Luiz Henrique de Almeida Pinto Couto

Códigos NMDS sob a Métrica Poset

Dissertação apresentada à Universidade Federal de Viçosa, como parte das exigências do Programa de Pós Graduação em Matemática, para obtenção do título de *Magister Scientiae*.

VIÇOSA
MINAS GERAIS - BRASIL
2014

Ficha catalográfica preparada pela Biblioteca Central da Universidade Federal de Viçosa - Câmpus Viçosa

T
C871c
2014

Couto, Luiz Henrique de Almeida Pinto, 1989-
Códigos NMDS sob a métrica poset / Luiz Henrique de Almeida Pinto Couto. – Viçosa, MG, 2014.
vii, 96f. : il. ; 29 cm.

Orientador: Allan de Oliveira Moura.
Dissertação (mestrado) - Universidade Federal de Viçosa.
Referências bibliográficas: f.94-96.

1. Teoria da codificação. 2. Códigos corretores de erros. 3. Métricas poset. 4. Códigos NMDS. I. Universidade Federal de Viçosa. Departamento de Matemática. Programa de Pós-graduação em Matemática. II. Título.

CDD 22. ed. 519.7

Luiz Henrique de Almeida Pinto Couto

Códigos NMDS sob a Métrica Poset

Dissertação apresentada à Universidade Federal de Viçosa, como parte das exigências do Programa de Pós Graduação em Matemática, para obtenção do título de *Magister Scientiae*.

APROVADA: 17 de fevereiro de 2014.

Anderson Luiz Pedrosa Porto

Marinês Guerreiro

Allan de Oliveira Moura
(Orientador)

Poesia Matemática

Às folhas tantas
do livro matemático
um Quociente apaixonou-se
um dia
doidamente
por uma Incógnita.
Olhou-a com seu olhar inumerável
e viu-a do ápice à base
uma figura ímpar;
olhos rombóides, boca trapezóide,
corpo retangular, seios esferóides.
Fez de sua uma vida
paralela à dela
até que se encontraram
no infinito.
"Quem és tu?", indagou ele
em ânsia radical.
"Sou a soma do quadrado dos catetos.
Mas pode me chamar de Hipotenusa."
E de falarem descobriram que eram
(o que em aritmética corresponde
a almas irmãs)
primos entre si.
E assim se amaram
ao quadrado da velocidade da luz
numa sexta potenciação
traçando
ao sabor do momento
e da paixão
retas, curvas, círculos e linhas sinoidais
nos jardins da quarta dimensão.
Escandalizaram os ortodoxos das fórmulas euclidiana
e os exegetas do Universo Finito.
Romperam convenções newtonianas e pitagóricas.
E enfim resolveram se casar
constituir um lar,
mais que um lar,
um perpendicular.
Convidaram para padrinhos
o Poliedro e a Bissetriz.
E fizeram planos, equações e diagramas para o futuro
sonhando com uma felicidade

integral e diferencial.
E se casaram e tiveram uma secante e três cones
muito engraçadinhos.
E foram felizes
até aquele dia
em que tudo vira afinal monotonia.
Foi então que surgiu
O Máximo Divisor Comum
freqüentador de círculos concêntricos,
viciosos.
Ofereceu-lhe, a ela,
uma grandeza absoluta
e reduziu-a a um denominador comum.
Ele, Quociente, percebeu
que com ela não formava mais um todo,
uma unidade. Era o triângulo,
tanto chamado amoroso.
Desse problema ela era uma fração,
a mais ordinária.
Mas foi então que Einstein descobriu a Relatividade
e tudo que era espúrio passou a ser
moralidade
como aliás em qualquer
sociedade.

Millôr Fernandes

Sumário

Resumo

COUTO, Luiz Henrique de Almeida Pinto, M.Sc., Universidade Federal de Viçosa, fevereiro de 2014. **Códigos NMDS sob a métrica poset**. Orientador: Allan de Oliveira Moura.

Neste trabalho, a partir de uma generalização da métrica de Hamming por uma métrica ponderada por uma ordem parcial, definimos os espaços poset e estudamos os códigos lineares NMDS em tais espaços, obtendo caracterizações para estes. Com o auxílio de tais caracterizações, apresentamos duas aplicações com respeito à distribuições: a distribuição de pesos de um código e, no caso particular da métrica obtida por um poset Rosenblomm-Tsfasman, a distribuição de pontos no cubo unitário $U^n = [0, 1)^n$. Fornecemos também algumas construções de códigos NMDS em espaços Rosenbloom-Tsfasman.

Abstract

COUTO, Luiz Henrique de Almeida Pinto, M.Sc., Universidade Federal de Viçosa, February, 2014. **NMDS codes under the poset metric**. Advisor: Allan de Oliveira Moura.

In this work, from a generalization of the metric Hamming for a weighted metric by a partial order, we define the poset spaces and we study linear NMDS codes in such spaces, gaining characterizations for these. With the aid of such characterizations, we present two applications with respect to distributions: the weight distribution of a code and, in particular case of the metric obtained by a poset Rosenblomm-Tsfasman, the distribution of points in the unit cube $U^n = [0, 1)^n$. We also provide some constructions of NMDS codes in Rosenbloom-Tsfasman spaces.

Introdução

O estudo dos fenômenos oscilatórios tem importantes aplicações. Uma delas ocorre, por exemplo, na cabine de aviões. Da Teoria Ondulatória da Física, sabemos que duas ondas podem interferir destrutivamente, proporcionando o anulamento de seus efeitos [4]. Na cabine de uma aeronave é possível que haja um som de fundo, devido aos motores. A exposição a esses sons durante uma longa viagem pode incomodar os tripulantes e, para resolver esse problema, um esquema prático pode ser executado.

Um computador instalado na cabine recebe o som de fundo proveniente dos motores por meio de um microfone e o analisa. Em seguida, emite por meio de alto-falantes uma onda sonora idêntica à recebida, mas com a fase invertida. A superposição dessas duas ondas idênticas, porém em oposição de fase, irá proporcionar o "silêncio" dentro da cabine.

Poderíamos, num modelo bem simplista, codificar os sons de fundo com base nas notas musicais:

Nota	Codificação
Dó	1000000
Ré	0100000
Mi	0010000
Fá	0001000
Sol	0000100
Lá	0000010
Si	0000001
Silêncio	0000000

e todos os possíveis sons de fundo seriam gerados pela combinação (soma) destes. Assim, o computador analisaria as frequências dos sons emitidos e codificaria como o vetor 1010100 o som proveniente da combinação das notas Dó, Mi e Sol (que juntas formam o acorde de Dó maior). Após essa codificação, o computador emitiria o mesmo sinal 1010100, mas com fase invertida e o resultado seria

$$1010100 + 1010100.$$

Se cada uma das entradas desses vetores estão em $\mathbb{Z}_2$ (e, portanto, $0+1=1=1+0$ e $0+0=0=1+1$), teríamos

$$1010100 + 1010100 = 0000000,$$

ou seja, o silêncio pretendido.

No entanto, caso o som emitido pelos motores fosse codificado erroneamente como 1010010, o som resultante pela combinação do som emitido pelos motores e do som emitido pelos alto-falantes seria percebido como

$$1010100 + 1010010 = 0000110,$$

isto é, uma combinação de Sol e Lá que não soaria agradável aos tripulantes (ondas sonoras muito próximas mas com frequências diferentes, como Sol e Lá, são muitas vezes dissonantes e caracterizam o fenômeno conhecido como "batimento" na Teoria Ondulatória).

Para evitarmos esse problema, poderíamos recodificar as notas repetindo as entradas do vetor, como segue:

Nota	Codificação
Dó	10000001000000
Ré	01000000100000
Mi	00100000010000
Fá	00010000001000
Sol	00001000000100
Lá	00000100000010
Si	00000010000001
Silêncio	00000000000000

Assim, supondo que se tenha introduzido um erro na recepção do som e o computador tivesse codificado este som como 10100101010100, por exemplo, como este vetor não é uma combinação dos vetores do código anterior (pois a primeira metade do vetor é diferente da segunda), o computador pode reconhecer que existe um erro. Além disso, como os vetores gerados pelas combinações anteriores mais próximos deste vetor erroneamente codificado são 10101001010100 e 10100101010010, poderíamos inferir que o som emitido pelos motores foi uma combinação de Dó, Mi e Sol ou uma combinação de Dó, Mi e Lá, respectivamente.

Esse tipo de situação é uma aplicação da Teoria de Códigos Corretores de Erros, um campo de pesquisa muito ativo na atualidade em diversas áreas do conhecimento, tais como a Matemática, a Computação, a Engenharia Elétrica e a Estatística. Um código corretor de erros é, basicamente, um modo organizado de acrescentar algum dado adicional a cada informação que se queira transmitir ou armazenar e que permita, ao recuperar a informação, detectar e corrigir os

erros no processo de transmissão da informação. Um dos objetivos principais da teoria baseia-se na transmissão e armazenamento de dados de forma eficiente, garantindo a confiabilidade destes.

Essa teoria teve início na década de 40, quando os computadores eram máquinas ainda muito caras e apenas instituições de grande porte como o governo ou as universidades tinham condições de mantê-los. Esses computadores eram utilizados para executar tarefas numéricas complexas, como calcular a órbita precisa de Marte ou avaliar dados estatísticos de um censo [19].

Em 1947, Richard W. Hamming trabalhava com estas máquinas no Laboratório Bell de Tecnologia [19]. Na época, os programas eram gravados em cartões perfurados cuja leitura pelo computador permitia detectar erros de digitação. Caso um erro fosse detectado, a leitura era interrompida e o computador passava automaticamente a ler o programa do próximo usuário. Aborrecido por perder vários de seus dados devido à presença de erros, Hamming indagou: se os computadores são capazes de detectar tais erros, não seriam também capazes de corrigí-los?

Essa questão levou Hamming a desenvolver um código capaz de detectar até dois erros e de corrigir um erro, se ele fosse único. No intuito de melhorar estas correções, ele questionava sobre a possibilidade de criar códigos mais eficientes que esse proposto inicialmente. Essa questão foi respondida indiretamente em outubro de 1948, por C. E. Shannon num artigo intitulado "*A Mathematical Theory of Communication*", artigo este que, pode-se dizer, fundamentou a Teoria dos Códigos Corretores de erros. A teoria continuou a ser desenvolvida por matemáticos nas décadas de 50 e 60 mas, com o advento das pesquisas espaciais e a popularização dos computadores, a partir da década de 70, a teoria também começou a interessar aos engenheiros.

Códigos corretores foram utilizados, por exemplo, para transmitir fotografias coloridas de Júpiter e Saturno pela nave Voyager em 1979 [12]. Atualmente, a utilidade dos códigos corretores apresenta-se sempre que fazemos uso de informações digitalizadas, como assistir programas de televisão, falar ao telefone, navegar pela internet, fazer compras (código de barras), cadastramentos (ISBN, CPF), dentre outras atividades. A situação inicial apresentada na introdução a respeito do barulho em cabines de aviões também pode ser adaptada para o bloqueio de celulares em presídios, por exemplo.

Nessa dissertação, começaremos abordando alguns tópicos da Teoria Clássica. Como veremos, a eficiência da detecção e correção de um código está intimamente ligada à distância mínima deste, conforme definida por Hamming [12] e a busca por essa distância mínima dá origem ao chamado "problema clássico da teoria" [21].

A classe de códigos MDS é definida como aquela onde os códigos possuem a maior distância mínima. Porém, o comprimento desses códigos não pode ser muito grande [2] e esta restrição levou ao estudo de classes de códigos com

distâncias mínimas próximas aos MDS e que, por isto, preservam muitas das propriedades estruturais associadas a estes. Podemos citar, dentre estas classes, a dos códigos *Near*-MDS (NMDS), *Near-Near*-MDS (N^2-MDS) e dos A^μ-MDS [30]. Dentre estes, daremos enfoque aos códigos NMDS.

Na década de 90, estudos mais avançados possibilitaram uma generalização do problema clássico por H. Niederreider [23], a partir da definição de uma nova classe de métricas. Essas métricas foram, posteriormente, esquematizadas em um modelo geral baseado em uma métrica ponderada por uma ordem parcial (*poset metric*, em inglês).

Neste trabalho, definiremos os códigos corretores lineares sob a métrica ponderada e faremos um breve estudo da família dos códigos *near*-MDS (NMDS) sob essa métrica. Com este objetivo, esta dissertação conta com três capítulos. No Capítulo 1, focaremos alguns resultados da Teoria Clássica dos Códigos corretores e alguns rudimentos da Teoria das Matrizes Ortogonais. No Capítulo 2, introduziremos a métrica *poset* e faremos uma análise de códigos corretores considerando esta métrica. No Capítulo 3, restringiremos o nosso estudo à classe dos códigos NMDS, visando obter resultados sobre a distribuição de pesos do código e a correspondente distribuição de pontos no Cubo Unitário $U^n = [0, 1)^n$, utilizando, para isso, conexões com a Teoria de Matrizes Ortogonais.

Capítulo 1

Conceitos Preliminares

Neste capítulo, trataremos dos conceitos preliminares necessários para o desenvolvimento desta dissertação. Começaremos abordando alguns tópicos da Teoria Clássica de Códigos Corretores de Erros, como a métrica de Hamming e suas consequentes isometrias. Em nosso estudo, focaremos a classe de códigos mais utilizada na Teoria Clássica, a dos códigos lineares.

Finalizaremos o capítulo apresentando alguns rudimentos da teoria de matrizes ortogonais, que possuem conexões com a Teoria de Códigos e que nos serão necessários no Capítulo 3.

O conteúdo da primeira seção deste capítulo pode ser encontrado em [12]. O leitor poderá omitir as demonstrações desta seção, se preferir, uma vez que estas foram fornecidas aqui para auxiliar aquele que não esteja familiarizado com as notações e resultados apresentados em [12] e também por questões de completude.

1.1 Códigos corretores de erros

O ponto de partida para a construção de um código corretor de erros é fornecer um conjunto finito não-vazio A, chamado **alfabeto**. Neste trabalho, consideraremos $|A| > 1$.

Definição 1.1 *Dados $n \in \mathbb{N}$ e um alfabeto A, definimos $\boldsymbol{A^n}$ como o conjunto formado pelas n-uplas cujas entradas são tomadas em A, isto é,*

$$A^n = \{x = x_1 x_2 \dots x_n; x_i \in A, i = 1, \dots, n\}.$$

Observação 1.2 *Por questões de simplicidade, daremos preferência à notação justaposta dos elementos de A^n, representando os elementos por $x_1 x_2 \dots x_n$ em vez de $(x_1, x_2, \dots, x_n)$.*

Definição 1.3 *Um **código corretor de erros** é um subconjunto próprio $\mathcal{C} \subset A^n$, isto é,*

$$\emptyset \neq \mathcal{C} \subsetneq A^n.$$

Denotaremos por $|A|$ o número de elementos do conjunto A. Para nosso estudo, se $|A| = q$, um código $\mathcal{C} \subset A^n$ será denominado **código q-ário**. Os elementos de $\mathcal{C}$ são sequências finitas dos símbolos do alfabeto, denominadas **palavras** do código e o número de letras de uma palavra é denominado **comprimento** da palavra e corresponde ao número n.

Exemplo 1.4 *Quando o alfabeto utilizado é o conjunto $\mathbb{Z}_2 = \{0, 1\}$, o código diz-se binário. O conjunto*

$$\mathcal{C}_1 = \{00000, 10011, 10110, 11101\}$$

é um código binário de comprimento 5.

A fim de tornar precisa a noção intuitiva de proximidade entre as palavras, apresentamos a seguir um modo de medir a distância entre as palavras em A^n.

1.1.1 Métrica de Hamming

A métrica de Hamming é a métrica mais importante em termos de aplicações práticas e pode ser definida através da noção de distância que leva em conta a diferença entre as palavras, comparadas entrada a entrada:

Definição 1.5 *Dados dois elementos $x = x_1x_2\ldots x_n$ e $y = y_1y_2\ldots y_n$ de A^n, chama-se* ***distância de Hamming*** *de x a y ao número de coordenadas em que estes elementos diferem, isto é,*

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

Exemplo 1.6 *No código $\mathcal{C}_1 = \{00000, 10011, 10110, 11101\}$, temos:*

$$\begin{aligned} d(10011, 10110) &= 2 \\ d(10011, 11101) &= 3 \\ d(10110, 11101) &= 3. \end{aligned}$$

A distância de Hamming, de fato, define uma métrica em A^n:

Proposição 1.7 *[12] Dados $x, y, z \in A^n$, valem as seguintes afirmações:*

(i) $d(x,y) \geq 0$*, para todos $x, y \in A^n$, e $d(x,y) = 0$ se, e somente se, $x = y$;*

(ii) $d(x,y) = d(y,x)$*, para todos $x, y \in A^n$;*

(iii) $d(x,y) \leq d(x,z) + d(z,y)$*, para todos $x, y, z \in A^n$.*

Demonstração:

(*i*) Nota-se facilmente que $d(x,y) \geq 0$, pois a função cardinalidade é não-negativa e

$$d(x,y) = 0 \Leftrightarrow x_i = y_i, \text{ para todo } i = 1, \ldots, n \Leftrightarrow x = y.$$

(*ii*) Repare que

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

(*iii*) Note que a contribuição de cada uma das i-ésimas coordenadas de x e y para o cálculo de $d(x,y)$ é igual a zero se $x_i = y_i$ e igual a um se $x_i \neq y_i$. Assim, vamos comparar as contribuições das coordenadas para $d(x,y)$ e $d(x,z) + d(z,y)$.

Se $x_i = y_i$ para todo i, $1 \leq i \leq n$, então a contribuição de cada coordenada é zero em $d(x,y)$. Como a contribuição de cada coordenada em $d(x,z) + d(z,y)$ pode ser 0, 1 ou 2, temos $d(x,y) \leq d(x,z) + d(z,y)$.

Se $x_i \neq y_i$ para algum i, então devemos ter $x_i \neq z_i$ ou $z_i \neq y_i$. Logo, a contribuição de cada uma das i-ésimas coordenadas de x, y e z em $d(x,z) + d(z,y)$ é maior ou igual a um, que é a contribuição de cada uma das i-ésimas entradas de x e y em $d(x,y)$ e o resultado segue.

□

Chama-se **decodificação** ao procedimento de detecção e correção de erros num determinado código. Na Teoria Clássica, esse procedimento se baseia na noção de proximidade entre as palavras. Essa noção surge naturalmente no espaço métrico (A^n, d) com as seguintes definições:

Definição 1.8 *Definimos a* ***bola*** *de raio $r \geq 0$ e centro em x como*

$$B(x, r) = \{y \in A^n; d(x, y) \leq r\}$$

e a ***esfera*** *de raio $r \geq 0$ e centro em x como*

$$S(x, r) = \{y \in A^n; d(x, y) = r\}.$$

Lema 1.9 *[12] Se $|A| = q$, para todo $a \in A^n$ e todo número natural $r > 0$, temos*

$$|B(a, r)| = \sum_{i=0}^{r} \binom{n}{i} (q-1)^i .$$

Demonstração: Os elementos da esfera

$$S(a, i) = \{v \in A^n; d(a, v) = i\}$$

são aqueles cujas coordenadas coincidem com as coordenadas de a, exceto por i delas. Assim, para formarmos um desses vetores devemos escolher quais das suas n entradas deverão ser distintas das correspondentes entradas em a e determinar, para cada uma dessas i entradas, um elemento do alfabeto que seja distinto daquele presente na mesma entrada em a.

Como a primeira decisão pode ser tomada de $\binom{n}{i}$ maneiras distintas e a segunda pode ser tomada de $(q-1)^i$ maneiras distintas, segue, pelo Princípio Multiplicativo, que

$$|S(a, i)| = \binom{n}{i}(q-1)^i.$$

Notando que as esferas $S(a, i)$ e $S(a, j)$ são disjuntas se $i \neq j$ e que

$$\bigcup_{i=0}^{r} S(a, i) = B(a, r),$$

segue, pelo Princípio da Inclusão-Exclusão que

$$|B(a, r)| = \sum_{i=0}^{r} \binom{n}{i} (q-1)^i .$$

□

Definição 1.10 *Dado um código $\mathcal{C} \subset A^n$, chama-se* ***distância mínima*** *de $\mathcal{C}$ ao número*

$$d = min\{d(x, y); x, y \in \mathcal{C}, x \neq y\}.$$

Exemplo 1.11 *No código $\mathcal{C}_1$, dado no Exemplo 1.6, temos $d = 2$.*

Dado um código $\mathcal{C}$ com distância mínima d, definiremos $\kappa = \left\lfloor \frac{d-1}{2} \right\rfloor$, onde $\lfloor a \rfloor$ representa o **maior inteiro menor ou igual a** (também chamado de **piso**) de a.

Lema 1.12 *[12] Seja $\mathcal{C}$ um código com distância mínima d. Se c e c' são palavras distintas do código $\mathcal{C}$, então*

$$B(c, \kappa) \cap B(c', \kappa) = \emptyset.$$

Demonstração: Se existisse $v \in B(c, \kappa) \cap B(c', \kappa)$, então $d(v, c) \leq \kappa$ e $d(v, c') \leq \kappa$. Assim, pelas partes (iii) e (ii) da Proposição 1.7, teríamos

$$d(c, c') \leq d(c, v) + d(v, c') \leq 2\kappa \leq d - 1 < d,$$

o que é um absurdo, pois d é a distância mínima do código e, portanto, deveríamos ter $d(c, c') \geq d$. □

Com base no lema acima, surge a noção de raio de empacotamento:

Definição 1.13 *O* ***raio de empacotamento*** *de um código $\mathcal{C}$ é o maior número real R tal que as bolas de raio R e centro nas palavras (distintas) do código são disjuntas.*

Repare que, para a métrica de Hamming, temos $R = \kappa$ e este raio de empacotameto depende apenas da distância mínima d. A importância da distância mínima é traduzida no teorema a seguir:

Teorema 1.14 *[12] Seja $\mathcal{C}$ um código com distância mínima d. Então $\mathcal{C}$ pode corrigir até $\kappa = \left\lfloor \frac{d-1}{2} \right\rfloor$ erros e detectar até $d - 1$ erros.*

Demonstração: Se ao transmitirmos uma palavra c do código cometermos t erros e recebermos a palavra b, então $d(b, c) = t$. Se $t \leq \kappa$, então $d(b, c) \leq \kappa$. Sabemos que a distância de b a qualquer outra palavra do código é maior do que κ, pelo Lema 1.12. Assim, determinamos c univocamente a partir de b.

Por outro lado, dada uma palavra no código, podemos introduzir nela até $d-1$ erros sem encontrar outra palavra do código, e assim, a detecção do erro será possível. □

Em virtude do Teorema 1.14, um código terá maior capacidade de correção de erros quanto maior for a sua distância mínima. Portanto, é fundamental, para a Teoria Clássica de Códigos Corretores, poder calcular d ou estimá-lo por cotas inferiores. Esse problema é conhecido como **problema clássico da teoria**.

O Teorema 1.14 também permite traçar uma estratégia para a decodificação, denominada **decodificação por palavra mais próxima**. Seja $\mathcal{C}$ um código com distância mínima d e seja κ como descrito anteriormente.

Quando o receptor recebe uma palavra b, uma das seguintes situações é verificada:

(i) A palavra b encontra-se num disco de raio κ em torno de uma palavra c do código (essa palavra é única, pela demonstração do Teorema 1.14). Neste caso, substitui-se b por c.

(ii) A palavra b não se encontra em nenhum disco de raio κ em torno de uma palavra c do código. Neste caso, não é possível decodificar b com boa margem de segurança.

Observe que em (i) não se pode ter certeza absoluta de que c tenha sido a palavra transmitida, pois poderíamos ter cometido mais do que κ erros, afastando assim b da palavra transmitida e aproximando-a de outra palavra do código. A questão deve ser encarada em termos probabilísticos. A situação (ii) não ocorre em determinada classe de códigos, denominados **códigos perfeitos**.

Definição 1.15 *Seja $\mathcal{C} \subset A^n$ um código com distância mínima d e seja $\kappa = \left\lfloor \frac{d-1}{2} \right\rfloor$. O código $\mathcal{C}$ será dito **perfeito** se*

$$\bigcup_{c \in \mathcal{C}} B(c, \kappa) = A^n.$$

Note que, na definição acima, $B(c,\kappa) \cap B(c',\kappa) = \emptyset$ se $c \neq c'$. Isto nos permite obter a seguinte caracterização, que decorre do Princípio da Inclusão-Exclusão e do Lema 1.9:

Proposição 1.16 *Seja $\mathcal{C} \subset A^n$ um código que possua M palavras e distância mínima d e seja $\kappa = \left\lfloor \frac{d-1}{2} \right\rfloor$. Então $\mathcal{C}$ é perfeito se, e somente se,*

$$M \sum_{i=0}^{\kappa} \binom{n}{i} (q-1)^i = q^n.$$

A obtenção dos códigos perfeitos com a Métrica de Hamming foi trabalhada arduamente por matemáticos e estes constataram a existência de apenas um número pequeno deles, tais como os Códigos de Hamming, algumas classes dos códigos Golay e outros códigos de menor interesse, conhecidos como "códigos trivialmente perfeitos"[13]. No próximo capítulo, introduziremos uma nova métrica com a qual obteremos um número maior de códigos perfeitos.

Definição 1.17 *Dado um código $\mathcal{C}$ sobre um alfabeto A, diremos que as entradas da terna (n, M, d) constituem os* ***parâmetros fundamentais do código****, onde n é o* **comprimento das palavras***, M é o* **número de palavras do código** *e d a sua* **distância mínima***.*

São de particular interesse os códigos para os quais M e d são grandes relativamente à n. Dados três números naturais n, M e d, nem sempre existe um código que possua parâmetros (n, M, d), pois há uma interdependência complexa entre esses três números. Estudar esta interpendência constitui um dos problemas fundamentais desta teoria.

1.1.2 Equivalência de códigos

A noção de equivalência de códigos repousa sobre o conceito de isometria que definiremos abaixo:

Definição 1.18 *Seja A um alfabeto e n um número natural. Diremos que uma função $F : A^n \to A^n$ é uma* ***isometria*** *de A^n se ela preserva distâncias de Hamming, isto é,*

$$d\left(F(x), F(y)\right) = d(x, y)$$

para todo $x, y \in A^n$.

As isometrias para a métrica de Hamming possuem propriedades notáveis, dentre as quais, destacamos as seguintes:

Proposição 1.19 *[12] Toda isometria de A^n é uma bijeção de A^n.*

Demonstração: Seja $F : A^n \to A^n$ uma isometria. Suponha que, para x e y em A^n, tenhamos $F(x) = F(y)$. Assim, $d(x, y) = d(F(x), F(y)) = 0$, o que implica $x = y$. Portanto, F é injetora e como toda aplicação injetora de um conjunto finito nele próprio é sobrejetora, então F é uma bijeção. □

Proposição 1.20 *[12]*

(*i*) *A função identidade de A^n é uma isometria de A^n;*

(*ii*) *Se F é uma isometria de A^n, então F^{-1} é uma isometria de A^n;*

(*iii*) *Se F e G são isometrias de A^n, então $F \circ G$ é uma isometria de A^n.*

Demonstração:

(*i*) Denotemos a identidade de A^n por Id e, assim, $d\left(Id(x), Id(y)\right) = d(x, y)$, para todo $x, y \in A^n$. Logo, Id é uma isometria de A^n.

(*ii*) Se F é uma isometria, pela Proposição 1.19 existe a aplicação inversa F^{-1} de F. Como F é isometria, então

$$d\left(F^{-1}(x), F^{-1}(y)\right) = d\left(F\left(F^{-1}(x)\right), F\left(F^{-1}(y)\right)\right) = d(x, y)$$

para todo $x, y \in A^n$, o que prova que F^{-1} é uma isometria de A^n.

(*iii*) Sejam $x, y \in A^n$. Se F e G são isometrias, então

$$d\left(F\left(G(x)\right), F\left(G(y)\right)\right) = d\left(G(x), G(y)\right) = d(x, y),$$

o que prova que $F \circ G$ é uma isometria de A^n.

□

Observação 1.21 *Note que o conjunto $\{F : A^n \to A^n\}$ de isometrias de A^n é um grupo com a operação de composição. Dessa forma, $(F, \circ)$ pode ser dito o* ***grupo de isometrias de*** *A^n.*

Definição 1.22 *Dados dois códigos $\mathcal{C}$ e $\mathcal{C}'$ em A^n, diremos que $\mathcal{C}'$ é* ***equivalente*** *a $\mathcal{C}$ se existir uma isometria F de A^n tal que $F(\mathcal{C}) = \mathcal{C}'$.*

A equivalência de códigos é, de fato, uma relação de equivalência, pelas proposições anteriores. Além disso, decorre imediatamente da definição que dois códigos equivalentes têm os mesmos parâmetros.

Exemplo 1.23 *Se $f : A \to A$ é uma bijeção e i é um número inteiro tal que $1 \leq i \leq n$, então a aplicação*

$$\begin{array}{rccc} T_f^i : & A^n & \to & A^n \\ & (a_1, \ldots, a_i, \ldots, a_n) & \mapsto & (a_1, \ldots, f\left(a_i\right), \ldots, a_n) \end{array}$$

é uma isometria, uma vez que, dados $x = x_1 x_2 \ldots x_n$, $y = y_1 y_2 \ldots y_n \in A^n$, temos $f(x_i) = f(y_i)$ se, e somente se, $x_i = y_i$.

Exemplo 1.24 *Se π é uma permutação de $\{1,\ldots,n\}$ a aplicação permutação de coordenadas*

$$\begin{array}{rccc} T_\pi: & A^n & \to & A^n \\ & (a_1,\ldots,a_n) & \mapsto & \left(a_{\pi(1)},\ldots,a_{\pi(n)}\right) \end{array}$$

é uma isometria, uma vez que, dados $x = x_1x_2\ldots x_n$, $y = y_1y_2\ldots y_n \in A^n$, temos $x_{\pi(i)} = y_{\pi(i)}$ se, e somente se, $x_i = y_i$.

O próximo teorema nos fornecerá uma caracterização que geralmente é a apresentada em textos sobre códigos como uma definição de códigos equivalentes, como veremos a seguir. O leitor interessado poderá consultar [12] para uma demonstração deste resultado.

Teorema 1.25 *[12] Se $F: A^n \to A^n$ é uma isometria, então existem uma permutação π de $\{1,\ldots,n\}$ e bijeções f_i de A, $i = 1,\ldots,n$, tais que*

$$F = T_\pi \circ T^1_{f_1} \circ \ldots \circ T^n_{f_n}.$$

Corolário 1.26 *[12] Sejam $\mathcal{C}$ e $\mathcal{C}'$ dois códigos em A^n. Então $\mathcal{C}$ e $\mathcal{C}'$ são equivalentes se, e somente se, existem uma permutação π de $\{1,\ldots,n\}$ e bijeções $f_1,\ldots,f_n$ de A tais que*

$$\mathcal{C}' = \left\{\left(f_{\pi(1)}\left(x_{\pi(1)}\right),\ldots,f_{\pi(n)}\left(x_{\pi(n)}\right)\right); (x_1,\ldots,x_n) \in \mathcal{C}\right\}.$$

Com este corolário, temos a caracterização alternativa para códigos equivalentes:

Proposição 1.27 *[12] Dois códigos de comprimento n sobre um alfabeto A são equivalentes se, e somente se, um deles puder ser obtido do outro mediante uma sequência de operações do tipo:*

(*i*) *Substituição dos elementos de A numa dada posição fixa em todas as palavras do código por meio de uma bijeção de A.*

(*ii*) *Permutação das posições dos elementos de A em todas as palavras do código, mediante uma permutação fixa de $\{1,2,\ldots,n\}$.*

1.1.3 Códigos lineares

Em geral, se não colocarmos uma boa estrutura em um código, sua utilidade será um pouco limitada. A estrutura utilizada mais comum é a linearidade. Tomando o alfabeto $A = \mathbb{F}_q$, o corpo finito com q elementos, temos a seguinte definição:

Definição 1.28 *Um **código linear** é um subespaço vetorial próprio de $\mathbb{F}_q^n$.*

Todo código linear é, por definição, um espaço vetorial de dimensão finita sobre $\mathbb{F}_q$. Seja k a dimensão do código $\mathcal{C}$ e seja $\{v_1, v_2, \ldots, v_k\}$ uma de suas bases. Assim, todo elemento de $\mathcal{C}$ se escreve de modo único na forma

$$\lambda_1 v_1 + \lambda_2 v_2 + \ldots + \lambda_k v_k,$$

onde $\lambda_i \in \mathbb{F}_q$, $i = 1, \ldots, k$.

Pelo Princípio Fundamental da Contagem, temos

$$M = |\mathcal{C}| = q^k$$

e, consequentemente,

$$\dim_{\mathbb{F}_q}(\mathcal{C}) = k = \log_q\left(q^k\right) = \log_q(M).$$

Definição 1.29 *Dado $x \in \mathbb{F}_q^n$, o **peso da palavra** x é o número inteiro*

$$\omega(x) = |\{i; x_i \neq 0\}| = d(x, 0)$$

*e o **peso de um código linear** $\mathcal{C}$ é o natural*

$$\omega(\mathcal{C}) = min\{\omega(x); x \in \mathcal{C}\backslash\{0\}\}.$$

Proposição 1.30 *[12] Seja $\mathcal{C} \subset \mathbb{F}_q^n$ um código linear com distância mínima d. Então:*

(*i*) *Para quaisquer $x, y \in \mathbb{F}_q^n$, $d(x, y) = \omega(x - y)$;*

(*ii*) *$d = \omega(\mathcal{C})$.*

Demonstração:

(*i*) Temos $\omega(x - y) = |\{i; x_i - y_i \neq 0\}| = |\{i; x_i \neq y_i\}| = d(x, y)$.

(*ii*) Para todo par de elementos $x, y \in \mathcal{C}$ com $x \neq y$ temos $z = x - y \in \mathcal{C}\backslash\{0\}$. Assim, $\omega(\mathcal{C}) = min\{\omega(z); z \in \mathcal{C}\backslash\{0\}\} = min\{\omega(x - y); x \neq y\} = min\{d(x, y); x \neq y\} = d$.

□

A proposição acima nos mostra que, em códigos lineares com M elementos, podemos calcular a distância mínima d a partir de $M - 1$ cálculos de distâncias, em vez dos $\binom{M}{2}$ cálculos anteriormente requeridos, em que se fazia necessário

comparar as distâncias de todas as palavras, duas a duas. Em virtude da proposição anterior, a distância mínima de um código linear $\mathcal{C}$ será também chamada **peso do código** $\mathcal{C}$.

A princípio, conhecemos duas maneiras de se descrever subespaços vetoriais $\mathcal{C}$ de um espaço vetorial $\mathbb{F}_q^n$: uma como imagem, e outra como núcleo de transformações lineares.

Uma possível representação de $\mathcal{C}$ como imagem de uma transformação é dada escolhendo-se uma base $\beta = \{v_1, v_2, \ldots, v_k\}$ de $\mathcal{C}$ e definindo-se a transformação linear

$$\begin{array}{rccc} T: & \mathbb{F}_q^k & \to & \mathbb{F}_q^n \\ & x = (x_1, x_2, \ldots, x_k) & \mapsto & x_1v_1 + x_2v_2 + \ldots + x_kv_k \end{array}.$$

Como o núcleo da transformação $\ker(T)$ é constituído apenas pelo vetor nulo, T é uma transformação linear injetora. Assim, pelo Teorema do Núcleo e da Imagem, temos $\dim(Im\ (T)) = k$, o que implica

$$Im(T) = \mathcal{C}.$$

Portanto, dar um código $\mathcal{C} \subset \mathbb{F}_q^n$ de dimensão k é equivalente a dar uma transformação linear injetora

$$T : \mathbb{F}_q^k \to \mathbb{F}_q^n$$

e definir $\mathcal{C} = Im(T)$.

Essa é a forma paramétrica dos subespaço $\mathcal{C}$, pois os elementos de $\mathcal{C}$ estão parametrizados pelos elementos x de $\mathbb{F}_q^k$ através de T, o que torna fácil gerar todos os elementos de $\mathcal{C}$.

No entanto, é difícil decidir se um elemento $v \in \mathbb{F}_q^n$ pertence ou não ao código $\mathcal{C}$, pois, para tal, é necessário resolver o sistema de n equações nas k incógnitas $x_1, \ldots, x_k$ abaixo

$$x_1v_1 + x_2v_2 + \ldots + x_kv_k = v$$

e essa solução, em geral, representa um custo computacional muito elevado.

A outra maneira de descrevermos um código $\mathcal{C}$ é através do núcleo de uma transformação linear. Assim, tomando uma base para $\mathcal{C}$ e completando-a, a fim de que os vetores adicionados constituam uma base para um subespaco $\mathcal{C}'$ de $\mathbb{F}_q^n$ complementar de $\mathcal{C}$, isto é,

$$\mathcal{C} \oplus \mathcal{C}' = \mathbb{F}_q^n,$$

e considerando a aplicação linear

$$\begin{array}{rccc} H: & \mathcal{C} \oplus \mathcal{C}' & \to & \mathbb{F}_q^{n-k} \\ & u \oplus v & \mapsto & v \end{array},$$

temos $\ker(H) = \mathcal{C}$. Computacionalmente, é muito mais simples determinar se um certo elemento $v \in \mathbb{F}_q^n$ pertence ou não a $\mathcal{C}$. Para isto, basta verificar se $H(v)$ é ou não o vetor nulo de $\mathbb{F}_q^{n-k}$, o que tem um custo bem pequeno.

Exemplo 1.31 *Considere o corpo* $\mathbb{F}_3 = \{0, 1, 2\}$ *e seja* $\mathcal{C} \subset \mathbb{F}_3^4$ *o código gerado pelos vetores* $v_1 = 1011$ *e* $v_2 = 0112$. *Esse código possui* $9 = 3^2$ *elementos, pois tem dimensão* 2 *sobre um corpo de* 3 *elementos. Uma representação paramétrica de* $\mathcal{C}$ *é dada por*

$$x_1v_1 + x_2v_2 = x_1(1, 0, 1, 1) + x_2(0, 1, 1, 2)$$

ao variar x_1 *e* x_2 *em* $\mathbb{F}_3$.

Definindo a aplicação

$$\begin{array}{rccc} H: & \mathbb{F}_3^4 & \to & \mathbb{F}_3^2 \\ & (x_1, x_2, x_3, x_4) & \mapsto & (2x_1 + 2x_2 + x_3, 2x_1 + x_2 + x_4) \end{array},$$

o código $\mathcal{C}$ *pode ser representado como núcleo desta transformação linear, uma vez que*

$$\begin{array}{rcl} Ker(H) & = & \left\{(x_1, \ldots, x_4) \in \mathbb{F}_3^4; 2x_1 + 2x_2 + x_3 = 0 \text{ e } 2x_1 + x_2 + x_4 = 0\right\} \\ & = & \left\{(x_1, \ldots, x_4) \in \mathbb{F}_3^4; x_3 = x_1 + x_2 \text{ e } x_4 = x_1 + 2x_2\right\} \\ & = & \{x_1(1, 0, 1, 1) + x_2(0, 1, 1, 2); x_1, x_2 \in \mathbb{F}_3\} = \mathcal{C}. \end{array}$$

Definição 1.32 *Seja* $\mathcal{C} \subset \mathbb{F}_q^n$ *um código linear. Chamamos* ***parâmetros do código*** $\mathcal{C}$ *a terna de inteiros* (n, k, d), *onde* k *é a dimensão de* $\mathcal{C}$ *sob* $\mathbb{F}_q$ *e* d *é a distância mínima de* $\mathcal{C}$.

Seja $\beta = \{v_1, v_2, \cdots, v_k\}$ uma base ordenada de $\mathcal{C}$ e considere a matriz G de ordem $k \times n$ dada por

$$G = \begin{pmatrix} v_1 \\ \vdots \\ v_k \end{pmatrix} = \begin{pmatrix} v_{11} & v_{12} & \ldots & v_{1n} \\ \vdots & \vdots & & \vdots \\ v_{k1} & v_{k2} & \ldots & v_{kn} \end{pmatrix}$$

A matriz G é chamada **matriz geradora** do código $\mathcal{C}$ associada à base β. A matriz geradora G gera uma transformação linear injetora definida por

$$\begin{array}{rccc} T: & \mathbb{F}_q^k & \to & \mathbb{F}_q^n \\ & x & \mapsto & x \cdot G \end{array}.$$

Se $x = (x_1, \ldots, x_k)$, então

$$T(x) = x \cdot G = x_1v_1 + \ldots + x_kv_k$$

e assim G gera uma transformação linear T cuja imagem $Im(T) = T(\mathbb{F}_q^k)$ é o código $\mathcal{C}$.

Note que a matriz G não é univocamente determinada por $\mathcal{C}$, pois ela depende da escolha da base β. Como uma base de um espaço vetorial pode ser obtida de uma outra base qualquer através de sequências de operações do tipo:

(i) Permutação de dois elementos da base;

(ii) Multiplicação de um elemento da base por um escalar não nulo; ou

(iii) Substituição de um vetor da base por ele mesmo somado com um múltiplo escalar de um outro vetor da base,

segue que duas matrizes geradoras de um mesmo código $\mathcal{C}$ podem ser obtidas uma da outra por uma sequência de operações do tipo:

(L_1) Permutação de duas linhas;

(L_2) Multiplicação de uma linha por um escalar não nulo;

(L_3) Adição de um múltiplo escalar de uma linha a outra.

Inversamente, podemos construir códigos a partir de matrizes geradoras G. Para isso, basta tomarmos uma matriz $k \times n$ cujas linhas são linearmente independentes e definir um código como sendo a imagem da transformação linear

$$\begin{array}{rccc} T: & \mathbb{F}_q^k & \to & \mathbb{F}_q^n \\ & x & \mapsto & x \cdot G \end{array} .$$

Exemplo 1.33 *Seja* $G = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 \end{pmatrix}$ *uma matriz com entradas em* $\mathbb{F}_2$ *e considere a transformação linear injetora*

$$\begin{array}{rccc} T: & \mathbb{F}_2^3 & \to & \mathbb{F}_2^5 \\ & x & \mapsto & x \cdot G \end{array} .$$

Assim, obtemos um código $\mathcal{C}$ *de dimensão* 3 *em* $\mathbb{F}_2^5$ *que é a imagem de* T*. A palavra* 101 *do código da fonte, por exemplo, é codificada como* 01010*.*

Definição 1.34 *Uma matriz geradora* G *de um código* $\mathcal{C}$ *está na* ***forma padrão*** *se tivermos*

$$G = (Id_k | A)\,,$$

onde Id_k *é a matriz identidade de ordem* k *e* A *é uma matriz* $k \times (n-k)$*.*

Dado um código $\mathcal{C}$, nem sempre é possível encontrar uma matriz geradora de $\mathcal{C}$ na forma padrão efetuando operações sobre as linhas. No entanto, efetuando também sequências de operações sobre as colunas de G como:

(C_1) Permutação de duas colunas;

(C_2) Multiplicação de uma coluna por um escalar não nulo,

obteremos uma matriz G' de um código $\mathcal{C}'$ equivalente a $\mathcal{C}$ e G' estará na forma padrão.

Teorema 1.35 *[12] Dado um código $\mathcal{C}$, existe um código equivalente $\mathcal{C}'$ com matriz geradora na forma padrão.*

Demonstração: Seja G uma matriz geradora de $\mathcal{C}$. Mostraremos que com uma sequência de operações do tipo (L_1), (L_2), (L_3) e (C_1) podemos colocar G na forma padrão. Suponhamos

$$G = \begin{pmatrix} g_{11} & g_{12} & \dots & g_{1n} \\ \vdots & \vdots & & \vdots \\ g_{k1} & g_{k2} & \dots & g_{kn} \end{pmatrix}.$$

Como as linhas de G são vetores da base de $\mathcal{C}$, elas são linearmente independentes e, assim, a primeira linha de G é não nula. Por (C_1), podemos supor $g_{11} \neq 0$. Multiplicando a primeira linha por g_{11}^{-1} (operação (L_2)), podemos colocar 1 no lugar de g_{11}.

Somando à linha i, onde $2 \leq i \leq k$, a primeira linha multiplicada por $(-1)g_{i1}$ (operações (L_3)), obtemos uma matriz da forma

$$\begin{pmatrix} 1 & b_{12} & \dots & b_{1n} \\ 0 & b_{22} & \dots & b_{2n} \\ \vdots & \vdots & & \vdots \\ 0 & b_{k2} & \dots & b_{kn} \end{pmatrix}.$$

Agora, na segunda linha dessa matriz, temos certamente um elemento não nulo que, por meio de uma operação (C_1), pode ser colocado na segunda linha e segunda coluna. Multiplicando a segunda linha pelo inverso desse elemento, a matriz se transforma em

$$\begin{pmatrix} 1 & c_{12} & c_{13} & \dots & c_{1n} \\ 0 & 1 & c_{23} & \dots & c_{2n} \\ 0 & c_{32} & c_{33} & \dots & c_{3n} \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & c_{k2} & c_{23} & \dots & c_{kn} \end{pmatrix}.$$

Novamente, usando operações (L_3), obtemos a matriz

$$\begin{pmatrix} 1 & 0 & d_{13} & \dots & d_{1n} \\ 0 & 1 & d_{23} & \dots & d_{2n} \\ 0 & 0 & d_{33} & \dots & d_{3n} \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & d_{23} & \dots & d_{kn} \end{pmatrix}$$

e assim sucessivamente, até encontrarmos uma matriz na forma padrão

$$G' = (Id_k|A)\,.$$

□

1.1.4 Dualidade

Definição 1.36 *Sejam $u = (u_1, \ldots, u_n)$ e $v = (v_1, \ldots, v_n)$ elementos de $\mathbb{F}_q^n$. O **produto interno formal** de u e v é dado por*

$$\langle u, v\rangle = u_1v_1 + \ldots + u_nv_n = \sum_{i=1}^{n} u_iv_i.$$

*Se $\langle u, v\rangle = 0$, diremos que u e v são **ortogonais**.*

Note que o produto interno formal é uma forma bilinear simétrica sobre $\mathbb{F}_q$.

Definição 1.37 *Seja $\mathcal{C} \subset \mathbb{F}_q^n$ um código linear. O **dual** de $\mathcal{C}$ é dado por*

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

Lema 1.38 *[12] Seja $\mathcal{C}$ um (n, k) código linear com matriz geradora G na forma padrão. Então:*

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

(*ii*) *$x \in \mathcal{C}^{\perp}$ se, e somente se, $G \cdot x^t = 0$;*

(*iii*) $\dim\left(\mathcal{C}^{\perp}\right) = n - k$;

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

Demonstração:

(*i*) Sejam $u, v \in \mathcal{C}^{\perp}$ e $\lambda \in \mathbb{F}_q$. Assim, $\langle u, x\rangle = \langle v, x\rangle = 0$ para todo $x \in \mathcal{C}$ e, daí,

$$\langle v + u, x\rangle = \langle v, x\rangle + \langle u, x\rangle = 0 + 0 = 0,$$

donde temos $u + v \in \mathcal{C}^{\perp}$.

Além disso, como $\langle \lambda v, x\rangle = \lambda\langle v, x\rangle = 0$ e $\mathcal{C}^{\perp} \neq \emptyset$ (pois $0 \in \mathcal{C}^{\perp}$), segue que $\mathcal{C}^{\perp}$ é um subespaço de $\mathbb{F}_q^n$.

(*ii*) Note que $x \in \mathcal{C}^{\perp}$ se, e somente se, x é ortogonal a todas as palavras de $\mathcal{C}$ e esta última condição ocorre se, e somente se, x é ortogonal a todos os vetores de uma base de $\mathcal{C}$. Como as linhas da matriz geradora G são vetores de uma base de $\mathcal{C}$, segue que a última condição é equivalente a $G \cdot x^t = 0$.

(*iii*) Pela parte (*ii*), $x \in \mathcal{C}^{\perp}$ se, e somente se, $G \cdot x^t = 0$. Como G está na forma padrão, podemos reescrever esta última igualdade como

$$(Id_k|A) \cdot x^t = 0.$$

Assim,

$$\left(\begin{array}{cccc|ccc} 1 & 0 & \dots & 0 & a_{1,k+1} & \dots & a_{1,n} \\ 0 & 1 & \dots & 0 & a_{2,k+1} & \dots & a_{2,n} \\ \vdots & \vdots & & \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & 1 & a_{k,k+1} & \dots & a_{k,n} \end{array}\right) \cdot \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

e efetuando o produto de matrizes, obtemos

$$\begin{pmatrix} x_1 + a_{1,k+1}x_{k+1} + \ldots + a_{1n}x_n \\ x_2 + a_{2,k+1}x_{k+1} + \ldots + a_{2n}x_n \\ \vdots \\ x_k + a_{k,k+1}x_{k+1} + \ldots + a_{kn}x_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix},$$

o que é equivalente a

$$\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_k \end{pmatrix} + \begin{pmatrix} a_{1,k+1} & \dots & a_{1n} \\ a_{2,k+1} & \dots & a_{2n} \\ \vdots & & \vdots \\ a_{k,k+1} & \dots & a_{kn} \end{pmatrix} \cdot \begin{pmatrix} x_{k+1} \\ x_{k+2} \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Isto é,

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

se fizermos

$$A = \begin{pmatrix} a_{1,k+1} & \dots & a_{1n} \\ a_{2,k+1} & \dots & a_{2n} \\ \vdots & & \vdots \\ a_{k,k+1} & \dots & a_{kn} \end{pmatrix}.$$

Dessa forma, $\mathcal{C}^{\perp}$ possui q^{n-k} elementos, pois existem q escolhas para cada uma das $n-k$ entradas do vetor $(x_{k+1} \ldots x_n)^t$ e uma vez determinadas estas entradas, ficam determinadas as outras k entradas do vetor $(x_1 \ldots x_k)^t$.

Portanto,

$$\dim_{\mathbb{F}_q}\left(\mathcal{C}^{\perp}\right) = log_q\left|\mathcal{C}^{\perp}\right| = log_q(q^{n-k}) = n-k.$$

(*iv*) Se $H = (-A^t|Id_{n-k})$, as linhas de H são linearmente independentes por causa do bloco Id_{n-k} e, portanto, geram um subespaço de dimensão $n-k$. Repare que as linhas de H são ortogonais às linhas de $G = (Id_k|A)$. Assim, o espaço gerado pelas linhas de H está contido em $\mathcal{C}^\perp$. Como estes subespaços possuem a mesma dimensão, eles coincidem e, assim, H é uma matriz geradora de $\mathcal{C}^\perp$.

□

Definição 1.39 *Diremos que dois códigos lineares $\mathcal{C}$ e $\mathcal{C}'$ são* **linearmente equivalentes** *se existir uma isometria linear $T : \mathbb{F}_q^n \to \mathbb{F}_q^n$ tal que $T(\mathcal{C}) = \mathcal{C}'$, onde o termo* **isometria linear** *significa que T é uma transformação linear e uma isometria de $\mathbb{F}_q^n$.*

Note que se π é uma permutação de $\{1, \ldots, n\}$ então a isometria T_π definida no Exemplo 1.24 é linear. Além disso, se $f_i : \mathbb{F}_q \to \mathbb{F}_q$, $i = 1, \ldots, n$, são bijeções lineares, então a aplicação T_f^i definida no Exemplo 1.23 é uma isometria linear de $\mathbb{F}_q^n$.

Lema 1.40 *[12] Se π é uma permutação de $\{1, \ldots, n\}$ e $f_i : \mathbb{F}_q \to \mathbb{F}_q$, $i = 1, \ldots, n$, são bijeções, então:*

(*i*) *Uma função $f : \mathbb{F}_q \to \mathbb{F}_q$ é linear se, e somente se, existe um elemento $c \in \mathbb{F}_q$ tal que $f(x) = cx$, para qualquer $x \in \mathbb{F}_q$.*

(*ii*) *A aplicação $T_\pi \circ T_{f_1}^1 \circ \ldots \circ T_{f_n}^n$ é linear se, e somente se, cada f_i é linear.*

(*iii*) *Seja $\mathcal{C}$ um código linear em $\mathbb{F}_q^n$, $f(x) = cx$ a lei de formação da aplicação $f : \mathbb{F}_q \to \mathbb{F}_q$, com $c \in \mathbb{F}_q$. Defina $T_c^i = T_f^i$, para cada $i = 1, \ldots, n$; então $(T_\pi(\mathcal{C}))^\perp = T_\pi\left(\mathcal{C}^\perp\right)$ e, para $c \in \mathbb{F}_q \backslash \{0\}$, tem-se que $(T_c^i(\mathcal{C}))^\perp = T_{c^{-1}}^i\left(\mathcal{C}^\perp\right)$.*

Demonstração:

(*i*) Se existe um elemento $c \in \mathbb{F}_q$ tal que $f(x) = cx$, para qualquer $x \in \mathbb{F}_q$, então f é linear, pois dados $x, y \in \mathbb{F}_q$

$$f(x+y) = c(x+y) = cx + cy = f(x) + f(y)$$

e

$$f(\lambda x) = c(\lambda x) = \lambda(cx) = \lambda f(x).$$

Note que $f(1) = c$, para algum $c \in \mathbb{F}_q$. Supondo agora que f é uma transformação linear, devemos ter $f(\lambda y) = \lambda f(y)$, para $\lambda, y \in \mathbb{F}_q$ e, assim, para todo $x \in \mathbb{F}_q$,

$$f(x) = f(x \cdot 1) = xf(1) = xc = cx.$$

(*ii*) Se cada f_i é linear então cada T_f^i também o é. Como T_π também é linear e a composição de operadores lineares é linear, segue que a aplicação $T_\pi \circ T_{f_1}^1 \circ \ldots \circ T_{f_n}^n$ é linear. Por outro lado, $T_\pi \circ T_{f_1}^1 \circ \ldots \circ T_{f_n}^n$ é linear se, e somente se, $T_{f_1}^1 \circ \ldots \circ T_{f_n}^n$ o é, e o efeito desta última composição sobre a entrada i de um vetor $v \in \mathbb{F}_q^n$ é aplicação de f_i nesta entrada. Para que essa composição seja linear, ela deve ser linear em cada entrada, e isto só é possível se cada f_i for linear.

(*iii*) Seja $x = (x_1, \ldots, x_n) \in \mathbb{F}_q^n$. Temos

$$\begin{aligned}
x \in (T_\pi(\mathcal{C}))^\perp &\Leftrightarrow \langle x, T_\pi(y)\rangle = 0, \quad \text{para todo } y = (y_1, \ldots, y_n) \in \mathcal{C} \\
&\Leftrightarrow x_1 y_{\pi(1)} + \ldots + x_n y_{\pi(n)} = 0, \quad \text{para todo } y \in \mathcal{C} \\
&\overset{(i)}{\Leftrightarrow} x_{\pi^{-1}(1)} y_1 + \ldots + x_{\pi^{-1}(n)} y_n = 0, \quad \text{para todo } y \in \mathcal{C} \\
&\Leftrightarrow \langle T_{\pi^{-1}}(x), y\rangle = 0, \quad \text{para todo } y \in \mathcal{C} \\
&\Leftrightarrow T_{\pi^{-1}}(x) \in \mathcal{C}^\perp \\
&\overset{(ii)}{\Leftrightarrow} T_\pi^{-1}(x) \in \mathcal{C}^\perp \\
&\Leftrightarrow x \in T_\pi\left(\mathcal{C}^\perp\right),
\end{aligned}$$

onde em (i) usamos o fato que $\pi(i) = j$ se, e somente se, $i = \pi^{-1}(j)$ e reordenamos as parcelas, se necessário e, em (ii), fizemos $T_{\pi^{-1}}(x) = T_\pi^{-1}(x)$, uma vez que $\left(T_{\pi^{-1}} \circ T_\pi\right)(x) = x$.

Além disso, fixado $i \in \{1, \ldots, n\}$, temos

$$\begin{aligned}
x \in \left(T_c^i(\mathcal{C})\right)^\perp &\Leftrightarrow \langle x, T_c^i(y)\rangle = 0, \quad \text{para todo } y = (y_1, \ldots, y_n) \in \mathcal{C} \\
&\Leftrightarrow x_1 y_1 + \ldots + x_i(c y_i) + \ldots + x_n y_n = 0, \quad \text{para todo } y \in \mathcal{C} \\
&\Leftrightarrow y_1 x_1 + \ldots + y_i(c x_i) + \ldots + y_n x_n = 0, \quad \text{para todo } y \in \mathcal{C} \\
&\Leftrightarrow \langle y, T_c^i(x)\rangle = 0, \quad \text{para todo } y \in \mathcal{C} \\
&\Leftrightarrow T_c^i(x) \in \mathcal{C}^\perp \\
&\Leftrightarrow x \in \left(T_c^i\right)^{-1}\left(\mathcal{C}^\perp\right) = T_{c^{-1}}^i\left(\mathcal{C}^\perp\right),
\end{aligned}$$

uma vez que $\left(T_c^i \circ T_{c^{-1}}^i\right)(x) = x$.

□

Observação 1.41 *O Lema 1.40 e o Teorema 1.25 nos permitem concluir que dois códigos lineares $\mathcal{C}$ e $\mathcal{C}'$ são linearmente equivalentes se, e somente se, existem uma permutação π de $\{1, \ldots, n\}$ e elementos $c_1, \ldots, c_n$ de $\mathbb{F}_q \backslash \{0\}$ tais que*

$$\mathcal{C}' = \left\{\left(c_1 x_{\pi(1)}, \ldots, c_n x_{\pi(n)}\right); (x_1, \ldots, x_n) \in \mathcal{C}\right\},$$

ou seja, dois códigos lineares são linearmente equivalentes se, e somente se, um deles pode ser obtido do outro mediante uma sequência de operações do tipo:

(*i*) *Multiplicação dos elementos numa dada posição fixa por um escalar não nulo em todas as palavras.*

(*ii*) *Permutação das posições das coordenadas de todas as palavras do código, mediante uma permutação fixa de* $\{1, \ldots, n\}$.

Esta caracterização nos permitirá estender o item (*iii*) do Lema 1.38 para códigos em que a matriz geradora não pode ser colocada na forma padrão:

Proposição 1.42 *[12] Sejam* $\mathcal{C}$ *e* $\mathcal{D}$ *dois códigos lineares em* $\mathbb{F}_q^n$.

(*i*) *Se* $\mathcal{C}$ *e* $\mathcal{D}$ *são linearmente equivalentes, então* $\mathcal{C}^\perp$ *e* $\mathcal{D}^\perp$ *são linearmente equivalentes;*

(*ii*) *Se* $\dim_{\mathbb{F}_q}(\mathcal{D}) = k$, *então* $\dim_{\mathbb{F}_q}\left(\mathcal{D}^\perp\right) = n - k$.

Demonstração:

(*i*) Como $\mathcal{C}$ e $\mathcal{D}$ são linearmente equivalentes, pela Observação 1.41 existem uma permutação π de $\{1, \ldots, n\}$ e elementos $c_1, \ldots, c_n$ de $\mathbb{F}_q \backslash \{0\}$ tais que

$$\mathcal{D} = T_\pi \circ T_{c_1}^1 \circ \ldots \circ T_{c_n}^n(\mathcal{C}).$$

Assim,

$$\begin{aligned}
\mathcal{D}^\perp &= \left(T_\pi \circ T_{c_1}^1 \circ \ldots \circ T_{c_n}^n(\mathcal{C})\right)^\perp \\
&= \left(T_\pi\left(T_{c_1}^1 \circ \ldots \circ T_{c_n}^n(\mathcal{C})\right)\right)^\perp \\
&\overset{(1)}{=} T_\pi\left(T_{c_1}^1 \circ \ldots \circ T_{c_n}^n(\mathcal{C})\right)^\perp \\
&\overset{(2)}{=} T_\pi\left(T_{c_1^{-1}}^1\left(T_{c_2}^2 \ldots \circ T_{c_n}^n(\mathcal{C})\right)^\perp\right) \\
&\quad \vdots \\
&\overset{(n+1)}{=} T_\pi \circ T_{c_1^{-1}}^1 \circ \ldots \circ T_{c_n^{-1}}^n\left(\mathcal{C}^\perp\right),
\end{aligned}$$

onde em $(1), (2), \ldots, (n+1)$ usamos repetidas vezes o Lema 1.40.

Portanto, $\mathcal{C}^\perp$ e $\mathcal{D}^\perp$ são linearmente equivalentes, pois existe a isometria linear

$$T_\pi \circ T_{c_1^{-1}}^1 \circ \ldots \circ T_{c_n^{-1}}^n$$

que faz a correspondência entre $\mathcal{C}^\perp$ e $\mathcal{D}^\perp$.

(*ii*) Pelo Teorema 1.35, existe um código $\mathcal{C}$ de dimensão k que é linearmente equivalente a $\mathcal{D}$, com matriz geradora na forma padrão. Pelo Lema 1.38 (*iii*), $\dim\left(\mathcal{C}^\perp\right) = n - k$ e, pelo item (*i*) da Proposição 1.42, $\dim_{\mathbb{F}_q}(\mathcal{D}^\perp) = n - k$, uma vez que $\mathcal{D}^\perp$ e $\mathcal{C}^\perp$ são linearmente equivalentes e, portanto, têm os mesmos parâmetros.

□

Lema 1.43 *[12] Seja $\mathcal{C}$ um (n,k) código linear com matriz geradora G. Uma matriz H de ordem $(n-k)\times n$ com coeficientes em $\mathbb{F}_q$ e com linhas linearmente independentes é uma matriz geradora de $\mathcal{C}^\perp$ se, e somente se,*

$$G \cdot H^t = 0.$$

DEMONSTRAÇÃO: Como H possui $n-k$ linhas linearmente independentes, estas geram um subespaço vetorial de $\mathbb{F}_q^n$ de dimensão $n-k$, portanto, igual à dimensão de $\mathcal{C}^\perp$. Representando por $h_1,\ldots,h_{n-k}$ as linhas de H e por $g_1,\ldots,g_k$ as linhas de G, segue que o elemento que está na linha i e na coluna j da matriz $G\cdot H^t$ é dado por $\langle g_i, h_j\rangle$.

Desta forma, $G\cdot H^t = 0$ equivale a dizer que $\langle g_i, h_j\rangle = 0$, para todos i,j, isto é, os vetores do subespaço gerado pelas linhas de H estão em $\mathcal{C}^\perp$. Como esse subespaço possui a mesma dimensão que $\mathcal{C}^\perp$, eles coincidem e, assim, $\mathcal{C}^\perp$ é gerado pelas linhas de H, isto é, H é uma matriz geradora de $\mathcal{C}^\perp$. □

Corolário 1.44 $\left(\mathcal{C}^\perp\right)^\perp = \mathcal{C}$.

DEMONSTRAÇÃO: Sejam G e H as matrizes geradoras de $\mathcal{C}$ e $\mathcal{C}^\perp$, respectivamente. Assim, $G\cdot H^t = 0$ e, daí, $H\cdot G^t = (G\cdot H^t)^t = 0$, donde concluímos pelo Lema 1.43 que G é uma matriz geradora de $\left(\mathcal{C}^\perp\right)^\perp$ e, assim, $\left(\mathcal{C}^\perp\right)^\perp = \mathcal{C}$. □

Proposição 1.45 *Seja $\mathcal{C}$ um código linear e seja H uma matriz geradora de $\mathcal{C}^\perp$. Então:*

$$v \in \mathcal{C} \text{ se, e somente se, } H\cdot v^t = 0.$$

DEMONSTRAÇÃO: Pelo Lema 1.38 (ii), $x\in\mathcal{C}^\perp$ se, e somente se $G\cdot x^t = 0$. Assim,

$$v \in \mathcal{C} = \left(\mathcal{C}^\perp\right)^\perp \Leftrightarrow H\cdot v^t = 0.$$

□

Pela Proposição 1.45, H também é chamada uma **matriz teste de paridade** do código $\mathcal{C}$, pois permite caracterizar os elementos de um código $\mathcal{C}$ por uma condição de anulamento. O vetor $H\cdot v^t$ é chamado **síndrome** de v.

Exemplo 1.46 *Seja $\mathcal{C}$ o código sobre $\mathbb{F}_2$ com matriz geradora*

$$G = \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \end{array}\right).$$

Como G está na forma padrão, a matriz H, teste de paridade para $\mathcal{C}$ é dada por

$$H = \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{array}\right),$$

devido ao Lema 1.38 (iv). Tomando $v = 100111$ e $v' = 010101$, temos $v \in \mathcal{C}$ e $v' \notin \mathcal{C}$, pois

$$H \cdot v^t = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

e

$$H \cdot (v')^t = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \neq \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}.$$

Lema 1.47 *Se H é uma matriz teste de paridade de um código $\mathcal{C}$ então $\omega(\mathcal{C}) \geq s$ se, e somente se, quaisquer $s-1$ colunas de H são linearmente independentes.*

Demonstração: Faremos essa demonstração por absurdo.

Suponhamos que cada conjunto de $s-1$ colunas de H seja linearmente independente e $\omega(\mathcal{C}) < s$. Seja $c = (c_1, \ldots, c_n)$ uma palavra não nula de $\mathcal{C}$ e sejam $h^1, h^2, \ldots, h^n$ as colunas de H. Como H é matriz teste de paridade de $\mathcal{C}$, temos $H \cdot c^t = 0$, pela Proposição 1.45. Assim,

$$0 = H \cdot c^t = 0 = \sum_{i=1}^{n} c_1 h^i.$$

Como $\omega(c)$ é o número de componentes não nulas de c, se

$$\omega(c) \leq s - 1,$$

então existe um número t de coordenadas não nulas de c (com $1 \leq t \leq s-1$) e, consequentemente, existe uma combinação linear nula de t colunas de H onde os coeficientes são não nulos, o que é um absurdo pois supomos que qualquer conjunto de $s-1$ colunas (e consequentemente qualquer conjunto com um número menor dessas colunas) é linearmente independente.

Reciprocamente, supondo $\omega(\mathcal{C}) \geq s$ e que existam $s-1$ colunas de H linearmente dependentes, digamos $h^{i_1}, \ldots, h^{i_{s-1}}$, existiria uma combinação linear

$$\sum_{k=1}^{s-1} c_{i_k} h^{i_k} = 0,$$

onde os elementos $c_{i_1}, \ldots, c_{i_{s-1}} \in \mathbb{F}_q$ não são todos nulos.

Note que o vetor $c = (c_l)$, $1 \leq l \leq n$, onde

$$c_l = \begin{cases} c_{i_k}, & k = 1, \ldots, s-1 \\ 0, & \text{caso contrário} \end{cases}$$

é uma palavra de $\mathcal{C}$ (pois $H \cdot c^t = 0$) e possui peso

$$\omega(c) \leq s - 1 < s,$$

o que é um absurdo, pois estamos supondo $\omega(\mathcal{C}) \geq s$. □

Teorema 1.48 *[12] Se H é uma matriz teste de paridade de um código $\mathcal{C}$, então $\omega(\mathcal{C}) = s$ se, e somente se, quaisquer $s-1$ colunas de H são linearmente independentes e existem s colunas de H linearmente dependentes.*

Demonstração: Novamente, faremos a prova por absurdo.

Suponhamos que $\omega(\mathcal{C}) = s$. Assim, todo conjunto de $s-1$ colunas de H é linearmente independente pelo Lema 1.47. Se não existissem s colunas de H linearmente dependentes, todo conjunto de s colunas de H seria linearmente independente e, novamente pelo Lema 1.47,

$$s = \omega(\mathcal{C}) \geq s + 1,$$

um absurdo.

Reciprocamente, suponhamos que todo conjunto de $s-1$ colunas de H seja linearmente independente e que existam s colunas linearmente dependentes. Pelo Lema 1.47, $\omega(\mathcal{C}) \geq s$. Se tivéssemos $\omega(\mathcal{C}) > s$, isto é, $\omega(\mathcal{C}) \geq s + 1$, pelo mesmo lema, quaisquer s colunas de H seriam linearmente independentes, uma contradição. Logo, $\omega(\mathcal{C}) = s$. □

Corolário 1.49 (Limitante de Singleton) *[12] Os parâmetros (n, k, d) de um código linear satisfazem à desigualdade*

$$d \leq n - k + 1.$$

Demonstração: Se H é uma matriz teste de paridade de $\mathcal{C}$, então o posto de H (isto é, o número máximo de colunas linearmente independentes de H) é $n-k$, pela Proposição 1.42 (ii). Seja $d = \omega(\mathcal{C})$. Pelo teorema anterior, devemos ter $d - 1 \leq n - k$ e, assim, concluímos que $d \leq n - k + 1$. □

Definição 1.50 *Um código será chamado* ***separado por distância máxima (MDS)*** *(Maximum Distance Separable, em inglês) se valer a igualdade*

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

A classe dos códigos MDS é de particular interesse pois, por possuir a maior distância mínima possível, fornece códigos com a maior capacidade de correção e detecção de erros (ver Teorema 1.14). Além disso, como veremos no Capítulo 3, os códigos MDS possuem boa interpretação geométrica.

Definição 1.51 *Um código $\mathcal{C}$ é dito* ***degenerado*** *se existe uma matriz geradora de $\mathcal{C}$ com uma coluna nula. Caso contrário, ele é dito* ***não-degenerado****.*

Teorema 1.52 *[12] Um código $\mathcal{C} \subset \mathbb{F}_q^n$ é não-degenerado se, e somente se, $d(\mathcal{C}^\perp) \geq 2$.*

Demonstração: Pela contra-positiva, basta mostrar que

$$d(\mathcal{C}^\perp) = 1 \Leftrightarrow \mathcal{C} \text{ é degenerado.}$$

De fato, se $d(\mathcal{C}^\perp) = 1$, então existe uma palavra $v \in \mathcal{C}^\perp$ tal que v possui apenas uma entrada não-nula. Como $v \in \mathcal{C}^\perp$, v é ortogonal a todos os vetores linha de uma matriz geradora de $\mathcal{C}$ e isto só será possível se uma coluna dessa matriz for nula. Assim, $\mathcal{C}$ é degenerado. Para a recíproca, tome uma matriz geradora de $\mathcal{C}$ que possui uma coluna nula e perceba que existirá $v \in \mathcal{C}^\perp$ tal que a única entrada não nula de v corresponda à posição da coluna nula da matriz geradora de $\mathcal{C}$. Assim, $\omega(v) = 1$. □

Neste trabalho, lidaremos apenas com códigos não-degenerados.

1.2 Matrizes ortogonais

Na década de 40, em uma série de artigos, C. R. Rao introduziu determinados arranjos combinatórios visando aplicações em Estatística. Embora Rao tenha considerado num primeiro momento apenas uma subclasse desses arranjos, toda a classe rapidamente se popularizou e ficou conhecida como **matrizes ortogonais** ou **OA**s (*Orthogonal Arrays*, em inglês). Apesar do nome, uma "matriz ortogonal" não é uma matriz cujas colunas são ortogonais, como infere o senso comum, nem tampouco há alguma menção a um produto interno em sua definição. O adjetivo "ortogonal" possui uma aplicação específica em Estatística e seu nome é devido a Bush [6].

Além da Estatística, matrizes ortogonais também são usadas em Computação e Criptografia. Na Matemática, possuem ligações com a Geometria Projetiva Finita, Teoria de Algoritmos e, como veremos, códigos corretores de erros.

Aqui temos um exemplo de uma matriz ortogonal de força 2:

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

Escolhendo quaisquer duas colunas, digamos a primeira e a última:

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

cada um dos vetores linha $(0,0)$, $(0,1)$, $(1,0)$ e $(1,1)$, aparece uma mesma quantidade de vezes (3 vezes, na verdade) nessa escolha de colunas. Essa propriedade caracteriza uma matriz ortogonal. O número de colunas escolhido é denominado **força** e o número de repetições de cada vetor é denominado **índice**.

Como apenas 0s e 1s aparecem, esta é chamada uma **matriz de dois níveis**. Existem 12 linhas e 11 colunas, o que significa que esta é uma **matriz de tamanho** 12 e 11 **restrições**.

Numa forma compacta, dizemos que esta é uma $OA(11, 12, 2, 2)$.

Nesta representação, a primeira coordenada indica o número de colunas, a segunda o número de linhas, a terceira a quantidade de níveis e a quarta a força da matriz. Como veremos, não há necessidade de explicitar o índice, uma vez que este fica determinado pelos outros parâmetros anteriores.

Definição 1.53 *Sejam k, N e t inteiros positivos tais que $t \leq N$. Uma matriz A com entradas em $\{0, 1, 2, \ldots, n\}$ é chamada uma* ***matriz ortogonal de força*** *t,*

tamanho *k, N* ***restrições*** *e s* ***níveis*** *se a matriz A possui N colunas, k linhas, seus elementos podem ser escolhidos dentre s números e, em cada submatriz de A de ordem $k \times t$, todos os possíveis vetores linha (de ordem $1 \times t$) aparecem com a mesma frequência λ. Denotaremos esta matriz por $OA(N, k, s, t)$ e chamaremos o número λ de* ***índice*** *da matriz ortogonal.*

Exemplo 1.54 *Aqui temos uma $OA(7, 18, 3, 2)$ de índice $\lambda = 2$:*

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

Note que, escolhendo quaisquer $t = 2$ colunas, cada um dos vetores linha $(0, 0)$, $(0, 1)$, $(0, 2)$, $(1, 0)$, $(1, 1)$, $(1, 2)$, $(2, 0)$, $(2, 1)$ e $(2, 2)$ ocorrem exatamente $\lambda = 2$ vezes.

Exemplo 1.55 *A seguinte matriz é uma $OA(8, 4, 2, 3)$ de índice $\lambda = 1$:*

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

Matrizes ortogonais podem não existir para valores arbitrários dos parâmetros N, k, s e t. Sabe-se, por exemplo, que nenhuma $(8, 5, 2, 3)$ matriz ortogonal existe (veja em [18]). Um importante problema neste contexto é a construção de matrizes com o maior número possível de colunas [18]. Sabe-se, por exemplo, que quanto maior a força, mais difícil é a construção de uma OA que possua essa força [11].

Teorema 1.56 *[11] Se A é uma (N, k, s, t) matriz ortogonal de índice λ, então $k = \lambda s^t$.*

Demonstração: Note que, como A têm força t e índice λ, escolhendo quaisquer t colunas de A, um vetor linha v aparecerá exatamente λ vezes. Como as entradas da matriz A podem ser escolhidas dentre s elementos, existem s^t vetores v distintos de ordem $1 \times t$. Portanto, como a matriz A possui k linhas, os s^t vetores distintos aparecem

$$\lambda = \frac{k}{s^t}$$

vezes, o que implica $k = \lambda s^t$. □

Teorema 1.57 *[11] Qualquer matriz ortogonal de força t é também uma matriz ortogonal de força t', para $0 \leq t' < t$. O índice da matriz quando considerado como uma matriz de força t' é $\lambda s^{t-t'}$, onde λ denota o índice da matriz quando considerada com força t.*

Embora a descrição de matrizes ortogonais por forças menores do que a maximal esteja correta, muitas vezes é enganosa. A seguinte observação diz respeito ao efeito da permutação de linhas e colunas em matrizes ortogonais:

Observação 1.58 *[11] Seja $OA(N, k, s, t)$ uma matriz ortogonal. Então:*

(*i*) *Uma permutação das linhas ou colunas dessa OA resulta em outra OA com os mesmos parâmetros.*

(*ii*) *Uma permutação dos níveis dessa OA resulta em outra OA com os mesmos parâ- metros.*

(*iii*) *Qualquer $k \times N'$ submatriz de $OA(N, k, s, t)$ é uma $OA(N', k, s, t')$, onde $t' = \min\{N', t\}$.*

Finalmente, a associação entre códigos corretores de erros e matrizes ortogonais é dada pelo seguinte teorema, cuja extensão daremos no próximo capítulo:

Teorema 1.59 *[11] Se $\mathcal{C} \subset \mathbb{F}_q^n$ é um (n, k, d) código linear tal que a distância mínima do seu código dual $\mathcal{C}^\perp$ é $d^\perp$, então as palavras de $\mathcal{C}$ formam as linhas de uma matriz ortogonal de força $d^\perp - 1$ e índice $q^{k-d^\perp+1}$.*

Demonstração: Seja G uma matriz geradora de $\mathcal{C}$ e seja M uma matriz onde as linhas são as palavras de $\mathcal{C}$, isto é, suas linhas são os vetores do espaço gerado pelas linhas de G. Como G é uma matriz teste de paridade para $\mathcal{C}^\perp$ e $\omega(\mathcal{C}^\perp) = d^\perp$,

pelo Teorema 1.48, quaisquer $d^\perp - 1$ colunas de G são linearmente independentes e, assim, quaisquer $d^\perp - 1$ linhas de G serão linearmente independentes.

Escolhendo quaisquer $d^\perp - 1$ colunas de M e formando uma nova matriz D, existirão $d^\perp - 1$ linhas de D linearmente independentes e essas linhas geram todas as outras linhas de D. Como D possui q^k linhas (pois M possui q^k linhas) e as $d^\perp - 1$ linhas de D geram um espaço com $q^{d^\perp - 1}$ vetores (distintos), cada linha de D deverá se repetir um mesmo número

$$\frac{q^k}{q^{d^\perp - 1}} = q^{k - d^\perp + 1}$$

de vezes, donde concluímos o resultado. □

Exemplo 1.60 *Tome o* $(6, 3, 2)$ *código linear* $\mathcal{C}$ *dado no Exemplo 1.46, que possui uma matriz teste de paridade dada por*

$$H = \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{array}\right).$$

Note que as palavras de $\mathcal{C}^\perp$ *são*

000000	011110
100100	010101
111010	001011
110001	101111

e que, portanto, $\omega(\mathcal{C}^\perp) = 2$.

Note também que as palavras de $\mathcal{C}$ *formam a matriz*

$$M = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$

que é uma matriz ortogonal de força $t = 1 = \omega(\mathcal{C}^\perp) - 1$ *e índice* $\lambda = 2^{3 - \omega(\mathcal{C}^\perp) + 1} = 2^2 = 4$*, uma vez que escolhendo qualquer uma de suas colunas, os vetores linha* 1 *e* 0 *aparecem exatamente* 4 *vezes.*

Capítulo 2

Códigos Poset

O objetivo maior deste capítulo é introduzir ao leitor deste trabalho as principais ideias sobre códigos ponderados por ordens parciais. Iniciaremos tratando das definições e resultados concernentes ao estudo das relações de ordem, suas representações gráficas e da definição de uma nova métrica, baseada em tais relações.

O conceito de métricas ponderadas por ordens parciais (*poset metrics*, em inglês) foi iniciado em 1991 por Niederreider [23] e, posteriormente, generalizado por Brualdi, Graves e Lawrence [5]. Nos últimos anos, muitos trabalhos têm aprofundado o conhecimento sobre esses espaços, especialmente para alguns casos de conjuntos parcialmente ordenados, tais como as ordens coroa [16, 1], hierárquico (ordem fraca) [17] e Rosenbloom-Tsfasman [27, 9].

Após essas considerações, iniciaremos o estudo de códigos lineares com essa nova métrica. Tal estudo possibilitou uma série de avanços teóricos para questões clássicas da Teoria de Códigos, uma vez que generalizou a distância de Hamming definida anteriormente e garantiu a existência de um número maior de códigos perfeitos.

Encerraremos esse capítulo tratando de resultados sobre uma determinada sequência de pesos relacionada aos códigos introduzida em 1991 por V. Wei [31]. Inicialmente com motivações na área da Criptografia, essa sequência possibilitou o estudo da estrutura algébrica de códigos sob uma nova perspectiva e sua extensão para as métricas poset nos concede a generalização de resultados anteriormente conhecidos e o estudo profícuo de determinadas classes de códigos.

2.1 Conjuntos parcialmente ordenados

Definição 2.1 *Uma **ordem parcial** sobre um conjunto X não vazio é uma relação binária $\preceq$ que satisfaz as seguintes propriedades para quaisquer $a, b, c \in X$:*

(i) $a \preceq a$ *(Reflexividade);*

(ii) *Se* $a \preceq b$ *e* $b \preceq a$ *então* $a = b$ *(Antissimetria);*

(iii) *Se* $a \preceq b$ *e* $b \preceq c$ *então* $a \preceq c$ *(Transitividade).*

Definição 2.2 *Seja X um conjunto não vazio. O par ordenado $(X, \preceq)$ é denominado **conjunto parcialmente ordenado** ou **poset** (partial ordered set, em inglês) se $\preceq$ é uma ordem parcial sobre X.*

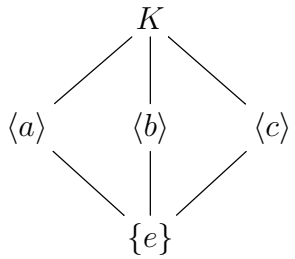
Se $a \preceq b$ ou $b \preceq a$ dizemos que a e b são **comparáveis**. Caso contrário, eles são ditos **incomparáveis**.

Exemplo 2.3 *Seja $X = \{1, 2, 3, 4, 5, 6, 12\}$ e faça $x \preceq y$ se x é um divisor de y, para $x, y \in X$. Então $(X, \preceq)$ é um poset.*

Exemplo 2.4 *Seja $\mathcal{P}(X)$ o conjunto formado por todos os subconjuntos de um conjunto X e tome a relação $\preceq$ tal que $A \preceq B$ se, e somente se, A é um subconjunto de B, para A e B em $\mathcal{P}(X)$. Então $(\mathcal{P}(X), \preceq)$ é um poset.*

Exemplo 2.5 *O conjunto dos números inteiros sob a relação maior do que ou igual a $(\geq)$ é um poset.*

Exemplo 2.6 *Seja $K = \{e, a, b, c\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ o **grupo de Klein**, onde e é o elemento neutro de K. Sabemos que os subgrupos de K são $\{e\}$, $\langle a \rangle = \{e, a\}$, $\langle b \rangle = \{e, b\}$, $\langle c \rangle = \{e, c\}$ e K. Um reticulado para esse grupo está descrito abaixo.*



Seja X o conjunto dos subgrupos de K. Com a ordenação

$$x \preceq y \Leftrightarrow x \text{ é um subgrupo de } y,$$

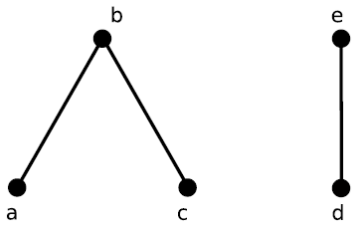
$(X, \preceq)$ é um poset onde os elementos $\langle a \rangle$ e $\langle b \rangle$ são incomparáveis. O mesmo vale para os pares $(\langle a \rangle, \langle c \rangle)$ e $(\langle b \rangle, \langle c \rangle)$ de elementos de X.

Definição 2.7 *Dados dois elementos $a, b \in (X, \preceq)$, diremos que b* ***cobre*** *a quando $a \preceq c \preceq b$ implicar $c = a$ ou $c = b$.*

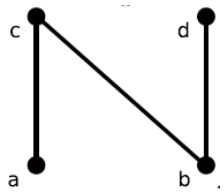
Se X é finito, então dizemos que o poset é finito e a cardinalidade do conjunto X é chamada de **comprimento** do poset.

Os posets finitos podem ser representados graficamente através dos **diagramas de Hasse**, onde os elementos de X são representados por vértices e as comparações entre os elementos $a, b \in X$ são representadas por uma aresta se a cobre b ou b cobre a. No diagrama, os elementos cobertos são dispostos em posição inferior aos que lhe cobrem.

Exemplo 2.8 *Considere a ordem $\preceq$ sobre o conjunto $X = \{a, b, c, d, e\}$ com as comparações $a \preceq a$, $b \preceq b$, $c \preceq c$, $d \preceq d$, $e \preceq e$, $a \preceq b$, $c \preceq b$, $d \preceq e$. O diagrama de Hasse do poset $(X, \preceq)$ é o seguinte:*



Exemplo 2.9 *Seja $X = \{a, b, c, d\}$ e tome a relação binária $\preceq$ definida através das comparações $a \preceq a$, $b \preceq b$, $c \preceq c$, $d \preceq d$, $a \preceq c$, $b \preceq c$ e $b \preceq d$. Então $(X, \preceq)$ é um poset, chamado* ***poset letra N*** *e denotado por $\mathcal{N}$.*



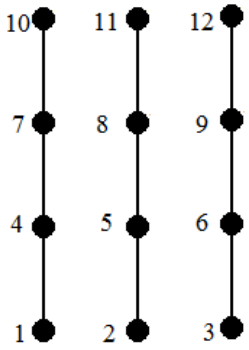
Doravante consideraremos $[n] := \{1, 2, 3, \ldots, n\}$.

Exemplo 2.10 *Seja $X = [n]$ e tome a ordem parcial $\preceq$ formada apenas pelas relações reflexivas dos elementos de X. O poset $(X, \preceq)$ é dito* ***poset anticadeia*** *ou* ***poset de Hamming*** *e será denotado por $\mathcal{H}_n$. Abaixo, o diagrama de Hasse para o poset $\mathcal{H}_4$.*

Note que, no poset $\mathcal{H}_n$, quaisquer dois elementos são incomparáveis.

Exemplo 2.11 *Um poset $([n], \preceq)$ no qual quaisquer dois elementos são comparáveis é dito* ***totalmente ordenado*** *ou* ***poset linear*** *(ou* ***cadeia****) e será denotado por $\mathcal{L}_n$.*

Exemplo 2.12 *O poset* ***Rosenbloom-Tsfasman (RT)*** *é constituído pela união disjunta de posets lineares de mesmo comprimento. Abaixo, temos o diagrama de Hasse de um poset RT formado por 3 cadeias e 4 níveis.*



2.2 Rotulamentos

Quando representamos posets finitos através dos diagramas de Hasse, é conveniente denotar os pontos como números naturais ao invés de letras do alfabeto ou outros símbolos especiais. No entanto, a disposição destes números é importante para alguns posets, pois de acordo com as disposições, obtemos diferentes relações e, consequentemente, diferentes posets. A esse processo de denotar os pontos através de números naturais damos o nome de rotulamento. A fim de tornarmos a noção de rotulamento mais precisa, temos a seguinte definição:

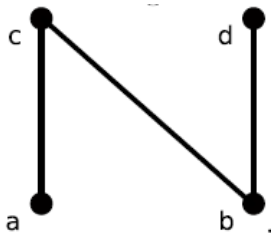
Definição 2.13 *Seja $(X, \preceq)$ um poset com $|X| = n$. Um* ***rotulamento*** *de X é uma aplicação bijetora*

$$R : [n] = \{1, 2, \ldots, n\} \to V(X),$$

onde $V(X)$ é o conjunto de todos os pontos do poset $(X, \preceq)$. O poset $(X, \preceq)$ com um rotulamento R para X será chamado ***poset rotulado*** *e será denotado pela tripla*

$$(X, \preceq, R).$$

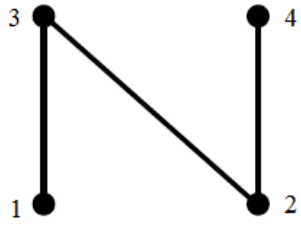
Exemplo 2.14 *Considere o conjunto $X = \{a, b, c, d\}$ e a ordem parcial $\preceq$ que define o poset $\mathcal{N}$ na forma do seguinte diagrama de Hasse:*



Definindo uma aplicação

$$R : \{1, 2, 3, 4\} \to V(X) = \{a, b, c, d\}$$

tal que $R(1) = a$, $R(2) = b$, $R(3) = c$ e $R(4) = d$, temos que R é uma aplicação bijetora e o poset rotulado resultante $(X, \preceq, R)$ possui o seguinte diagrama de Hasse:



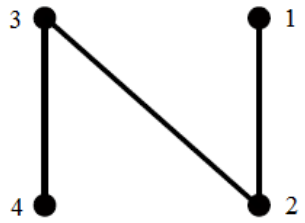
Em geral, qualquer poset pode ser transformado num poset rotulado de muitas formas diferentes. Note que, pelo Princípio Fundamental da Contagem, para o poset $\mathcal{N}$ existem $4! = 24$ diferentes rotulamentos e diferentes posets associados.

Dentre todos os posets rotulados, poderíamos pensar em qual deles possui o rotulamento mais natural. Nesse sentido, convencionaremos que um poset é rotulado naturalmente quando o rotulamento preserva a ordem natural $\leq$ dos naturais, como segue:

Definição 2.15 *Um rotulamento R de um poset $(\overrightarrow{\mathcal{P}}, \preceq)$ é dito* ***natural*** *se, caso $x \preceq y$ em $V(X)$, então $R^{-1}(x) \leq R^{-1}(y)$ em $[n]$.*

Exemplo 2.16 *Tome o poset $\mathcal{N}$ com o rotulamento R dado no Exemplo 2.14. Note que R é natural pois, se $x, y \in X$ e $x \preceq y$, temos $R^{-1}(x) \leq R^{-1}(y)$ em $\{1, 2, 3, 4\}$.*

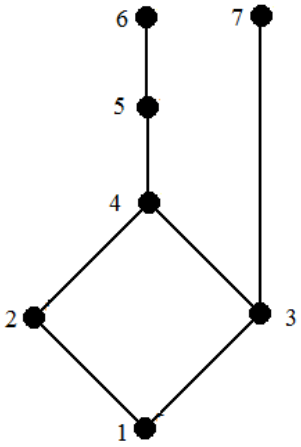
No entanto, o rotulamento $L : [4] \to \{a, b, c, d\}$ definido por $L(1) = d$, $L(2) = b$, $L(3) = c$ e $L(4) = a$ conforme descrito pelo diagrama de Hasse a seguir **não é natural** *pois $a \preceq c$, mas $4 = L^{-1}(a) \geq L^{-1}(c) = 3$.*



Como veremos a seguir, podemos mostrar que todo poset pode ser rotulado naturalmente. Assim, focaremos os nossos estudos em posets que possuem rotulamentos naturais. As definições a seguir se farão úteis:

Definição 2.17 *Seja $(X, \preceq)$ um poset. Um elemento $x \in X$ é dito* ***elemento maximal*** *se nenhum elemento $y \in X - \{x\}$ cobre x. Um elemento $x \in X$ é dito* ***elemento minimal*** *se nenhum elemento $y \in X - \{x\}$ é coberto por x. Um elemento $x \in X$ é dito* ***elemento máximo (mínimo)*** *se $y \preceq x$ $(x \preceq y)$, para todo $y \in X$.*

Exemplo 2.18 *Considere o poset sobre* $[7]$ *descrito no diagrama de Hasse abaixo:*



Observe que 1 *é elemento mínimo e minimal,* 6 *e* 7 *são elementos maximais e não existem elementos máximos neste poset.*

Lema 2.19 *Se X é um conjunto finito parcialmente ordenado, então X possui um elemento minimal.*

DEMONSTRAÇÃO: Suponha que X seja um conjunto que possua n elementos. Escolhamos $x_1 \in X$. Se x_1 é minimal, temos o resultado. Caso contrário, existe $x_2 \in X\backslash\{x_1\}$ tal que x_2 é coberto por x_1. Se x_2 for minimal, temos o resultado. Caso contrário, escolhamos $x_3 \in X\backslash\{x_1, x_2\}$ tal que x_3 é coberto por x_2. Como X é finito, após um número finito de passos, obtemos um elemento minimal $x_i \in X$, para algum $i = 1, \ldots, n$. □

Teorema 2.20 *Todo poset finito $(X, \preceq)$ possui um rotulamento natural.*

DEMONSTRAÇÃO: Seja X um conjunto não vazio com cardinalidade n e seja $\preceq$ uma ordem parcial definida em X. Como X é finito e parcialmente ordenado, então possui ao menos um elemento minimal, pelo Lema 2.19. Seja x_1 um elemento minimal de X e faça $x_1 = R(1)$.

Denote $X = X_1$ e considere agora $X_2 = X - \{x_1\}$, que é um conjunto parcialmente ordenado com a ordem induzida de X. Assim, X_2 tem um elemento minimal. Seja x_2 esse elemento e defina $x_2 = R(2)$. Seguindo esse procedimento, cada subconjunto $X_i \subset X$, onde $1 \leq i \leq n$, é não vazio e possui um elemento minimal. Tomando x_i como o minimal de X_i e pondo $x(i) = R(i)$, obtemos uma aplicação bijetora de $V(X)$ em $[n] = \{1, 2, \ldots, n\}$. Logo, esse poset admite rotulamento natural. □

Dessa forma, podemos rotular naturalmente qualquer conjunto finito munido de uma ordem parcial. Seguiremos daqui em diante com o rotulamento natural, onde os elementos minimais, no mesmo nível, serão dispostos sempre da esquerda para a direita.

2.3 Códigos ponderados por ordens parciais

Doravante, se $\overrightarrow{\mathcal{P}} = (X, \preceq)$, cometeremos o abuso de notação $S \subset \overrightarrow{\mathcal{P}}$ para nos referirmos ao subconjunto $S \subset X$ cujos elementos são ordenados de acordo com o poset $\overrightarrow{\mathcal{P}}$. O mesmo vale para $x \in \overrightarrow{\mathcal{P}}$.

Sejam $\overrightarrow{\mathcal{P}} = ([n], \preceq)$ um poset e $\mathbb{F}_q$ um corpo de cardinalidade q. O conjunto $[n]$ e as coordenadas de $x \in \mathbb{F}_q^n$ estão em correspondência biunívoca através da

aplicação

$$\begin{array}{rccc} F: & [n] & \to & \mathbb{F}_q \\ & i & \mapsto & x_i \end{array}$$

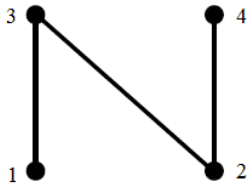
Assim, podemos definir uma distância sobre os elementos de $\mathbb{F}_q^n$, ponderada pela ordem $\preceq$ do poset $\overrightarrow{\mathcal{P}}$. No entanto, se fazem necessárias algumas definições preliminares:

Definição 2.21 *Seja $\overrightarrow{P} = ([n], \preceq)$. Um **ideal** $I \subset N$ **alinhado à esquerda** desse poset é um subconjunto $I \subset \overrightarrow{\mathcal{P}}$ tal que, para todo $i \in \overrightarrow{\mathcal{P}}$,*

$$j \in I \text{ e } i \preceq j \Rightarrow i \in I.$$

Exemplo 2.22 *No poset $\mathcal{H}$, qualquer subconjunto é um ideal, pois a única relação existente é a relação reflexiva entre os elementos.*

Exemplo 2.23 *Considere o poset $\mathcal{N}$ com o seguinte diagrama de Hasse:*



Os conjuntos $I_1 = \{1, 2, 3\}$, $I_2 = \{2, 4\}$ e $I_3 = \{2\}$ são ideais de $\mathcal{N}$ mas $I_4 = \{2, 3\}$ não o é, visto que $1 \preceq 3$ e $1 \notin I_4$.

Lema 2.24 *Se I_1 e I_2 são ideais em um poset $\overrightarrow{\mathcal{P}}$, então $I_1 \cap I_2$ e $I_1 \cup I_2$ também o são.*

Demonstração: Basta notarmos que, dados x e y em $\overrightarrow{\mathcal{P}}$ tais que $x \in I_1 \cap I_2$ e $y \preceq x$, como $x \in I_1$ e $x \in I_2$ e I_1 e I_2 são ideais, segue que $y \in I_1$ e $y \in I_2$, donde concluímos $y \in I_1 \cap I_2$.

Da mesma forma, dados x e y tais que $x \in I_1 \cup I_2$ e $y \preceq x$, temos $x \in I_1$ ou $x \in I_2$. Suponha, sem peda de generalidade, que $x \in I_1$. Assim, como I_1 é ideal, temos $y \in I_1$ e, portanto, $y \in I_1 \cup I_2$. □

Definição 2.25 *O* ***poset dual*** $\overleftarrow{\mathcal{P}}$ *é o conjunto* X *com as relações definidas por* $\overrightarrow{\mathcal{P}}$*, mas com a ordem invertida, isto é,*

$$j \preceq i \text{ em } \overleftarrow{\mathcal{P}} \Leftrightarrow i \preceq j \text{ em } \overrightarrow{\mathcal{P}}.$$

Definição 2.26 *Para um subconjunto* $S \subset \overrightarrow{\mathcal{P}}$*, denotaremos por* $\langle S \rangle = \langle S \rangle_{\overrightarrow{\mathcal{P}}}$ *a intersecção de todos os ideais em relação a* $\overrightarrow{\mathcal{P}}$ *que contém o conjunto* S*. Este ideal será chamado* **ideal gerado** *por* S*.*

Note que o ideal gerado por $S \subset \overrightarrow{\mathcal{P}}$ é o menor (no sentido de inclusão de conjuntos) ideal de $\overrightarrow{\mathcal{P}}$ que contém o conjunto S.

Denotaremos por $\Omega(I)$ o conjunto dos elementos maximais de I. Repare que $I \subset \overrightarrow{\mathcal{P}}$ é um ideal se, e somente se, $\langle \Omega(I) \rangle_{\overrightarrow{\mathcal{P}}} = I$.

Definição 2.27 *Dados dois posets* $\overrightarrow{\mathcal{P}_1}, \overrightarrow{\mathcal{P}_2}$ *sobre* $[n]$*, sendo* $\preceq_1$ *a ordem parcial de* $\overrightarrow{\mathcal{P}_1}$ *e* $\preceq_2$ *a ordem parcial de* $\overrightarrow{\mathcal{P}_2}$*, dizemos que* $\overrightarrow{\mathcal{P}_2}$ *é um* **refinamento** *de* $\overrightarrow{\mathcal{P}_1}$ *e escrevemos* $\overrightarrow{\mathcal{P}_1} \subset \overrightarrow{\mathcal{P}_2}$ *se, dados quaisquer* $x_1, x_2 \in [n]$ *tais que* $x_1 \preceq_1 x_2$*, tivermos* $x_1 \preceq_2 x_2$*.*

Exemplo 2.28 *Como o poset de Hamming* $\mathcal{H}$ *é formado somente pelas relações reflexivas, dado qualquer poset* $\overrightarrow{\mathcal{P}}$ *sobre* $[n]$*, temos* $\mathcal{H} \subset \overrightarrow{\mathcal{P}}$*.*

Definição 2.29 *O* ***suporte*** *de um elemento* x *é o subconjunto* $supp(x) \subset [n]$ *formado pelos índices de todas as entradas não nulas de* x*.*

Exemplo 2.30 *Seja* $x = 10110101 \in \mathbb{F}_2^8$*. Então*

$$supp(x) = \{1, 3, 4, 6, 8\}.$$

Definição 2.31 *O conjunto* $\langle supp(x) \rangle \subset \overrightarrow{\mathcal{P}}$ *será chamado* **ideal gerado pelo suporte de** x *(ou* ***suporte alinhado à esquerda*** *de* x*) e corresponde ao menor ideal de* $\overrightarrow{\mathcal{P}}$ *que contém o suporte de* x*.*

Definição 2.32 *Seja* $\overrightarrow{\mathcal{P}}$ *um poset definido em* $[n]$ *e sejam* $x, y, \in \mathbb{F}_q^n$*. O* ***peso*** *de* x *com respeito ao poset* $\overrightarrow{\mathcal{P}}$ *é dado por*

$$\omega_{\overrightarrow{\mathcal{P}}}(x) = |\langle supp(x) \rangle_{\overrightarrow{\mathcal{P}}}|.$$

Exemplo 2.33 *Sejam $x = 0110 \in \mathbb{F}_2^4$ e os posets $\mathcal{H}$ e $\mathcal{N}$, com os rotulamentos anteriormente descritos nos Exemplos 2.22 e 2.23, respectivamente. Então*

$$\omega_{\mathcal{H}}(0110) = |\langle supp(0110)\rangle_{\mathcal{H}}| = |\langle (2,3)\rangle_{\mathcal{H}}| = |\{2,3\}| = 2.$$

$$\omega_{\mathcal{N}}(0110) = |\langle supp(0110)\rangle_{\mathcal{N}}| = |\langle (2,3)\rangle_{\mathcal{N}}| = |\{1,2,3\}| = 3.$$

Observação 2.34 *Note que $\langle supp(x)\rangle_{\mathcal{H}} = supp(x)$, isto é, quando o poset em questão é o poset de Hamming, o peso de x com relação ao poset e o peso de Hamming se equivalem.*

Lema 2.35 *Seja $\overrightarrow{\mathcal{P}}$ um poset definido em $[n]$ e sejam $x, y \in \mathbb{F}_q^n$. Então*

$$\omega_{\overrightarrow{\mathcal{P}}}(x+y) \leq \omega_{\overrightarrow{\mathcal{P}}}(x) + \omega_{\overrightarrow{\mathcal{P}}}(y).$$

Demonstração: Como as entradas não nulas do vetor $x + y$ são, necessariamente, não nulas em x ou y, temos

$$supp(x+y) \subseteq supp(x) \cup supp(y).$$

Como $supp(x) \subseteq \langle supp(x)\rangle_{\overrightarrow{\mathcal{P}}}$ e $supp(y) \subseteq \langle supp(y)\rangle_{\overrightarrow{\mathcal{P}}}$, temos

$$supp(x) \cup supp(y) \subseteq \langle supp(x)\rangle_{\overrightarrow{\mathcal{P}}} \cup \langle supp(y)\rangle_{\overrightarrow{\mathcal{P}}}$$

e, assim,

$$supp(x+y) \subseteq supp(x) \cup supp(y) \subseteq \langle supp(x)\rangle_{\overrightarrow{\mathcal{P}}} \cup \langle supp(y)\rangle_{\overrightarrow{\mathcal{P}}}.$$

Como $\langle supp(x)\rangle_{\overrightarrow{\mathcal{P}}}$ e $\langle supp(y)\rangle_{\overrightarrow{\mathcal{P}}}$ são ideais, pelo Lema 2.24, $\langle supp(x)\rangle_{\overrightarrow{\mathcal{P}}} \cup \langle supp(y)\rangle_{\overrightarrow{\mathcal{P}}}$ é um ideal e este contém $supp(x+y)$. Logo,

$$\langle supp(x+y)\rangle_{\overrightarrow{\mathcal{P}}} \subseteq \langle supp(x)\rangle_{\overrightarrow{\mathcal{P}}} \cup \langle supp(y)\rangle_{\overrightarrow{\mathcal{P}}},$$

pois $\langle supp(x+y)\rangle_{\overrightarrow{\mathcal{P}}}$ é o menor ideal de $\overrightarrow{\mathcal{P}}$ que contém $supp(x+y)$.

Portanto,

$$\omega_{\overrightarrow{\mathcal{P}}}(x+y) = |\langle supp(x+y)\rangle_{\overrightarrow{\mathcal{P}}}| \leq |\langle supp(x)\rangle_{\overrightarrow{\mathcal{P}}} \cup \langle supp(y)\rangle_{\overrightarrow{\mathcal{P}}}|$$

$$\leq |\langle supp(x)\rangle_{\overrightarrow{\mathcal{P}}}| + |\langle supp(y)\rangle_{\overrightarrow{\mathcal{P}}}| = \omega_{\overrightarrow{\mathcal{P}}}(x) + \omega_{\overrightarrow{\mathcal{P}}}(y).$$

□

O conceito de métricas ponderadas por ordens parciais foi introduzido em 1995, por Brualdi, Graves e Lawrence [5] a partir da noção de distância ponderada por uma ordem parcial da seguinte forma:

Definição 2.36 *Seja $\overrightarrow{\mathcal{P}}$ um poset definido em $[n]$ e sejam $x, y \in \mathbb{F}_q^n$. A **distância** entre x e y em relação ao poset $\overrightarrow{\mathcal{P}}$ é definida por*

$$d_{\overrightarrow{\mathcal{P}}}(x,y) = \omega_{\overrightarrow{\mathcal{P}}}(x-y) = |\langle supp(x-y)\rangle_{\overrightarrow{\mathcal{P}}}|.$$

Teorema 2.37 *Se $\overrightarrow{\mathcal{P}}$ é um poset sobre $[n]$, então a distância $d_{\overrightarrow{\mathcal{P}}}(x,y) = \omega_{\overrightarrow{\mathcal{P}}}(x-y)$ é uma métrica em $\mathbb{F}_q^n$.*

Demonstração: Sejam x, y e $z \in \mathbb{F}_q^n$.

(*i*) Temos $d_{\overrightarrow{\mathcal{P}}}(x,y) = |\langle supp(x-y)\rangle| \geq 0$, pois a cardinalidade de um conjunto é não negativa. Observe ainda as equivalências

$$d_{\overrightarrow{\mathcal{P}}}(x,y) = |\langle supp(x-y)\rangle| = 0 \Leftrightarrow \langle supp(x-y)\rangle = \emptyset \Leftrightarrow x-y = \overrightarrow{0} \Leftrightarrow x = y,$$

onde $\overrightarrow{0}$ é o vetor nulo de $\mathbb{F}_q^n$;

(*ii*) Repare que $d_{\overrightarrow{\mathcal{P}}}(x,y) = d_{\overrightarrow{\mathcal{P}}}(y,x)$, pois o suporte do vetor $x-y$ é o mesmo suporte do vetor $-(x-y) = y-x$;

(*iii*) Pelo Lema 2.35,

$$\begin{aligned} d_{\overrightarrow{\mathcal{P}}}(x,y) = \omega_{\overrightarrow{\mathcal{P}}}(x-y) = \omega_{\overrightarrow{\mathcal{P}}}\left((x-z)+(z-y)\right) &\leq \omega_{\overrightarrow{\mathcal{P}}}(x-z) + \omega_{\overrightarrow{\mathcal{P}}}(z-y) \\ &= d_{\overrightarrow{\mathcal{P}}}(x,z) + d_{\overrightarrow{\mathcal{P}}}(z,y). \end{aligned}$$

□

Definição 2.38 *O par ordenado $\left(\mathbb{F}_q^n, d_{\overrightarrow{\mathcal{P}}}\right)$ é denominado **espaço poset**. Um subconjunto próprio $\mathcal{C}$ do espaço métrico $\left(\mathbb{F}_q^n, d_{\overrightarrow{\mathcal{P}}}\right)$ é chamado **código poset**. Se este subconjunto $\mathcal{C} \subset \mathbb{F}_q^n$ é um subespaço vetorial, então $\mathcal{C}$ é chamado **código poset linear**.*

Definição 2.39 *Um código poset $\mathcal{C}$ possui **distância mínima** d se*

$$d = min\{d_{\overrightarrow{\mathcal{P}}}(x,y); x, y \in \mathcal{C}, x \neq y\}.$$

Definição 2.40 *Dado um código poset linear $\mathcal{C} \subset \mathbb{F}_q^n$, seu **código dual** é o conjunto*

$$\mathcal{C}^{\perp} = \left\{ y \in \mathbb{F}_q^n; \sum_{i=1}^{n} x_i y_i = 0, \forall x \in \mathcal{C} \right\}.$$

Observação 2.41 *Os pesos no dual $\mathcal{C}^{\perp}$ são considerados de acordo com o poset dual $\overleftarrow{\mathcal{P}}$.*

No capítulo anterior, vimos que o raio de empacotamento R é muito importante no esquema de decodificação das palavras. Sabemos ainda que, na métrica de Hamming, o raio de empacotamento é dado por $\left\lfloor \frac{d-1}{2} \right\rfloor$.

Sabemos também que o raio de empacotamento não pode exceder d, se d é a distância mínima das palavras do código. Assim, parece natural que, independente da métrica utilizada, tenhamos

$$\left\lfloor \frac{d-1}{2} \right\rfloor \leq R \leq d-1.$$

Veremos que existem códigos poset cujo raio de empacotamento é justamente o limitante superior da desigualdade acima e, portanto, maiores do que o proveniente da métrica de Hamming. Para isto, basta tomarmos posets totalmente ordenados ($\mathcal{L}_n$).

Teorema 2.42 *Se $\mathcal{C} \subset \mathbb{F}_q^n$ é um código poset com distância mínima d, onde o poset é linear, então*

$$R = d - 1.$$

Demonstração: Note que o raio de empacotamento deve ser menor que d, pois toda bola de centro $a \in \mathcal{C}$ e raio d, contém uma outra palavra do código. Assim, vamos mostrar que

$$B(a, d-1) \cap B(b, d-1) = \emptyset,$$

para todos $a, b \in \mathcal{C} \backslash \{0\}$ distintos. Se tívessemos $x \in B(a, d-1) \cap B(b, d-1)$, então teríamos $d(x, a) \leq d-1$ e $d(x, b) \leq d-1$. Isto significa que as possíveis entradas não nulas de $\langle supp(x-a) \rangle$ e $\langle supp(x-b) \rangle$ pertencem ao conjunto das primeiras $d-1$ entradas ajustadas à esquerda, isto é, as coordenadas de $\langle supp(x-a) \rangle$ e $\langle supp(x-b) \rangle$ são nulas para as coordenadas i ajustadas à esquerda tais que $i \geq d$. Como

$$supp(a-b) \subset supp(a-x) \cup supp(x-b) \subset \langle supp(x-a) \rangle \cup \langle supp(x-b) \rangle$$

e $\langle supp(x-a) \rangle \cup \langle supp(x-b) \rangle = \emptyset$, para as entradas ajustadas à esquerda $n \geq d$, temos

$$\langle supp(a-b) \rangle = \emptyset$$

para as entradas ajustadas à esquerda $i \geq d$. Isto significa que

$$d(a, b) = |\langle supp(a-b) \rangle| \leq d-1 < d,$$

um absurdo. □

Este teorema é importante no sentido que permite a construção de um número maior de códigos perfeitos, bastanto para isto tomar a métrica linear.

O leitor interessado poderá consultar a referência [8] sobre raios de empacotamento de códigos poset, para posets arbitrários.

2.4 Peso de Hamming generalizado

Dado um código $\mathcal{C}$ com a métrica de Hamming, existe uma sequência crescente de inteiros positivos associada ao código chamada **pesos de Hamming generalizados**. Inicialmente motivado por problemas em Criptografia, V. Wei introduziu essa sequência em 1991, possibilitando o estudo da estrutura algébrica de códigos sob uma nova perspectiva, uma vez que os termos desta sequência satisfazem certos limitantes baseados nos parâmetros fundamentais do código. O que faremos aqui é um estudo elementar desta sequência de pesos e da extensão de algumas de suas propriedades para códigos com métricas poset.

Definição 2.43 *Seja D um subespaço de $\mathbb{F}_q^n$. Definimos*

$$supp(D) = \bigcup_{x \in D} supp(x).$$

Definição 2.44 *O t-**ésimo peso poset generalizado** de um (n,k) código linear $\mathcal{C}$ é definido como*

$$d_t(\mathcal{C}) = min\big\{|\langle supp(D)\rangle|; D \text{ é um } (n,t) \text{ subcódigo de } \mathcal{C}\big\}.$$

Cabe observar que $d_1(\mathcal{C}) = d$, onde d é a distância mínima de $\mathcal{C}$ e que o t-ésimo peso poset generalizado de um código $\mathcal{C}$ **depende** do poset considerado.

Definição 2.45 *O conjunto $\{d_r(\mathcal{C}); 1 \leq r \leq k)\}$ é chamado **hierarquia de $\overrightarrow{\mathcal{P}}$-pesos de $\mathcal{C}$**.*

Os seguintes resultados, abordados por A. Moura [21] e A. Barg e P. Purkayashta [2] em 2010, sobre os pesos da hierarquia serão utilizados fortemente na caracterização dos códigos NMDS, objetivo principal dos nossos estudos:

Lema 2.46 (Monotocidade da Hierarquia dos pesos Generalizados) *[26, 21, 2] Seja $\mathcal{C}$ um (n,k) código poset linear com dimensão k. Então*

$$0 < d_1(\mathcal{C}) < d_2(\mathcal{C}) < \ldots < d_k(\mathcal{C}) \leq n.$$

DEMONSTRAÇÃO: Seja $D_t \subset \mathcal{C}$ um subespaço linear tal que $|\langle supp(D_t)\rangle| = d_t(\mathcal{C})$ e dimensão de $D_t = t$, para $t \geq 1$. Seja $\Omega(D_t)$ o conjunto de todos os elementos maximais do ideal $\langle supp(D_t)\rangle$. Para cada coordenada em $\Omega(D_t)$, D_t possui ao menos um vetor onde a posição dessa coordenada é não nula. Escolhamos $i \in \Omega(D_t)$ e seja D_t^i o conjunto que obtemos retirando somente os vetores $v \in D_t$, com $v_i = 0$. Então

$$d_{t-1}(\mathcal{C}) \leq |\langle supp(D_t^i)\rangle| \leq |\langle supp(D_t)\rangle| - 1 \leq d_t(\mathcal{C}) - 1 < d_t(\mathcal{C}).$$

□

O Corolário 1.49 pode ser generalizado, como segue:

Lema 2.47 (Limitante de Singleton Generalizado) *Seja $\mathcal{C}$ um código poset linear em $\mathbb{F}_q^n$ de dimensão k. Então, para todo $t \geq 1$,*

$$d_t(\mathcal{C}) \leq n - k + t.$$

DEMONSTRAÇÃO: Pelo Lema 2.46, $d_k(\mathcal{C}) \leq n$ e $d_t(\mathcal{C}) \leq d_{t+1}(\mathcal{C}) - 1$. Assim,

$$d_{k-1}(\mathcal{C}) \leq d_k(\mathcal{C}) - 1 \leq n - 1 = n - k + (k-1)$$

$$\Rightarrow d_{k-2}(\mathcal{C}) \leq d_{k-1}(\mathcal{C}) - 1 \leq n - 2 = n - k + (k-2).$$

Prosseguindo com esse argumento, temos

$$d_{k-s}(\mathcal{C}) \leq n - s = n - k + (k-s).$$

Façamos $k - s = t$ e teremos o resultado. □

Teorema 2.48 (Dualidade de Wei) *[21, 2] Seja $\mathcal{C}$ um código poset linear em $\mathbb{F}_q^n$ de dimensão k e seja $\mathcal{C}^\perp$ o seu código dual. Considerando a hierarquia de pesos de $\mathcal{C}$*

$$X = \{d_1(\mathcal{C}), d_2(\mathcal{C}), \ldots, d_k(\mathcal{C})\}$$

e o conjunto

$$Y = \{n + 1 - d_1(\mathcal{C}^\perp), n + 1 - d_2(\mathcal{C}^\perp), \ldots, n + 1 - d_{n-k}(\mathcal{C}^\perp)\},$$

então X e Y são disjuntos e $X \cup Y = \{1, 2, \ldots, n\}$.

DEMONSTRAÇÃO: Temos $X \subset [n]$, pelo Lema 2.46 e, como

$$1 \leq d_s(\mathcal{C}^\perp) \leq n \Rightarrow 1 \leq n + 1 - d_s(\mathcal{C}^\perp) \leq n$$

para $1 \leq s \leq n-k$, temos também $Y \subset [n]$. Assim, $X \cup Y \subseteq [n]$, $|X| = k$ e $|Y| = n-k$. Pelo Princípio da Inclusão-Exclusão,

$$X \cup Y = [n] \Leftrightarrow X \cap Y = \emptyset.$$

Logo, basta mostrarmos que $X \cap Y = \emptyset$.

Devemos ter $d_{n-k}(\mathcal{C}^\perp) = n$, pois se $d_{n-k}(\mathcal{C}^\perp) < n$, o código seria degenerado. Assim,

$$d_{n-k}(\mathcal{C}^\perp) = n \Rightarrow n + 1 - d_{n-k}(\mathcal{C}^\perp) = 1$$

e, como $\mathcal{C}^\perp$ também é não degenerado, pelo Teorema 1.52, temos $d(\mathcal{C}) \geq 2$ e, assim,

$$n + 1 - d_{n-k}(\mathcal{C}^\perp) < d_r(\mathcal{C}),$$

para todo $r = 1, \ldots, k$.

Mostraremos agora que, para todo $1 \leq s \leq n-k-1$,

$$n + 1 - d_s(\mathcal{C}^\perp) \notin X = \{d_r(\mathcal{C}); 1 \leq r \leq k\}.$$

Seja $t = k + s - d_s(\mathcal{C}^\perp)$ e considere os seguintes casos:

(i) 1º Caso: $r \leq t$

Tome $D_s \subseteq \mathcal{C}^\perp$ tal que $\dim(D_s) = s$ e $|\langle supp(D_s)_{\overleftarrow{\mathcal{P}}}\rangle| = d_s(\mathcal{C}^\perp)$. Este subcódigo existe pela definição de D_s.

Como $\dim(D_s) = s$, podemos formar uma matriz teste de paridade H do código $\mathcal{C}$ tal que as suas primeiras linhas sejam s vetores linearmente independentes de D_s. Seja D o complementar de $\langle supp(D_s)\rangle_{\overleftarrow{\mathcal{P}}}$, em relação ao conjunto de coordenadas e seja $H[D]$ a submatriz de H formada por todas as colunas em D.

O posto de $H[D]$ será no máximo $(n-k)-s$ e, pelo Teorema do Núcleo e da Imagem, a nulidade de $H[D]$ será no mínimo

$$|D| - (n-k-s) = n - d_s(\mathcal{C}^\perp) - n + k + s = k + s - d_s(\mathcal{C}^\perp) = t.$$

Assim, tomemos a aplicação

$$\begin{array}{rccc} T: & \mathbb{F}_q^{|D|} & \to & \mathbb{F}_q^{n-k} \\ & x & \mapsto & H[D] \cdot x^t \end{array}.$$

Note que a aplicação está bem definida pois x é um vetor $1 \times \left(n - d_s(\mathcal{C}^\perp)\right)$, $H[D]$ tem ordem $(n-k) \times \left(n - d_s(\mathcal{C}^\perp)\right)$ e x^t é um vetor $\left(n - d_s(\mathcal{C}^\perp)\right) \times 1$.

Assim, obtemos o subcódigo $\widetilde{\mathcal{C}} = ker(T) \subset \mathbb{F}_q^{|D|}$ tal que

$$dim(\widetilde{\mathcal{C}}) = \text{nulidade de } H[D] \geq t$$

e, fazendo nulas as $n - |D|$ entradas restantes, obteremos um subcódigo $\mathcal{C}' \subset \mathcal{C}$ de dimensão no mínimo t.

Logo, existe um código linear de dimensão no mínimo t no qual todas as palavras têm suporte dentro das coordenadas indexadas por D e possuem todas as coordenadas que não estão em D como zero, isto é, existe um subcódigo $\mathcal{C}'$ desse código linear com $\dim(\mathcal{C}') = t$ em que todas as palavras são não nulas somente nas coordenadas indexadas por D.

Portanto,

$$d_t(\mathcal{C}) \leq \left|\langle supp(\mathcal{C}')\rangle_{\overrightarrow{\mathcal{P}}}\right| = |D| = n - d_s(\mathcal{C}^\perp)$$

e, assim, como $1 \leq r \leq t$, segue

$$d_r(\mathcal{C}) \leq d_t(\mathcal{C}) \leq n - d_s(\mathcal{C}^\perp) < n + 1 - d_s(\mathcal{C}^\perp).$$

(ii) 2º Caso: $r \geq t + 1$

Vamos mostrar que, para $r = t + i$, onde $1 \leq i \leq k - t$, temos

$$d_{t+i}(\mathcal{C}) \neq n + 1 - d_s(\mathcal{C}^\perp).$$

Supondo $d_{t+i}(\mathcal{C}) = n + 1 - d_s(\mathcal{C}^\perp)$, para algum $1 \leq i \leq k - t$, considere o subcódigo $D_{t+i} \subseteq \mathcal{C}$ tal que

$$|\langle supp(D_{t+i})\rangle_{\overrightarrow{\mathcal{P}}}| = d_{t+i}(\mathcal{C})$$

e tome uma matriz geradora de $\mathcal{C}$ onde as primeiras $t + i$ linhas sejam correspondentes ao subcódigo $D_{t+i} \subseteq \mathcal{C}$.

Seja D o complementar de $\langle supp(D_{t+i})\rangle_{\overrightarrow{\mathcal{P}}}$ no conjunto das coordenadas e seja $G[D]$ a submatriz de G formada por todas as colunas em D. Então $G[D]$ é uma matriz de ordem $k \times (n - d_{t+i}(\mathcal{C}))$ e de posto no máximo $k-t-i$. Assim, $n - d_{t+i}(\mathcal{C}) \geq k - t - i$ e então

$$\begin{aligned}
\dim\left(ker(G[D])\right) &\geq n - d_{t+i}(\mathcal{C}) - k + t + i \\
&= n - d_{t+i}(\mathcal{C}) - (t - s + d_s(\mathcal{C}^\perp)) + t + i \\
&= s + i - (d_s(\mathcal{C}^\perp) - n + d_{t+i}(\mathcal{C})) \\
&= s + i - (d_s(\mathcal{C}^\perp) - n + (n + 1 - d_s(\mathcal{C}^\perp))) \\
&= s + i - 1.
\end{aligned}$$

Portanto, denotando por $\mathcal{C}'$ o subcódigo de $\mathcal{C}^\perp$ obtido a partir do código gerado por $ker(G[D])$ pelo completamento com zeros nas entradas fora de D, temos

$$d_{s+i-1}(\mathcal{C}^\perp) \leq \left|\langle supp(\mathcal{C}')\rangle_{\overleftarrow{\mathcal{P}}}\right| = |D| = n - d_{t+i}(\mathcal{C}) = d_s(\mathcal{C}^\perp) - 1,$$

o que contradiz o Lema 2.46 (faça $i = 1$).

□

O seguinte resultado é uma generalização do Teorema 1.48:

Lema 2.49 *[2] Seja $\mathcal{C}$ um código poset linear em $\mathbb{F}_q^n$ de dimensão k e seja H a matriz teste de paridade de $\mathcal{C}$. Então $d_t(\mathcal{C}) = \delta$ se, e somente se,*

(*a*) *Quaisquer $\delta - 1$ colunas alinhadas à esquerda de H têm posto no mínimo $\delta - t$;*

(*b*) *Existem δ colunas alinhadas à esquerda de H com posto exatamente $\delta - t$.*

Demonstração: Suponha $d_t(\mathcal{C}) = \delta$. Vamos demonstrar a parte (a).

Suponha, por absurdo, que existam $\delta - 1$ colunas alinhadas à esquerda com posto menor que $\delta - t$. Denotemos o conjunto formado pelos índices dessas $\delta - 1$ colunas por D e construamos a submatriz $H[D]$ de H. Como temos $posto(H[D]) < \delta - t$ e

$$posto(H[D]) + coposto(H[D]) = \delta - 1,$$

segue que $coposto(H[D]) \geq t$.

Assim, existe um subcódigo de $\mathcal{C}$ de dimensão no mínimo t e em que todas as suas palavras possuem coordenadas não-nulas apenas nas entradas que estão em D. Portanto,

$$d_t(\mathcal{C}) \leq |D| = \delta - 1 < \delta.$$

Vamos demonstrar agora a parte (b):

Se $d_t(\mathcal{C}) = \delta$, então existe um subcódigo $\mathcal{C}' \subseteq \mathcal{C}$ tal que $|\langle supp(\mathcal{C}')\rangle_{\overrightarrow{\mathcal{P}}}| = \delta$ e $\dim(\mathcal{C}') = t$.

Seja $X = \langle supp(\mathcal{C}')\rangle_{\overrightarrow{\mathcal{P}}}$ e seja $H[X]$ a submatriz de H formada pela restrição desta às colunas indexadas por X. Assim, como $|X| = \delta$ e $coposto(H[X]) = t$, temos

$$posto(H[X]) = \delta - coposto(H[X]) = \delta - t,$$

donde concluímos que existem δ colunas alinhadas à esquerda de H com posto $\delta - t$.

Por outro lado, suponha agora que quaisquer $\delta - 1$ colunas alinhadas à esquerda de H têm posto no mínimo $\delta - t$ e que existam δ colunas alinhadas à esquerda de H com posto exatamente $\delta - t$.

Assim, fazendo D o conjunto formado pelas δ colunas de posto exatamente $\delta - t$ e construindo a submatriz $H[D]$ de H, temos:

$$coposto(H[D]) = \delta - (\delta - t) = t,$$

donde concluímos que existe um subcódigo $\mathcal{C}' \subseteq \mathcal{C}$ tal que $\dim(\mathcal{C}') = t$ e $|\langle supp(\mathcal{C}')\rangle_{\overrightarrow{\mathcal{P}}}| \leq \delta$. Assim,

$$d_t(\mathcal{C}) \leq \delta.$$

Como as $\delta - 1$ colunas de H têm posto no mínimo $\delta - t$, a submatriz de H formada por quaisquer $\delta - 1$ colunas tem coposto no máximo $\delta - 1 - (\delta - t) = t - 1 < t$, ou seja, nenhum conjunto de coordenadas de tamanho menor que δ dá suporte a um subcódigo de dimensão t. Assim,

$$d_t(\mathcal{C}) \geq \delta$$

e, portanto,

$$d_t(\mathcal{C}) = \delta.$$

□

Exemplo 2.50 *Considere o código poset $\mathcal{C} \subset \mathbb{F}_2^5$ dado pela matriz geradora*

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

e cuja distância é definida pelo poset $\mathcal{L}_5$. As palavras de $\mathcal{C}$ são:

00000	11000
10101	01101
10110	01110
00011	11011

Tomando a palavra $x = 11000 \in \mathcal{C}$, o peso desta é dado por

$$\omega_{\mathcal{L}_5}(x) = 2,$$

que é a distância mínima de $\mathcal{C}$. Pelo Lema 1.43, a matriz H dada por

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

é uma matriz teste de paridade para $\mathcal{C}$, visto que as suas linhas são linearmente independentes e ortogonais às linhas de G.

Note que as palavras de $\mathcal{C}^\perp$ são

00000	11011
11100	00111

e, destas, a palavra não nula que possui menor peso, a dizer 3, é 00111.

Vamos determinar a hierarquia de $\overrightarrow{\mathcal{P}}$-pesos para $\mathcal{C}$ e a hierarquia de $\overleftarrow{\mathcal{P}}$-pesos para $\mathcal{C}^\perp$:

(*i*) *Hierarquia de* $\overrightarrow{\mathcal{P}}$*-pesos para* $\mathcal{C}$*:*

(*a*) *Cálculo de* $d_1(\mathcal{C})$*.*
Como a palavra $x = 11000$ *é a que possui o menor peso, temos*

$$d_1(\mathcal{C}) = \omega_{\overrightarrow{\mathcal{P}}}(x) = 2.$$

(*b*) *Cálculo de* $d_2(\mathcal{C})$*.*
Devemos formar todos os subespaços de dimensão 2*, a partir das palavras de* $\mathcal{C}$ *e determinar aquele cujo ideal gerado possui a menor cardinalidade. Note que podemos tomar as palavras das matriz geradora, duas a duas, para formar cada subespaço.*

(1) $\mathcal{D}_1 \subset \mathcal{C}$ *com* $\mathcal{D}_1$ *gerado por* 11000 *e* 10110*.*
As palavras de $\mathcal{D}_1$ *são:*

00000	11000
10110	01110

e, portanto,

$$supp(\mathcal{D}_1) = \bigcup_{x \in \mathcal{D}_1} supp(x) = \{1, 2, 3, 4\},$$

donde concluímos que $|\langle supp(\mathcal{D}_1 \rangle| = 4$*.*

(2) $\mathcal{D}_2 \subset \mathcal{C}$ *com* $\mathcal{D}_2$ *gerado por* 11000 *e* 10101*.*
As palavras de $\mathcal{D}_2$ *são:*

00000	11000
10101	01101

e, portanto,

$$supp(\mathcal{D}_2) = \bigcup_{x \in \mathcal{D}_2} supp(x) = \{1, 2, 3, 5\},$$

donde concluímos que $|\langle supp(\mathcal{D}_2 \rangle| = 5$*.*

(3) $\mathcal{D}_3 \subset \mathcal{C}$ *com* $\mathcal{D}_3$ *gerado por* 10110 *e* 10101*.*
As palavras de $\mathcal{D}_3$ *são:*

00000	10110
10101	00011

e, portanto,

$$supp(\mathcal{D}_3) = \bigcup_{x \in \mathcal{D}_3} supp(x) = \{1, 3, 4, 5\},$$

donde concluímos que $|\langle supp(\mathcal{D}_3 \rangle| = 5$*.*

Portanto,

$$d_2(\mathcal{C}) = min\{4, 5\} = 4.$$

(*c*) *Cálculo de* $d_3(\mathcal{C})$.

Devemos formar todos os subespaços de dimensão 3*, a partir das palavras de* $\mathcal{C}$ *e determinar aquele cujo ideal gerado possui a menor cardinalidade. Note que o único subespaço de dimensão* 3 *é o próprio código* $\mathcal{C}$.

Assim,

$$supp(\mathcal{C}) = \bigcup_{x \in \mathcal{C}} supp(x) = \{1, 2, 3, 4, 5\},$$

donde concluímos que $|\langle supp(\mathcal{C})\rangle| = 5$ *e então*

$$d_3(\mathcal{C}) = 5.$$

Portanto, a hierarquia de $\overrightarrow{\mathcal{P}}$*-pesos para* $\mathcal{C}$ *é* $\{2, 4, 5\}$.

(*ii*) *Hierarquia de* $\overleftarrow{\mathcal{P}}$*-pesos para* $\mathcal{C}^\perp$*:*

(*a*) *Cálculo de* $d_1(\mathcal{C}^\perp)$.

Como a palavra $x = 00111$ *é a que possui o menor peso, temos*

$$d_1(\mathcal{C}^\perp) = \omega_{\overleftarrow{\mathcal{P}}}(x) = 3.$$

(*b*) *Cálculo de* $d_2(\mathcal{C}^\perp)$.

Devemos formar todos os subespaços de dimensão 2*, a partir das palavras de* $\mathcal{C}^\perp$ *e determinar aquele cujo ideal gerado possui a menor cardinalidade. Note que o único subespaço de dimensão* 2 *é o próprio código* $\mathcal{C}^\perp$.

Assim,

$$supp(\mathcal{C}^\perp) = \bigcup_{x \in \mathcal{C}^\perp} supp(x) = \{1, 2, 3, 4, 5\},$$

donde concluímos que $|\langle supp(\mathcal{C})\rangle| = 5$ *e, então*

$$d_2(\mathcal{C}^\perp) = 5.$$

Portanto, a hierarquia de $\overleftarrow{\mathcal{P}}$*-pesos para* $\mathcal{C}^\perp$ *é* $\{3, 5\}$.

Note que ambas as hierarquias de $\overrightarrow{\mathcal{P}}$*-pesos de* $\mathcal{C}$ *e* $\mathcal{C}^\perp$ *formam uma sequência crescente, o que está de acordo com o Lema 2.46 e, além disso, os conjuntos*

$$\{d_r(\mathcal{C}); 1 \leq r \leq 3\} = \{2, 4, 5\}$$

e

$$\{5 + 1 - d_s(\mathcal{C}^\perp); s = 1, 2\} = \{5 + 1 - 3, 5 + 1 - 5\} = \{1, 3\}$$

formam uma partição de $\{1, 2, 3, 4, 5\}$*, o que está de acordo com o Teorema 2.48.*

Finalmente, note que, como $d_1(\mathcal{C}) = 2$*, quaisquer* $1 = 2 - 1$ *colunas alinhadas à esquerda da matriz teste de paridade*

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

são linearmente independentes e existem 2 *colunas alinhadas à esquerda linearmente dependentes, a dizer, a primeira e a segunda.*

De modo análogo, como $d_2(\mathcal{C}^\perp) = 5$*, quaisquer* $4 = 5 - 1$ *colunas alinhadas à esquerda da matriz geradora de* $\mathcal{C}$

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

têm posto no mínimo $3 = 5 - 2$ *e existem* 5 *colunas alinhadas à esquerda com posto exatamente* 3*. Estas observações estão de acordo com o Lema 2.49.*

Capítulo 3

Códigos Poset NMDS

Neste capítulo, vamos estudar a classe de códigos NMDS em um espaço poset visando estabelecer caracterizações e algumas expressões para a sua distribuição de $\overrightarrow{\mathcal{P}}$-pesos, com base nos resultados do capítulo anterior. No caso particular de um poset RT, obteremos a chamada "métrica de Hamming ordenada" e, com o apoio desta, faremos algumas conexões com a distribuição de pontos no cubo unitário $U^n = [0,1)^n$ e com as (t,m,s)-redes, comparando essa classe de códigos aos conhecidos códigos MDS.

Os códigos MDS são definidos como aqueles em que a distância mínima é a máxima possível. No entanto, o comprimento destes não pode ser muito grande [2] e isto os torna, de certa forma, raros. Esta restrição levou ao estudo de classes de códigos com distâncias mínimas próximas a dos códigos MDS, tais como os códigos NMDS, que foram definidos por S. Dodunekov e I. Landjev [7] como a melhor dessas classes, por possuir propriedades similares às dos códigos MDS e admitir uma boa interpretação geométrica.

Além da distribuição de pontos no cubo unitário e da distribuição de pesos na métrica de Hamming Ordenada, discutiremos alguns exemplos de códigos poset NMDS para casos com uma, duas e três cadeias.

3.1 Códigos NMDS

Nessa seção, estudaremos uma família de códigos obtida pelo enfraquecimento das restrições da definição dos clássicos códigos MDS.

Definição 3.1 *Um (n, k, d) código linear $\mathcal{C}$ é chamado **near-MDS (NMDS)** se*

$$d(\mathcal{C}) = n - k \text{ e } d_2(\mathcal{C}) = n - k + 2.$$

Exemplo 3.2 *Note que o $(5, 3, 2)$ código linear $\mathcal{C}$ apresentado no Exemplo 2.50 é NMDS pois*

$$d(\mathcal{C}) = 2 = 5 - 3$$

e

$$d_2(\mathcal{C}) = 4 = 5 - 3 + 2.$$

Uma outra caracterização dessa família de códigos, via matriz teste de paridade, é a seguinte:

Lema 3.3 *Um (n, k, d) código linear $\mathcal{C}$ no poset $\overrightarrow{\mathcal{P}}$ é NMDS se, e somente se,*

(a) *Quaisquer $n - k - 1$ colunas alinhadas à esquerda da matriz de paridade H são linearmente independentes;*

(b) *Existem $n - k$ colunas de H alinhadas à esquerda linearmente dependentes;*

(c) *Quaisquer $n - k + 1$ colunas de H alinhadas à esquerda têm posto cheio.*

Demonstração: Suponha que $\mathcal{C}$ seja NMDS. Assim,

$$\begin{cases} d_1 &= n - k \\ d_2 &= n - k + 2 \end{cases}$$

e, pelo Lema 2.49,

(a) Quaisquer $n - k - 1$ colunas de H tem posto maior ou igual a $n - k - 1$. Logo, quaisquer $n - k - 1$ colunas de H tem posto $n - k - 1$, isto é, elas são linearmente independentes.

(b) Existem $n - k$ colunas de H com posto $n - k - 1$, isto é, existem $n - k$ colunas linearmente dependentes.

(c) Quaisquer $n - k + 1$ colunas de H têm posto maior do que ou igual a $n - k + 2 - 2 = n - k$ e este é o posto máximo de H.

Suponha agora que:

(a) Quaisquer $n-k-1$ colunas alinhadas à esquerda da matriz de paridade H são linearmente independentes (ou seja, quaisquer $n-k-1$ colunas têm posto
$\geq n-k-1$);

(b) Existem $n-k$ colunas de H alinhadas à esquerda linearmente dependentes (isto é, existem $n-k$ colunas com posto $\leq n-k-1$);

(c) Quaisquer $n-k+1$ colunas de H alinhadas à esquerda têm posto $n-k$.

Fazendo $\delta = n-k$ temos por (a) que quaisquer $\delta-1$ colunas têm posto $\geq \delta-1$. Por (b) e (c), adicionando uma coluna ao conjunto das $n-k$ colunas com posto $\leq n-k-1$, esse conjunto passa a ter posto $n-k$. Assim, o posto do conjunto das $n-k$ colunas era $n-k-1$ e então existem $n-k=\delta$ colunas com posto $n-k-1=\delta-1$.

Pelo Lema 2.49, temos $d_1(\mathcal{C}) = \delta = n-k$. Fazendo agora $\delta = n-k+2$, temos por (c) que quaisquer $\delta-1 = n-k+1$ colunas têm posto

$$n-k \geq n-k = n-k+2-2 = \delta-2.$$

Repare também que quaisquer $n-k+2$ colunas têm posto exatamente

$$n-k = n-k+2-2 = \delta-2,$$

pois quaisquer $n-k+2$ colunas contém $n-k+1$ colunas e estas já possuem o posto máximo $(n-k)$ por hipótese. Assim, pelo Lema 2.49, $d_2(\mathcal{C}) = n-k+2 = \delta$ e, portanto, $\mathcal{C}$ é NMDS. □

Essa caracterização nos auxilia a demonstrar muitos resultados a respeito de códigos poset NMDS. Uma primeira observação é a seguinte:

Lema 3.4 *Seja $\mathcal{C}$ um (n,k,d) código linear no poset $\overrightarrow{\mathcal{P}}$. Então $\mathcal{C}$ é NMDS se, e somente se, seu dual $\mathcal{C}^\perp$ também o é.*

Demonstração: Se $\mathcal{C}$ é NMDS, então $d_1(\mathcal{C}) = n-k$ e $d_2(\mathcal{C}) = n-k+2$.

Como existem $n-k$ números entre 1 e $n-k$ (incluindo 1 e $n-k$) e $d_r(\mathcal{C}) \geq d_2(\mathcal{C})$ para todo $r \in \{2,\ldots,k\}$, devemos ter, pelo Teorema 2.48,

$$Y = \{n+1-d_t(\mathcal{C}^\perp); 1 \leq t \leq n-k\} = \{1,\ldots,n-k-1,n-k+1\}.$$

Repare que, quanto menor o valor de $d_t(\mathcal{C}^\perp)$, maior o valor de $n+1-d_t(\mathcal{C}^\perp)$. Como o menor peso de $\mathcal{C}^\perp$ é $d_1(\mathcal{C}^\perp)$ e o maior valor do conjunto Y é $n-k+1$, temos

$$n+1-d_1(\mathcal{C}^\perp) = n-k+1 \Rightarrow d_1(\mathcal{C}^\perp) = k = n-(n-k).$$

Como o segundo menor peso de $\mathcal{C}^\perp$ é $d_2(\mathcal{C}^\perp)$ e o segundo maior valor do conjunto Y é $n-k-1$, temos

$$n+1-d_2(\mathcal{C}^\perp) = n-k-1 \Rightarrow d_2(\mathcal{C}^\perp) = k+2 = n-(n-k)+2.$$

Portanto, $\mathcal{C}^\perp$ é NMDS. □

Exemplo 3.5 *Note que o* $(5,2,3)$ *código linear, dual do código NMDS* $\mathcal{C}$ *apresentado nos Exemplos 2.50 e 3.2, é NMDS uma vez que*

$$d(\mathcal{C}^\perp) = 3 = 5-2$$

e

$$d_2(\mathcal{C}^\perp) = 5 = 5-2+2.$$

Repare que este último resultado também vale para códigos MDS:

Proposição 3.6 *Seja* $\mathcal{C}$ *um* (n,k,d) *código linear no poset* $\overrightarrow{\mathcal{P}}$*. Então* $\mathcal{C}$ *é MDS se, e somente se, seu dual* $\mathcal{C}^\perp$ *também o é.*

Demonstração: Se $\mathcal{C}$ é MDS, então $d_1(\mathcal{C}) = n-k+1$.

Como existem $n-k$ números entre 1 e $n-k$ (incluindo 1 e $n-k$) e $d_r(\mathcal{C}) \geq d_1(\mathcal{C})$, para todo $r \in \{1,\ldots,k\}$, devemos ter

$$Y = \{n+1-d_t(\mathcal{C}^\perp); 1 \leq t \leq n-k\} = \{1,\ldots,n-k\}.$$

Quanto menor o valor de $d_t(\mathcal{C}^\perp)$, maior o valor de $n+1-d_t(\mathcal{C}^\perp)$. Assim, como o menor peso de $\mathcal{C}^\perp$ é $d_1(\mathcal{C}^\perp)$ e o maior valor do conjunto Y é $n-k$, temos

$$n+1-d_1(\mathcal{C}^\perp) = n-k \Rightarrow d_1(\mathcal{C}^\perp) = k+1 = n-(n-k)+1$$

e, assim, $\mathcal{C}^\perp$ é MDS. □

Assim, embora obtidos pelas restrições da definição dos códigos MDS, os códigos NMDS ainda apresentam alguma estrutura similar a estes quanto à dualidade.

Vamos enunciar agora uma outra caracterização para códigos NMDS, em termos de um código e de seu dual.

Teorema 3.7 *Um* (n,k,d) *código linear* $\mathcal{C}$ *no poset* $\overrightarrow{\mathcal{P}}$ *é NMDS se, e somente se,*

$$d(\mathcal{C}) + d(\mathcal{C}^\perp) = n.$$

DEMONSTRAÇÃO: Se o código $\mathcal{C}$ é NMDS, então, pelo Lema 3.4, $\mathcal{C}^\perp$ é NMDS. Assim, $d(\mathcal{C}) = n - k$ e $d(\mathcal{C}^\perp) = k = n - (n - k)$. Portanto,

$$d(\mathcal{C}) + d(\mathcal{C}^\perp) = (n - k) + k = n.$$

Suponha agora $d(\mathcal{C}^\perp) = n - d(\mathcal{C})$. Como $d_2(\mathcal{C}^\perp) \geq d(\mathcal{C}^\perp) + 1$, temos

$$d_2(\mathcal{C}^\perp) \geq n - d(\mathcal{C}) + 1.$$

Afirmação: $d_2(\mathcal{C}^\perp) \geq n - d(\mathcal{C}) + 2$.

De fato, se tivéssemos $d_2(\mathcal{C}^\perp) < n - d(\mathcal{C}) + 2$, então

$$n - d(\mathcal{C}) + 1 \leq d_2(\mathcal{C}^\perp) < n - d(\mathcal{C}) + 2 \Rightarrow d_2(\mathcal{C}^\perp) = n - d(\mathcal{C}) + 1,$$

o que contraria a partição de $\{1, \ldots, n\}$ dada pelo Teorema 2.48.

Pelo Limitante de Singleton Generalizado,

$$\begin{array}{rcl} n & & d_2(\mathcal{C}^\perp) + n - k - 2 \\ & \overset{\text{Afirmação}}{\geq} & (n - d(\mathcal{C}) + 2) + n - k - 2 \\ & = & 2n - k - d(\mathcal{C}). \end{array}$$

Dessa forma,

$$-n \geq -k - d(\mathcal{C}) \Rightarrow d(\mathcal{C}) \geq n - k.$$

Pelo Limitante de Singleton, temos duas possibilidades:

$$d(\mathcal{C}) = n - k \text{ ou } d(\mathcal{C}) = n - k + 1.$$

Se tivéssemos $d(\mathcal{C}) = n - k + 1$, então, pelo Teorema 2.48,

$$n - k + 1 = d_1(\mathcal{C}) < d_2(\mathcal{C}) < \ldots < d_k(\mathcal{C}) = n - k + k = n$$

e, assim, $n + 1 - d(\mathcal{C}^\perp) = n - k$, donde $d(\mathcal{C}^\perp) = k + 1$ e então

$$d(\mathcal{C}) + d(\mathcal{C}^\perp) = (n - k + 1) + (k + 1) = n + 2 \neq n,$$

um absurdo. Logo, $d(\mathcal{C}) = n - k$.

Pelo mesmo raciocínio da afirmação anterior, $d_2(\mathcal{C}) \geq n - d(\mathcal{C}^\perp) + 2$ e, portanto,

$$d_2(\mathcal{C}) \geq n - d(\mathcal{C}^\perp) + 2 = d(\mathcal{C}) + 2 = n - k + 2.$$

Pelo Limitante de Singleton Generalizado, temos $d_2(\mathcal{C}) = n - k + 2$. □

O próximo resultado nos garante a existência de códigos NMDS com parâmetros ligeiramente próximos aos parâmetros de um código NMDS dado. Por iteração, este resultado garante que podemos encontrar códigos NMDS de comprimentos menores a partir de código NMDS de grandes comprimentos.

Lema 3.8 *Seja $\mathcal{C}$ um (n,k,d) código linear no poset $\overrightarrow{\mathcal{P}}$. Se $\mathcal{C}$ é NMDS então existe um código NMDS com parâmetros $(n-1,k-1,d)$ e um código NMDS com parâmetros $(n-1,k,d-1)$.*

Demonstração: Como $\mathcal{C}$ é NMDS, então $d = n-k$. Para obtermos um $(n-1,k-1,d)$ código NMDS, basta deletarmos uma coluna da matriz teste de paridade H de $\mathcal{C}$ preservando um conjunto de $n-k$ colunas alinhadas à esquerda linearmente dependentes. Como $d = n-k$, quaisquer $n-k-1$ colunas alinhadas à esquerda da matriz H são linearmente independentes. Deletando uma coluna de H e mantendo um conjunto de $n-k$ colunas linearmente dependentes, a matriz resultante H' terá $n-1$ colunas, quaisquer $n-k-1$ colunas alinhadas à esquerda de H' serão linearmente independentes e existirão $n-k$ colunas linearmente dependentes (as que estamos mantendo).

Dessa forma, o comprimento do código $\mathcal{C}^*$ gerado por H' passa a ser $n-1$ e, pelo Lema 3.3, o código $\mathcal{C}^*$ será NMDS, de dimensão $n-k$. Como $\mathcal{C}^*$ é NMDS, segue que $\mathcal{C}_1 = (\mathcal{C}^*)^{\perp}$ é NMDS, possui comprimento $n-1$ e possui dimensão $n-1-(n-k) = k-1$. Por ser NMDS, sua distância mínima é dada por $(n-1)-(k-1) = n-k = d$. Portanto, o código $\mathcal{C}_1$ é NMDS e tem parâmetros $(n-1,k-1,d)$.

Para obtermos um $(n-1,k,d-1)$ código NMDS basta deletarmos, da mesma forma, uma coluna da matriz geradora G de $\mathcal{C}$ preservando um conjunto de k colunas alinhadas à direita linearmente dependentes.

A justificativa segue do fato que, se $\mathcal{C}$ é NMDS com parâmetros (n,k,d), então $\mathcal{C}^{\perp}$ é NMDS com parâmetros $(n,n-k,k)$ e possui matriz teste de paridade G. Aplicando a construção anterior, obteremos um código $\mathcal{C}_1$ com parâmetros $(n-1,n-k-1,k)$ e o dual deste código $\mathcal{C}_1$ será NMDS e terá dimensão $(n-1)-(n-k-1) = k$. Por ser NMDS, a distância mínima de $\mathcal{C}_1^{\perp}$ será

$$(n-1)-(k) = (n-k)-1 = d-1.$$

Logo, $\mathcal{C}_1^{\perp}$ é um $(n-1,k,d-1)$ código NMDS. □

Lema 3.9 *Seja $\mathcal{C}$ um código linear em $\overrightarrow{\mathcal{P}}$ com distância mínima d e seja $\mathcal{C}^{\perp}$ seu código dual. Então a matriz M cujas linhas são as palavras de $\mathcal{C}^{\perp}$ formam uma matriz ortogonal de força $d-1$ com respeito a $\overrightarrow{\mathcal{P}}$.*

Demonstração: A demonstração segue a mesma linha de raciocínio daquela apresentada no Teorema 1.59. O único cuidado a ser tomado é a consideração que fazemos com respeito ao poset $\overrightarrow{\mathcal{P}}$, onde, ao invés de considerarmos colunas linearmente independentes, consideramos colunas linearmente independentes alinhadas à esquerda. □

Exemplo 3.10 *Seja $\mathcal{C}$ o código que possui matriz geradora G dada por*

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

em relação ao poset RT com 3 cadeias e 3 níveis.

Das 32 palavras de $\mathcal{C}$, as que possuem o menor peso, a dizer 4, são

$$100111000, \qquad 100100110 \qquad e \qquad 111000100.$$

Assim, temos $d(\mathcal{C}) = 4$. Pelo Lema 3.9, as palavras de $\mathcal{C}^{\perp}$ formarão uma matriz ortogonal de força $d(\mathcal{C}) - 1 = 3$ em relação ao poset RT mencionado.

De fato, notando que a matriz H dada por

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

é uma matriz teste de paridade para $\mathcal{C}$, suas palavras formarão a matriz

$$M = \left(\begin{array}{ccc|ccc|ccc} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{array}\right).$$

Perceba que os conjuntos possíveis de três colunas alinhadas à esquerda (de acordo com o poset RT) são as seguintes:

$$\begin{array}{lll} \{1,2,3\} & \{1,2,4\} & \{1,8,9\} \\ \{4,5,6\} & \{1,2,7\} & \{4,8,9\} \\ \{7,8,9\} & \{1,5,6\} & \{1,4,7\} \end{array}$$

onde o conjunto $\{1, 4, 7\}$ *indica que escolhemos a* 1^a*, a* 4^a *e a* 7^a *coluna, por exemplo. Tomando quaisquer um desses conjuntos de* 3 *colunas ajustadas à esquerda, os vetores linha*

000	100
001	101
010	110
011	111

aparecem exatamente 2 *vezes, o que caracteriza uma matriz ortogonal.*

3.2 Códigos NMDS e distribuições

Veremos agora uma nova caracterização de códigos NMDS que nos fornecerá uma associação entre palavras de um código NMDS sobre uma métrica definida por um poset Rosembloom-Tsfasman e distribuições uniformes de pontos do cubo unitário $U^n = [0, 1)^n$.

3.2.1 Métrica de Hamming ordenada

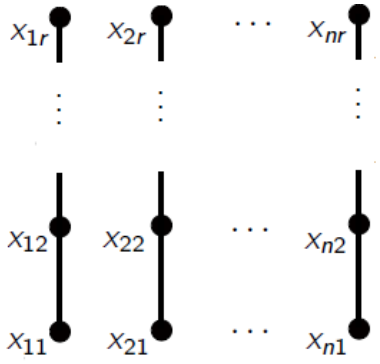
Definição 3.11 *Chamaremos de* ***distância ordenada*** *à distância definida por um poset* $\overrightarrow{\mathcal{P}}$ *que é uma união disjunta de* n *cadeias (também chamadas* ***blocos****) de comprimento* r*, isto é, um poset Rosembloom-Tsfasman.*

A ***métrica de Hamming ordenada*** *é a métrica proveniente desta distância ordenada.*

Nesta métrica, como $\overrightarrow{\mathcal{P}}$ é uma união de n blocos de comprimento r, será conveniente escrever um vetor $x \in \overrightarrow{\mathcal{P}}$ como

$$x = (x_{11}, \ldots, x_{1r}, \ldots, x_{n1}, \ldots, x_{nr}) \in \mathbb{F}_q^{r,n}.$$

Note que as entradas de x estão em correspondência com os vértices de um poset RT com r níveis e n cadeias da seguinte forma:



Proposição 3.12 *O peso de x é dado por*

$$\omega_{\overrightarrow{\mathcal{P}}}(x) = \sum_{i=1}^{n} máx\{j; x_{ij} \neq 0\}.$$

Demonstração: Como $\omega_{\overrightarrow{\mathcal{P}}}(x) = \left|\langle supp(x)\rangle_{\overrightarrow{\mathcal{P}}}\right|$, escrevendo x como um elemento de $\mathbb{F}_q^{r,n}$, o ideal gerado pelo seu suporte será a união dos ideais gerados pelos elementos maximais não nulos de cada coluna e a cardinalidade de cada um desses ideais é dada pela quantidade de elementos situados abaixo do maximal, incluindo este. Nessa representação, j é um contador de quantos elementos estão abaixo de x_{ij}, incluindo o x_{ij}. Logo,

$$\omega_{\overrightarrow{\mathcal{P}}}(x) = \sum_{i=1}^{n} \text{máx}\{j; x_{ij} \neq 0\}.$$

□

Definição 3.13 *Seja x um vetor formado por n blocos de comprimento r. Definimos e_i, $i = 1, \ldots, r$ como o número de blocos de x nos quais a entrada não nula mais à direita (em relação à ordem dada pelo poset) está na i-ésima posição, contabilizada a partir do início do bloco. O vetor de comprimento r dado por $e = (e_1, \ldots, e_r)$ será chamado de* ***shape*** *de x.*

Usaremos as seguintes notações:

$$|e| = \sum_{i=1}^{r} e_i$$

$$|e|' = \sum_{i=1}^{r} ie_i$$

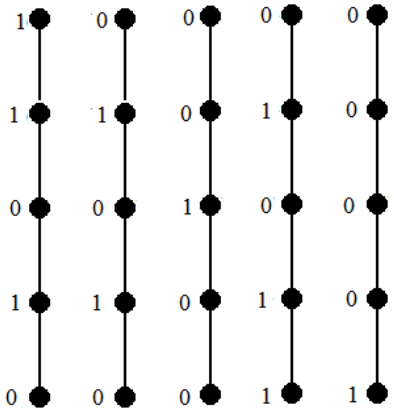
$$e_0 = n - |e|.$$

Repare que, $shape(x) = e$ equivale a dizer $\omega(x) = |e|'$, pela Proposição 3.12.

Exemplo 3.14 *Seja $x \in \mathbb{F}_q^{5,5}$ dado por*

$$x = 01011|01010|00100|11010|10000.$$

Analisando o poset Rosembloom-Tsfasman seguinte,



obtemos

$$e_1 = 1 \quad e_2 = 0 \quad e_3 = 1 \quad e_4 = 2 \quad e_5 = 1$$

e, portanto, o shape de x é dado por

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

Além disso, o número de maximais é dado por

$$|e| = \sum_{i=1}^{5} e_i = 1 + 0 + 1 + 2 + 1 = 5,$$

o número de cadeias sem maximais é dado por

$$e_0 = n - |e| = 5 - 5 = 0$$

e o peso de x é dado por

$$\omega(x) = |e|' = \sum_{i=1}^{5} ie_i = 1 \cdot 1 + 2 \cdot 0 + 3 \cdot 1 + 4 \cdot 2 + 5 \cdot 1 = 17.$$

Se $I = \langle supp(x) \rangle$, então denotaremos o *shape* do ideal I por $shape(I)$. Observe que, pela Proposição 3.12, $shape(I) = shape(x)$.

Em analogia às propriedades de ideais no espaço de Hamming ordenado, usaremos o termo "ajustado à esquerda" para ideais em um poset $\overrightarrow{\mathcal{P}}$.

Definição 3.15 *Um (nr, M, d) **código poset ordenado** $\mathcal{C} \subset \mathbb{F}_q^{r,n}$ é um subconjunto arbitrário de M vetores em $\mathbb{F}_q^{r,n}$ tais que a distância ordenada entre quaisquer dois vetores distintos em $\mathcal{C}$ é, no mínimo, d.*

*O espaço poset $\mathbb{F}_q^{r,n}$ será chamado **espaço de Hamming ordenado** e, se $\mathcal{C}$ é um código linear de dimensão k sobre $\mathbb{F}_q$ e distância ordenada mínima d, denotaremos este como um $[nr, k, d]$ código.*

A noção de matrizes ortogonais no espaço de Hamming ordenado $\mathbb{F}_q^{r,n}$ é derivada da noção apresentada para espaços poset no Lema 3.9 e, neste espaço, serão chamadas **matrizes ortogonais ordenadas (OOA)**.

Definição 3.16 *Um subconjunto $A \subset \mathbb{F}_q^{r,n}$ tal que $|A| = M$ é chamada uma (t, n, r, q)* ***matriz ortogonal ordenada (OOA)*** *de* ***força*** *t se sua projeção em qualquer conjunto de t coordenadas ajustadas à esquerda contém todas as q^t linhas uma mesma quantidade, digamos λ, de vezes. O parâmetro λ será chamado* ***índice*** *de A.*

Temos $M = \lambda q^t$ e, se $\mathcal{C}$ é um $[nr, k, d]$ código, então o código dual forma uma $(d-1, n, r, q)$ OOA de índice

$$\lambda = q^{nr-k-d+1},$$

pelo Lema 3.9.

As OOAs são também chamadas **estruturas hipercúbicas** e foram introduzidas por Lawrence [18] e Mullen e Schmid [22] como uma equivalente combinatória a conjuntos formados por pontos que apresentam multiplicidade mais apropriada para a integração numérica sobre o cubo unitário.

3.2.2 Distribuição de pontos no cubo unitário

Definição 3.17 *Diremos que a* ***bola*** *centrada em x com respeito ao poset $\overrightarrow{\mathcal{P}}$ (também chamada I-***bola***) é o conjunto*

$$B_I(x) = \{v \in \mathbb{F}_q^n; supp(v - x) \subseteq I\}$$

e a ***vizinhança*** *de um código poset $\mathcal{C}$ com respeito a um ideal I (também chamada I-***vizinhança***) é definida como*

$$B_I(\mathcal{C}) = \bigcup_{c \in \mathcal{C}} B_I(c).$$

Definição 3.18 *Um código linear $\mathcal{C}$ de dimensão k forma um I-***telhado** *se existe uma partição*

$$\mathcal{C} = \mathcal{C}_1 \cup \mathcal{C}_2 \cup \ldots \cup \mathcal{C}_{q^{k-1}}$$

*tal que as componentes da partição possuem mesma cardinalidade e as I-vizinhanças de componentes distintas são disjuntas. Se, além disso, as I-vizinhanças formarem uma partição de $\mathbb{F}_q^n$, diremos que $\mathcal{C}$ forma um I-***telhado perfeito**.

Teorema 3.19 *Seja $\mathcal{C}$ um (n, k, d) código linear no poset $\overrightarrow{\mathcal{P}}$. Então $\mathcal{C}$ é NMDS se, e somente se,*

(*i*) *Para todo $I \subset \overrightarrow{\mathcal{P}}$ com $|I| = n - k + 1$, o código $\mathcal{C}$ forma um I-telhado perfeito.*

(*ii*) *Existe um ideal $I \subset \overrightarrow{\mathcal{P}}$ com $|I| = n - k$ tal que $\mathcal{C}$ forma um I-telhado com respeito a esse ideal. Não existe nenhum ideal de tamanho menor que possui essa propriedade.*

Demonstração: Dado um vetor $v \in \mathbb{F}_q^n$ e um ideal $I \subset \overrightarrow{\mathcal{P}}$, denotaremos por $v[I]$ a restrição do vetor v às coordenadas indexadas por I.

Para provar a afirmação (i), seja $\mathcal{C}$ um código NMDS e seja I um ideal de tamanho $n - k + 1$. Seja $H[I]$ a submatriz da matriz teste de paridade H do código $\mathcal{C}$ obtida deletando todas as colunas de H que não estão em I. Assim, $H[I]$ é uma matriz de ordem $(n - k) \times (n - k + 1)$.

Como $\mathcal{C}$ é NMDS, pelo Lema 3.3, quaisquer $n-k+1$ colunas de H alinhadas à esquerda têm posto máximo, a dizer $n - k$. Desta forma, posto $H[I] = n - k$ e, portanto, pelo Teorema do Núcleo e da Imagem, a nulidade de $H[I]$ é

$$n - k + 1 - (n - k) = 1,$$

donde concluímos que o subespaço $ker(H[I])$ possui dimensão 1 e, portanto,

$$|ker(H[I])| = q^1 = q.$$

Como um subespaço vetorial é, em particular, um subgrupo aditivo, façamos $\mathcal{C}_1$ o espaço obtido tomando-se $ker(H[I])$ e acrescentando zeros às entradas que não pertencem a I e seja $\mathcal{C}_j$ a j-ésima classe lateral de $\mathcal{C}_1$ em $\mathcal{C}$, para $j = 2, \ldots, q^{k-1}$.

Dessa forma, temos a partição

$$\mathcal{C} = \bigcup_{i=1}^{q^{k-1}} \mathcal{C}_i.$$

Note que se c' e c'' são duas palavras de uma mesma classe $\mathcal{C}_j$, para algum j, então

$$c' - c'' \in \mathcal{C}_1 = ker(H[I]).$$

Pela construção, as palavras de $\mathcal{C}_1$ possuem todas as entradas nulas nas coordenadas indexadas por I^C. Desta forma, se $\overrightarrow{0}$ é o vetor nulo,

$$(c' - c'')\,[I^C] = 0[I^C] \Rightarrow c'[I^C] = c''[I^C].$$

Vamos mostrar que, se c' e c'' são de classes distintas, devemos ter $c'[I^C] \neq c''[I^C]$.

Como a distância mínima de $\mathcal{C}$ é d e, como $\mathcal{C}$ é NMDS, pelo Lema 3.4, $\mathcal{C}^\perp$ é NMDS e possui distância mínima $d^\perp = n - (n-k) = k$.

Pelo Lema 3.9, o código $\mathcal{C} = \underbrace{\left(\mathcal{C}^\perp\right)^\perp}_{\mathcal{P}}$ forma uma matriz ortogonal de força $d-1 = k-1$ e índice q em relação à $\mathcal{P}$. Portanto, cada vetor $z \in \mathbb{F}_q^{k-1}$ aparece exatamente q vezes nas restrições das palavras $c \in \mathcal{C}$ às coordenadas de $J = I^C$, pois

$$|J| = n - |I| = n - (n-k+1) = k-1.$$

Como as palavras de uma mesma classe coincidem em I^C e cada classe possui exatamente q elementos, segue que as entradas das palavras de classes distintas diferem em I^C e temos o resultado.

Considerando agora duas classes distintas $\mathcal{C}_i$ e $\mathcal{C}_j$, temos $B_I(\mathcal{C}_i) \cap B_I(\mathcal{C}_j) = \emptyset$ pois, caso contrário, existiria $z \in B_I(\mathcal{C}_i) \cap B_I(\mathcal{C}_j)$ e daí $z \in B_I(c') \cap B_I(c'')$, para algum $c' \in \mathcal{C}_i$ e para algum $c'' \in \mathcal{C}_j$. Mas, dessa forma, teríamos

$$supp(z - c') \subset I \quad \text{e} \quad supp(z - c'') \subset I$$

e, como

$$supp(c' - c'') = supp(c'' - z + z - c'') \subset supp(c'' - z) \cup supp(z - c') \subset I,$$

teríamos

$$(c' - c'')[I^C] = 0[I^C] \Rightarrow c'[I^C] = c''[I^C],$$

um absurdo. Isto implica que $\mathcal{C}$ forma um I-telhado.

Este telhado é perfeito, pois $\mathbb{F}_q^n = \bigcup_{i=1}^{q^{k-1}} B_I(\mathcal{C}_i)$.

De fato, temos $B_I(\mathcal{C}_j) = \bigcup_{c \in \mathcal{C}_j} B_I(c)$ e se

$$v \in B_I(c) = \{v \in \mathbb{F}_q^n; supp(v - c) \subset I\},$$

então

$$v[I^C] = c[I^C],$$

isto é, os elementos de $B_I(\mathcal{C}_j)$ são aqueles cujas entradas em I^C são iguais às de $c \in \mathcal{C}_j$. Assim, $B_I(\mathcal{C}_j)$ possui $q^{|I|}$ elementos. Como as classes $\mathcal{C}_j$ são disjuntas e $|B_I(\mathcal{C}_j)| = q^{|I|}$, então, para qualquer $m \in \{1, \ldots, q^{k-1}\}$,

$$\left| \bigcup_{i=1}^{q^{k-1}} B_I(\mathcal{C}_i) \right| = q^{k-1} \cdot |B_I(\mathcal{C}_m)| = q^{k-1} \cdot q^{|I|} = q^{k-1} \cdot q^{n-k+1} = q^n = \left|\mathbb{F}_q^n\right|$$

e, assim,

$$\mathbb{F}_q^n = \bigcup_{i=1}^{q^{k-1}} B_I(\mathcal{C}_i),$$

isto é, $\mathcal{C}$ forma um I-telhado perfeito.

Vamos provar, agora, a afirmação (ii). Seja $\mathcal{C}$ um código NMDS e seja I um ideal de tamanho $n-k$, tomado a partir do suporte de uma palavra de peso mínimo $(n-k)$. Seja $H[I]$ a submatriz da matriz teste de paridade H do código $\mathcal{C}$ obtida deletando todas as colunas de H que não estão em I. Assim, $H[I]$ é uma matriz de ordem $(n-k)\times(n-k)$.

Como $\mathcal{C}$ é NMDS, pelo Lema 3.3, *posto* $H[I] = n-k-1$. Portanto, pelo Teorema do Núcleo e da Imagem, a nulidade de $H[I]$ é

$$n-k-(n-k-1) = 1,$$

donde concluímos que o subespaço $ker(H[I])$ possui dimensão 1.

Pelo mesmo raciocínio apresentado em (i), façamos $\mathcal{C}_1$ o subespaço obtido partir de $ker(H[I])$ pela adjunção de zeros e seja $\mathcal{C}_j$ a j-ésima classe lateral de $\mathcal{C}_1$ em $\mathcal{C}$, para $j = 2, \ldots, q^{k-1}$. Dessa forma, temos a partição

$$\mathcal{C} = \bigcup_{i=1}^{q^{k-1}} \mathcal{C}_i.$$

Como $\mathcal{C}$ é NMDS, $\mathcal{C}^\perp$ é NMDS, pelo Lema 3.4, e assim $d(\mathcal{C}^\perp) = k$. Dessa forma, pelo Lema 3.9, o código $\mathcal{C}$ forma uma matriz ortogonal de força $k-1$ e índice q em relação à $\overleftarrow{\mathcal{P}}$. Fazendo $J = I^C$, temos

$$|J| = n-(n-k) = k$$

e, tomando um ideal (ajustado à direita) $L \subset J$ com $|L| = k-1$, teremos

$$c'[L] = c'[L]$$

para c' e c'' na mesma classe $\mathcal{C}_j$ e

$$c'[L] \neq c'[L]$$

para c' e c'' em classes distintas.

Note que, se c' e c'' diferem nas entradas em L, então diferirão nas entradas em J. Pelos mesmos argumentos anteriores, $B_I(\mathcal{C}_i) \cap B_I(\mathcal{C}_j) = \emptyset$ para $i \neq j$ e, assim, $\mathcal{C}$ forma um I-telhado. Não existem ideais F com $|F| < n-k$ que possuem essa propriedade pois, caso existissem, poderíamos tomar a matriz correspondente $H[F]$ e teríamos um subcódigo $\mathcal{C}_1$ de $\mathcal{C}$ com suporte apenas nas coordenadas indexadas por F, obtendo assim uma palavra com peso menor que a distância mínima do código.

Suponha agora que $I \subset \overrightarrow{\mathcal{P}}$ é um ideal tal que $|I| = n - k + 1$ e seja $\{\mathcal{C}_1, \ldots, \mathcal{C}_{q^{k-1}}\}$ uma partição de $\mathcal{C}$ tal que $|\mathcal{C}_i| = q$, para todo $i = 1, \ldots, q^{k-1}$, que forma um I-telhado perfeito. Isto implica que $c'[I^C] \neq c''[I^C]$, para $c' \in \mathcal{C}_i$, $c'' \in C_j$, com $1 \leq i < j \leq q^{k-1}$.

Em outras palavras, $\mathcal{C}$ forma uma matriz ortogonal com respeito ao poset $\overleftarrow{\mathcal{P}}$ de índice q e força $k-1$. Assim, $d(\mathcal{C}^\perp) \geq k$ pelo Lema 3.9 e, pelo Limitante de Singleton, temos $d\left(\mathcal{C}^\perp\right) = k$ ou $d\left(\mathcal{C}^\perp\right) = k+1$.

Se tivéssemos $d\left(\mathcal{C}^\perp\right) = k+1 = n - (n-k) + 1$, então $\mathcal{C}^\perp$ seria MDS com respeito à $\overleftarrow{\mathcal{P}}$ e, daí, $\mathcal{C}$ seria MDS em relação ao poset $\overrightarrow{\mathcal{P}}$, o que viola a hipótese (ii). Logo, $d\left(\mathcal{C}^\perp\right) = k$ e, assim, $d(\mathcal{C}) \leq n - k$. Se tivéssemos $d(\mathcal{C}) < n - k$, existiria um ideal I tal que $|I| < n - k$ que fornece suporte a um subcódigo de dimensão 1 de $\mathcal{C}$. Então $\mathcal{C}$ forma um I-telhado, o que contradiz (ii). Assim, $d(\mathcal{C}) + d\left(\mathcal{C}^\perp\right) = n - k + (k) = n$ e, portanto, $\mathcal{C}$ é NMDS. □

Exemplo 3.20 *Considere novamente o* $[5, 3, 2]$ *código* $\mathcal{C} \subset \mathbb{F}_2^5$ *dado pela matriz geradora*

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

e cuja distância é definida pelo poset $\mathcal{L}_5$. *Vimos no Exemplo 2.50 que a matriz* H *dada por*

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

é uma matriz teste de paridade para $\mathcal{C}$ *e também que* $d(\mathcal{C}) = 2$ *e* $d(\mathcal{C}^\perp) = 3$.

Assim,

$$d(\mathcal{C}) + d(\mathcal{C}^\perp) = 2 + 3 = 5 = n \ \Rightarrow \mathcal{C} \text{ é NMDS.}$$

Tomando um ideal $I = \{1, 2, 3\} \subset \mathcal{L}_5$, *temos*

$$|I| = 3 = 5 - 3 + 1 = n - k + 1,$$

e assim, como a matriz $H[I]$ *é dada pela restrição de* H *às colunas em* I, *temos*

$$H[I] = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}.$$

Note que posto $(H[I]) = 2$ *e, pelo Teorema do Núcleo e da Imagem, a nulidade de* $H[I]$ *é* 1. *Assim, existe um subcódigo* $\mathcal{C}_1 \subset \mathcal{C}$ *tal que* $\dim(\mathcal{C}_1) = 1$ *e cujo suporte está contido na primeira ou segunda entradas. Desta forma,* $\mathcal{C}_1$ *será o espaço gerado pela palavra* 11000 *e as classes laterais de* $\mathcal{C}_1$ *em* $\mathcal{C}$ *serão, respectivamente:*

$$\begin{aligned} \mathcal{C}_1 &= \{00000, 11000\} \\ \mathcal{C}_2 &= \{10110, 01110\} \\ \mathcal{C}_3 &= \{01101, 10101\} \\ \mathcal{C}_4 &= \{11011, 00011\}. \end{aligned}$$

Tomando vetores na mesma classe, o suporte da diferença entre eles está em I e, para vetores em classes distintas, o suporte da diferença não está contido em I.

Para exemplicar esta última afirmação, tome $10110 \in \mathcal{C}_2$ *e* $00011 \in \mathcal{C}_4$. *Temos* $supp(x-y) = supp(10101) \notin I = \{1,2,3\}$ *pois a quinta entrada de* $supp(x-y)$ *é não nula e* $5 \notin I$.

Calcularemos agora as I-vizinhanças das classes.

(*i*) *Os elementos de* $B_I(\mathcal{C}_1) = B_I(00000) \cup B_I(11000)$ *são:*

00000	11000
01000	10100
00100	01100
10000	11100

(*ii*) *Os elementos de* $B_I(\mathcal{C}_2) = B_I(10110) \cup B_I(01110)$ *são:*

00010	11010
01010	10110
00110	01110
10010	11110

(*iii*) *Os elementos de* $B_I(\mathcal{C}_3) = B_I(01101) \cup B_I(10101)$ *são:*

00001	11001
01001	10101
00101	01101
10001	11101

(*iv*) *Os elementos de* $B_I(\mathcal{C}_4) = B_I(11011) \cup B_I(00011)$ *são:*

00011	11011
01011	10111
00111	01111
10011	11111

Perceba ainda que $B_I(\mathcal{C}_i) \cap B_I(\mathcal{C}_j) = \emptyset$ *se* $i \neq j$ *e*

$$\left| \bigcup_{k=1}^{4} B_I(\mathcal{C}_k) \right| = 4 \cdot 8 = 32 = 2^5 = \left| \mathbb{F}_2^5 \right|,$$

donde obtemos

$$\mathbb{F}_2^5 = \bigcup_{k=1}^{4} B_I(\mathcal{C}_k),$$

isto é, $\mathcal{C}$ *forma um I-telhado perfeito.*

Além disso, tomando agora o ideal $J = \{1, 2\}$*, teremos*

$$H[J] = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$$

e assim, $posto\,(H[J]) = 1$ *e a nulidade de* $H[J]$ *será* 1*, donde concluímos que existe um subcódigo* $\widetilde{\mathcal{C}}_1 \subset \mathcal{C}$ *tal que* $dim(\widetilde{\mathcal{C}}_1) = 1$ *e* $\widetilde{\mathcal{C}}_1$ *possui suporte contido na primeira ou na segunda entrada. Analisando as palavras de* $\mathcal{C}$*, segue que* $\widetilde{\mathcal{C}}$ *é o subespaço gerado pela palavra* 11000 *e as classes laterais de* $\widetilde{\mathcal{C}}_1$ *em* $\mathcal{C}$ *serão as mesmas classes encontradas para o ideal* I *no caso anterior:*

$$\begin{aligned} \widetilde{\mathcal{C}}_1 &= \{00000, 11000\} \\ \widetilde{\mathcal{C}}_2 &= \{10110, 01110\} \\ \widetilde{\mathcal{C}}_3 &= \{01101, 10101\} \\ \widetilde{\mathcal{C}}_4 &= \{11011, 00011\}. \end{aligned}$$

Calcularemos agora as J*-vizinhanças das classes.*

(*i*) *Os elementos de* $B_J(\widetilde{\mathcal{C}}_1) = B_J(00000) \cup B_J(11000)$ *são:*

00000	10000
01000	11000

(*ii*) *Os elementos de* $B_J(\widetilde{\mathcal{C}}_2) = B_J(10010) \cup B_J(01010)$ *são:*

00010	10010
01010	11010

(*iii*) *Os elementos de* $B_J(\widetilde{\mathcal{C}}_3) = B_J(01001) \cup B_J(10001)$ *são:*

00001	10001
01001	11001

(*iv*) *Os elementos de* $B_J(\widetilde{\mathcal{C}}_4) = B_J(11011) \cup B_J(00011)$ *são:*

00011	10011
01011	11011

Como as J*-vizinhanças são disjuntas,* $\mathcal{C}$ *formará um* J*-telhado mas este não será perfeito pois o elemento* $11111 \in \mathbb{F}_2^5$ *não pertence a nenhuma das* J*-vizinhanças das classes.*

Grosso modo, uma **distribuição** no cubo unitário é qualquer coleção arbitrária de pontos deste. Utilizaremos a caracterização de códigos NMDS precedente para relacionarmos códigos no espaço de Hamming ordenado a distribuições. Um código ordenado dá origem a uma distribuição de pontos no cubo unitário pela aplicação

$$\begin{array}{rccc} P: & \mathbb{F}_q^{r,n} & \to & U^n = [0,1)^n \\ & (c_{11},\ldots,c_{1r},\ldots,c_{n1},\ldots,c_{nr}) & \mapsto & (x_1,\ldots,x_n) \end{array}$$

onde

$$x_i = \sum_{j=1}^{r} c_{ij} q^{j-r-1} = \frac{c_{i1}}{q^r} + \frac{c_{i2}}{q^{r-1}} + \ldots + \frac{c_{ir}}{q},$$

para $1 \leq i \leq n$.

Note que esta aplicação está bem definida pois $x_i \in [0,1)$. De fato, como $\mathbb{F}_q$ é um corpo de característica q e $c_{ij} \in \mathbb{F}_q$, sempre podemos considerar $0 \leq c_{ij} \leq q-1$. Assim,

$$\begin{aligned} 0 \leq x_i = \frac{c_{i1}}{q^r} + \frac{c_{i2}}{q^{r-1}} + \ldots + \frac{c_{ir}}{q} &\leq \frac{q-1}{q^r} + \frac{q-1}{q^{r-1}} + \ldots + \frac{q-1}{q} \\ &= \frac{\frac{q-1}{q}\left(\frac{1}{q^r}-1\right)}{\frac{1}{q}-1} = \frac{q-1}{1-q}\left(\frac{1}{q^r}-1\right) \\ &= \frac{q-1}{1-q}\left(\frac{1-q^r}{q^r}\right) = \frac{q^r-1}{q^r} < 1. \end{aligned}$$

A noção idealizada da distribuição uniforme de pontos no cubo unitário diz que um conjunto $\mathcal{C}$ possui tal distribuição (uniforme) se, para qualquer qualquer conjunto mensurável $A \subset U^n$, temos

$$\frac{1}{|\mathcal{C}|} \sum_{x \in \mathcal{C}} 1(x \in A) = vol(A),$$

onde $vol(A)$ é o volume com a medida dada em U^n, neste caso a medida Euclideana.

As distribuições que consideraremos aproximam essa noção pela restrição dos subconjuntos $A \subset U^n$ a blocos retangulares com lados paralelos aos eixos coordenados. Cada um desses blocos será chamado um **intervalo elementar**.

Definição 3.21 *Seja $q \geq 2$ um número inteiro. Um **intervalo elementar na base** q do cubo unitário U^n é um intervalo da forma*

$$E = \prod_{i=1}^{n} \left[\frac{a_i}{q^{d_i}}, \frac{a_i+1}{q^{d_i}}\right),$$

onde $0 \leq a_i \leq q^{d_i}, 0 \leq d_i \leq r$ e $1 \leq i \leq n$.

Exemplo 3.22 *O conjunto $E = \left[0, \frac{1}{2}\right) \times \left[\frac{9}{16}, \frac{10}{16}\right) \times [0,1)$, contido no cubo cnitário U^3 é um intervalo elementar na base 2 que possui volume $\frac{1}{2^5} = \frac{1}{2} \cdot \frac{1}{16} \cdot 1$.*

Definição 3.23 *Uma* (t, m, s)***-rede na base*** q *é um conjunto* R *de* q^m *pontos em* $U^s = [0, 1)^s$ *com a propriedade que qualquer intervalo elementar* E *de volume* q^{t-m} *contém exatamente* q^t *pontos de* R*.*

Definição 3.24 *Seja* ε *uma coleção de intervalos elementares no cubo unitário* $U^n = [0, 1)^n$*. Uma* (nr, k) **distribuição** *na base* q*, com respeito a* ε *é uma coleção arbitrária de pontos em* U^n*.*

Definição 3.25 *Uma distribuição é denominada* **ótima** *se cada intervalo elementar de volume* q^{-k} *contém exatamente um ponto.*

Em 2001, M. Skriganov mostrou que valem os seguintes resultados:

Proposição 3.26 *[29] Um* (nr, k, d) *código MDS na métrica de Hamming ordenada existe se, e somente se, existe uma* (nr, k) *distribuição ótima.*

Teorema 3.27 *[29] Seja* $\mathcal{C}$ *um* (nr, k, d) *código linear MDS em* $\mathbb{F}_q^{r,n}$ *e seja* $P(\mathcal{C})$ *o correspondente conjunto de pontos em* U^n*. Então qualquer intervalo elementar de volume* $\dfrac{1}{q^{k-1}}$ *tem exatamente* q *pontos de* $P(\mathcal{C})$ *e, além disso, a distribuição de pontos* $P(\mathcal{C})$ *dá origem a uma* $(k - r, k, n)$*-rede para* $k \geq r$*.*

Omitiremos as demonstrações desses dois resultados, pois estas fogem ao foco desta dissertação.

Em suma, a Proposição 3.26 diz que códigos MDS na métrica Ordenada correspondem a distribuições ótimas no cubo unitário. Veremos que os códigos ordenados NMDS aproximam essa e as outras propriedades dadas no Teorema 3.27. Para isto, utilizaremos o seguinte resultado, cuja demonstração também omitiremos, provado por K. Lawrence em 1995:

Teorema 3.28 *[18] Uma* $(m - t, n, r, q)$ *OOA de índice* q^t *e tamanho* q^m *corresponde a uma distribuição na qual todo intervalo elementar de volume* q^{t-m} *contém exatamente* q^t *pontos. Além disso, uma* $(m - t, n, m - t, q)$ *OOA de índice* q^t *e tamanho* q^m *dá origem a uma* (t, m, n)*-rede.*

Assim, com a caracterização precedente de códigos ordenados NMDS, obtemos o seguinte teorema:

Teorema 3.29 *[2] Seja* $\mathcal{C}$ *um* (nr, k, d) *código linear em* $\mathbb{F}_q^{r,n}$ *e seja* $P(\mathcal{C})$ *o correspondente conjunto de pontos em* U^n*. Então* $\mathcal{C}$ *é NMDS se, e somente se,*

(*i*) *Qualquer intervalo elementar de volume* $\frac{1}{q^{k-1}}$ *tem exatamente* q *pontos de* $P(\mathcal{C})$.

(*ii*) *Existe um intervalo elementar* $\prod_{i=1}^{n}\left[0,\frac{1}{q^{l_i}}\right)$ *de volume* $\frac{1}{q^k}$ *contendo exatamente* q *pontos e não existem intervalos elementares menores dessa forma que contenham exatamente* q *pontos.*

Demonstração: Suponha que $\mathcal{C}$ seja NMDS. Vamos, inicialmente, provar a afirmação (i). Como $\mathcal{C}$ é NMDS, para todo $I \subset \overrightarrow{\mathcal{P}}$ com $|I| = nr - k + 1$, o código $\mathcal{C}$ forma um I-telhado perfeito pelo Teorema 3.19. Desta forma, $\mathcal{C}$ forma uma matriz ortogonal de força $k-1$ e índice q com respeito à $\overleftarrow{\mathcal{P}}$ ou, de forma equivalente, $\mathcal{C}$ forma uma $(k-1,n,r,q)$ OOA de índice $q = q^1$ e tamanho q^k. Esta matriz corresponde, pelo Teorema 3.28, a uma distribuição na qual todo intervalo elementar de volume

$$q^{1-k} = \frac{q}{q^k}$$

contém exatamente q^1 pontos.

Para demonstrar o item (ii), suponha que $\mathcal{C}$ seja NMDS. Assim, pelo Teorema 3.19, existe um ideal $I \subset \overrightarrow{\mathcal{P}}$ tal que $|I| = nr - k$ ao qual $\mathcal{C}$ forma um I-telhado e nenhum ideal de tamanho menor possui essa propriedade. Desta forma, $\mathcal{C}$ forma uma matriz ortogonal de força k e índice $q^t = q^1$ com respeito à $\overleftarrow{\mathcal{P}}$ e, como uma $(k,n,r,q) = ((k+1)-1,n,r,q) = (m-t,n,r,q)$ OOA de índice q e tamanho q^{k+1} corresponde a uma distribuição na qual todo intervalo elementar de volume

$$q^{t-m} = q^{1-(k+1)} = q^{-k} = \frac{1}{q^k}$$

contém exatamente $q^t = q$ pontos e não existem intervalos elementares de volume menor contendo q pontos. Note que o ponto 0 sempre estará nesse intervalo pois a palavra nula $\overrightarrow{0} \in \mathcal{C}$ está dentro de qualquer ideal I.

Vamos agora demonstrar a recíproca. Supondo que qualquer intervalo elementar de volume $q^{-(k+1)}$ possui exatamente q pontos de $P(\mathcal{C})$, pelo Teorema 3.28, quaisquer $k-1$ colunas alinhadas à esquerda de $\mathcal{C}$ formam uma $(k-1,n,r,q)$ OOA de índice $q^1 = q$. Assim, podemos separar as palavras de $\mathcal{C}$ em classes de equivalência onde uma palavra está relacionada com a outra se as $k-1$ entradas correspondentes coincidem. Desta forma, teremos $\frac{q^k}{q} = q^{k-1}$ classes de equivalência e, escolhendo um ideal $I \subset \overrightarrow{\mathcal{P}}$ com

$$|I| = nr - (k-1) = nr - k + 1$$

tal que as palavras das classes coincidem fora desse ideal obteremos a condição (i) do Teorema 3.19.

Supondo agora que exista um intervalo elementar de volume q^{-k} contendo exatamente q pontos e que nenhum intervalo elementar de volume menor contendo exatamente q pontos existe, pela correspondência dada no Teorema 3.28, existirá uma

$$((k+1)-1, n, r, q) = (k, n, r, q)\ OOA$$

de índice $q = q^1$ e tamanho q^{k+1} e não existem OOAs de força maior que k com essa propriedade. Assim, as palavras do código coincidirão em k entradas para alguma organização das colunas e não coincidirão em mais do que k entradas. Sendo J o ideal formado por estas entradas, temos $|J| = k$ e, assim, fazendo I o complementar de J no conjunto das coordenadas, temos

$$|I| = nr - k.$$

Estabelecendo a relação de equivalência $\sim$ entre as palavras de $\mathcal{C}$ tal que, para $c_1, c_2 \in \mathcal{C}$

$$c_1 \sim c_2 \text{ se, e somente se, } c_1[J] = c_2[J],$$

obteremos a condição (ii) do Teorema 3.19. Combinando (i) e (ii), $\mathcal{C}$ será NMDS.
□

Corolário 3.30 *[2] Um $[nr, k, d]$ código $\mathcal{C}$ NMDS no espaço de Hamming ordenado forma uma $(k-1, n, r, q)$ OOA de índice q. A correspondente distribuição $P(\mathcal{C}) \subset U^n$ forma uma $(k-r, k, n)$-rede para $k - 1 \geq r$.*

Demonstração: A primeira parte do corolário segue de $\mathcal{C}^\perp$ ser um $(nr, nr-k, k)$ código NMDS e, assim, o dual deste $(\mathcal{C})$ forma uma matriz de força $t = k-1$ e índice q, pelo Lema 3.9. A segunda parte segue do fato que uma

$$(k-1, n, r, q)\ OOA$$

é também uma

$$(r, n, r, q)\ OOA = (k-(k-r), n, k-(k-r), q)\ \ OOA$$

para $r \leq k-1$ devido ao Teorema 1.57 e à Observação 1.58(iii) e, pela correspondência dada no Teorema 3.28, essa matriz ortogonal gera uma $(k-r, k, n)$-rede.
□

Com estes resultados, podemos perceber que as distribuições de pontos no cubo unitário provenientes de códigos NMDS possuem propriedades similares aquelas distribuições obtidas a partir dos códigos MDS. Note que os códigos MDS também satisfazem a parte (i) do teorema anterior e dão origem a uma $(k-r, k, n)$-rede para $k \geq r$ (é o que diz o Teorema 3.27).

Exemplo 3.31 *Tomando novamente o código $\mathcal{C}$ do Exemplo 3.20, dado pela matriz geradora*

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

no espaço de Hamming ordenado $\mathbb{F}_2^{5,1}$, vimos que as palavras de $\mathcal{C}$ são

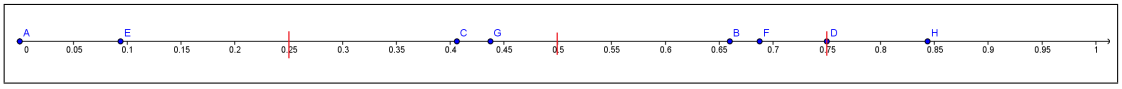
00000	11000
10101	01101
10110	01110
00011	11011

e que $\mathcal{C}$ é NMDS.

Vamos agora estudar a distribuição de pontos no cubo unitário gerada por $\mathcal{C}$. A correspondência entre as palavras e os pontos do cubo unitário $U^1 = [0,1)$ se dá através da seguinte associação:

$$\begin{aligned}
00000 &\mapsto A = \frac{0}{2^5} + \frac{0}{2^4} + \frac{0}{2^3} + \frac{0}{2^2} + \frac{0}{2} = 0; \\
10101 &\mapsto B = \frac{1}{2^5} + \frac{0}{2^4} + \frac{1}{2^3} + \frac{0}{2^2} + \frac{1}{2} = 0,65625; \\
10110 &\mapsto C = \frac{1}{2^5} + \frac{0}{2^4} + \frac{1}{2^3} + \frac{1}{2^2} + \frac{0}{2} = 0,40625; \\
00011 &\mapsto D = \frac{0}{2^5} + \frac{0}{2^4} + \frac{0}{2^3} + \frac{1}{2^2} + \frac{1}{2} = 0,75; \\
11000 &\mapsto E = \frac{1}{2^5} + \frac{1}{2^4} + \frac{0}{2^3} + \frac{0}{2^2} + \frac{0}{2} = 0,09375; \\
01101 &\mapsto F = \frac{0}{2^5} + \frac{1}{2^4} + \frac{1}{2^3} + \frac{0}{2^2} + \frac{1}{2} = 0,6875; \\
01110 &\mapsto G = \frac{0}{2^5} + \frac{1}{2^4} + \frac{1}{2^3} + \frac{1}{2^2} + \frac{0}{2} = 0,4375; \\
11011 &\mapsto H = \frac{1}{2^5} + \frac{1}{2^4} + \frac{0}{2^3} + \frac{1}{2^2} + \frac{1}{2} = 0,84375;
\end{aligned}$$

descrita pela figura abaixo:



Note que os intervalos elementares de volume $\frac{1}{4}$ são

$$\left[\frac{0}{4}, \frac{1}{4}\right), \left[\frac{1}{4}, \frac{2}{4}\right), \left[\frac{2}{4}, \frac{3}{4}\right) \text{ e } \left[\frac{3}{4}, \frac{4}{4}\right)$$

e cada um deles contém exatamente $q = 2$ pontos. Além disso, existe um único intervalo elementar da forma

$$\left[0, \frac{1}{2^{l_i}}\right)$$

de volume $\frac{1}{2^3} = \frac{1}{8}$ contendo exatamente 2 pontos: $\left[0, \frac{1}{2^3}\right)$. Note que não existem intervalos menores que possuem essa forma e com essa propriedade.

Exemplo 3.32 *Considere o código $\mathcal{C}$ dado pela matriz geradora*

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

no espaço de Hamming ordenado $\mathbb{F}_2^{4,2}$. Note que as linhas de G são linearmente independentes e, portanto, $dim(\mathcal{C}) = 4$.

As palavras de $\mathcal{C}$ são:

00000000	11001100
00000001	11001101
00010000	11011100
00010001	11011101
00100010	11101110
00100011	11101111
00110010	11111110
00110011	11111111

Note que uma das palavras de peso mínimo (ajustado à esquerda) é $x = 11001100$, cujo peso é dado por $\omega(x) = \omega(\mathcal{C}) = 4$.

Tomando a matriz H, teste de paridade de $\mathcal{C}$, dada por:

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

segue que as palavras de $\mathcal{C}^\perp$ são:

00000000	00100010
11000000	11100010
10001000	10101010
01001000	01101010
10000100	10100110
01000100	01100110
00001100	00101110
11001100	11101110

e uma das que possuem o peso mínimo (ajustado à direita) é $x = 11000000$*, com*

$$\omega(x) = \omega\left(\mathcal{C}^{\perp}\right) = 4.$$

Como

$$d(\mathcal{C}) + d(\mathcal{C}^{\perp}) = 4 + 4 = 8 = 4 \cdot 2 = nr,$$

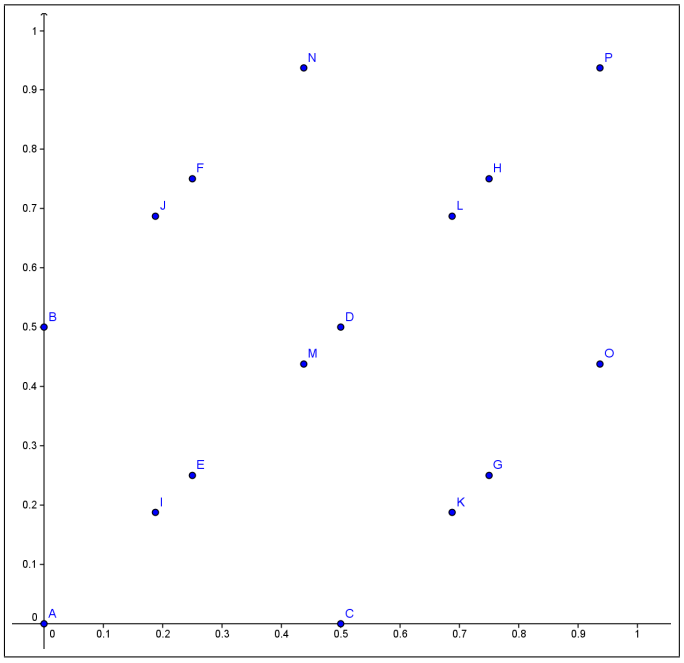
segue que $\mathcal{C}$ *é NMDS.*

Vamos agora estudar a distribuição de pontos no cubo unitário gerada por $\mathcal{C}$*.*

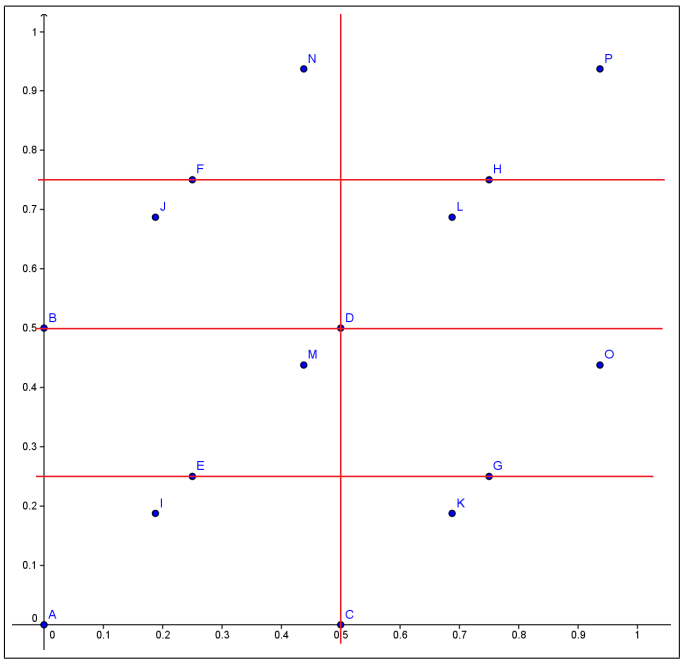
A correspondência entre as palavras e os pontos do cubo unitário $U^2 = [0,1) \times [0,1)$ *se dá através da seguinte associação:*

$$\begin{aligned}
00000000 &\mapsto A = \left(\tfrac{0}{2^4} + \tfrac{0}{2^3} + \tfrac{0}{2^2} + \tfrac{0}{2^1}, \tfrac{0}{2^4} + \tfrac{0}{2^3} + \tfrac{0}{2^2} + \tfrac{0}{2^1}\right) = (0,0)\,;\\
00000001 &\mapsto B = \left(\tfrac{0}{2^4} + \tfrac{0}{2^3} + \tfrac{0}{2^2} + \tfrac{0}{2^1}, \tfrac{0}{2^4} + \tfrac{0}{2^3} + \tfrac{0}{2^2} + \tfrac{1}{2^1}\right) = \left(0, \tfrac{1}{2}\right)\,;\\
00010000 &\mapsto C = \left(\tfrac{0}{2^4} + \tfrac{0}{2^3} + \tfrac{0}{2^2} + \tfrac{1}{2^1}, \tfrac{0}{2^4} + \tfrac{0}{2^3} + \tfrac{0}{2^2} + \tfrac{0}{2^1}\right) = \left(\tfrac{1}{2}, 0\right)\,;\\
00010001 &\mapsto D = \left(\tfrac{0}{2^4} + \tfrac{0}{2^3} + \tfrac{0}{2^2} + \tfrac{1}{2^1}, \tfrac{0}{2^4} + \tfrac{0}{2^3} + \tfrac{0}{2^2} + \tfrac{1}{2^1}\right) = \left(\tfrac{1}{2}, \tfrac{1}{2}\right)\,;\\
00100010 &\mapsto E = \left(\tfrac{0}{2^4} + \tfrac{0}{2^3} + \tfrac{1}{2^2} + \tfrac{0}{2^1}, \tfrac{0}{2^4} + \tfrac{0}{2^3} + \tfrac{1}{2^2} + \tfrac{0}{2^1}\right) = \left(\tfrac{1}{4}, \tfrac{1}{4}\right)\,;\\
00100011 &\mapsto F = \left(\tfrac{0}{2^4} + \tfrac{0}{2^3} + \tfrac{1}{2^2} + \tfrac{0}{2^1}, \tfrac{0}{2^4} + \tfrac{0}{2^3} + \tfrac{1}{2^2} + \tfrac{1}{2^1}\right) = \left(\tfrac{1}{4}, \tfrac{3}{4}\right)\,;\\
00110010 &\mapsto G = \left(\tfrac{0}{2^4} + \tfrac{0}{2^3} + \tfrac{1}{2^2} + \tfrac{1}{2^1}, \tfrac{0}{2^4} + \tfrac{0}{2^3} + \tfrac{1}{2^2} + \tfrac{0}{2^1}\right) = \left(\tfrac{3}{4}, \tfrac{1}{4}\right)\,;\\
00110011 &\mapsto H = \left(\tfrac{0}{2^4} + \tfrac{0}{2^3} + \tfrac{1}{2^2} + \tfrac{1}{2^1}, \tfrac{0}{2^4} + \tfrac{0}{2^3} + \tfrac{1}{2^2} + \tfrac{1}{2^1}\right) = \left(\tfrac{3}{4}, \tfrac{3}{4}\right)\,;\\
11001100 &\mapsto I = \left(\tfrac{1}{2^4} + \tfrac{1}{2^3} + \tfrac{0}{2^2} + \tfrac{0}{2^1}, \tfrac{1}{2^4} + \tfrac{1}{2^3} + \tfrac{0}{2^2} + \tfrac{0}{2^1}\right) = \left(\tfrac{3}{16}, \tfrac{3}{16}\right)\,;\\
11001101 &\mapsto J = \left(\tfrac{1}{2^4} + \tfrac{1}{2^3} + \tfrac{0}{2^2} + \tfrac{0}{2^1}, \tfrac{1}{2^4} + \tfrac{1}{2^3} + \tfrac{0}{2^2} + \tfrac{1}{2^1}\right) = \left(\tfrac{3}{16}, \tfrac{11}{16}\right)\,;\\
11011100 &\mapsto K = \left(\tfrac{1}{2^4} + \tfrac{1}{2^3} + \tfrac{0}{2^2} + \tfrac{1}{2^1}, \tfrac{1}{2^4} + \tfrac{1}{2^3} + \tfrac{0}{2^2} + \tfrac{0}{2^1}\right) = \left(\tfrac{11}{16}, \tfrac{3}{16}\right)\,;\\
11011101 &\mapsto L = \left(\tfrac{1}{2^4} + \tfrac{1}{2^3} + \tfrac{0}{2^2} + \tfrac{1}{2^1}, \tfrac{1}{2^4} + \tfrac{1}{2^3} + \tfrac{0}{2^2} + \tfrac{1}{2^1}\right) = \left(\tfrac{11}{16}, \tfrac{11}{16}\right)\,;\\
11101110 &\mapsto M = \left(\tfrac{1}{2^4} + \tfrac{1}{2^3} + \tfrac{1}{2^2} + \tfrac{0}{2^1}, \tfrac{1}{2^4} + \tfrac{1}{2^3} + \tfrac{1}{2^2} + \tfrac{0}{2^1}\right) = \left(\tfrac{7}{16}, \tfrac{7}{16}\right)\,;\\
11101111 &\mapsto N = \left(\tfrac{1}{2^4} + \tfrac{1}{2^3} + \tfrac{1}{2^2} + \tfrac{0}{2^1}, \tfrac{1}{2^4} + \tfrac{1}{2^3} + \tfrac{1}{2^2} + \tfrac{1}{2^1}\right) = \left(\tfrac{7}{16}, \tfrac{15}{16}\right)\,;\\
11111110 &\mapsto O = \left(\tfrac{1}{2^4} + \tfrac{1}{2^3} + \tfrac{1}{2^2} + \tfrac{1}{2^1}, \tfrac{1}{2^4} + \tfrac{1}{2^3} + \tfrac{1}{2^2} + \tfrac{0}{2^1}\right) = \left(\tfrac{15}{16}, \tfrac{7}{16}\right)\,;\\
11111111 &\mapsto P = \left(\tfrac{1}{2^4} + \tfrac{1}{2^3} + \tfrac{1}{2^2} + \tfrac{1}{2^1}, \tfrac{1}{2^4} + \tfrac{1}{2^3} + \tfrac{1}{2^2} + \tfrac{1}{2^1}\right) = \left(\tfrac{15}{16}, \tfrac{15}{16}\right)\,;
\end{aligned}$$

descrita pela Figura abaixo:



Alguns intervalos elementares de volume $\frac{1}{8} = \frac{1}{2^{4-1}}$ *estão esboçados na figura seguinte.*



Note que cada um deles contém, exatamente, 2 *pontos.*

3.2.3 Distribuição de pesos de um código poset NMDS

Nesta seção, explicitaremos a distribuição de pesos de um $[n, k, d]$ código poset linear em termos da distância mínima d e dos ideais e também estudaremos o caso onde o poset considerado é o que dá origem à métrica de Hamming Ordenada.

Seja $\mathcal{C}$ um $[n, k, d]$ código poset NMDS linear. Lembre-se que $\Omega(I)$ é o conjunto de elementos maximais de um ideal I e faça

$$\widetilde{I} = I \setminus \Omega(I).$$

As seguintes definições nos ajudarão na elaboração da expressão que caracteriza a distribuição de pesos de $\mathcal{C}$:

Definição 3.33 *Seja A_I é o número de palavras do código cujo suporte ajustado à esquerda é exatamente I, isto é,*

$$A_I = |\{x \in \mathcal{C}; \langle supp(x)\rangle = I\}|$$

e, dado um inteiro s, seja A_s é o número de palavras do código $\mathcal{C}$ com peso s, ou seja,

$$A_s = \sum_{I:|I|=s} A_I.$$

Definição 3.34 *Dado um inteiro s, seja $\mathcal{I}_s$ o conjunto dos ideais em relação ao poset $\overrightarrow{\mathcal{P}}$ com cardinalidade s, isto é*

$$\mathcal{I}_s = \{I \subseteq \overrightarrow{\mathcal{P}}; |I| = s\}$$

e, dado um ideal $L \subset \overrightarrow{\mathcal{P}}$, seja $\mathcal{I}_s(L)$ o conjunto dos ideais de L com cardinalidade s, isto é,

$$\mathcal{I}_s(L) = \{J; J \subseteq L \text{ e } |J| = s\}.$$

Teorema 3.35 *A distribuição de pesos do código $\mathcal{C}$ possui a seguinte forma:*

$$A_s = \sum_{I\in\mathcal{I}_s} \sum_{l=0}^{s-d-1} (-1)^l \binom{|\Omega(I)|}{l} \left(q^{s-d-l} - 1\right) + (-1)^{s-d} \sum_{I\in\mathcal{I}_s} \sum_{\substack{J\in\mathcal{I}_d(I)\\ J\supseteq\widetilde{I}}} A_J,$$

para $d \leq s \leq n$.

DEMONSTRAÇÃO: O número de palavras de peso s é dado por

$$A_s = \left| \bigcup_{I \in \mathcal{I}_s} (\mathcal{C} \cap S_I) \right|,$$

onde $S_I = \{x \in \mathbb{F}_q^n; \langle supp(x) \rangle = I\}$ é a esfera com suporte ajustado à esquerda exatamente I.

Note que a expressão acima pode ser reescrita como

$$\left| \bigcup_{I \in \mathcal{I}_s} (\mathcal{C} \cap S_I) \right| = \sum_{I \in \mathcal{I}_s} \left(|\mathcal{C} \cap B_I^*| - \left| \bigcup_{J \in \mathcal{I}_{s-1}(I)} (\mathcal{C} \cap B_J^*) \right| \right), \tag{3.1}$$

onde $B_I = \{x \in \mathbb{F}_q^n; \langle supp(x) \rangle \subset I\}$ é a bola que contém os elementos do espaço que possuem todas as entradas nulas nas coordenadas indexadas por aquelas que não pertencem a I e $B_I^* = B_I \backslash \{\overrightarrow{0}\}$. Isto é possível pois $\mathcal{C} \cap S_I$ e $\mathcal{C} \cap S_J$ são disjuntos para $I, J \in \mathcal{I}_s$ distintos e, assim, pelo Princípio da Inclusão-Exclusão,

$$\left| \bigcup_{I \in \mathcal{I}_s} (\mathcal{C} \cap S_I) \right| = \sum_{I \in \mathcal{I}_s} |\mathcal{C} \cap S_I| = \sum_{I \in \mathcal{I}_s} \left| \mathcal{C} \cap \left(B_I - \bigcup_{J \in \mathcal{I}_{s-1}(I)} B_J \right) \right|$$

$$= \sum_{I \in \mathcal{I}_s} \left(|\mathcal{C} \cap B_I| - \left| \bigcup_{J \in \mathcal{I}_{s-1}(I)} (\mathcal{C} \cap B_J) \right| \right) = \sum_{I \in \mathcal{I}_s} \left(|\mathcal{C} \cap B_I^*| - \left| \bigcup_{J \in \mathcal{I}_{s-1}(I)} (\mathcal{C} \cap B_J^*) \right| \right).$$

Note que se I é um ideal de cardinalidade s e J é um ideal contido em I com cardinalidade $s-1$, pela diferença das cardinalidades concluímos que J não contém um maximal de I e, assim, os ideais $J \in \mathcal{I}_{s-1}(I)$ estão determinados pelos $|\Omega(I)|$ maximais de I, de forma que existem exatamente $|\Omega(I)|$ ideais J nas condições dadas. Portanto, a cardinalidade do último termo da equação (3.1) pode ser determinada pelo Princípio da Inclusão-Exclusão:

$$\begin{aligned} \left| \bigcup_{J \in\, \mathcal{I}_{s-1}(I)} (\mathcal{C} \cap B_J^*) \right| \;=\; & \sum_{J \in\, \mathcal{I}_{s-1}(I)} |\mathcal{C} \cap B_J^*| - \sum_{\substack{J_1, J_2 \in\, \mathcal{I}_{s-1}(I) \\ J_1 \neq J_2}} \left| \mathcal{C} \cap B_{J_1}^* \cap B_{J_2}^* \right| + \ldots + \\ & + (-1)^{|\Omega(I)|-1} \sum_{\substack{J_1, \ldots, J_{|\Omega(I)|} \in\, \mathcal{I}_{s-1}(I) \\ J_1 \neq \ldots \neq J_{|\Omega(I)|}}} \left| \mathcal{C} \cap \left(\bigcap_{i=1}^{|\Omega(I)|} B_{J_i}^* \right) \right|. \end{aligned} \tag{3.2}$$

Como $\mathcal{C}$ é NMDS, segue que $\mathcal{C}^\perp$ é NMDS e, assim, $d\left(\mathcal{C}^\perp\right) = n - d = n - (n - k) = k$ e, portanto, pelo Lema 3.9, $\mathcal{C} = \left(\mathcal{C}^\perp\right)^\perp$ forma uma matriz ortogonal de

força $k-1$ com respeito ao poset dual $\overleftarrow{\mathcal{P}}$. Em outras palavras, os vetores de $\mathcal{C}$ formam uma matriz cujas $k-1$ últimas colunas ajustadas à direita se repetem q vezes. Isto nos fornece uma estimativa para cada termo individual na equação acima.

Para cada $s \geq d+1$, considere o complementar I^C de um ideal $I \in I_s$. Assim, $|I| = s \geq d+1$ e, como

$$\left|I^C\right| = n - |I| = n - s \leq n - (d-1) = (n-d) - 1 = k - 1,$$

o código $\mathcal{C}$ suporta uma matriz ortogonal de força $n-s$ e índice $\dfrac{q^k}{q^{n-s}} = q^{k-n+s} = q^{s-d}$ nas coordenadas definidas por I^C.

Note que, para distintos $J_1, \ldots, J_l \in \mathcal{I}_{s-1}(I)$, como os ideais são determinados pelo conjunto dos elementos maximais, o conjunto

$$\{\{J_1, \ldots, J_l\}; J_i\text{s são distintos e } J_i \in \mathcal{I}_{s-1}(I), i = 1, \ldots, l\}$$

possui $\binom{|\Omega(I)|}{l}$ elementos.

Façamos

$$J = \bigcap_{i=1}^{l} J_i.$$

Como

$$B_J = \{x \in \mathbb{F}_q^n; \langle supp(x)\rangle \subseteq J\}$$

e

$$B_{J_i} = \{x \in \mathbb{F}_q^n; \langle supp(x)\rangle \subseteq J_i\},$$

segue, por dupla inclusão, a igualdade

$$B_J = \bigcap_{i=1}^{l} B_{J_i}$$

e, consequentemente,

$$B_J^* = \bigcap_{i=1}^{l} B_{J_i}^*.$$

Como cada J_i não contém um elemento maximal de I e J é a intersecção de l J_is, segue que J não contém l elementos maximais de I. Assim, as entradas correspondentes a esses maximais são todas nulas nas palavras que possuem suporte em J. Lembrando que as palavras com suporte em J são nulas nas coordenadas definidas por I^C e nas coordenadas definidas por $I - J$ e que as primeiras ocorrem em número de q^{s-d} e incluem as q^l palavras que são também nulas em $I - J$, concluímos que as palavras que possuem suporte em J são em número de

$$\frac{q^{s-d}}{q^l} = q^{s-d-l}.$$

Assim,

$$\left|\mathcal{C}\cap\left(\bigcap_{i=1}^{l}B_{J_i}\right)\right| = |\mathcal{C}\cap B_J| = \frac{q^{s-d}}{q^l} = q^{s-d-l}$$

e, como B_J^* não contém o vetor nulo $\overrightarrow{0}$, obtemos

$$\left|\mathcal{C}\cap\left(\bigcap_{i=1}^{l}B_{J_i}^*\right)\right| = |\mathcal{C}\cap B_J^*| = \frac{q^{s-d}}{q^l} - 1 = q^{s-d-l} - 1,$$

para $1 \leq l \leq s-d-1$.

Finalmente, para $l = s-d$, J não irá conter $l = s-d$ maximais de I. Como $J^C = I^C \cup (I-J)$, temos $\left|J^C\right| = \left|I^C\right| + |I-J| = (n-s) + (s-d) = n-d$ e, assim, $|J| = d$, o que implica

$$\left|\mathcal{C}\cap\left(\bigcap_{i=1}^{l}B_{J_i}^*\right)\right| = |\mathcal{C}\cap B_J^*| = |\{x\in\mathcal{C};\langle supp(x)\rangle = J\}| = A_J,$$

pois se o suporte das palavras em $B_{J_i}^*$ estivesse contido propriamente em J, existiria uma palavra com peso menor que a distância mínima.

Neste caso, como J não contém $s-d$ maximais de I, temos, pela construção, $\widetilde{I}\subseteq J\subseteq I$. Assim, quando $s-1=d$, temos

$$\sum_{\substack{J_i\in\ \mathcal{I}_{s-1}(I)\\ J\supseteq\widetilde{I},\ J_i s\ distintos}}\left|\mathcal{C}\cap\left(\bigcap_{i=1}^{l}B_{J_i}^*\right)\right| = \sum_{\substack{J\in\ \mathcal{I}_d(I)\\ J\supseteq\widetilde{I}}}A_J = \sum_{\substack{J\in\ \mathcal{I}_d(I)\\ J\supseteq\widetilde{I}}}(-1)^{s-d-1}A_J. \qquad (3.3)$$

Quando $s-1>d$, como

$$\left|\mathcal{C}\cap\left(\bigcap_{i=1}^{l}B_{J_i}^*\right)\right| = q^{s-d-l}-1,$$

para dados $J_1,\ldots,J_l$ distintos, temos

$$\sum_{\substack{J_1,\ldots,J_l\in\ \mathcal{I}_{s-1}(I)\\ J_i s\quad distintos}}\left|\mathcal{C}\cap\left(\bigcap_{i=1}^{l}B_{J_i}^*\right)\right| = \binom{|\Omega(I)|}{l}\left(q^{s-d-l}-1\right).$$

Portanto, observando a igualdade

$$\left|\bigcup_{J\in\ \mathcal{I}_{s-1}(I)}(\mathcal{C}\cap B_J^*)\right| = \left|\bigcup_{\substack{J\in\ \mathcal{I}_{s-1}(I)\\ s-1>d}}(\mathcal{C}\cap B_J^*)\right| + \left|\bigcup_{\substack{J\in\ \mathcal{I}_{s-1}(I)\\ s-1=d}}(\mathcal{C}\cap B_J^*)\right|$$

e, pelas equações 3.2 e 3.3, temos

$$\left|\bigcup_{J\in\ \mathcal{I}_{s-1}(I)}(\mathcal{C}\cap B_J^*)\right| = \sum_{l=1}^{s-d-1}(-1)^{l-1}\binom{|\Omega(I)|}{l}\left(q^{s-d-l}-1\right)+ + \sum_{\substack{J\in\ \mathcal{I}_d(I)\\ J\supseteq\widetilde{I}}}(-1)^{s-d-1}A_J. \tag{3.4}$$

Temos ainda

$$\sum_{I\in\ \mathcal{I}_s}|\mathcal{C}\cap B_I^*| = q^{s-d}-1, \tag{3.5}$$

e, como,

$$A_s = \left|\bigcup_{I\in\mathcal{I}_s}(\mathcal{C}\cap S_I)\right|,$$

pelas Equações 3.1, 3.4 e 3.5, temos

$$A_s = \sum_{I\in\ \mathcal{I}_s}\left(\left(q^{s-d}-1\right)-\left(\sum_{l=1}^{s-d-1}(-1)^{l-1}\binom{\Omega(I)}{l}\left(q^{s-d-l}-1\right)+\sum_{\substack{J\in\ \mathcal{I}_d(I)\\ J\supseteq\widetilde{I}}}(-1)^{s-d-1}A_J\right)\right)$$

e, portanto,

$$A_s = \sum_{I\in\mathcal{I}_s}\sum_{l=0}^{s-d-1}(-1)^l\binom{|\Omega(I)|}{l}\left(q^{s-d-l}-1\right)+(-1)^{s-d}\sum_{I\in\mathcal{I}_s}\sum_{\substack{J\in\mathcal{I}_d(I)\\ J\supseteq\widetilde{I}}}A_J.$$

□

Como um corolário do teorema acima, obteremos a distribuição de pesos de um código NMDS no espaço de Hamming ordenado $\mathbb{F}_q^{r,n}$. Para isso, utilizaremos a seguinte definição:

Definição 3.36 *Seja $\mathcal{C}\subset\mathbb{F}_q^{r,n}$ um código ordenado NMDS com distância mínima d e seja s um inteiro tal que $d\leq s\leq nr$. Então denotaremos por A_e o número de palavras do código que possuem shape exatamente e.*

Lema 3.37 *O número de palavras com peso ordenado s em um código $\mathcal{C}\subset\mathbb{F}_q^{r,n}$ é dado por*

$$A_s = \sum_{e:|e|'=s}A_e.$$

DEMONSTRAÇÃO: Como A_e representa o número de palavras do código que possuem *shape* exatamente e, e o peso de uma palavra que possui *shape* e é dado por $|e|'$, segue que o número de palavras com peso ordenado s é dado por

$$A_s = \sum_{e:|e|'=s} A_e.$$

□

Corolário 3.38 *A distribuição de pesos de um código ordenado NMDS* $\mathcal{C} \subset \mathbb{F}_q^{r,n}$ *é dada por*

$$A_s = \sum_{l=0}^{s-d-1} (-1)^l \left(\sum_{e:|e|'=s} \binom{|e|}{l} \binom{n}{e_0, \ldots, e_r} \right) \left(q^{s-d-l} - 1\right) + (-1)^{s-d} \sum_{e:|e|'=d} N_s(e) A_e,$$

para $d \leq s \leq n$, *onde*

$$N_s(e) = \sum_{f;|f|'=s} \binom{e_{r-1}}{f_r - e_r} \binom{e_{r-2}}{(f_r + f_{r-1}) - (e_r + e_{r-1})} \cdots \binom{e_0}{|f| - |e|}.$$

DEMONSTRAÇÃO: Lembrando que o *shape* de um ideal I é dado por

$$shape(I) = e = (e_1, \ldots, e_r),$$

onde e_j, para $j = 1, \ldots, r$ é o número de cadeias de comprimento j contidas em I, obtemos

$$|\Omega(I)| = |e|$$

e

$$\sum_{I \in \mathcal{I}_s} \binom{|\Omega(I)|}{l} = \sum_{e:|e|'=s} \binom{|e|}{l} \binom{n}{e_0, \ldots, e_r}.$$

O termo $\sum_{I \in \mathcal{I}_s} \sum_{\substack{J \in \mathcal{I}_d(I) \\ J \supseteq \widetilde{I}}} A_J$ pode ser reescrito como

$$\begin{aligned} \sum_{I \in \mathcal{I}_s} \sum_{\substack{J \in \mathcal{I}_d(I) \\ J \supseteq \widetilde{I}}} A_J &= \sum_{J \in \mathcal{I}_d} \left| \left\{ I \in \mathcal{I}_s; \widetilde{I} \subseteq J \subseteq I \right\} \right| A_J \\ &= \sum_{e:|e|'=d} N_s(e) \sum_{J:shape(J)=e} A_J, \end{aligned}$$

onde $N_s(e) = \left| \left\{ I \in \mathcal{I}_s; \widetilde{I} \subseteq J \subseteq I, J \text{ é fixo e } shape(J) = e \right\} \right|$.

Observemos que

$$\sum_{J:shape(J)=e} A_J = A_e$$

e, então, só necessitamos determinar a quantidade $N_s(e)$ no somando acima.

Lembrando que o que determina um ideal I é a disposição dos seus maximais e esta disposição pode ser abordada através dos *shape*s do ideal, façamos J fixo, $e = shape(J)$, $f = shape(I)$ e $|f|' = s$. Para que

$$\tilde{I} \subset J \subset I,$$

em cada cadeia, todo maximal de I deve estar no mesmo nível ou em algum nível acima de um maximal de J. Dessa forma, as componentes do *shape* f devem satisfazer as desigualdades

$$\begin{aligned} f_r &\geq e_r \\ f_r + f_{r-1} &\geq e_r + e_{r-1} \geq f_r \\ &\vdots \\ f_1 + \ldots + f_r = |f| &\geq |e| = e_1 + \ldots + e_r \geq f_2 + \ldots + f_r \\ f_0 + f_1 + \ldots + f_r = |f| + f_0 &= |e| + e_0 = e_0 + e_1 + \ldots + e_r \geq |f|, \end{aligned}$$

e $|f|' = s$.

Das desigualdades acima, decorre

$$\begin{aligned} e_{r-1} &\geq f_r - e_r \geq 0 \\ e_{r-2} &\geq (f_r + f_{r-1}) - (e_r + e_{r-1}) \geq 0 \\ &\vdots \\ e_0 &\geq |f| - |e| \geq 0. \end{aligned}$$

Para calcularmos $N_s(e)$, basta contabilizarmos a quantidade de ideais I (distintos) que possuem *shape*s satisfazendo todas as desigualdades acima. Se uma delas não for satisfeita, devemos ter $N_s(e) = 0$. Se todas as desigualdades forem satisfeitas para $f = shape(I)$, um possível esquema é descrito a seguir.

No nível r, devemos escolher e_r dos f_r maximais de I para dispor nas posições ocupadas pelos e_r maximais de J e, depois, dispor (ainda no nível r) os $f_r - e_r$ maximais de I restantes acima dos e_{r-1} maximais de J presentes no nível $r-1$. Como os ideais são determinados pelas posições ocupadas pelos maximais e não pelos maximais, temos $\binom{e_{r-1}}{f_r - e_r}$ possibilidades para as disposições dos f_r maximais.

No nível $r-1$, os f_{r-1} maximais de I serão distribuídos de forma que

$$e_{r-1} - (f_r - e_r) = (e_r + e_{r-1} - f_r)$$

deles ocupem as posições correspondentes às dos maximais de J neste nível e os

$$f_{r-1} - (e_r + e_{r-1} - f_r) = (f_r + f_{r-1}) - (e_r + e_{r-1})$$

restantes ocupem posições acima dos e_{r-2} maximais de J do nível $r-2$. Assim, temos $\binom{e_{r-2}}{(f_r+f_{r-1})-(e_r+e_{r-1})}$ para as disposições dos f_{r-1} maximais.

Continuando esse raciocínio, temos, pelo Princípio Multiplicativo, que

$$\begin{aligned} N_s(e) &= \left|\left\{I \in \mathcal{I}_s; \widetilde{I} \subseteq J \subseteq I, J \text{ é fixo e } shape(J) = e\right\}\right| \\ &= \sum_{f:|f|'=s} \binom{e_{r-1}}{f_r - e_r}\binom{e_{r-2}}{(f_r+f_{r-1})-(e_r+e_{r-1})}\cdots\binom{e_0}{|f|-|e|} \end{aligned}$$

e a demonstração está completa. □

Corolário 3.39 *A distribuição de pesos para um (n,k,d) código linear NMDS no espaço de Hamming é dada por*

$$A_s = \sum_{l=0}^{s-d-1} (-1)^l \binom{s}{l}\binom{n}{s}\left(q^{s-d-l}-1\right) + (-1)^{s-d}\binom{n-d}{s-d}A_d.$$

Demonstração: Basta fazermos $r=1$ e obteremos a métrica de Hamming, a partir da métrica ordenada. Desta forma,

$$|e| = |e|' = e_1 = d,$$

$$|f| = f_1 = s,$$

$$\sum_{e:|e|'=s}\binom{|e|}{l}\binom{n}{e_0,\ldots,e_r} = \sum_{e:|e|'=s}\binom{|e|}{l}\binom{n}{e_0}\binom{n-e_0}{e_1} = \sum_{e:|e|'=s}\binom{|e|}{l}\binom{n}{e_0}\binom{e_1}{e_1}$$

$$= \binom{s}{l}\binom{n}{n-d} = \binom{s}{l}\binom{n}{d} = \binom{s}{l}\binom{n}{s}$$

e

$$N_s(e) = \binom{n-d}{s-d}$$

e temos o resultado. □

Exemplo 3.40 *Considere o código poset $\mathcal{C} \subset \mathbb{F}_2^5$ dado pela matriz geradora*

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

e cuja distância é definida pelo poset $\mathcal{L}_5$. As palavras de $\mathcal{C}$ são:

00000	11000
10101	01101
10110	01110
00011	11011

Tomando a palavra $x = 11000 \in \mathcal{C}$*, o peso desta é dado por*

$$\omega_{\mathcal{L}_5}(x) = 2,$$

que é a distância mínima de $\mathcal{C}$*. Note que, por inspeção,*

$$A_2 = 1, \quad A_3 = 0, \quad A_4 = 2 \quad e \quad A_5 = 4.$$

Vamos verificar esses valores pela expressão obtida no Corolário 3.38. Para isto, observe que o único shape e *tal que* $|e|' = d = 2$ *é dado por* $e = (0, 1, 0, 0, 0)$.

- *Cálculo de* A_3*:*
  Fazendo $s = 3$*, o único shape* f *que satisfaz* $|f|' = s = 3$ *é dado por* $f = (0, 0, 1, 0, 0)$ *e como* $A_e = A_2 = 1$*, pela expressão do Corolário 3.38 temos*

$$\sum_{e:|e|'=2} N_3(e)A_e = \binom{e_4}{f_5 - e_5}\binom{e_3}{(f_5+f_4)-(e_5+e_4)}\binom{e_2}{(f_5+f_4+f_3)-(e_5+e_4+e_3)}\cdot$$

$$\cdot\binom{e_1}{(f_5+\ldots+f_2)-(e_5+\ldots e_2)}\binom{e_0}{|f|-|e|} = \binom{0}{0}\binom{0}{0}\binom{1}{1}\binom{0}{0}\binom{0}{0} = 1.$$

  Portanto,

$$\begin{aligned} A_3 &= \sum_{l=0}^{3-2-1}(-1)^l\left(\sum_{e:|e|'=3}\binom{|e|}{l}\binom{1}{e_0,\ldots,e_r}\right)\left(2^{3-2-l}-1\right) + \\ &\quad +(-1)^{3-2}\sum_{e:|e|'=2}N_3(e)A_e \\ &= (-1)^0\binom{1}{0}\frac{1!}{0!0!0!1!0!0!}\left(2^{1-0}-1\right)+(-1)\cdot 1 = 0. \end{aligned}$$

- *Cálculo de* A_4*:*
  Fazendo $s = 4$*, o único shape* f *que satisfaz* $|f|' = s = 4$ *é dado por* $f = (0, 0, 0, 1, 0)$ *e como* $A_e = A_2 = 1$*, pela expressão do Corolário 3.38 temos*

$$\sum_{e:|e|'=2} N_4(e)A_e = 0,$$

  pois $e_3 = 0 < 1 = (f_5 + f_4) - (e_5 + e_4)$ *e, assim, o é nulo o termo dado por* $\binom{e_3}{(f_5+f_4)-(e_5+e_4)} = \binom{0}{1} = 0$*. Portanto,*

$$\begin{aligned} A_4 &= \sum_{l=0}^{4-2-1}(-1)^l\left(\sum_{e:|e|'=4}\binom{|e|}{l}\binom{1}{e_0,\ldots,e_r}\right)\left(2^{4-2-l}-1\right) + \\ &\quad +(-1)^{4-2}\sum_{e:|e|'=2}N_4(e)A_e \end{aligned}$$

$$\begin{aligned} &= (-1)^0\binom{1}{0}\frac{1!}{0!0!0!0!1!0!}\left(2^{4-2-0}-1\right)+ \\ &\quad +(-1)^1\binom{1}{1}\frac{1!}{0!0!0!0!1!0!}\left(2^{4-2-1}-1\right)+(+1)\cdot 0 \\ &= 1\cdot(4-1)-1(2-1)+0=2. \end{aligned}$$

- *Cálculo de A_5:*
  Fazendo $s=5$, o único shape f que satisfaz $|f|'=s=5$ é dado por $f=(0,0,0,0,1)$ e como $A_e=A_2=1$, pela expressão do Corolário 3.38 temos
  $$\sum_{e:|e|'=2} N_5(e)A_e = 0,$$
  pois $e_4=0<1=f_5-e_5$ e, assim, é nulo o termo dado por $\binom{e_4}{f_5-e_5}=\binom{0}{1}=0$. Portanto,

$$\begin{aligned} A_5 &= \sum_{l=0}^{5-2-1}(-1)^l\left(\sum_{e:|e|'=5}\binom{|e|}{l}\binom{1}{e_0,\ldots,e_r}\right)\left(2^{5-2-l}-1\right)+ \\ &\quad +(-1)^{5-2}\sum_{e:|e|'=2}N_5(e)A_e \\ &= (-1)^0\binom{1}{0}\frac{1!}{0!0!0!0!0!1!}\left(2^{5-2-0}-1\right)+ \\ &\quad +(-1)^1\binom{1}{1}\frac{1!}{0!0!0!0!0!1!}\left(2^{5-2-1}-1\right)+(-1)\cdot 0 \\ &= 1\cdot(8-1)-1(4-1)+0=4. \end{aligned}$$

Exemplo 3.41 *Considere o código $\mathcal{C}$ dado pela matriz geradora*

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

no espaço de Hamming ordenado $\mathbb{F}_2^{4,2}$. Note que as linhas de G são linearmente independentes e, portanto, $dim(\mathcal{C})=4$.

Já mencionamos que as palavras de $\mathcal{C}$ são:

00000000	11001100
00000001	11001101
00010000	11011100
00010001	11011101
00100010	11101110
00100011	11101111
00110010	11111110
00110011	11111111

e que uma das palavras de peso mínimo (ajustado à esquerda) é $x = 11001100$, *cujo peso é dado por* $\omega(x) = \omega(\mathcal{C}) = 4$. *Note que, por inspeção,*

$$A_4 = 3, \quad A_5 = 0, \quad A_6 = 4 \quad A_7 = 4 \quad e \quad A_8 = 4.$$

Vamos verificar o valor de A_6 *pela expressão obtida no Corolário 3.38. Para isto, observemos que os possíveis shapes* e *tais que* $|e|' = d = 4$ *são dados por*

$$e' = (0,0,0,1), \quad e'' = (0,2,0,0) \quad e \quad e''' = (1,0,1,0).$$

Como queremos calcular A_6, *devemos perceber que os possíveis* f *tais que* $|f|' = 6$ *são dados por*

$$\tilde{f} = (0,1,0,1) \quad e \quad f^* = (0,0,2,0).$$

Dessa forma, analisaremos separadamente as contribuições dos shapes e', e'' *e* e''' *no termo* $\displaystyle\sum_{e:|e|'=4} N_6(e)A_e$:

- *Shape* e':
  Note que

$$\begin{aligned} N_6(e')A_{e'} &= \sum_{f:|f|'=6} \binom{e'_3}{f_4 - e'_4}\binom{e'_2}{(f_4+f_3)-(e'_4+e'_3)}\binom{e'_1}{(f_4+\ldots+f_2)-(e'_4+\ldots e'_2)}\binom{e'_0}{|f|-|e'|}A_{e'} \\ &= 0 \cdot 2 = 0, \end{aligned}$$

  pois, como

$$e'_1 = 0 < 1 = \left(\tilde{f}_4 + \ldots + \tilde{f}_2\right) - (e'_4 + \ldots e'_2)$$

  e

$$e'_4 = 0 < 1 = f^*_4 - e'_4,$$

  os binomiais que envolvem as entradas de $\tilde{f}$ *e* e' *e as entradas de* f^* *e* e' *não contribuem para* $N_6(e')$.

- *Shape* e'':
  Note que

$$\begin{aligned} N_6(e'')A_{e''} &= \sum_{f:|f|'=6} \binom{e''_3}{f_4 - e''_4}\binom{e'_2}{(f_4+f_3)-(e''_4+e''_3)}\binom{e''_1}{(f_4+\ldots+f_2)-(e''_4+\ldots e''_2)}\binom{e''_0}{|f|-|e''|}A_{e''} \\ &= \binom{e''_3}{f^*_4 - e''_4}\binom{e'_2}{(f^*_4+f^*_3)-(e''_4+e'_3)}\binom{e''_1}{(f^*_4+\ldots+f^*_2)-(e''_4+\ldots e''_2)}\binom{e''_0}{|f^*|-|e''|}A_{e''} \end{aligned}$$

  pois $e'_3 = 0 < 1 = \tilde{f}_4 - e'_4$ *e, assim, apenas os binomiais que envolvem os termos de* f^* *e* e'' *contribuem para* $N_6(e'')$. *De fato,*

$$N_6(e'')A_{e''} = \binom{0}{0}\binom{2}{2}\binom{0}{0}\binom{0}{0} \cdot 1 = 1.$$

- *Shape e''':*

  Note que

  $$N_6(e''')A_{e'''} = 0$$

  pois $A_{e'''} = 0$, já que nenhuma palavra do código $\mathcal{C}$ possui o shape $e''' = (1,0,1,0)$.

Portanto,

$$\sum_{e:|e|'=4} N_6(e)A_e = N_6(e')A_{e'} + N_6(e'')A_{e''} + N_6(e''')A_{e'''} = 0+1+0 = 1.$$

Como

$$\begin{aligned}\sum_{e:|e|'=6} \binom{|e|}{l}\binom{n}{e_0,\ldots,e_4} &= \binom{2}{l}\frac{2!}{0!0!1!0!1!} + \binom{2}{l}\frac{2!}{0!0!0!2!0!} \\ &= \binom{2}{l}\cdot 2 + \binom{2}{l}\cdot 1,\end{aligned}$$

segue que

$$\begin{aligned}A_6 &= \sum_{l=0}^{6-4-1}(-1)^l\left(\sum_{e:|e|'=6}\binom{|e|}{l}\binom{2}{e_0,\ldots,e_4}\right)\left(2^{6-4-l}-1\right) + \\ &\quad +(-1)^{6-4}\sum_{e:|e|'=4}N_6(e)A_e \\ &= (-1)^0\left(2\binom{2}{0}+\binom{2}{0}\right)\left(2^{6-4-0}-1\right) + (-1)^1\left(2\binom{2}{1}+\binom{2}{1}\right)\left(2^{6-4-1}-1\right) \\ &\quad +(-1)^2\cdot 1 \\ &= 9-6+1 = 4.\end{aligned}$$

3.3 Construções de alguns códigos NMDS

Nesta seção, apresentaremos algumas construções de códigos NMDS no espaço de Hamming ordenado, para os casos $n = 1, 2$ e 3.

3.3.1 Caso $n = 1$: códigos lineares formados por apenas uma cadeia

Para $n = 1$ a construção é quase imediata se reconhecermos que um $[r, k, d]$ código NMDS é também uma matriz ortogonal ordenada de força $k-1$ ajustada à direita e índice q.

Denotando por I_l a matriz identidade de ordem l, tome $x = (x_1, \ldots, x_r)$ qualquer vetor de peso ajustado à esquerda $d = n - k$. Assim, $x \neq 0$ e $x_l = 0$, para $l = d + 1, \ldots, r$. Então a seguinte matriz de ordem $k \times r$ gera um código NMDS com os parâmetros acima citados:

$$G = \begin{pmatrix} x_1 \ldots x_d & 0 & 0 \\ M & 1 & I_{k-1} \end{pmatrix},$$

onde os 0s e 1s são blocos de matrizes com as dimensões apropriadas e $M \in \mathbb{F}_q^{(k-1)\times d}$ é uma matriz arbitrária.

Repare que o código dado no Exemplo 3.20 foi construído tomando-se $x = 11000$ e $M = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$.

3.3.2 Caso $n = 2$: códigos lineares formados por duas cadeias

O processo aqui será parecido com o correspondente ao caso $n = 1$. No entanto, como temos agora duas cadeias, precisamos de mais elementos em nossa matriz geradora.

Definição 3.42 *Seja D_l a matriz quadrada de ordem l cujos elementos da diagonal secundária são todos iguais a 1 e todos os outros elementos são iguais a 0, isto é,*

$$D_l = \begin{pmatrix} 0 & \ldots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \ldots & 0 \end{pmatrix}.$$

Tomando u e v dois vetores de comprimento r em $\mathbb{F}_q^{r,1}$ e pesos ajustados à esquerda $r - k_1$ e $r - k_2$, respectivamente, faça $K = k_1 + k_2$. A seguinte matriz gera um $[2r, K, 2r - K]$ código linear NMDS em $\mathbb{F}_q^{r,2}$:

$$G = \left(\begin{array}{cccc|cccc} u_1 \ldots u_{r-k_1-1} & u_{r-k_1} & 0 & 0 & v_1 \ldots v_{r-k_2-1} & v_{r-k_2} & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & I_{k_1-1} & E_r(k_1, k_2) & 0 & 0 & 0 \\ E_r(k_2, k_1) & 0 & 0 & 0 & 0 & 0 & 0 & I_{k_2-1} \end{array}\right),$$

onde $E_r(i, j)$ é uma matriz de ordem $(i - 1) \times (r - j - 1)$ que possui a seguinte forma:

$$E_r(i,j) = \begin{cases} \left[\dfrac{D_{r-j-1}}{0_{(i+j-r)\times(r-j-1)}}\right] & i + j > r, \\ \left[0_{(i-1)\times(r-i-j)} | D_{i-1}\right] & i + j \leq r. \end{cases}$$

Pela forma da matriz geradora podemos perceber que quaisquer $K - 1$ colunas alinhadas à direita da matriz acima são linearmente independentes. No entanto,

as últimas k_1 e k_2 colunas do primeiro e segundo blocos, respectivamente são linearmente dependentes. Isto implica que essa matriz constitui uma matriz ortogonal ordenada de peso ajustado à direita exatamente igual a $K-1$. Portanto, o dual deste código possui distância mínima K. Por fim, o peso mínimo de qualquer vetor produzido pela matriz geradora é $2r-K$. Portanto, pelo Teorema 3.7, esta matriz gera um código NMDS.

3.3.3 Caso $n = 3$: códigos lineares formados por três cadeias

Para o caso $n = 3$, daremos um código NMDS com parâmetros bem específicos. Sejam $u, v, w \in \mathbb{F}_q^{r,1}$ três vetores tais que o peso ajustado à esquerda de cada um deles é $r-2$. Então, a matriz G mostrada abaixo será a matriz geradora de um $[3r, 6, d]$ código na base $q \geq 3$. Note que quaisquer $K-1 = 6-1 = 5$ colunas alinhadas à direita são linearmente independentes e existem $K = 6$ colunas alinhadas à direita linearmente dependentes (as duas últimas de cada bloco). Além disso, ela é formada de três blocos, correspondendo às três dimensões dadas por n.

$$G = [\ B_1 \mid B_2 \mid B_3\ ],$$

onde

$$B_1 = \begin{bmatrix} u_1 \dots u_{r-6} & u_{r-5} & u_{r-4} & u_{r-3} & u_{r-2} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{bmatrix},$$

$$B_2 = \begin{bmatrix} v_1 \dots v_{r-6} & v_{r-5} & v_{r-4} & v_{r-3} & v_{r-2} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

e

$$B_3 = \begin{bmatrix} w_1 \dots w_{r-6} & w_{r-5} & w_{r-4} & w_{r-3} & w_{r-2} & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

Note que, dependendo da escolha para os vetores u, v e w, o código gerado pela matriz G pode ser degenerado (o mesmo vale para os vetores x, u e v para

os casos $n = 1$ e $n = 2$). Note também que a matriz dada no último caso possui a restrição de que seus elementos são tomados em $\mathbb{F}_q$ com $q \geq 3$. Para gerar um código binário ($q = 2$) nas mesmas condições descritas anteriormente, basta trocarmos o bloco B_1 anterior pelo bloco B_1' dado por

$$B_1' = \begin{bmatrix} u_1 \dots u_{r-6} & u_{r-5} & u_{r-4} & u_{r-3} & u_{r-2} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}.$$

Dessa forma, quaisquer $K - 1 = 6 - 1 = 5$ colunas alinhadas à direita são linearmente independentes e existem $K = 6$ colunas alinhadas à direita linearmente dependentes (as duas últimas de cada bloco).

Capítulo 4

Considerações Finais

O objetivo deste trabalho foi estudar caracterizações para códigos NMDS que possibilitassem a comparação destes com os códigos MDS, além de apresentar duas aplicações dessas caracterizações no que diz respeito a dois tipos de distribuições: a distribuição de pontos no cubo unitário e a distribuição de pesos do código. Quanto ao primeiro tipo, vimos que as distribuições originadas por códigos NMDS, embora não sejam ótimas, possuem propriedades similares às distribuições ótimas obtidas pelos códigos MDS.

Quanto ao segundo, vimos que, ao contrário dos códigos poset MDS [14], a distribuição de pesos dos códigos NMDS não é completamente determinada se não conhecemos o número de palavras que possuem suporte alinhado à esquerda em ideais J de cardinalidade d, onde d é a distância mínima do código. Em particular, para códigos NMDS no espaço de Hamming, é necessário saber o número de palavras de todos os *shape*s e tais que $|e|' = d$. Isso ressalta o fato de que a combinatória de códigos em espaços poset depende dos ideais tomados e a cardinalidade dos seus suportes.

Como perspectivas futuras, podemos buscar expressões para outros tipos de distribuição de pesos para os códigos (distribuições para subcódigos, por exemplo). Tal estudo é de grande interesse, uma vez que é importante saber a probabilidade de decodificação correta quando uma informação é transmitida utilizando-se um código e, para calcular isto na prática, é necessário conhecer a distribuição de pesos dos códigos [3].

Um outro interesse surge na estensão de propriedades específicas dos códigos NMDS com a Métrica de Hamming clássica para espaços poset, uma vez que estes possuem boa interpretação geométrica [7]. Um possível estudo, nesse sentido, envolve a noção de gênero e a busca por condições necessárias para que o análogo para códigos lineares da Hipótese de Riemann para curvas algébricas [15] valha para códigos NMDS em espaços poset.

Referências Bibliográficas

[1] J. Ahn, H. K. Kim, J. S. Kim, M. Kim, Classification of perfect linear codes with crown poset structure, *Discrete Math*, 268 (2003), no. 1-3, pp. 21-30.

[2] A. Barg, P. Purkayastha, Near MDS Poset Codes and Distributions, *Error-Correcting Codes, Finite Geometries, and Cryptography, AMS Series: Contemporary Mathematics*, 523 (2010), pp.135-147.

[3] W. Bernardi, "Distribuição de Pesos dos Códigos", Dissertação de mestrado, UFSC, 1986.

[4] N. V. Bôas, R. H. Doca, G. J. Biscuola. "Tópicos de Física 2 - Termologia, Ondulatória, Óptica", São Paulo: Saraiva, 2007.

[5] R. A. Brualdi, J. S. Graves, K. M. Lawrence, Codes with a poset metric, *Discrete Math*, 147 (1995), no. 1-3, pp. 57-72.

[6] K. A. Bush, "Orthogonal Arrays", Ph.D. Thesys, Universidade da Carolina do Norte, Chapel Hill, (1950).

[7] S. Dodunekov, I. Landgev, "On Near-MDS codes", *J. Geometry*, 54 (1995), 30-43.

[8] D'Oliveira, R. G. L., Firer, M, The Packing Radius of a Code and Partitioning Problems: the Case for Poset Metrics, s. CoRR abs/1301.5915 (2013).

[9] S. T. Dougherty, M.M. Skriganov, Maximum distance separable codes in the ρ metric over arbitrary alphabets, *J. Algebraic Combin.*, 16 (2002), no. 1, pp. 71-81.

[10] G. Günther, "Finite field Fourier transform for vectors of arbitrary length", *Communications and Cryptography: Two Sides of One Tapestry (R. E. Blahut, Jr. D. J. Costello, U. Maurer, and T. Mittelholzer, eds.), Norwell, MA, and Dordrecht, NL: Kluwer Academic*, (1994), pp. 141-153.

[11] A. S. Hedayat, N. J. A. Sloane, J. Stufken, "Orthogonal Arrays - Theory and Applications", *Springer Series in Statistics*, 23, Springer, 1999.

[12] A. Hefez, M. L. T. Villela, "Códigos Corretores de Erros", 2ª Edição, Rio de Janeiro, IMPA, 2008.

[13] W. C. Huffman, V. Pless, "Fundamentals of Error-Correcting Codes", Cambridge, 2003.

[14] J. Y. Hyun and H. K. Kim, Maximum distance separable poset codes, *Des. Codes Cryptogr.* 28 (2008), no. 3, 247261.

[15] D. C. Kim, J. Y. Hyun, A Riemann hypothesis analogue for near-MDS codes, *Discrete Applied Mathematics*, 160 (2012) 24402444.

[16] D. S. Kim, S. H. Cho, Wheight distribution of the crown-wheight space, *European J. Combin*, 28 (2007), no 1, pp 356-370.

[17] D. S. Kim, D. Y. Oh, A classification of posets admitting the MacWilliams identity, *IEEE Trans. Inform. Theory*, 51 (2005), no 4, pp 1424-1431.

[18] K. Lawrence, A combinatorial characterization of (t, m, s)-nets in base b, *J. Combin. Designs 4*, (1996), 275-293.

[19] C. P. Milies, "Breve introdução à Teoria dos Códigos Corretores de Erros ", SBM, Colóquio de Matemática da Região Centro-Oeste, UFMS, 2006.

[20] L. H. Jacy Monteiro. "Elementos de Álgebra", Rio de Janeiro: Livros Tecnicos e Cientificos, 1978.

[21] A. O. Moura, "Dualidade em Espaços Poset", Tese de doutorado, IMECC-Unicamp, 2010.

[22] G. L. Mullen, W. Ch. Schmid, An equivalence between $(t; m; s)$-nets and strongly orthogonal hypercubes, Journal of Combin. Theory, Ser. A 76 (1996), 164-174.

[23] H. Niederreiter, A combinatorial problem for vector spaces over finite fields, *Discrete Math* 96 (1991) no 3, pp 221-228.

[24] R. Nielsen, A class of Sudan-decodable codes, *IEEE Trans. Inform. Theory 46*, (2000), no. 4, 1564-1572.

[25] J. Neggers, H. S. Kim, "Basic Posets", 1ª Edição, World Scientific, 1999.

[26] L. Panek, E. Lazarotto, F.M. Bando, Codes satisfying the chain condition over Rosenbloom-Tsfasman spaces, *Int. J. Pure Appl. Math.*, (2008) 48:217-222.

[27] L. Panek, M. Firer, M. M. S. Alves, Symmetry groups of Rosenbloom-Tsfasman spaces, *Discrete Math* 309 (2009) no 4, pp 763-771.

[28] D. Ritter, "Um estudo sobre códigos corretores de erros sobre posets", Dissertação de mestrado, IMECC-Unicamp, 2009.

[29] M. Skriganov, Coding theory and uniform distributions, *Algebra i Analiz* 13 (2001), no. 2, 191-239, English translation in St. Petersburg Math. J. vol. 13 (2002), no. 2, 301-337.

[30] G. Viswanath, B. S. Rajan, Matriz characterization of linear codes with arbitrary Hamming weight hierarchy, *Elsevier, Linear Algebra and its Applications* (2006), no. 412, 396-407.

[31] V. Wei, Generalized Hamming weights for linear codes, *IEEE Trans. Infor. Theory*, 37 (1991), no. 5, 1412-1418.

[32] M. Yu. Rosenbloom, M. A. Tsfasman, "Codes for the m-metric", *Problems of Information Transmission*, 33 (1997), no. 1, 45-52.