega) = \rho_{1,s}(\omega_1) + \cdots + \rho_{1,s}(\omega_n) \geqslant ns - k + 1.$$

Vamos dividir a demonstração em três casos.

Caso a) Se $s = s'$ e $n' < n$.

$$\begin{aligned}
\rho_{n',s}(\pi(\Omega)) &= \rho_{1,s}(\omega_1) + \cdots + \rho_{1,s}(\omega_{n'}) \\
&= \rho_{1,s}(\omega_1) + \cdots + \rho_{1,s}(\omega_n) - \rho_{1,s}(\omega_{n'+1}) - \cdots - \rho_{1,s}(\omega_n) \\
&= \rho_{n,s}(\Omega) - \rho_{1,s}(\omega_{n'+1}) - \cdots - \rho_{1,s}(\omega_n) \\
&\geqslant ns - k + 1 - s(n - n') \\
&= n's - k + 1.
\end{aligned}$$

Caso b) Se $s < s'$ e $n = n'$.

$$\rho_{1,s'}(\omega_i) = \begin{cases} \rho_{1,s}(\omega_i) - (s - s') & se \quad \rho_{1,s}(\omega_i) \geqslant (s - s') \\ 0 = \rho_{1,s}(\omega_i) - \rho_{1,s}(\omega_i) & se \quad \rho_{1,s}(\omega_i) < (s - s') \end{cases}$$

Sem perda de generalidade, suponha que a segunda relação vale para as linhas $i = 1, \ldots, l$ e a primeira para as linhas $i = l + 1, \ldots, n$. Então

$$\begin{aligned}
\rho_{n,s'}(\pi(\Omega)) &= \sum_{i=1}^{l} (\rho_{1,s}(\omega_i) - \rho_{1,s}(\omega_i)) + \sum_{i=l+1}^{n} [\rho_{1,s}(\omega_i) - (s - s')] \\
&= \rho_{n,s}(\Omega) - \rho_{1,s}(\omega_1) - \cdots - \rho_{1,s}(\omega_l) - (n - l)(s - s') \\
&\geqslant ns - k + 1 - \rho_{1,s}(\omega_1) - \cdots - \rho_{1,s}(\omega_l) - (n - l)(s - s') \\
&= ns' - k + 1 + l(s - s') - \sum_{i=1}^{l} \rho_{1,s}(\omega_i) \\
&\geqslant ns' - k + 1.
\end{aligned}$$

pois, $\rho_{1,s}(\omega_i) \leqslant s - s'$ para $i = 1, \ldots, l$.

Caso c) Se $s' < s$ e $n' < n$.

Este caso segue dos anteriores, pois a projeção correspondente é a composição das projeções $\pi_1 : Mat_{n,s}(\mathcal{A}) \to Mat_{n',s}(\mathcal{A})$ e $\pi_2 : Mat_{n',s}(\mathcal{A}) \to Mat_{n',s'}(\mathcal{A})$.

□

Corolário 3.24 *Seja $C \subseteq \mathcal{A}^n$ um código MDS na métrica de Hamming com q^k elementos, suponha que $k \leqslant n' \leqslant n$, então a projeção $\pi(C)$ em $\mathcal{A}^{n'}$ também é um código MDS na métrica de Hamming.*

Demonstração. Segue do fato que um código MDS na métrica de Hamming é simplesmente um código MDS na $\rho_{n,s}$-métrica com $s = 1$ e então, pelo Teorema 3.23, $\pi(C)$ é MDS com respeito a $\rho_{n',s'}$-métrica com $s' = 1$, ou seja, $\pi(C)$ é MDS na métrica de Hamming. □

3.8 Existência de Códigos MDS sobre $\mathbb{Z}_q$

Utilizaremos o Teorema Chinês do Resto para construir códigos MDS e mostrar quando tais códigos podem existir. Assumiremos que tais códigos são lineares em $Mat_{n,s}(\mathbb{Z}_q)$. Seja q um inteiro maior que 1 onde

$$q = \prod_{i=1}^{t} p_i,$$

com p_i primo e $p_i \neq p_j$ se $i \neq j$. Sendo C_i códigos em $Mat_{n,s}(\mathbb{Z}_{p_i})$ definiremos o código C por

$$C = CRT(C_1, \cdots, C_t) = \{c \in \mathbb{Z}_q : c \, mod(p_i) \in C_i \; \forall i\}. \tag{3.62}$$

Assim definido, C equivale ao conjunto $\{\Psi^{-1}(v_1, \ldots, v_t) : v_i \in C_i\}$, para o isomorfismo de grupos $\Psi : Mat_{n,s}(\mathbb{Z}_{p_1}) \times ... \times Mat_{n,s}(\mathbb{Z}_{p_t}) \to Mat_{n,s}(\mathbb{Z}_q)$, $\Psi(v) = (\Psi_1(v), \ldots, \Psi_t(v))$ com $\Psi_k(v) = \Psi_k(v_1, \ldots, v_t) = (v_1 \, mod(k), \ldots, v_t \, mod(k))$. Resumindo C é obtido aplicando o Teorema Chinês dos Restos coordenada a coordenada em todos os elementos de $C_1 \times C_2 \times \cdots \times C_t$.

Lema 3.25 *Seja $C = CRT(C_1, \ldots, C_t)$ onde $C_1, \ldots, C_t$ são códigos sobre $Mat_{n,s}(\mathbb{Z}_{p_i})$, respectivamente, então*

$$|C| = |C_1| \, |C_2| \cdots |C_t|$$

e ainda vale $\rho(C) \geqslant \min\{\rho(C_i)\}$.

Demonstração. A cardinalidade segue imediatamente pois Ψ é um isomorfismo de grupos entre C e $C_1 \times \cdots \times C_t$. Agora seja $v \in C$ com $\rho(v) < \rho(C_i)$ para todos os i, $1 \leqslant i \leqslant t$, o que implica que $\rho(v \ mod(p_i)) < \rho(C_i)$ para todo i. Logo $v \ mod(p_i) = 0$ para todo i, o que é impossível no caso em que $v \neq 0$ pois Ψ é isomorfismo, donde $v = 0$ e, portanto, $\rho(C) \geqslant \min\{\rho(C_i)\}$. □

Lema 3.26 *Sejam $C_1, \ldots, C_t$ códigos MDS em relação a ρ-métrica em $\mathbb{Z}_{p_i}$ com $|C_i| = (p_i)^k$ então $C = CRT(C_1, \ldots, C_t)$ é um código MDS sobre $\mathbb{Z}_q$ em relação a ρ-métrica com $|C| = q^k$.*

Demonstração. Segue do Lema 3.25 pois para a cardinalidade temos,

$$\begin{aligned} |C| &= |C_1|\,|C_2| \cdots |C_t| = \prod_{i=1}^{t} (p_i)^k \\ &= \left(\prod_{i=1}^{t} p_i \right)^k = q^k. \end{aligned}$$

Como $\rho(C) \geqslant \min\{\rho(C_i)\}$ então $\rho(C) \geqslant ns - k + 1$, ou seja, $\rho(C) = ns - k + 1$ provando que C é um código MDS em relação a ρ-métrica. □

Teorema 3.27 *Existem códigos MDS em $Mat_{n,s}(\mathbb{Z}_q)$ para $q \geqslant 2$ com $q = \prod_{i=1}^{t} p_i$, onde p_i's são primos distintos.*

Demonstração. O resultado segue do Lema 3.26. □

Capítulo 4

Códigos Posets

Neste Capítulo trabalharemos com códigos posets a fim de demonstrar resultados análogos, porém mais gerais aos resultados obtidos no capítulo anterior. Seguiremos como referência principal [5].

4.1 Conjuntos Parcialmente Ordenados (Posets)

Inicialmente faremos uma breve discussão sobre conjuntos parcialmente ordenados (Posets).

Definição 4.1 *Uma relação de ordem parcial em um conjunto X é uma relação binária $\preceq$ satisfazendo, para todo $x, y, z \in X$:*

i) $x \preceq x$;

ii) Se $x \preceq y$ *e* $y \preceq x$ *então,* $x = y$;

iii) Se $x \preceq y$ *e* $y \preceq z$ *então,* $x \preceq z$.

Dizemos que a relação $\preceq$ é de ordem total se, quaisquer dois elementos do conjunto X sobre o qual $\preceq$ está definida são comparáveis, isto é, $x \preceq y$ ou $y \preceq x$ para todos $x, y \in X$.

Definição 4.2 *Se $\preceq$ é uma relação de ordem parcial em um conjunto X, chamamos o par $\mathbb{P} = (X, \preceq)$ de poset.*

Exemplo 4.3 *O conjunto $[n] := \{1, 2, \ldots, n\}$, com a relação de divisibilidade $'|'$, $x|y \iff y = kx$ $k \in \mathbb{Z}$ formam um poset $\mathbb{P} = ([n], |)$.*

Definição 4.4 *Dados $x, y, z \in X$, dizemos que y cobre x se $x \preceq y$ e se $x \preceq z \preceq y$ então, $x = y$ ou $x = z$.*

Definição 4.5 *Seja $(X, \preceq)$ um poset.*

*i) Um elemento $x \in X$ é dito **elemento maximal** se não existe $y \in X - \{x\}$ tal que $x \preceq y$;*

*ii) Um elemento $x \in X$ é dito **elemento minimal** se não existe $y \in X - \{x\}$ tal que $y \preceq x$;*

*iii) Um elemento $x \in X$ é dito **máximo(mínimo)** se, $y \preceq x (x \preceq y)$ para todo $y \in X$.*

Vamos denotar por $M(I)$ o conjunto de todos os elementos maximais de um subconjunto $I \subseteq \mathbb{P}$.

Definição 4.6 *Um subconjunto I de um poset $\mathbb{P}$ é dito um **ideal** se $x \in I$ e $y \preceq x$ implica que $y \in I$.*

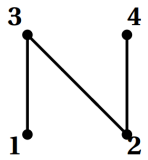
Definição 4.7 *Sejam $\mathbb{P}_1 = (X, \preceq_1)$ e $\mathbb{P}_2 = (X, \preceq_2)$ dois posets. Temos que $\mathbb{P}_1 \subseteq \mathbb{P}_2$ se, dados x_1, x_2 com $x_1 \preceq_1 x_2$ temos que $x_1 \preceq_2 x_2$.*

Uma representação gráfica dos posets, quando X é finito, é dado pelo **Diagrama de Hasse**. Dado um poset finito $(X, \preceq)$, os elementos de X são representados por vértices e as relações dos elementos por arestas, convencionando que um elemento $x \in X$ está abaixo de $y \in X$ se, e somente se, y cobre x.

Exemplo 4.8 *Seja $N = ([4], \preceq)$ o poset definido sobre $\{1, 2, 3, 4\}$ e com ordem*

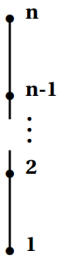
$$\preceq := \{1 \preceq 1, 2 \preceq 2, 3 \preceq 3, 4 \preceq 4, 1 \preceq 3, 2 \preceq 3, 2 \preceq 4\}$$

possui diagrama de Hasse dado por

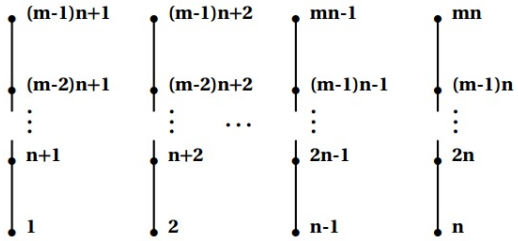


Definição 4.9 *Um poset $\mathbb{P}$, definido sobre $[n]$, com relação de ordem parcial $\preceq$ formada apenas pelas relações reflexivas dos elementos é dito **poset anticadeia** ou **poset de Hamming** e será denotado por $\mathbb{H}_n$. Este poset possui diagrama de Hasse dado por*

Definição 4.10 *Seja $n \in \mathbb{N}$. O poset $\mathbb{L}_n$, definido sobre $[n]$ com ordem total "$\leqslant$", é dito linear ou cadeia. Este poset possui diagrama de Hasse dado por*



Definição 4.11 *O poset **Niederreiter-Rosembloon-Tsfasman (NRT)** é definido com a união disjunta de posets totalmente ordenados de mesmo comprimento. Este poset possui diagrama de Hasse dado por:*



Seja $\mathbb{P} = ([n], \preceq)$ um poset finito de n elementos. Sempre podemos fixar uma numeração dos elementos de $\mathbb{P}$, digamos, $x_1, x_2, \ldots, x_n$; esta numeração fornece uma bijeção com $[n]$ e podemos supor, sem perda de generalidade, que $\mathbb{P} = ([n], \preceq)$. Dado um corpo $\mathbb{F}_q$, veremos a seguir que a ordem parcial em $[n]$ induz uma métrica em $\mathbb{F}_q^n$.

Sejam $\mathbb{P} = ([n], \preceq)$ um poset e $\mathbb{F}_q$ um corpo. O conjunto $[n]$ e as coordenadas de $x \in \mathbb{F}_q^n$ estão em correspondência biunívoca através da função f dada por $f(i) = x_i$. Devido este fato vamos definir a seguir o $\mathbb{P}$-peso de um elemento em $\mathbb{F}_q^n$.

Definição 4.12 *O $\mathbb{P}$-peso de um elemento $x \in \mathbb{F}_q^n$ é a **cardinalidade do ideal** de $\mathbb{P}$ gerado pelo suporte de x. Ou seja,*

$$w_{\mathbb{P}}(x) := |\langle supp(x) \rangle|$$

onde $supp(x) := \{i : x_i \neq 0\}$.

Exemplo 4.13 *Seja $x = (1,0,1,0) \in \mathbb{F}_2^4$, considere o poset de Hamming $\mathbb{H}_4$ e o poset N do Exemplo 4.8 sobre $[4]$. Então,*

$$w_{\mathbb{H}_4}((1,0,1,0)) = |\langle supp(x)\rangle_{\mathbb{H}_4}| = |\langle 1,3\rangle_{\mathbb{H}_4}| = |\{1,3\}| = 2.$$

$$w_N((1,0,1,0)) = |\langle supp(x)\rangle_N| = |\langle 1,3\rangle_N| = |\{1,2,3\}| = 3.$$

Note que $\langle supp(x)\rangle_{\mathbb{H}} = supp(x)$, ou seja, quando o poset considerado é o poset de Hamming então o $\mathbb{H}$-peso e o peso de Hamming equivalem.

Definição 4.14 *Defina a $\mathbb{P}$-distância por*

$$\begin{aligned} d_{\mathbb{P}} : \mathbb{F}_q^n \times \mathbb{F}_q^n &\longrightarrow \mathbb{N}_0 \\ (x,y) &\longmapsto w_{\mathbb{P}}(x-y) \end{aligned}$$

Teorema 4.15 *Se $\mathbb{P} = ([n], \preceq)$ é um poset, então a $\mathbb{P}$-distância é uma métrica em $\mathbb{F}_q^n$.*

Demonstração. Sejam $x, y, z \in \mathbb{F}_q^n$. Para mostrar a positividade, observe que a desigualdade $d_{\mathbb{P}}(x,y) \geqslant 0$ é válida pois, por definição a cardinalidade de um conjunto é sempre positiva, e essa é zero somente quando $x_i = y_i,\ \forall i$. A simetria segue do fato que $supp(x-y) = supp(y-x)$, portanto,

$$d_{\mathbb{P}}(x,y) = d_{\mathbb{P}}(y,x).$$

Agora,

$$\begin{aligned} d_{\mathbb{P}}(x,y) = w_{\mathbb{P}}(x-y) &\leqslant w_{\mathbb{P}}(x-z) + w_{\mathbb{P}}(z-y) \\ &= d_{\mathbb{P}}(x,z) + d_{\mathbb{P}}(z,y), \end{aligned}$$

pois $supp(x+y) \subseteq supp(x) \cup supp(y)$ e daí

$$\begin{aligned} w_{\mathbb{P}}(x+y) &\leqslant |\langle supp(x)\rangle_{\mathbb{P}} \cup \langle supp(y)\rangle_{\mathbb{P}}| \\ &\leqslant |\langle supp(x)\rangle_{\mathbb{P}}| + |\langle supp(y)\rangle_{\mathbb{P}}| \\ &= w_{\mathbb{P}}(x) + w_{\mathbb{P}}(y). \end{aligned}$$

□

4.2 Códigos Posets

Definição 4.16 *O par ordenado $(\mathbb{F}_q^n, d_{\mathbb{P}})$ é chamado de um espaço poset ou $\mathbb{P}$-espaço. Um subconjunto do espaço métrico $(\mathbb{F}_q^n, d_{\mathbb{P}})$ é chamado **Código poset**. Se $C \subseteq \mathbb{F}_q^n$ é um subespaço vetorial de dimensão k então, C é um $[n,k]$ $\mathbb{P}$-código linear.*

Definição 4.17 *Sejam $x \in \mathbb{F}_q^n$ e r um inteiro positivo. Definimos:*

i) A $\mathbb{P}$-bola de centro em x e raio r como sendo o conjunto

$$B_{\mathbb{P}}(x,r) := \left\{ y \in \mathbb{F}_q^n : d_{\mathbb{P}}(x,y) \leqslant r \right\};$$

ii) A $\mathbb{P}$-esfera de centro em x e raio r como sendo o conjunto

$$S_{\mathbb{P}}(x,r) := \left\{ y \in \mathbb{F}_q^n : d_{\mathbb{P}}(x,y) = r \right\}.$$

Lema 4.18 *O número de vetores em $\mathbb{F}_q^n$ cuja distância ao vetor nulo é exatamente i, é igual a*

$$\begin{cases} 1 & se \quad i = 0 \\ \displaystyle\sum_{j=1}^{i} (q-1)^j q^{i-j} \Omega_j(i) & se \quad i > 0 \end{cases} \tag{4.1}$$

onde $\Omega_j(i)$ é o número de ideais de $\mathbb{P}$ com cardinalidade i possuindo exatamente j elementos maximais.

Demonstração. Se $i = 0$ então, $S_{\mathbb{P}}(0,0) = \{0\}$ e então $|S_{\mathbb{P}}(0,0)| = 1$. Suponha que $i \geqslant 1$. Se $x \in S_{\mathbb{P}}(0,i)$ então $w_{\mathbb{P}}(x) = i$, ou seja, o ideal gerado pelo suporte de x possui i elementos. Portanto, sendo I um ideal de $\mathbb{P}$ tal que $|I| = i$, devemos encontrar quantos vetores $y \in \mathbb{F}_q^n$ satisfazem $\langle supp(y) \rangle = I$. Supondo que $|M(I)| = j$, temos que $1 \leqslant j \leqslant i$. Daí como $y = (y_1, \ldots, y_n)$, se y_s é tal que $s \in M(I)$ segue que $y_s \neq 0$. Logo existem $(q-1)$ escolhas para y_s e portanto $(q-1)^j$ escolhas para as posições coordenadas de $y \in \mathbb{F}_q^n$ indexadas pelos elementos maximais de I. Para as posições coordenadas de $y \in \mathbb{F}_q^n$ indexadas pelos elementos do conjunto $I - M(I)$ temos q^{i-j} escolhas. Como as demais coordenadas são nulas, temos $(q-1)^j q^{i-j}$ vetores de $y \in \mathbb{F}_q^n$ tais que $\langle supp(y) \rangle = I$. Ainda como temos $\Omega_j(i)$ ideais de $\mathbb{P}$ com cardinalidade i e possuindo j elementos maximais, teremos

$$S_{\mathbb{P}}(0,i) = \sum_{j=1}^{i} (q-1)^j q^{i-j} \Omega_j(i).$$

□

Do fato de $d_{\mathbb{P}}(x,y) = d_{\mathbb{P}}(0, x-y)$, para todos $x, y \in \mathbb{F}_q^n$, temos que o número de elementos na $\mathbb{P}$-bola de raio r não depende do centro e este número é:

$$1 + \sum_{i=1}^{r} \sum_{j=1}^{i} (q-1)^j q^{i-j} \Omega_j(i). \tag{4.2}$$

4.3 Códigos Posets Perfeitos

Seja $\mathbb{P}$ um poset com elementos $\{1, 2, \ldots, n\}$ e seja C um código em $\mathbb{F}_q^n$, onde as posições coordenadas são indexadas pelos elementos de $\mathbb{P}$. Então C é um $\mathbb{P}$-código perfeito se existe um inteiro r tal que as $\mathbb{P}$-bolas de raio r com centro nas palavras códigos de C são duas a duas disjuntas e a sua união é todo $\mathbb{F}_q^n$.

O próximo teorema nos dá uma caracterização dos posets $\mathbb{P}$-perfeitos no caso em que $\mathbb{P}$ é um poset do tipo cadeia. Na demonstração do teorema usaremos um resultado que nos dá a cardinalidade de uma $\mathbb{P}$-bola no caso em que $\mathbb{P}$ é do tipo cadeia. Neste trabalho enunciaremos este resultado como o seguinte lema.

Lema 4.19 *Seja $\mathbb{P}$ um poset do tipo cadeia. Então, cada $\mathbb{P}$-bola de raio r possui cardinalidade q^r.*

Demonstração. Pela Equação (4.2) temos que o número de elementos em uma $\mathbb{P}$-bola de raio r para um poset $\mathbb{P}$ qualquer é dado por

$$1 + \sum_{i=1}^{r} \sum_{j=1}^{i} (q-1)^j q^{i-j} \Omega_j(i)$$

que pode ser escrito como

$$1 + \sum_{i=1}^{r} (q-1)q^{i-1}\Omega_1(i) + (q-1)^2 q^{i-2}\Omega_2(i) + \cdots + (q-1)^i \Omega_i(i).$$

Porém $\Omega_1(i) = 1$ e $\Omega_j(i) = 0$ se $j \geqslant 2$, se $\mathbb{P}$ é um poset do tipo cadeia. Logo,

$$\begin{aligned}
|B_{\mathbb{P}}(0,r)| &= 1 + \sum_{i=1}^{r} (q-1)q^{i-1}\Omega_1(i) + (q-1)^2 q^{i-2}\Omega_2(i) + \cdots + (q-1)^i \Omega_i(i) \\
&= \sum_{i=1}^{r} (q-1)q^{i-1} \\
&= \sum_{i=1}^{r} q^i - q^{i-1} \\
&= 1 - q^0 + q^r \\
&= q^r.
\end{aligned}$$

Como o número de elementos em uma $\mathbb{P}$-bola não depende do centro escolhido temos o resultado desejado. □

Teorema 4.20 *Seja $\mathbb{P}$ um poset com elementos $\{1, 2, \ldots, n\}$ onde $1 \preceq 2 \preceq \cdots \preceq n$ e seja C um código em $\mathbb{F}_q^n$. Então C é um $\mathbb{P}$-código perfeito se, e somente se, existe um inteiro*

k, com $0 \leqslant k \leqslant n$, tal que $|C| = q^k$ e o conjunto de todos os vetores $(x_{n-k+1}, \ldots, x_n)$ tais que $(x_1, x_2, \ldots, x_{n-k}, x_{n-k+1}, \ldots, x_n) \in C$ para algum $(x_1, x_2, \ldots, , x_{n-k}) \in \mathbb{F}_q^{n-k}$ é igual a $\mathbb{F}_q^k$. Em particular, o código linear C_k de dimensão k consistindo de todos os vetores $(0, \ldots, 0, a_{n-k+1}, \ldots, a_n) \in \mathbb{F}_q^n$, das quais as $n-k$ primeiras coordenadas são nulas, é um $\mathbb{P}$-código perfeito com $\mathbb{P}$-distância mínima igual a $n-k+1$.

Demonstração.
$\Rightarrow$) Assuma que C é um $\mathbb{P}$-código perfeito. Seja r um inteiro tal que as $\mathbb{P}$-bolas de raio r sobre as palavras códigos de C são duas a duas disjuntas e sua união é $\mathbb{F}_q^n$. Pelo Lema 4.19 as $\mathbb{P}$-bolas de raio r possuem cardinalidade q^r e então $|C| = q^{n-r}$. Seja $y = (y_1, \ldots, y_n)$ um vetor em $\mathbb{F}_q^n$. Então existe uma (única) palavra código c tal que $y \in B_{\mathbb{P}}(c; r)$ e então a palavra código c é da forma $c = (c_1, \ldots, c_r, y_{r+1}, \ldots, y_n)$. Donde C possui a forma dada no teorema com $k = n - r$.
$\Leftarrow$) Temos que pelas definições estes códigos possuem cardinalidade q^k e $\mathbb{P}$-distância mínima $n-k+1$. Cada vetor $(y_1, \ldots, y_n) \in \mathbb{F}_q^n$ está contido na $\mathbb{P}$-bola de raio $n-k$ sobre alguma palavra código da forma $(x_1, \ldots, x_{n-k}, y_{n-k+1}, \ldots, y_n)$, porém não está contida na $\mathbb{P}$-bola de raio $n-k+1$ sobre qualquer outra palavra código. Donde C_k é um $\mathbb{P}$-código perfeito. □

Nosso interesse agora é classificar os $\mathbb{P}$-códigos perfeitos no caso em que $\mathbb{P}$ é um poset formado pela união de duas cadeias distintas de mesmo tamanho.

Teorema 4.21 *Seja $n = 2l$ um número inteiro par maior que zero. Seja $\mathbb{P}$ o poset consistindo de duas cadeias disjuntas N e N' de mesmo tamanho l. Então os únicos $\mathbb{P}$-códigos perfeitos em $\mathbb{F}_q^n$ são $C = \mathbb{F}_q^n$ e $C = \{x\}$ para qualquer $x \in \mathbb{F}_q^n$.*

Demonstração. Claramente $C = \mathbb{F}_q^n$ e $C = \{x\}$ são $\mathbb{P}$-códigos perfeitos. Vamos mostrar agora que não existe outro $\mathbb{P}$-código perfeito. Seja $N := \{1, 2, \ldots, l\}$, onde $1 \leq 2 \leq \cdots \leq l$, e $N' := \{1', 2', \ldots, l'\}$, onde $1' \leq 2' \leq \cdots \leq l'$. Suponha que existe $C \subseteq \mathbb{F}_q^n$ que é um $\mathbb{P}$-código perfeito e $1 \leq |C| \leq q^k$. Se r é o inteiro tal que as $\mathbb{P}$-bolas de raio r e centros nas palavras código de C são duas a duas disjuntas e cobrem $\mathbb{F}_q^{2l}$ então, $1 \leqslant r \leqslant 2l-1$. Primeiro assuma que $r \geqslant l$. Seja $x = (x_1, \ldots, x_l, x_{1'}, \ldots, x_{l'})$, $y = (y_1, \ldots, y_l, y_{1'}, \ldots, y_{l'})$ dois vetores quaisquer em $\mathbb{F}_q^{2l}$. Então o vetor $(x_1, \ldots, x_l, y_{1'}, \ldots, y_{l'}) \in B_{\mathbb{P}}(x; r) \cap B_{\mathbb{P}}(y; r)$. Em particular as $\mathbb{P}$-bolas de raio r sobre quaisquer duas palavras interceptam-se contradizendo o fato de C ser perfeito. Vamos calcular primeiro a cardinalidade das $\mathbb{P}$-bolas de raio r. Seja i um inteiro tal que $1 \leqslant i \leqslant l$. Por (4.2) o número de vetores que estão a uma distância i de um vetor fixo $x \in \mathbb{F}_q^n$ é

$$\alpha_i \;=\; 2(q-1)q^{i-1} + (i-1)(q-1)^2 q^{i-2}$$

$$= \quad (q-1)q^{i-2}\left[(i+1)q-i+1\right].$$

Logo, para cada vetor $x \in \mathbb{F}_q^n$ temos que

$$|B_{\mathbb{P}}(x;r)| = 1 + \sum_{i=1}^{r} \alpha_i$$

e assim, por indução temos

$$|B_{\mathbb{P}}(x;r)| = q^{r-1}\left[r(q-1)+q\right]$$

e como C é perfeito, $q^{2l} = |C|\,|B_{\mathbb{P}}(x;r)|$. Logo existe um inteiro j tal que $r(q-1)+q = q^j$ então,

$$|B_{\mathbb{P}}(x;r)| = q^{r+j-1}.$$

Além disso,

$$r = \frac{q^j - q}{q-1}$$

e como $r \geqslant 1$ temos $j \geqslant 2$. Então,

$$r = q(1+q+\ldots+q^{j-2}) \geqslant 2(j-1) \geqslant j.$$

Temos

$$|C| = q^{2l-r-j+1} = q^{2(l-r)+r-(j-1)}$$

e como $r > j-1$ temos que

$$|C| \geq q^{2(l-r)}.$$

Pelo princípio da casa dos pombos, existem duas palavras código $x = (x_1, \ldots, x_l, x_{1'}, \ldots, x_{l'})$ e $y = (y_1, \ldots, y_l, y_{1'}, \ldots, y_{l'})$ distintas tais que $x_i = y_i$ e $x_{i'} = y_{i'}$, para $i = r+1, \ldots, l$. Como o vetor $(x_1, \ldots, x_l, y_{1'}, \ldots, y_{l'}) \in B_{\mathbb{P}}(x;r) \cap B_{\mathbb{P}}(y;r)$, as $\mathbb{P}$-bolas de raio r sobre as palavras código x e y interceptam-se. Contradizendo novamente o fato de C ser $\mathbb{P}$-perfeito. □

Definição 4.22 *Seja $\mathbb{P}$ um poset em $[n]$. Vamos denotar por $\mathcal{I}(\mathbb{P})$ o conjunto dos ideais de $\mathbb{P}$ e por $\mathcal{I}^r(\mathbb{P})$ o conjunto dos ideais de $\mathbb{P}$ que possuem cardinalidade r.*

Proposição 4.23 *Com as notações da Definição 4.22, segue-se que*

i) Se $0 \leqslant s \leqslant r \leqslant n$ e $I \in \mathcal{I}^r(\mathbb{P})$, então existe $J \in \mathcal{I}^s(\mathbb{P})$ tal que $J \subseteq I$;

ii) Se $0 \leqslant r \leqslant s \leqslant n$ e $I \in \mathcal{I}^r(\mathbb{P})$, então existe $J \in \mathcal{I}^s(\mathbb{P})$ tal que $I \subseteq J$.

Demonstração.

i) Basta considerarmos o caso em que $s = r - 1$, pois se $s = r - t$, realizando o processo da demonstração $t - 1$ vezes teremos o resultado desejado. Se $s = r - 1$, seja j um elemento maximal de I. Note que $J = I - \{j\}$ é um ideal de $\mathbb{P}$ já que I é um ideal e retiramos apenas um elemento maximal de I. Portanto $J \subseteq I$ com $|J| = r - 1$.

ii) Novamente basta considerarmos o caso em que $s = r + 1$, pois se $s = r + t$, realizando o processo da demonstração $t - 1$ vezes que teremos o resultado desejado. Se $s = r + 1$, seja $j \in I^c = \mathbb{P} - I$ um elemento minimal. Defina $J = I \cup \{j\}$ e assim definido J é um ideal em $\mathbb{P}$. De fato, dados $x \in \mathbb{P}$ e $y \in J$ com $x \preceq y$, se $y \in I$, então $x \in I$ pois I é um ideal e se $y = j$ com $x \preceq y$, então $x \notin I^c$, pois j é minimal de I^c. Logo $x \in I$. Portanto J é um ideal de $\mathbb{P}$ e além disso $I \subseteq J$ com $|J| = r + 1$. □

Definição 4.24 *Dado um poset $\mathbb{P}$ definimos o poset dual de $\mathbb{P}$ como sendo o poset $\mathbb{P}^*$ tal que $\mathbb{P}$ e $\mathbb{P}^*$ estão definidos sobre o mesmo conjunto e*

$$x \leqslant y \; em \; \mathbb{P} \Longleftrightarrow y \leqslant x \; em \; \mathbb{P}^*.$$

Lema 4.25 *Sejam $\mathbb{P}$ um poset em $[n]$ e $\mathbb{P}^*$ seu poset dual. Então os ideais de $\mathbb{P}^*$ são precisamente os complementares dos ideais de $\mathbb{P}$. Isto é, $\mathcal{I}(\mathbb{P}^*) := \{I^c : I \in \mathcal{I}(\mathbb{P})\}$.*

Demonstração. Dado um ideal I de $\mathbb{P}$, mostraremos que I^c é um ideal de $\mathbb{P}^*$. De fato, seja $x \in I^c$ e $y \in \mathbb{P}^*$ tais que $y \leqslant x$. Pela definição de $\mathbb{P}^*$ temos que $x \leqslant y$ em $\mathbb{P}$ donde, $y \notin I$ do contrário $x \in I$. Assim, $y \in I^c$ provando que $I^c \in \mathcal{I}(\mathbb{P}^*)$.

Deste modo, para um ideal $I \in \mathcal{I}(\mathbb{P}^*)$ temos que o ideal $I^c \in \mathcal{I}((\mathbb{P}^*)^*) = \mathcal{I}(\mathbb{P})$, portanto, I é o complementar de um ideal de $\mathbb{P}$. □

Os dois próximos resultados aparecerão nas demonstrações de alguns dos resultados mais importantes deste capítulo.

Lema 4.26 *Para um conjunto finito A e um subconjunto C de A temos*

$$\sum_{C \subseteq B \subseteq A} (-1)^{|B|} = \begin{cases} (-1)^{|A|} & se \quad C = A; \\ 0 & se \quad C \neq A. \end{cases}$$

Demonstração. *No caso em que $C = A$ teremos apenas uma parcela na soma, a saber, $B = A$, então temos que*

$$\sum_{C \subseteq B \subseteq A} (-1)^{|B|} = (-1)^{|A|}.$$

Agora se $C \neq A$, temos que $B = B' \cup C$ onde $B' \subseteq A'$; $A' = A - C$. Assim

$$\sum_{C \subseteq B \subseteq A} (-1)^{|B|} = (-1)^{|C|} \sum_{B' \subseteq A'} (-1)^{|B'|}$$

porém,

$$\sum_{B' \subseteq A'} (-1)^{|B'|} = \sum_{k=0}^{|A'|} \left(\sum_{B' \subseteq A'; |B'|=k} (-1)^k \right) = \sum_{k=0}^{|A'|} (-1)^k \begin{pmatrix} |A'| \\ k \end{pmatrix} = 0$$

provando que

$$\sum_{C \subseteq B \subseteq A} (-1)^{|B|} = 0.$$

□

Proposição 4.27 *(Fórmula da Inversão de Mobius). Sejam X um conjunto finito, $P(X)$ o conjunto dos subconjuntos de X e considere f, g funções de $P(X)$ em um anel Λ. Então*

$$f(A) = \sum_{B \subseteq A} g(B) \qquad (A \subseteq X)$$

se, e somente se,

$$g(A) = \sum_{B \subseteq A} (-1)^{|A|-|B|} f(B) \qquad (A \subseteq X).$$

Demonstração. Para a implicação

$$f(A) = \sum_{B \subseteq A} g(B) \qquad (A \subseteq X) \Longrightarrow g(A) = \sum_{B \subseteq A} (-1)^{|A|-|B|} f(B) \qquad (A \subseteq X)$$

veja [15]. Mostraremos aqui a recíproca.

Suponha que $g(A) = \sum_{B \subseteq A} (-1)^{|A|-|B|} f(B) \qquad (A \subseteq X)$. Então pelo Lema 4.26 temos que

$$\begin{aligned} \sum_{B \subseteq A} g(B) &= \sum_{B \subseteq A} \sum_{C \subseteq B} (-1)^{|B|-|C|} f(C) \\ &= \sum_{C \subsetneq A} (-1)^{-|C|} \left(\sum_{C \subseteq B \subseteq A} (-1)^{|B|} \right) f(C) + (-1)^{|A|}(-1)^{|A|} f(A) \\ &= f(A). \end{aligned}$$

□

4.4 Códigos Posets MDS e Códigos I-Perfeitos

Proposição 4.28 *(Limitante de Singleton para códigos posets). Sejam $\mathbb{P}$ um poset em $[n]$ e $C(\subseteq \mathbb{F}_q^n)$ um $\mathbb{P}$-código. Então*

$$|C| \leqslant q^{n-d_{\mathbb{P}}(C)+1}$$

Demonstração. Escolha duas palavras código $x, y \in C$ tais que, $d_{\mathbb{P}}(x, y) = d_{\mathbb{P}}(C)$. Sendo I o ideal gerado por $supp(x - y)$ temos que

$$|supp(x - y)| = |I| = d_{\mathbb{P}}(c).$$

Pela Proposição 4.23 existe um ideal J de cardinalidade $d_{\mathbb{P}}(C) - 1$ que está contido em I. Duas palavras códigos de C nunca coincidem em todos os pontos fora de J, pois caso contrário sua distância seria menor do que a distância mínima de C. Isto prova que existe uma função injetiva de C para $\mathbb{F}_q^{n-d_{\mathbb{P}}(C)+1}$ e daí, vale o resultado. □

A função f da proposição pode ser definida ordenando os índices das coordenadas dos elementos de C sem perda de generalidade de modo que,

$$\begin{aligned} f : C &\longrightarrow \mathbb{F}_q^{n-d_{\mathbb{P}}(C)+1} \\ (x_1, \ldots, x_n) &\longmapsto (x_1, \ldots, x_{n-d_{\mathbb{P}(C)}+1}). \end{aligned}$$

Corolário 4.29 *Seja C um $[n, k]_q$ $\mathbb{P}$-código. Então*

$$d_{\mathbb{P}}(C) \leqslant n - k + 1. \tag{4.3}$$

Definição 4.30 *Seja $\mathbb{P}$ um poset em $[n]$. Um código linear C sobre $\mathbb{F}_q^n$ é dito $\mathbb{P}$-código de Maximun distance separable (ou $\mathbb{P}$-código MDS) se este atinge a identidade de Singleton. Consequentemente um $[n, k]_q$ $\mathbb{P}$-código é MDS se, e somente se, $d_{\mathbb{P}}(C) = n - k + 1$.*

Definição 4.31 *Sejam $\mathbb{P}$ um poset em $[n]$, I um ideal de $\mathbb{P}$. Para $u \in \mathbb{F}_q^n$ definimos a I-bola (respectivamente, I-esfera) com centro em u como o conjunto:*

$$B_I(u) := \left\{ v \in \mathbb{F}_q^n : \langle supp(u - v) \rangle \subseteq I \right\}.$$

$$S_I(u) := \left\{ v \in \mathbb{F}_q^n : \langle supp(u - v) \rangle = I \right\}.$$

A I-bola (respectivamente, I-esfera) centrada na origem é denotada por B_I (S_I).

Proposição 4.32 *Sejam $\mathbb{P}$ um poset em $[n]$ e I um ideal de $\mathbb{P}$. Então*

i) B_I *é um subespaço de* $\mathbb{F}_q^n$ *de dimensão* $|I|$*;*

ii) Para $u \in \mathbb{F}_q^n$*,* $B_I(u)$ *é a classe lateral de* B_I *contendo* u*, isto é,*$B_I(u) = u + B_I$*;*

iii) Para $u, v \in \mathbb{F}_q^n$ *duas* I*-bolas* $B_I(u)$ *e* $B_I(v)$ *são idênticas ou disjuntas. Além disso,*

$$B_I(u) = B_I(v) \iff supp(u - v) \subseteq I;$$

iv) O espaço $\mathbb{F}_q^n$ *é particionado em* I*-bolas.*

Demonstração.

i) Sejam, u, v dois vetores em B_I isto é, $\langle supp(u)\rangle \subseteq I$ e $\langle supp(v)\rangle \subseteq I$. Assim,

$$\langle supp(u+v)\rangle \subseteq \langle supp(u)\rangle \cup \langle supp(v)\rangle \subseteq I \cup I = I$$

então $u + v \in B_I$. Sejam $u \in B_I$ e $\alpha \in \mathbb{F}_q$. Então é claro que $\alpha u \in B_I$, e isto prova que B_I é subespaço de $\mathbb{F}_q^n$. Claramente $\{e_i\}_{i\in I}$ forma uma base para B_I, onde $e_i = (0, \ldots, 1, \ldots, 0)$ com 1 na i-ésima coordenada.

ii) Se $v \in B_I(u)$ então $\langle supp(u - v)\rangle \subseteq I$. Daí, $u - v \in B_I$ e $v = u + (v - u) \in u + B_I$. Agora para $w \in B_I$, $\langle supp(u - (u + w))\rangle = \langle supp(-w)\rangle = \langle supp(w)\rangle \in I$ então, $u + w \in B_I(u)$, e isto prova que $B_I(u) = u + B_I$.
Os itens $iii)$ e $iv)$ são safisfeitos por $ii)$.

□

Definição 4.33 *Sejam* $\mathbb{P}$ *um poset em* $[n]$ *e* I *um ideal de* $\mathbb{P}$*. Um* $\mathbb{P}$*-código linear* C *sobre* $\mathbb{F}_q$ *de tamanho* n *é dito* I*-perfeito se as* I*-bolas de centro nas palavras códigos de* C *são duas a duas disjuntas e sua união é todo o* $\mathbb{F}_q^n$*.*

Propriedade 4.34 *Se* C *é um* $[n, k]_q$ *código poset e* C *é* I*-perfeito então o ideal* I *possui cardinalidade* $n - k$*.*

Demonstração. De fato, temos que

$$\begin{aligned} q^n = \left|\mathbb{F}_q^n\right| &= \left|\bigcup_{x\in C} B_I(x)\right| \\ &= |C|\,|I| \\ &= q^k\,|I|\,. \end{aligned}$$

Donde, $|I| = q^{n-k}$.

□

Propriedade 4.35 *A $\mathbb{P}$-bola de raio r pode ser representada em forma de I-bolas do seguinte modo, para $u \in \mathbb{F}_q^n$*

$$B_{r,\mathbb{P}}(u) = \bigcup_{I \in \mathcal{I}^r(\mathbb{P})} B_{I,\mathbb{P}}(u).$$

Demonstração. Seja $v \in B_{r,\mathbb{P}}(u)$ então por definição $d_{\mathbb{P}}(u,v) = |\langle supp(u-v)\rangle| \leqslant r$. Pela Proposição 4.23 existe um ideal $I \in \mathcal{I}^r(\mathbb{P})$ tal que $\langle supp(u-v)\rangle \subseteq I$ provando que $v \in B_{I,\mathbb{P}}(u)$. Portanto,

$$B_{r,\mathbb{P}}(u) \subseteq \bigcup_{I \in \mathcal{I}^r(\mathbb{P})} B_{I,\mathbb{P}}(u).$$

Por outro lado, se $v \in \bigcup_{I \in \mathcal{I}^r(\mathbb{P})} B_{I,\mathbb{P}}(u)$ existe $I \in \mathcal{I}^r(\mathbb{P})$ tal que $v \in B_{I,\mathbb{P}}(u)$ e então por definição $\langle supp(u-v)\rangle \subseteq I$ implicando que $|\langle supp(u-v)\rangle| \leqslant |I| = r$ donde $v \in B_{r,\mathbb{P}}(u)$. Portanto,

$$\bigcup_{I \in \mathcal{I}^r(\mathbb{P})} B_{I,\mathbb{P}}(u) \subseteq B_{r,\mathbb{P}}(u).$$

Assim vale a igualdade. □

Lema 4.36 *Sejam $\mathbb{P}$ um poset em $[n]$ e u, v dois vetores em $\mathbb{F}_q^n$. Então u, v pertencem a mesma I-bola para algum I de cardinalidade "s"se, e somente se, $d_{\mathbb{P}}(u,v) \leqslant s$.*

Demonstração. Sejam I um ideal de $\mathbb{P}$, com $|I| = s$, e $u, v \in B_I$. Temos que $u - v \in B_I$, pois B_I é um subespaço de $\mathbb{F}_q^n$. Assim

$$\langle supp(u-v)\rangle \subseteq I \Longrightarrow d_{\mathbb{P}}(u,v) = |\langle supp(u-v)\rangle| \leqslant |I| = s.$$

Reciprocamente, $d_{\mathbb{P}}(u,v) \leqslant s$ se, e somente se, $|\langle supp(u-v)\rangle| \leqslant s$. Agora como $\langle supp(u-v)\rangle$ é o menor ideal de $\mathbb{P}$ contendo $supp(u-v)$, assim, pela Proposição 4.23 existe um ideal $J \subseteq \mathbb{P}$ tal que $|J| = s$ e $\langle supp(u-v)\rangle \subseteq J$. Portanto, $v \in B_J(u)$. □

Teorema 4.37 *Sejam $\mathbb{P}$ um poset em $[n]$ e C um $[n,k]_q$ $\mathbb{P}$-código. Então C é um $\mathbb{P}$-código MDS se, e somente se, C é um $\mathbb{P}$-código I-perfeito para todo $I \in \mathcal{I}^{n-k}(\mathbb{P})$.*

Demonstração. Seja C um $\mathbb{P}$-código MDS de dimensão k. Então $d_{\mathbb{P}}(C) = n-k+1$. Escolha um ideal qualquer I com cardinalidade $n-k$. Pela Proposição 4.32 $iv)$, $\mathbb{F}_q^n$ pode ser particionado em I-bolas. O número de I-bolas nesta partição é $q^{n-|I|} = q^k = |C|$. Agora pelo fato de $d_{\mathbb{P}}(u,v) \geqslant n-k+1 > |I|$, $\forall u, v \in C$, temos pela Proposição 4.32 $iii)$ que $B_I(u) \cap B_I(v) = \emptyset$. Então, $\bigcup_{u \in C} B_I(u)$ é uma união disjunta que contém $|C|\, q^{|I|} = q^k q^{n-k} = q^n$ elementos, ou seja, $\bigcup_{u \in C} B_I(u) = \mathbb{F}_q^n$, e logo C é I-perfeito.

Suponha agora que C é I-perfeito para todo ideal I de cardinalidade $n-k$. Suponha que existem duas palavras código distintas $u, v \in C$ tais que $d_{\mathbb{P}}(C) \leqslant n-k$. Pelo Lema 4.36 u e v estão na mesma J-bola para algum ideal J de cardinalidade $\leqslant n-k$. Pela Proposição 4.23 existe um ideal I de cardinalidade $n-k$ que contém J. Então u, v estão na mesma I-bola. Assim C não poderá ser I-perfeito, isto é, uma contradição. O que prova que, $d_{\mathbb{P}}(C) > n-k$ e juntamente com Limitante de Singleton para posets temos $d_{\mathbb{P}}(C) = n-k+1$ ou seja, C é MDS. □

4.5 Distribuição de Pesos de um Código Poset

Seja $\mathbb{P}$ um poset em $[n]$ e C um $\mathbb{P}$-código de tamanho n sobre $\mathbb{F}_q$. O número de palavras código de $\mathbb{P}$-peso r é denotado por $A_{r,\mathbb{P}}(C)$ isto é,

$$\begin{aligned} A_{r,\mathbb{P}}(C) &= |\{u \in C \text{ tal que } w_{\mathbb{P}}(u) = r\}| \\ &= |S_{r,\mathbb{P}} \cap C| \,. \end{aligned}$$

Dizemos que o conjunto $\{A_{0,\mathbb{P}}, A_{1,\mathbb{P}}, \ldots, A_{n,\mathbb{P}}\}$ é o conjunto de distribuição de $\mathbb{P}$-pesos de C.

Proposição 4.38 *Sejam $\mathbb{P}$ um poset em $[n]$ e C um $[n,k]_q$ $\mathbb{P}$-código MDS. Então para um ideal I de $\mathbb{P}$ e $u \in \mathbb{F}_q^n$, o número de palavras código de C na I-bola $B_I(u)$ é dado por*

$$|B_I(u) \cap C| = \begin{cases} q^{|I|-n+k} & se \quad |I| > n-k, \\ 0 \text{ ou } 1 & se \quad |I| \leqslant n-k \end{cases}.$$

Demonstração. Seja I um ideal de $\mathbb{P}$ com cardinalidade s. Se $s < n-k$ então pelo Lema 4.36 toda I-bola centrada na origem não contém palavras códigos de C, exceto a palavra código nula.Como $B_I(u) = u + B_I$, temos que $B_I(u)$ contém uma palavra código se $u \in C$ ou $B_I(u)$ não contém palavra código de C se $u \notin C$. Se $s = n-k$, pelo Teorema 4.37, toda I-bola contém uma única palavra código de C. Agora assuma que $s > n-k$. Pela Proposição 4.23, I contém um ideal J, de cardinalidade $n-k$. Como B_J é um subespaço de B_I de codimensão $|I|-|J|$, o número de classes de B_J em B_I é $q^{|I|-|J|}$. Fixado $u \in \mathbb{F}_q^n$, a I-bola $B_I(u)$ contém $q^{|I|-|J|}$ classes de B_J e, como C é J-perfeito, segue do Teorema 4.37 que cada classe de B_J contém exatamente uma palavra código de C e, portanto, que $B_I(u)$ contém $q^{|I|-n+k}$ palavras código de C. □

Dado um ideal $I \subseteq \mathbb{P}$ onde $\mathbb{P}$ é um poset denotaremos por I_M o conjunto $I - M(I)$, ou seja, os elementos de I que não são maximais. Seja $\mathcal{J}(I) := \{J : I_M \subseteq J \subseteq I\}$ assim

definido temos que $\mathcal{J}(I) \subset \mathcal{I}(\mathbb{P})$. Seja agora, $\chi(E|-) : \mathbb{F}_q^n \mapsto \{0,1\}$ a função indicadora de um subconjunto dado E de $\mathbb{F}_q^n$, isto é,

$$\chi(E|x) = \begin{cases} 1 & se\ x \in E \\ 0 & se\ x \notin E \end{cases}.$$

Para qualquer subconjunto A de um poset $\mathbb{P}$ e para qualquer vetor $u \in \mathbb{F}_q^n$, definimos os subconjuntos $B_{A^\vee}(u)$ e $S_{A^\vee}(u)$ de $\mathbb{F}_q^n$ por,

$$B_{A^\vee}(u) := \left\{v \in \mathbb{F}_q^n : supp(u-v) \subseteq A\right\},$$

$$S_{A^\vee}(u) := \left\{v \in \mathbb{F}_q^n : supp(u-v) = A\right\}.$$

Lema 4.39 *Sejam A um subconjunto de um poset $\mathbb{P}$ e I um ideal de $\mathbb{P}$. Então temos,*

i)

$$\chi(S_{A^\vee}|x) = \sum_{E\subseteq A}(-1)^{|A|-|E|}\chi(B_{E^\vee}|x);$$

ii)

$$\chi(S_I|x) = \sum_{J\in\mathcal{J}(I)}(-1)^{|I|-|J|}\chi(B_J|x).$$

Demonstração.

i) Por definição temos que

$$\chi(B_{A^\vee}|x) = \sum_{E\subseteq A}\chi(S_{E^\vee}|x).$$

Aplicando a Formula de Mobius 4.27 teremos

$$\chi(B_{A^\vee}|x) = \sum_{E\subseteq A}\chi(S_{E^\vee}|x) \Longleftrightarrow \chi(S_{A^\vee}|x) = \sum_{E\subseteq A}(-1)^{|A|-|E|}\chi(B_{E^\vee}|x).$$

ii) Observe que,

$$\chi(S_I|x) = 1 \Longleftrightarrow \langle supp(x)\rangle = I \Longleftrightarrow M(I) \subseteq supp(x) \subseteq I.$$

Disto segue que,

$$\begin{aligned}
\chi(S_I|x) &= \sum_{M(I)\subseteq A\subseteq I}\chi(S_{A^\vee}|x) \\
&= \sum_{M(I)\subseteq A\subseteq I}\sum_{E\subseteq A}(-1)^{|A|-|E|}\chi(B_{E^\vee}|x) \\
&= \sum_{E\subseteq I}(-1)^{-|E|}\chi(B_{E^\vee}|x)\sum_{M(I)\cup E\subseteq A\subseteq I}(-1)^{|A|}
\end{aligned}$$

Onde na penúltima igualdade utilizamos $i)$ e pelo Lema 4.26 a última soma vale

$$\sum_{M(I)\cup E\subseteq A\subseteq I}(-1)^{|A|}=\begin{cases}(-1)^{|I|} & se \quad M(I)\cup E=I\\ 0 & se \quad M(I)\cup E\neq I\end{cases}$$

e como $M(I)\cup E=I\iff I_M\subseteq E\subseteq I\iff E\in\mathcal{J}(I)$, temos o resultado procurado.

□

Teorema 4.40 *Sejam $\mathbb{P}$ um poset em $[n]$ e C um $[n,k,d_{\mathbb{P}}]_q$ $\mathbb{P}$-código. Suponha que C é MDS então*

$$A_{r,\mathbb{P}}(C)=\begin{cases}1 & se \quad r=0\\ 0 & se \quad 1\leqslant r\leqslant d_{\mathbb{P}}-1\\ (q-1)\sum\limits_{I\in\mathcal{I}^r(\mathbb{P})}\sum\limits_{j=0}^{r-d_{\mathbb{P}}}(-1)^j\begin{pmatrix}|M(I)|-1\\ j\end{pmatrix}q^{r-d_{\mathbb{P}}-j} & se \quad r\geqslant d_{\mathbb{P}}\end{cases}.$$

Demonstração. Se $r\leqslant d_{\mathbb{P}}-1$, então o resultado é trivial. Assuma então que, $r\geqslant d_{\mathbb{P}}$. Note que,

$$A_{r,\mathbb{P}}(C)=\sum_{I\in\mathcal{I}^r(\mathbb{P})}|S_I\cap C|$$

onde S_I denota a I-esfera de centro na origem. Vamos agora calcular o número de elementos em $S_I\cap C$ para $I\in\mathcal{I}^r(\mathbb{P})$,

$$\begin{aligned}|S_I\cap C| &= \sum_{x\in C}\chi(S_I|x)\\ &= \sum_{x\in C}\sum_{J\in\mathcal{J}(I)}(-1)^{|I|-|J|}\chi(B_J|x)\\ &= \sum_{J\in\mathcal{J}(I)}(-1)^{|I|-|J|}\,|B_J\cap C|\,.\end{aligned}$$

onde na segunda igualdade utilizamos o Lema 4.39. Uma vez que cada ideal $J\in\mathcal{J}(I)$ contém todos os elementos em I_M, bem como alguns elementos maximais de I, temos

$$|I|=|I_M|+|M(I)| \qquad e \qquad |J|=|I_M|+l$$

para algum $0\leqslant l\leqslant|M(I)|$. O número de ideais $J\in\mathcal{J}(I)$ de cardinalidade $|I_M|+l$ é claramente $\binom{|M(I)|}{l}$, e com isso temos

$$|S_I\cap C|=\sum_{l=0}^{|M(I)|}(-1)^{|M(I)|+l}\begin{pmatrix}|M(I)|\\ l\end{pmatrix}|B_J\cap C|\,. \tag{4.4}$$

Pela Proposição 4.38 temos

$$|B_J \cap C| = \begin{cases} 1 & se \quad |J| \leqslant n-k \\ q^{|J|-d_{\mathbb{P}}+1} & se \quad |J| \geqslant n-k+1. \end{cases} \tag{4.5}$$

Assim substituindo (4.5) em (4.4) obtemos

$$|S_I \cap C| = \sum_{l=0}^{n-k-|I_M|} (-1)^{|M(I)|+l} \begin{pmatrix} |M(I)| \\ l \end{pmatrix} + \sum_{l=n-k-|I_M|+1}^{|M(I)|} (-1)^{|M(I)|+l} \begin{pmatrix} |M(I)| \\ l \end{pmatrix} q^{|I_M|+l-(n-k)}. \tag{4.6}$$

e pelo fato de que $\sum_{l=0}^{n}(-1)^l \begin{pmatrix} n \\ l \end{pmatrix} = 0$ temos,

$$\sum_{l=0}^{n-k-|I_M|} (-1)^{|M(I)|+l} \begin{pmatrix} |M(I)| \\ l \end{pmatrix} = - \sum_{l=n-k-|I_M|+1}^{|M(I)|} (-1)^{|M(I)|+l} \begin{pmatrix} |M(I)| \\ l \end{pmatrix}. \tag{4.7}$$

Agora substituindo (4.7) em (4.6) obtemos,

$$\begin{aligned} |S_I \cap C| &= \sum_{l=d_{\mathbb{P}}-|I_M|}^{|M(I)|} (-1)^{|M(I)|+l} \begin{pmatrix} |M(I)| \\ l \end{pmatrix} (q^{|I_M|+l-d_{\mathbb{P}}+1} - 1) \\ &= \sum_{r=0}^{|I|-d_{\mathbb{P}}} (-1)^{|I|+r+d_{\mathbb{P}}} \begin{pmatrix} |M(I)| \\ r+d_{\mathbb{P}}-|I_M| \end{pmatrix} (q^{r+1} - 1) \\ &= \sum_{j=0}^{|I|-d_{\mathbb{P}}} (-1)^{j} \begin{pmatrix} |M(I)| \\ j \end{pmatrix} (q^{|I|-d_{\mathbb{P}}+1-j} - 1) \\ &= \sum_{j=0}^{|I|-d_{\mathbb{P}}} (-1)^{j} \left[\begin{pmatrix} |M(I)|-1 \\ j \end{pmatrix} + \begin{pmatrix} |M(I)|-1 \\ j-1 \end{pmatrix} \right] (q^{|I|-d_{\mathbb{P}}+1-j} - 1) \\ &= (q-1) \sum_{j=0}^{|I|-d_{\mathbb{P}}} (-1)^{j} \begin{pmatrix} |M(I)|-1 \\ j \end{pmatrix} q^{|I|-d_{\mathbb{P}}-j}. \end{aligned}$$

onde na segunda igualdade fizemos a mudança de variável $r = l - d_{\mathbb{P}} - |I_M|$ e na terceira igualdade fizemos $|I| - d_{\mathbb{P}} - r = j$. E a útima igualdade resulta do fato que $\binom{|M(I)|-1}{j-1} = \binom{|M(I)|-1}{k}$ onde $k = j-1$. Agora somando sobre todos os ideais com $|I| = r$, finalmente obtemos o resultado desejado. □

Vamos agora aplicar o Teorema 4.40 para um poset $\mathbb{P}$ do tipo Niederreiter-Rosenbloom-Tsfasman, ou seja, onde $\mathbb{P}$ é a união disjunta de n cadeias de comprimento s, para obter fórmulas concretas para distribuição de peso. Antes de afirmar o próximo teorema precisamos de uma definição adicional. Definimos,

$$\sigma_s(l,r) := \left|\left\{(a_1,\ldots,a_l) \in \mathbb{N}^l : a_1 + a_2 + \cdots + a_l = r, 0 < a_i \leqslant s, 1 \leqslant l \leqslant n\right\}\right|. \tag{4.8}$$

Note que se $\mathbb{P}$ é a soma de n cadeias C_j, onde cada cadeia possui comprimento s, então o número de ideais de cardinalidade r e com l elementos maximais é $\begin{pmatrix} n \\ l \end{pmatrix} \sigma_s(l,r)$. De fato, como temos l elementos maximais e de cada cadeia C_j que compõe $\mathbb{P}$ pode-se escolher no maximo um elemento para ser um elemento maximal de algum ideal, existem $\begin{pmatrix} n \\ l \end{pmatrix}$ escolhas possiveis para os elementos maximais. Agora para cada C_j da qual se escolheu um elemento a_i para ser maximal temos obrigatóriamente que todos os elementos desta cadeia que estão abaixo de a_i também pertencem ao ideal, ou seja, desta cadeia existem a_i elementos no ideal, com $0 < a_i \leqslant s$ e como a cardinalidade do ideal é r devemos ter $a_1 + \cdots + a_l = r$. Provando que existem $\begin{pmatrix} n \\ l \end{pmatrix} \sigma_s(l,r)$ ideais de cardinalidade r e l elementos maximais.

Proposição 4.41 *Sejam $\mathbb{P}$ a união disjunta de n cadeias de comprimento s e C um $[n,k,d_{\mathbb{P}}]_q$ $\mathbb{P}$-código MDS. Então o número de palavras código de $\mathbb{P}$-peso r é dado por*

$$A_{r,\mathbb{P}}(C) = \begin{cases} 1 & se \quad r = 0 \\ 0 & se \quad 1 \leqslant r \leqslant d_{\mathbb{P}} - 1 \\ (q-1)\displaystyle\sum_{l=1}^{n} \begin{pmatrix} n \\ l \end{pmatrix} \sigma_s(l,r) \sum_{j=0}^{r-d_{\mathbb{P}}} (-1)^j \begin{pmatrix} l-1 \\ j \end{pmatrix} q^{r-d_{\mathbb{P}}-j} & se \quad r \geqslant d_{\mathbb{P}} \end{cases}.$$

Demonstração. Se $r \leqslant d_{\mathbb{P}} - 1$ é trivial. Suponha $r \geqslant d_{\mathbb{P}}$. Pelo Teorema 4.40

$$A_{r,\mathbb{P}}(C) = (q-1) \sum_{I \in \mathcal{I}^r(\mathbb{P})} \sum_{j=0}^{r-d_{\mathbb{P}}} (-1)^j \begin{pmatrix} |M(I)| - 1 \\ j \end{pmatrix} q^{r-d_{\mathbb{P}}-j}$$

mas, como vimos acima o número de ideais de $\mathbb{P}$ possuindo cardinalidade r e com l elementos maximais é $\begin{pmatrix} n \\ l \end{pmatrix} \sigma_s(l,r)$. Logo a soma em todos os ideais de cardinalidade r pode ser substituída por $\displaystyle\sum_{l=1}^{n} \begin{pmatrix} n \\ l \end{pmatrix} \sigma_s(l,r)$ e temos

$$A_{r,\mathbb{P}}(C) = (q-1) \sum_{l=1}^{n} \begin{pmatrix} n \\ l \end{pmatrix} \sigma_s(l,r) \sum_{j=0}^{r-d_{\mathbb{P}}} (-1)^j \begin{pmatrix} l-1 \\ j \end{pmatrix} q^{r-d_{\mathbb{P}}-j}.$$

□

Corolário 4.42 *Seja C um $[n,k,d_{\mathbb{H}} = n-k+1]_q$-código MDS. Então o número de palavras código de peso de Hamming $r (r \geqslant d_{\mathbb{H}})$ é dado por*

$$A_r(C) = (q-1) \begin{pmatrix} n \\ r \end{pmatrix} \sum_{j=0}^{r-d_{\mathbb{H}}} (-1)^j \begin{pmatrix} r-1 \\ j \end{pmatrix} q^{r-d_{\mathbb{H}}-j}.$$

Demonstração. Fazendo $s = 1$ na Proposição 4.41, temos que nosso poset é anti-cadeia de cardinalidade n, e a métrica NRT coincide com a métrica de Hamming. Note que neste caso $\sigma_s(l,r) = 1$ se $l = r$ e $\sigma_s(l,r) = 0$ se $l \neq r$ assim,

$$\begin{aligned} A_{r,\mathbb{H}}(C) &= (q-1)\sum_{l=1}^{n}\begin{pmatrix} n \\ l \end{pmatrix}\sigma_1(l,r)\sum_{j=0}^{r-d_{\mathbb{H}}}(-1)^j\begin{pmatrix} l-1 \\ j \end{pmatrix}q^{r-d_{\mathbb{H}}-j} \\ &= (q-1)\begin{pmatrix} n \\ r \end{pmatrix}\sum_{j=0}^{r-d_{\mathbb{H}}}(-1)^j\begin{pmatrix} r-1 \\ j \end{pmatrix}q^{r-d_{\mathbb{H}}-j}. \end{aligned}$$

□

Corolário 4.43 *Seja $\mathbb{P}$ uma cadeia de cardinalidade s e C um $[n,k,d_{\mathbb{P}}]_q$-código MDS. Então o número de palavras código de $\mathbb{P}$-peso $r(r \geqslant d_{\mathbb{P}} = n-k+1)$ é dado por $A_{r,\mathbb{P}}(C) = (q-1)q^{r-d_{\mathbb{P}}}$.*

Demonstração. Fazendo $n = 1$ na Proposição 4.41, temos um poset $\mathbb{P}$ do tipo cadeia de cardinalidade s. Neste caso $l = 1$ sempre e além disso, $\sigma_s(1,r) = 1$. Assim $A_{r,\mathbb{P}}(C) = (q-1)q^{r-d_{\mathbb{P}}}$.

□

Definição 4.44 *Definimos o **poset Hieráquico** em $[n]$ como a soma de anticadeias: Sejam $n_1, n_2, \ldots, n_t$ números inteiros positivos tais que $n_1+n_2+\ldots, n_t = n$. Definimos $\mathbb{H}(n; n_1, \ldots, n_t)$ como o poset*

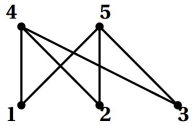
$$\{(i,j) : 1 \leqslant i \leqslant t, 1 \leqslant j \leqslant n_i\}$$

com relação de ordem dada por,

$$(i,j) \preceq (l,m) \Leftrightarrow i \preceq l.$$

O poset $\mathbb{H}(n; n_1, \ldots, n_t)$ é chamado de Poset Hieráquico de n-elementos e t-níveis.

Exemplo 4.45 *Considerando o poset Hieráquico $\mathbb{H}(5;3,2)$ temos que seu diagrama de Hasse é dado por*



É fácil ver que em posets Hieráquicos quaisquer dois ideais de mesma cardinalidade são isomorfos (basta definir um isomorfismo que apenas permute os elementos maximais dos ideais e

fixe os demais elementos). Agora para $1 \leqslant r \leqslant n$, definimos $l(= l(r))$ como o único inteiro satisfazendo

$$n_1 + n_2 + \cdots + n_{l-1} < r \leqslant n_1 + n_2 + \cdots + n_l \qquad (1 \leqslant l \leqslant t). \tag{4.9}$$

Da definição de poset hierárquico $\mathbb{H}(n; n_1, \ldots, n_t)$ segue que os maximais de um ideal estão todos no mesmo nível. Disso segue que um ideal de cardinalidade r possui $r - (n_1 + \cdots + n_{l-1})$ elementos maximais. Dados o número de maximais e o nível dos maximais, segue que existem $\begin{pmatrix} n_l \\ r - (n_1 + \cdots + n_{l-1}) \end{pmatrix}$ ideais de cardinalidade r. Essa descrição explícita dos ideais e o cálculo do número de elementos de um ideal é usada também no que foi afirmado acima, que ideais com mesma cardinalidade são isomorfos.

Proposição 4.46 *Sejam $\mathbb{P} = \mathbb{H}(n; n_1, \ldots, n_t)$ um poset hieráquico de n-elementos e t-níveis e C um $[n,k]_q - \mathbb{P}$-código MDS. Então o número de palavras código de C que possuem $\mathbb{P}$-peso igual a r ($r \geqslant d_{\mathbb{P}} = n - k + 1$) é dado por*

$$\begin{aligned} A_{r,\mathbb{P}}(C) &= (q-1) \begin{pmatrix} n_l \\ r - (n_1 + n_2 + \cdots + n_{l-1}) \end{pmatrix} \\ &\quad \cdot \sum_{j=0}^{r-d_{\mathbb{P}}} (-1)^j \begin{pmatrix} r - (n_1 + n_2 + \cdots + n_{l-1}) - 1 \\ j \end{pmatrix} q^{r-d_{\mathbb{P}}-j}. \end{aligned}$$

Onde l é dado por (4.9).

Demonstração. Pelo Teorema 4.40 temos que

$$A_{r,\mathbb{P}}(C) = (q-1) \sum_{I \in \mathcal{I}^r(\mathbb{P})} \sum_{j=0}^{r-d_{\mathbb{P}}} (-1)^j \begin{pmatrix} |M(I)| - 1 \\ j \end{pmatrix} q^{r-d_{\mathbb{P}}}.$$

Pelas observações acima existem $\begin{pmatrix} n_l \\ r - (n_1 + \cdots + n_{l-1}) \end{pmatrix}$ ideais de cardinalidade r e para cada um destes, $|M(I)| = r - (n_1 + \cdots + n_{l-1})$. Substituindo estes valores na fórmula obtemos o resultado desejado. □

Note que se $l = 1$, ou seja, $\mathbb{P}$ é anticadeia de cardinalidade n, a Proposição 4.46 se reduz ao Corolário 4.42. Se $n_1 = \ldots = n_l = 1$, isto é, $\mathbb{P}$ é uma cadeia de cardinalidade t temos $l = r - 1$ e neste caso a Proposição 4.46 se equivale ao Corolário 4.43.

Lema 4.47 *Seja I um ideal em $\mathbb{P}$ e seja $\lambda : \mathbb{F}_q \to \mathbb{C}^*$ caractere não-trivial. Para $u, v \in \mathbb{F}_q^n$, temos*

$$\hat{\chi}(B_{I,\mathbb{P}}(v)|u) = \lambda(u.v) q^{|I|} \chi(B_{I^C,\mathbb{P}^*}|u).$$

Em particular,

$$\hat{\chi}(B_{I,\mathbb{P}}|u) = q^{|I|}\chi(B_{I^C,\mathbb{P}^*}|u).$$

Demonstração. Pela definição da Transformada de Fourier e da função indicadora temos que,

$$\begin{aligned}\hat{\chi}(B_{I,\mathbb{P}}(v)|u) &= \sum_{w\in\mathbb{F}_q^n} \lambda(u.w)\chi(B_{I,\mathbb{P}}(v)|w) \\ &= \sum_{w\in B_{I,\mathbb{P}}(v)} \lambda(u.w) = \sum_{w\in B_{I,\mathbb{P}}} \lambda(u.(v+w)) \\ &= \lambda(u.v)\sum_{w\in B_{I,\mathbb{P}}} \lambda(u.w).\end{aligned}$$

Como $B_{I,\mathbb{P}}$ é um subespaço de $\mathbb{F}_q^n$, aplicando o Lema 2.29, obtemos

$$\sum_{w\in B_{I,\mathbb{P}}} \lambda(u.w) = \begin{cases} q^{|I|} & se \quad u \in B_{I,\mathbb{P}}^{\perp}, \\ 0 & se \quad u \notin B_{I,\mathbb{P}}^{\perp}. \end{cases}$$

Agora basta mostrar que $B_{I,\mathbb{P}}^{\perp} = B_{I^C,\mathbb{P}^*}$. Com efeito, $x \in B_{I^C,\mathbb{P}^*}$ se, e somente se, $\langle supp(x)\rangle \subseteq I^c$, e $y \in B_{I,\mathbb{P}}$ se, e somente se, $\langle supp(y)\rangle \subseteq I$. Daí,

$$supp(x) \cap supp(y) \subseteq I^c \cap I = \emptyset.$$

Logo,

$$x.y = \sum_{i\in supp(x)\cap supp(y)} x_i y_i = 0$$

ou seja, $B_{I^C,\mathbb{P}^*} \subseteq B_{I,\mathbb{P}}^{\perp}$. Agora se $y \in B_{I,\mathbb{P}}^{\perp}$, então $y.x = 0$ para todo $x \in B_{I,\mathbb{P}}$ ou seja, $y_i = 0$ para todo $i \in I$. Logo $\langle supp(y)\rangle \subseteq I^c$, então $y \in B_{I^c,\mathbb{P}^*}$ e assim, $B_{I,\mathbb{P}}^{\perp} \subseteq B_{I^C,\mathbb{P}^*}$ donde concluímos que $B_{I,\mathbb{P}}^{\perp} = B_{I^C,\mathbb{P}^*}$. Então

$$\hat{\chi}(B_{I,\mathbb{P}}(v)|u) = \lambda(u.v)q^{|I|}\chi(B_{I^C,\mathbb{P}^*}|u).$$

□

Teorema 4.48 *Sejam C um $[n,k]_q$-código e $C^{\perp}$ seu dual. Para um poset $\mathbb{P}$ em $[n]$ e um inteiro $\delta(0 \leqslant \delta \leqslant k)$ são equivalentes.*

i) Para qualquer ideal I de $\mathbb{P}$ de cardinalidade $n-k+\delta$, cada I-bola contém exatamente q^{δ} palavras código de C;

ii) $d_{\mathbb{P}^*}(C^{\perp}) \geqslant k-\delta+1$, onde $\mathbb{P}^*$ denota o poset dual de $\mathbb{P}$.

Demonstração. $i) \Rightarrow ii)$ Seja I um ideal de $\mathbb{P}$ com cardinalidade $n-k+\delta$. Pela soma discreta de Poisson com $f(x) = \chi(B_{I^C,\mathbb{P}^*}|x)$ e pelo Lema 4.47 temos,

$$\begin{aligned}\left|C^\perp \cap B_{I^C,\mathbb{P}^*}\right| &= \sum_{x\in C^\perp} \chi(B_{I^C,\mathbb{P}^*}|x) \\ &= \frac{1}{|C|}\sum_{x\in C} \hat{\chi}(B_{I^C,\mathbb{P}^*}|x) \\ &= \frac{1}{|C|}\sum_{x\in C} q^{|I^C|}\chi(B_{I,\mathbb{P}}|x) \\ &= q^{-\delta}\,|C\cap B_{I,\mathbb{P}}| = 1.\end{aligned}$$

Agora, suponha que existe uma palavra código não nula, digamos, $c \in C^\perp$ cuja $\mathbb{P}^*$-distância para a origem é menor ou igual a $k-\delta$. Pelo Lema 4.25 todo ideal de $\mathbb{P}^*$ pode ser escrito como I^C para algum ideal I de $\mathbb{P}$. Então pela Proposição 4.23, $supp(c)$ está contido em um ideal $J^C (J \in \mathcal{I}(\mathbb{P}))$ de $\mathbb{P}^*$ com cardinalidade $k-\delta$. Então J é um ideal de $\mathbb{P}$ de cardinalidade $n-k+\delta$. Isto mostra que c pertence a $C^\perp \cap B_{J^C}$ de modo que $\left|C^\perp \cap B_{J^C}\right| \geqslant 2$, contradizendo (3.8). Provando que $d_{\mathbb{P}^\perp}(C^\perp) \geqslant k-\delta+1$.

$ii) \Rightarrow i)$ Suponha que $d_{\mathbb{P}^*}(C^\perp) \geqslant k-\delta+1$. Então $C^\perp \cap B_{I^C,\mathbb{P}^*} = \{0\}$ para todo ideal $I \in \mathbb{P}$ de cardinalidade $|I| = n-k+\delta$. Aplicando a fórmula da soma discreta de Poisson para uma I-bola com $|I| = n-k+\delta$, temos

$$\begin{aligned}|C\cap B_{I,\mathbb{P}}(x)| &= \frac{q^{|I|}}{|C^\perp|}\sum_{z\in C^\perp} \lambda(z.x)\chi(B_{I^C,\mathbb{P}^*}|z) \\ &= q^\delta \sum_{z\in C^\perp \cap B_{I^C,\mathbb{P}^*}} \lambda(z.x) \\ &= q^\delta \lambda(0) = q^\delta.\end{aligned}$$

□

Teorema 4.49 *Sejam $\mathbb{P}$ um poset em $[n]$ e $\mathbb{P}^*$ seu poset dual. Um $[n,k]_q$-$\mathbb{P}$-código C é um $\mathbb{P}$-código MDS se, e somente se, $C^\perp$ é um $\mathbb{P}^*$-código MDS.*

Demonstração. Seja C um $[n,k]_q$-$\mathbb{P}$-código. Vamos aplicar o Teorema 4.48 com $\delta = 0$. Temos que C é um $\mathbb{P}$-código MDS se, e somente se, C é I-perfeito para todo ideal I de $\mathbb{P}$ com $|I| = n-k$ (pelo Teorema 4.37) e isto acontece se, e somente se, $d_{\mathbb{P}^*}(C^\perp) \geqslant k+1$ (pelo Teorema 4.48) e pelo limite de Singleton isto acontece se, e somente se, $d_{\mathbb{P}^*}(C^\perp) = k+1$ ou seja, se, e somente se, $C^\perp$ é um $\mathbb{P}^*$-código MDS. □

Dos resultados acima obtemos um limitante para códigos MDS relacionando a cardinalidade do corpo $\mathbb{F}_q$ e os parâmetros n e k.

Proposição 4.50 *Sejam $\mathbb{P}$ um poset em $[n]$ e C um $[n,k]_q$-$\mathbb{P}$-código MDS. Então temos,*

$$q \geqslant n-k+1-\frac{\sum_{I\in\mathcal{I}^{n-k+2}(\mathbb{P})}|I_M|}{|\mathcal{I}^{n-k+2}(\mathbb{P})|} \quad se \quad k \geqslant 2,$$

$$q \geqslant k+1-\frac{\sum_{I\in\mathcal{I}^{n-k+2}(\mathbb{P})}|I_M^c|}{|\mathcal{I}^{n-k+2}(\mathbb{P})|} \qquad se \quad k \leqslant n-2.$$

Demonstração. Fazendo $r = n-k+2$ no Teorema 4.40 temos,

$$\begin{aligned} A_{n-k+2,\mathbb{P}}(C) &= (q-1)\sum_{I\in\mathcal{I}^{n-k+2}(\mathbb{P})}(q-(n-k+2-|I_M|-1)) \\ &= (q-1)\left[\left|\mathcal{I}^{n-k+2}(\mathbb{P})\right|(q-n+k-1)+\sum_{I\in\mathcal{I}^{n-k+2}(\mathbb{P})}|I_M|\right]. \end{aligned}$$

Como $A_{n-k+2,\mathbb{P}}(C) \geqslant 0$ $(k \geqslant 2)$ obtemos,

$$q \geqslant n-k+1-\frac{\sum_{I\in\mathcal{I}^{n-k+2}(\mathbb{P})}|I_M|}{|\mathcal{I}^{n-k+2}(\mathbb{P})|}.$$

Agora pelo Teorema 4.50 $C^\perp$ é um $[n,n-k]_q$-$\mathbb{P}^*$-código MDS. De modo análogo obtém-se que,

$$q \geqslant k+1-\frac{\sum_{I\in\mathcal{I}^{n-k+2}(\mathbb{P})}|I_M^c|}{|\mathcal{I}^{n-k+2}(\mathbb{P})|}.$$

□

Os resultados obtidos nesta seção podem ser resumidos no seguinte teorema.

Teorema 4.51 *Sejam $\mathbb{P}$ um código poset em $[n]$ e $\mathbb{P}^*$ seu poset dual. Seja C um $[n,k]_q$-$\mathbb{P}$-código. Então são equivalentes.*

a) C é um $\mathbb{P}$-código MDS;

b) C é $\mathbb{P}$-código I-perfeito para todo $I \in \mathcal{I}^{n-k}$;

c) $C^\perp$ é um $\mathbb{P}^*$-código MDS.

4.6 Existência de Códigos posets MDS

Sejam $\mathbb{P}$ e $\mathbb{Q}$ dois posets definidos sobre o mesmo conjunto base. Dizemos que $\mathbb{Q}$ é **mais fino** que $\mathbb{P}$ ou que $\mathbb{Q}$ **refina** $\mathbb{P}$, se $x \preceq y$ em $\mathbb{P}$ implica que $x \preceq y$ em $\mathbb{Q}$.

Lema 4.52 *Sejam $\mathbb{P}$ e $\mathbb{Q}$ dois posets em $[n]$ tais que $\mathbb{Q}$ é mais fino que $\mathbb{P}$. Se C é um $\mathbb{P}$-código MDS então C é um $\mathbb{Q}$-código MDS.*

Demonstração. Seja C um $[n,k]_q$-$\mathbb{P}$-código MDS. Pela definição de métrica poset temos que $d_{\mathbb{P}}(u,v) \leqslant d_{\mathbb{Q}}(u,v)$ para quaisquer $u, v \in \mathbb{F}_q^n$. Além disso,

$$d_{\mathbb{P}}(C) \leqslant d_{\mathbb{Q}}(C).$$

Então pela desigualdade de Singleton temos,

$$n-k+1 = d_{\mathbb{P}}(C) \leqslant d_{\mathbb{Q}}(C) \leqslant n-k+1.$$

Portanto, $d_{\mathbb{Q}}(C) = n-k+1$, ou seja, C é $\mathbb{Q}$-código MDS. □

Corolário 4.53 *Seja C um código MDS de comprimento n com respeito a métrica de Hamming. Então este também é um $\mathbb{P}$-código MDS para todo poset $\mathbb{P}$ em $[n]$.*

Demonstração. Sabemos que se $\mathbb{Q}$ é um poset do tipo anticadeia a métrica de Hamming e a $\mathbb{Q}$-métrica coincidem, logo C é um $\mathbb{Q}$-código MDS. Como todo poset é mais fino que o poset $\mathbb{Q}$ em $[n]$ temos pelo Lema 4.52 que C é um $\mathbb{P}$-código MDS para todo poset $\mathbb{P}$. □

Vamos mostrar a seguir que $\mathbb{P}$-códigos binários perfeitos sempre são $\mathbb{P}$-códigos MDS. Para tanto utilizaremos a seguinte caracterização destes códigos que é dada pela proposição abaixo. Como o alfabeto é binário as palavras serão identificadas com subconjuntos de $[n]$.

Proposição 4.54 *Seja C um $[n,k]$-código linear binário. Então C será um $\mathbb{P}$-código perfeito r-corretor de erro se, e somente se, as duas condições são satisfeitas.*

a) $|B_{\mathbb{P}}(0;r)| = 2^{n-k}$;

b) Para qualquer palavra código c não nula e qualquer partição $\{x,y\}$ de c temos que $w_{\mathbb{P}}(x) \geqslant r+1$ ou $w_{\mathbb{P}}(y) \geqslant r+1$.

Demonstração. Vamos mostrar que a condição de partição $b)$ é equivalente a condição de

$$B_{\mathbb{P}}(0;r) \cap B_{\mathbb{P}}(c;r) = \emptyset$$

Para qualquer palavra código $c \in C$ assuma válida a condição de partição $b)$ e que existe $\alpha \in B_{\mathbb{P}}(0;r) \cap B_{\mathbb{P}}(c;r)$. Então $w_{\mathbb{P}}(\alpha) \leqslant r$ e $w_{\mathbb{P}}(\alpha+c) \leqslant r$. Como $\{\alpha \cap c, c-(\alpha \cap c)\}$ é uma partição de c a condição de partição implica que $w_{\mathbb{P}}(\alpha \cap c) \geqslant r+1$ ou $w_{\mathbb{P}}(c-(\alpha \cap c)) \geqslant r+1$. Como $w_{\mathbb{P}}(\alpha \cap c) \leqslant w_{\mathbb{P}}(\alpha) \leqslant r$ temos que, $w_{\mathbb{P}}(c-(\alpha \cap c)) \geqslant r+1$. Assim,

$$w_{\mathbb{P}}(\alpha+c) \;=\; w_{\mathbb{P}}(\alpha-(\alpha \cap c)+c-(\alpha \cap c))$$

$$\begin{aligned} &= |\langle \alpha - (\alpha \cap c) \cup c - (\alpha \cap c) \rangle| \\ &\geqslant |\langle c - (\alpha \cap c) \rangle| = w_{\mathbb{P}}(c - (\alpha \cap c)) \geqslant r + 1. \end{aligned}$$

uma contradição pois, $w_{\mathbb{P}}(\alpha + c) \leqslant r$. Logo não existe tal α e $B_{\mathbb{P}}(0; r) \cap B_{\mathbb{P}}(c; r) = \emptyset$. Por outro lado, se

$$B_{\mathbb{P}}(0; r) \cap B_{\mathbb{P}}(c; r) = \emptyset$$

teremos que para toda partição $\{x, y\}$ de c, $w_{\mathbb{P}}(x) \geqslant r + 1$ ou $w_{\mathbb{P}}(y) \geqslant r + 1$ pois se existisse uma partição tal que $w_{\mathbb{P}}(x) \leqslant r$ e $w_{\mathbb{P}}(y) \leqslant r + 1$ teríamos $x - y \in B_{\mathbb{P}}(0; r) \cap B_{\mathbb{P}}(c; r)$.

Reciprocamente, suponha que C é um $\mathbb{P}$-código linear binário $\mathbb{P}$-perfeito e r-corretor de erro. Então cada r-bola contém exatamente um ponto de C e $\mathbb{F}_2^k$ pode ser escrito como união destas r-bolas donde temos que $|B_{\mathbb{P}}(0, r)| = \frac{|\mathbb{F}_2^n|}{|C|} = 2^{n-k}$, logo vale *a)*. A segunda afirmação segue do fato que, se $w_{\mathbb{P}}(x) \leqslant r$ e $w_{\mathbb{P}}(y) \leqslant r$ temos que $x, y \in B_{\mathbb{P}}(0; r)$ contradizendo o fato de C ser $\mathbb{P}$-perfeito. □

Proposição 4.55 *Seja C um $[n, k]_q$-$\mathbb{P}$-código binário perfeito $(n - k)$-corretor de erro. Então C é um $\mathbb{P}$-código MDS.*

Demonstração. Vamos mostrar que C é I-perfeito para todo $I \in \mathcal{I}^{n-k}(\mathbb{P})$. Seja I um ideal de cardinalidade $(n - k)$. Como $u \in B_I(v)$ se, e somente se, $u - v \in B_I$, basta mostrar que a única palavra código em B_I é o vetor nulo. Suponha que exista uma palavra código $x \neq 0$ com $x \in B_I$. Então $\langle supp(x) \rangle \subseteq I$ e, como C é um $\mathbb{P}$-código perfeito $(n - k)$-corretor de erro, pela condição de partição temos que

$$n - k + 1 \leqslant w_{\mathbb{P}}(x) = |\langle supp(x) \rangle| \leqslant |I| = n - k.$$

uma contradição. □

Definição 4.56 *Sejam $\mathbb{P}$ e $\mathbb{Q}$ posets em X e Y. A soma ordinal $\mathbb{P} \oplus \mathbb{Q}$ dos posets $\mathbb{P}$ e $\mathbb{Q}$ é definida como o poset em $X \cup Y$ tal que $x \preceq y$ em $\mathbb{P} \oplus \mathbb{Q}$ se uma das condições é válida.*

i) $x, y \in \mathbb{P}$ *e* $x \preceq y$ *em* $\mathbb{P}$*;*

ii) $x, y \in \mathbb{Q}$ *e* $x \preceq y$ *em* $\mathbb{Q}$*;*

iii) $x \in \mathbb{P}$ *e* $y \in \mathbb{Q}$*.*

Definição 4.57 *Um subconjunto $A = \{j_1, \ldots, j_k\} \subseteq [n]$ é um conjunto de informação de um código linear C se as k-colunas $\{c_{j_1}, \ldots, c_{j_k}\}$ de uma matriz geradora $G = [c_1 c_2 \ldots c_n]$ de C são LI.*

Observe que, c é uma palavra código de C somente se $c = vG$, com $v \in \mathbb{F}_q^k$, e a j-ésima coordenada de c é $v.c_j$, onde c_j é a j-ésima coluna de G. Agora, se $j \notin A$ então, como o posto de A é k, c_j é combinação das colunas com índices em A. Disso segue que $c = 0$ se, e somente se, $c_A = 0$ onde, c_A denota a projeção de c em A.

Teorema 4.58 *Para todo código linear C sobre $\mathbb{F}_q$ existe um poset $\mathbb{P}$ para o qual C é um $\mathbb{P}$-código MDS.*

Demonstração. Sejam C um $[n, k]$-código sobre $\mathbb{F}_q$ e A um conjunto de informação de C. Temos que A é um subconjunto de $[n]$ com cardinalidade k e $c \in C$ é um vetor não nulo se, e somente se, $c_A \neq 0$ onde, c_A denota a projeção de c em A. Se $\mathbb{P}$ é a soma ordinal de posets arbitrários $\mathbb{P}_1$ e $\mathbb{P}_2$ em $[n] - A$ e A, então C é um $\mathbb{P}$-código MDS. Com efeito, se c é uma palavra código não nula de C então existe uma coordenada $i \in A$ tal que $c_i \neq 0$. Então, $w_{\mathbb{P}}(c) \geqslant n - k + 1$ onde a igualdade é válida quando $i \in A$ é um elemento minimal de A. Logo C é um $\mathbb{P}$-código MDS. □

Apêndice

4.7 A -Grupos

Nesta seção veremos alguns resultados que podem ser encontrados em [11]. Uma operação binária em um conjunto G é uma função $* : G \times G \mapsto G$.

Definição 4.59 *Um **Grupo** é um par $(G, *)$ onde G é um conjunto e $*$ uma operação binária tal que*

i) Para todos $g, h, t \in G$ vale a lei associativa, ou seja,

$$g * (h * t) = (g * h) * t;$$

ii) Existe um elemento $\mathbf{1} \in G$ chamado de identidade, com $\mathbf{1} * g = g * \mathbf{1} = g$ para todo $g \in G$;

iii) Todo elemento $g \in G$ possui um inverso, ou seja, existe $g^{-1} \in G$ tal que

$$g * g^{-1} = \mathbf{1} = g^{-1} * g.$$

Se além disso vale que $g * h = h * g$ para todos $g, h \in G$ dizemos que o grupo G é um **grupo Abeliano**.

Definição 4.60 *Um subconjunto H de um grupo G é um **Subgrupo** de G se*

i) $\mathbf{1} \in H$; onde $\mathbf{1}$ é a identidade do grupo G;

ii) Se $g, h \in H$, então $g * h \in H$;

iii) Se $h \in H$, então $h^{-1} \in H$.

Se H é subgrupo de G escrevemos $H \leq G$; Se H é um subgrupo própio de G, isto é, $H \neq G$ escrevemos $H < G$.

Proposição 4.61 *Seja H um subconjunto de um grupo G. Então*

a) H é um subgrupo de G se, e somente se, H é não vazio e para todos $g, h \in H$ temos $g * h^{-1} \in H$;

b) Se H é um subgrupo de G então o par $(H, *)$ é um grupo.

Definição 4.62 *Sejam G um grupo e $g \in G$. Se $g^k = \mathbf{1}$ para algum $k \geqslant 1$, então o menor expoente k tal que isto ocorre é chamado de ordem de g e se não existe tal potência dizemos que g possui ordem infinita.*

Definição 4.63 *Sejam G um grupo e $g \in G$, escrevemos*

$$\langle g \rangle := \{g^n : n \in \mathbb{Z}\}$$

$\langle g \rangle$ é chamado subgrupo cíclico de G gerado por g. Um grupo G é chamado de cíclico se, existe $g \in G$ tal que $G = \langle g \rangle$, neste caso g é dito um gerador de G.

Proposição 4.64 *Sejam G um grupo e $g \in G$. O elemento g possui ordem n se, e somente se, o subgrupo cíclico gerado por g possui n elementos.*

Proposição 4.65 *Sejam G um grupo e $g \in G$ um elemento de ordem n.*

i) Para cada inteiro m, $g^m = \mathbf{1}$ se, e somente se, n divide m;

ii) A ordem do elemento g^k onde $k \in \mathbb{Z}$ é $\frac{n}{mdc(n,k)}$.

Definição 4.66 *Se Hé subgrupo de um grupo G e $a \in G$, então a classe lateral $a * H$ é o subconjunto $a * H \subseteq G$, onde*

$$a * H := \{a * H : h \in H\}.$$

Classes laterais em geral não são grupos. Por exemplo se $a \notin H$ então $\mathbf{1} \notin a * H$. (do contrário $\mathbf{1} = a * h$ para algum $h \in H$ e isto nos dá a contradição $a = h^{-1}$.)

Lema 4.67 *Seja H um subgrupo de um grupo G e sejam $a, b \in G$.*

i) $a * H = b * H$ se, e somente se, $b^{-1} * a \in H$. Em particular, $a * H = H$ se, e somente se, $a \in H$;

ii) Se $a * H \cap b * H \neq \emptyset$ então $a * H = b * H$;

iii) $|a * H| = |H|$ *para todo* $a \in G$.

Teorema 4.68 *(Teorema de Lagrange). Se* H *é um subgrupo de um grupo finito* G*, então* $|H|$ *é um divisor de* $|G|$.

Corolário 4.69 *Se* G *é um grupo finito e* $g \in G$*, então a ordem de* g *é divisor de* $|G|$.

Corolário 4.70 *Se* G *é um grupo finito, então* $g^{|G|} = \mathbf{1}$ *para todo* $g \in G$.

Definição 4.71 *O índice de um subgrupo* H *em* G*, denotado por* $[G : H]$*, é o número de classes laterais de* H *em* G.

4.8 B - Anéis

Nesta seção veremos alguns resultados que podem ser encontrados em [7] e [11]. Um Anel é uma terna $(\mathbf{R}, +, *)$ onde $\mathbf{R}$ é um conjunto e $+, *$ são operações binárias tais que, (i) $\mathbf{R}$ é um grupo abeliano com $+$; (ii) $*$ é associativa, ou seja, $a * (b * c) = (a * b) * c$ para todos $a, b, c \in \mathbf{R}$; (iii) As leis distributivas são válidas, isto é, para todos $a, b, c \in \mathbf{R}$, temos $a * (b + c) = a * b + a * c$ e $(b + c) * a = b * a + c * a$.

Um anel é dito **anel com identidade** se possui uma identidade em relação a operação $*$, ou seja, existe um elemente e tal que $e * a = a * e = a$ para todo $a \in \mathbf{R}$. Dizemos que o anel é comutativo, se $*$ é uma operação comutativa. Se $\mathbf{R}$ é comutativo com identidade $e \neq 0$ tal que $a * b = 0$ implica $a = 0$ ou $b = 0$ (quando isto ocorre diz-se que $\mathbf{R}$ não possui divisores de zero) dizemos que $\mathbf{R}$ é um **domínio de integridade**. Um anel tal que os elementos não nulos de $\mathbf{R}$ formam um grupo com respeito a operação $*$ é chamado de **Anel de divisão**.

Seja $f : \mathbf{R} \mapsto \mathbf{S}$ uma função entre os anéis $\mathbf{R}$ e $\mathbf{S}$. Se f é tal que, para todos $a, b \in \mathbf{R}$, valem

$$f(a + b) = f(a) + f(b) \text{ e } f(a * b) = f(a) * f(b)$$

dizemos que f é um *Homomorfismo* entre os anéis $\mathbf{R}$ e $\mathbf{S}$. Um homomorfismo de $\mathbf{R}$ em $\mathbf{R}$ é chamado de *Endomorfismo*. Se f é um homomorfismo bijetor de $\mathbf{R}$ em $\mathbf{S}$, chamamos f de *Isomorfismo* de $\mathbf{R}$ em $\mathbf{S}$ e neste caso $\mathbf{R}$ e $\mathbf{S}$ são ditos isomorfos. Um isomorfismo de $\mathbf{R}$ em $\mathbf{R}$ é chamado de *Automorfismo*.

Proposição 4.72 *O conjunto de automorfismos de um anel forma um grupo com relação à composição.*

Definição 4.73 *Um anel $\mathbb{F}$ e comutativo, com unidade recebe o nome de Corpo se todo elemento não nulo de $\mathbb{F}$ admite simétrico multiplicativo, ou seja:*

$$\forall a \neq 0 \in \mathbb{F},\ \exists b \in \mathbb{F} \text{ tal que } a * b = 1.$$

Note que a definição pode ser simplificada apenas dizendo que "*Um Corpo $\mathbb{F}$ é um anel de divisão comutativo*". Se $\mathbb{F}$ possui um número finito de elementos dizemos que $\mathbb{F}$ é um corpo finito.

Exemplo 4.74 .

a) Seja R qualquer grupo abeliano em relação a operação $+$. Definindo $a * b = 0$ para todos $a, b \in R$ temos que R é um anel;

b) $\mathbb{Z}$ é um domínio de integridade, porém não um corpo;

c) Os números inteiros pares formam um anel comutativo sem identidade;

d) O conjunto de todas as matrizes 2×2 com entradas em $\mathbb{R}$ com as operações de multiplicação e adição de matrizes formam um anel não comutativo com identidade.

Teorema 4.75 *Todo corpo $\mathbb{F}$ é um domínio de integridade.*

Teorema 4.76 *Todo domínio de integridade finito é um corpo.*

Definição 4.77 *Um subconjunto $\mathbf{S}$ de um anel $\mathbf{R}$ é dito um Subanel de $\mathbf{R}$ se $\mathbf{S}$ é fechado em relação as operações de $\mathbf{R}$ e $\mathbf{S}$ é um anel com estas operações.*

Definição 4.78 *Um subconjunto $\mathbf{J}$ de um anel $\mathbf{R}$ é dito um Ideal se $a * r \in \mathbf{J}$ e $r * a \in \mathbf{J}$ para todos $a \in \mathbf{J}$ e $r \in \mathbf{R}$.*

Seja $\mathbf{R}$ um anel comutativo. Um ideal $\mathbf{J}$ de $\mathbf{R}$ é dito ser Principal se existe um $a \in \mathbf{R}$ tal que $\mathbf{J} = \langle a \rangle$. Neste caso dizemos que $\mathbf{J}$ é o ideal gerado por a. Um ideal $\mathbf{M} \neq \mathbf{R}$ é chamado de Ideal Maximal de $\mathbf{R}$ se para qualquer ideal $\mathbf{J}$ de $\mathbf{R}$ tal que $\mathbf{M} \subseteq \mathbf{J}$ implica que $\mathbf{J} = \mathbf{M}$ ou $\mathbf{J} = \mathbf{R}$.

Definição 4.79 *Sejam $\mathbf{R}$ um anel e um ideal $\mathbf{J} \subseteq \mathbf{R}$. Definimos o anel quociente $\mathbf{R}/\mathbf{J}$ como sendo o conjunto das classes de equivalência módulo $\mathbf{J}$ com as operaçõs definidas por*

i) $(a + \mathbf{J}) + (b + \mathbf{J}) = (a + b) + \mathbf{J}$ para todos $a, b \in \mathbf{R}$;

ii) $(a + \mathbf{J}) * (b + \mathbf{J}) = (a * b) + \mathbf{J}$ *para todos* $a, b \in \mathbf{R}$.

Teorema 4.80 *Sejam* $\mathbf{R}$ *um anel e* $\mathbf{I}$ *um ideal de* $\mathbf{R}$. *O Anel* $\mathbf{R}/\mathbf{I}$ *é um corpo se, e somente se,* $\mathbf{I}$ *é um ideal maximal.*

Exemplo 4.81 *(Anel dos Inteiros Módulo "*n*"). Denotamos a classe de equivalência de um inteira "*a*"módulo "*n*"por* $[a]$*, ou seja,* $a + \langle n \rangle$ *onde* $\langle n \rangle$ *é o ideal principal gerado por* n*. Os elementos de* $\mathbb{Z}/\langle n \rangle$ *(escrevemos* $\mathbb{Z}_n$ *para este quociente) são*

$$[0] = 0 + \langle n \rangle, [1] = 1 + \langle n \rangle, \ldots, [n-1] = (n-1) + \langle n \rangle.$$

Proposição 4.82 *O anel* $\mathbb{Z}_n$ *é um corpo se, e somente se,* n *é um número primo.*

Lembre-se que num anel $\mathbf{R}$ qualquer um polinômio sobre $\mathbf{R}$ é uma expressão da seguinte forma

$$f(x) = \sum_{i=0}^{n} a_i x^i.$$

Onde n é um inteiro não negativo e os *coeficientes* a_i $0 \leqslant i \leqslant n$, são elementos de $\mathbf{R}$. Escrevemos $\mathbf{R}[x]$ para o conjunto dos polinômios sobre $\mathbf{R}$. O conjunto $\mathbf{R}[x]$ com as operações usuais de multiplicação e soma de polinômio possui a estrutura de anel.

Definição 4.83 *Seja* $\mathbb{F}$ *um corpo. Um polinômio* $f(x) \in \mathbb{F}[x]$ *é dito irredutível sobre* $\mathbb{F}$ *(ou irredutível em* $\mathbb{F}[x]$*, ou primo em* $\mathbb{F}[x]$*) se* f *possui grau maior que um e se* $f(x) = g(x)h(x)$*, com* $g(x), h(x) \in \mathbb{F}[x]$*, implica que* $g(x)$ *ou* $h(x)$ *é um polinômio constante.*

Proposição 4.84 *Um ideal* $\langle f(x) \rangle$ *de* $\mathbb{F}[x]$ *é maximal se, e somente se,* $f(x)$ *é um polinômio irredutível em* $\mathbb{F}[x]$.

Um elemento $a \in \mathbb{F}$ é chamado de raiz do polinômio $f \in \mathbb{F}[x]$ se $f(a) = 0$.

Teorema 4.85 *Seja* $f \in \mathbb{F}[x]$ *um polinômio não constante. Um elemento* $a \in \mathbb{F}$ *é uma raiz de* $f \in \mathbb{F}[x]$ *se, e somente se,* $x - a$ *divide* $f(x)$.

Definição 4.86 *Se* $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \in \mathbb{F}[x]$*, então a derivada* f' *de* f *é definida como* $f'(x) = a_1 + 2a_2 x + \cdots + n a_n x^{n-1} \in \mathbb{F}[x]$.

Assim definida, temos que as mesmas propriedades usuais de derivadas são válidas para f' de um polinômio f. A saber,

a) $(f + g)' = f' + g'$ para todos $f(x), g(x) \in \mathbb{F}[x]$;

b) $(cf)' = c\,(f)'$ onde $c \in \mathbb{F}$;

c) $(fg)' = f'g + fg'$ para todos $f(x), g(x) \in \mathbb{F}[x]$;

d) $\left(\frac{f}{g}\right)' = \frac{f'g - fg'}{g^2}$ para $f(x), g(x) \in \mathbb{F}[x]$ com $g(x)$ não nulo.

Proposição 4.87 *Seja $f \in \mathbb{F}[x]$. Se $mdc(f, f') = 1$ então f só possui raízes simples.*

4.9 C - Teorema Chinês dos Restos

Enunciaremos aqui uma versão "fraca"do Teorema Chinês dos Restos e também o próprio teorema em si. Sua demontração pode ser encontrada em [12].

Teorema 4.88 *Dados dois inteiros $m_1, m_2 \geqslant 2$ primos entre si (isto é, $mdc(m_1, m_2) = 1$), e dados outros dois inteiros quaisquer a_1 e a_2, o sistema*

$$\begin{cases} x & \equiv & a_1 \; mod(m_1) \\ x & \equiv & a_2 \; mod(m_2) \end{cases}$$

possui uma solução $x = x_0$. Além disso, um inteiro x será solução do sistema se, e somente se, $x \equiv x_0 \; mod(m_1 m_2)$.

Teorema 4.89 *(Teorema Chinês do Restos). Sejam $m_1, \ldots, m_k$ inteiros maiores ou iguais a 2, dois a dois primos entre si (isto é, $mdc(m_i, mj) = 1$ sempre que $i \neq j$). Sejam $a_1, \ldots, a_k$ inteiros quaisquer. Então o sistema*

$$\begin{cases} x & \equiv & a_1 \; mod(m_1) \\ x & \equiv & a_2 \; mod(m_2) \\ \vdots & \vdots & \vdots \\ x & \equiv & a_k \; mod(m_k) \end{cases}$$

possui uma solução $x = x_0$. Além disso, um inteiro x é solução do sistema se, e somente se,

$$x \equiv x_0 \; mod(m_1 \ldots m_k).$$

Teorema 4.90 *Sejam $\mathbb{F}$ um corpo e $f_1(x), f_2(x), \ldots f_n(x) \in \mathbb{F}[x]$ polinômios dois a dois co-primos. Então dados $a_1(x), a_2(x), \ldots, a_n(x) \in \mathbb{F}[x]$, existe uma solução $g(x)$ do sistema*

$$\begin{cases} g(x) & \equiv & a_1(x) \; mod(f_1(x)) \\ g(x) & \equiv & a_2(x) \; mod(f_2(x)) \\ \vdots & \vdots & \vdots \\ g(x) & \equiv & a_n(x) \; mod(f_n(x)) \end{cases}$$

que é única módulo $(f_1(x) f_2(x) \ldots f_n(x))$.

Referências Bibliográficas

[1] BRUALDI, R. A., GRAVES, J. S., AND LAWRENCE, K. M. ***Codes with a poset metric***. Discrete Math. 147, 1-3 (Dec. 1995), 57-72.

[2] DOUGHERTY, S. T., AND SKRIGANOV, M. M. ***Maximum Distance Separable Codes in the ρ Metric over Arbitrary Alphabets***. Journal of Algebraic Combinatorics 16 (2002), 71-81.

[3] HEFEZ, A., AND VILLELA, M. ***Códigos corretores de erros***. Série de computação e Matemática. Instituto de Matemática Pura e Aplicada, 2008.

[4] HUFFMAN, W., AND PLESS, V. ***Fundamentals of Error-Correcting Codes***. Cambridge, Ma University Press, 2003.

[5] KIM, H. K., HYUN, J. Y. ***Maximum distance separable poset codes***. Designs, Codes and Cryptography. (2008) 48:247-261.

[6] LANE, S., AND BIRKHOFF, G. ***Algebra***. Chelsea Publishing Series. Chelsea Publishing Company, 1999.

[7] LIDL, R., AND NIEDERREITER, H. ***Finite Fields***. Encyclopedia of Mathematics and its Applications. Cambridge University Press, 1997.

[8] NIEDERREITER, H. ***Point sets and sequences with small discrepancy***, Monatsh. Math. 104(1987) 273-337.

[9] NIEDERREITER, H. ***A combinatorial problem for vectors spaces over finite fields***, Discrete Math. 96(1991) 221-228.

[10] ROSENBLOOM, M, Y. T. M. A. ***Codes for the m-metric***. Probl. Peredachi Inf. 33, 1 (1997), 55-63.

[11] ROTMAN, J.J. ***Advanced Modern Algebra***. Prentice-Hall, 2002.

[12] SANTOS, J.P.O ***Introdução à Teoria dos Números***- Terceira Edição. Coleção Matemática Universitária IMPA 03, 2014.

[13] SHANNON, C. E. ***A mathematical theory of communication***. Bell System Technical Journal 27 (1948), 379-423.

[14] SKRIGANOV, M. M. ***Coding Theory and Uniform Distributions***. Algebra i Analiz 13, 2 (Sept.2001), 191-239.

[15] STANLEY, R. ***Enumerative Combinatorics***. No. v. 1 in Cambridge studies in advanced mathematics. Cambridge University Press, 2002.