Universidade Estadual de Campinas

INSTITUTO DE MATEMÁTICA, ESTATÍSTICA E COMPUTAÇÃO CIENTÍFICA

Departamento de Matemática

Tese de Doutorado

Dualidade em Espaços Poset

por

Allan de Oliveira Moura †

Doutorado em Matemática - Campinas - SP

Orientador: Prof. Dr. Marcelo Firer

†Este trabalho contou com apoio financeiro da CAPES/CNPq.

Dualidade em Espaços Poset

Este exemplar corresponde à redação final da tese devidamente corrigida e defendida por **Allan de Oliveira Moura** e aprovada pela comissão julgadora.

Campinas, 25 de Fevereiro de 2010.

Marcelo Firer

Prof. Dr. Marcelo Firer

Banca examinadora:

Prof. Dr. Marcelo Firer.

Prof. Dr. Marcelo Muniz Silva Alves.

Prof. Dr. Orlando Stanley Juriaans.

Prof. Dr. Reginaldo Palazzo Jr.

Profa. Dra. Sueli Irene Rodrigues Costa.

Tese apresentada ao Instituto de Matemática, Estatística e Computação Científica, UNICAMP como requisito parcial para obtenção do título de **Doutor em Matemática**.

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA DO IMECC DA UNICAMP
Bibliotecária: Maria Fabiana Bezerra Müller – CRB8 / 6162

Moura, Allan de Oliveira
M865d Dualidade em espaços poset/Allan de Oliveira Moura-- Campinas, [S.P. : s.n.], 2010.

Orientador : Marcelo Firer
Tese (doutorado) - Universidade Estadual de Campinas, Instituto de Matemática, Estatística e Computação Científica.

1.Métricas sobre ordens parciais. 2.Hierarquia de pesos. 3. Peso generalizado de Hamming. I. Firer, Marcelo. II. Universidade Estadual de Campinas. Instituto de Matemática, Estatística e Computação Científica. III. Título.

Título em inglês: Duality for poset codes

Palavras-chave em inglês (Keywords): 1. Poset metric. 2. Weight hierarchy. 3. Generalized Hamming weight.

Área de concentração: Geometria e Aplicações

Titulação: Doutor em Matemática

Banca examinadora: Prof. Dr. Marcelo Firer (IMECC-UNICAMP)
Profa. Dra. Sueli Irene Rodrigues Costa (IMECC-UNICAMP)
Prof. Dr. Reginaldo Palazzo Junior (FEE-UNICAMP)
Prof. Dr. Marcelo Muniz Silva Alves (UFPR)
Prof. Dr. Orlando Stanley Juriaans (IME-USP)

Data da defesa: 25/02/2010

Programa de Pós-Graduação: Doutorado em Matemática

Tese de Doutorado defendida em 25 de fevereiro de 2010 e aprovada

Pela Banca Examinadora composta pelos Profs. Drs.

Prof(a). Dr(a). MARCELO FIRER

Prof(a). Dr(a). SUELI IRENE RODRIGUES COSTA

Prof(a). Dr(a). REGINALDO PALAZZO JUNIOR

Prof(a). Dr(a). MARCELO MUNIZ SILVA ALVES

Prof(a). Dr(a). ORLANDO STANLEY JURIAANS

Aos meus pais,
Juscelino e Madalena.

AGRADECIMENTOS

Aos meus pais Juscelino e Madalena por estarem sempre presentes, me apoiando nas horas mais difíceis, apesar da distância.

As minhas irmãs Francerly e Talita por me darem força, sabendo o quanto é difícil a carreira acadêmica.

A Daniela por ter me proporcionado momentos felizes e por ter me apoiado sempre e apesar de toda dificuldade estar sempre do meu lado.

Aos meus amigos da república, Marcelo Pereira, Marcelo Gonsalves, Neiton, Vinícios, Rafael, Weber, Leandro, Juca e Sr. Luís.

Aos meus amigos Jacson, Marcelão, Tiago e Heriveltom, que sempre me fizeram esquecer de todos os problemas durante minhas supostas férias e pela nossa amizade.

Aos meus amigos de curso que sempre me fizeram dar boas rizadas na hora do café e nos churrascos.

Aos meus amigos do grupo, Cristiano, João, Carina, Grasieli, Antônio, Muniz, Panek, Francis e Agnaldo, que de alguma forma ajudaram na elaboração desta Tese.

A todos os meus professores da UFV, UnB e Unicamp que contribuíram com o meu amadurecimento, em especial a Olímpio, Marinês, Sueli, Sueli Costa, Lana, Lucy e Roitman que me orientaram nesta vida academica com paciência, disposição e compreensão.

Ao meu orientador, Marcelo Firer, que é um "cara que dispensa comentários".

A CAPES/CNPq pelo apoio financeiro e a todos que contribuiram diretamente ou indiretamente com este trabalho.

Resumo

Considerando uma generalização da métrica de Hamming, a métrica ponderada por uma ordem parcial, fazemos uma descrição sistemática para os espaços com a métrica ponderada, dando ênfase aos códigos poset e à hierarquia de pesos contextualizada nesse novo ambiente. Técnicas de multiconjunto, para códigos ponderados, são utilizadas para estender o Teorema da Dualidade de Wei, uma relação entre as hierarquias do código e do seu dual. Como consequência desta Dualidade estendemos certos resultados sobre a discrepância, códigos MDS e uma relação entre a condição cadeia do código e do seu dual.

Palavras Chaves: Códigos poset, peso generalizado, dualidade de pesos.

Abstract

Considering a generalization of the Hamming metric, the metric weighted by a partial order, we make a systematic description of the spaces with those metrics, emphasizing poset codes and the weight hierarchy of weights of those codes. Techniques of multiset, for weighted codes, are used to extend the Duality Theorem of Wei, a relationship between the hierarchy of a code and its dual. As a consequence of Duality we extend some results about the discrepancy, MDS codes and a relationship between a chain code and its dual.

Keywords: Poset codes, generalized weight, weight duality.

Lista de Símbolos

$\|A\|$	cardinalidade do conjunto A
$\mathbb{F}_q$	corpo finito com q elementos
$\mathbb{F}_q^n$	espaço vetorial de dimensão n sobre $\mathbb{F}_q$
$supp(\mathbf{x})$	supporte do elemento $\mathbf{x}$
$d(C)$	peso mínimo
$supp(D)$	supporte do subespaço D
$V^{\perp}$	conjunto dual do conjunto V
$\preccurlyeq_P$	ordem segundo o poset P
$\overline{P}$	poset oposto do poset $\overline{P}$
$\langle A \rangle_P$	ideal do poset P gerado pelo conjunto A
$\mathcal{I}^r(P)$	conjunto de todos os ideais de carnidanidade r em P
$\mathcal{M}(J)$	conjunto de elementos maximais em J
$[n]$	o conjunto $\{1, 2, ..., n\}$
$w_P(\mathbf{x})$	P-peso de $\mathbf{x}$
$w_P(D)$	P-peso generalizado do subespaço D
$d_r^{(P)}(C)$	r-ésimo P-peso mínimo generalizado de C
$Q \subseteq P$	P é um refinamento de Q
m_C	multiconjunto das colunas de uma matriz geradora do código C
m_C^P	multiconjunto associado ao código C
$\mathcal{P}\left(\mathbb{F}_q^n\right)$	$\left\{X : X \subseteq \mathbb{F}_q^k \text{ é um subespaço vetorial}\right\}$
B_J	$\{V_j : j \in J\}$ com $V_j = [\{\mathbf{e}_i : i \in \langle j \rangle_{\overline{P}}\}]$
$\delta_P(C)$	P-discrepância

Sumário

Introdução

A teoria de códigos corretores de erros foi fundada por C. E. Shannon no trabalho "A mathematical theory of communication" [Sha48] publicado em 1948. Ele construiu o modelo matemático para a teoria de comunicação que é estudado até hoje.

Um *sistema de comunicação*, esquematizado pela figura 1 abaixo, é formado por:

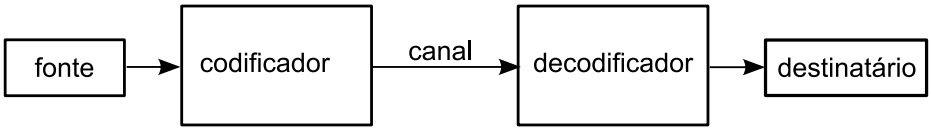


Figura 1: Sistema de Comunicação

Uma *fonte* é um conjunto de possíveis mensagens a serem enviadas por um codificador.

Um *codificador* é um dispositivo que transforma a fonte em um sinal que pode ser enviado por um canal.

Um *canal* é um meio físico pelo qual o sinal obtido do codificador é enviado para o decodificador.

O *decodificador* é um dispositivo que transforma o sinal enviado pelo codificador através do canal, em uma mensagem para o destinatário. Essa mensagem tem que ser uma das possíveis mensagens da fonte.

O *destinatário* pode ser uma pessoa ou qualquer outra coisa em que a mensagem está sendo encaminhada.

Nesse sistema de comunicação consideramos um conjunto finito A, chamado *alfabeto*, que são os dígitos. Um *código* é um subconjunto C de $A^n = A \times A \cdots \times A$, onde n é um número natural. Uma *palavra-código* é um elemento do código. Um *sistema de codificação* é um algoritmo utilizado no codificador que transforma a fonte em um código, que por sua vez é enviada pelo canal como um sinal. O decodificador recebe o sinal e aplica o algoritmo inverso para obter a mensagem.

Durante a transmissão da mensagem pode ocorrer uma interferência (erro) no canal de modo que o sinal recebido pelo decodificador não seja o enviado pelo codificador, comprometendo a mensagem original enviada. Uma forma simples para reduzir a probabilidade de erro

nessa comunicação é introduzir redundância na mensagem, por exemplo repetir a mensagem várias vezes.

Suponhamos que a fonte utilize o alfabeto binário, isto é, o conjunto $\{0,1\}$, e que a probabilidade p de 0 ou 1 ser enviado errado pelo canal seja a mesma e menor que meio, $p < 1/2$. O codificador produz uma palavra-código de comprimento n, que repete a mensagem $n \geq 3$ vezes, e a envia pelo canal, então decodificamos, fazendo o uso da lógica majoritária, isto é, pelo maior número de dígitos $0's$ ou $1's$. Nesse caso o código é $\{00\cdots0, 11\cdots1\}$. Por exemplo, fixando a mensagem a ser enviada como 0. O codificador envia uma palavra-código $00\cdots0$. Se houver algum erro pelo canal, digamos que foi recebida como $010\cdots0$, decodificamos a palavra-código errada como a mensagem 0 e o destinatário receberá corretamente a mensagem.

As possíveis palavras-código a serem decodificadas podem ser quantificadas e divididas pelos erros:

$\binom{n}{0}$ palavras com 0 erros, cada erro com probabilidade $p^0\,(1-p)^n$,
$\binom{n}{1}$ " " 1 " " " " " $p^1\,(1-p)^{n-1}$,
$\binom{n}{2}$ " " 2 " " " " " $p^2\,(1-p)^{n-2}$,
$\vdots$ $\vdots$ $\vdots$
$\binom{n}{n}$ " " n " " " " " $p^n\,(1-p)^0$.

Logo, a probabilidade da palavra-código ser recebida pelo decodificador com no máximo 1 erro é

$$\binom{n}{0}p^0\,(1-p)^n + \binom{n}{1}p\,(1-p)^{n-1} = (1-p)^{n-1}\,(1+(n-1)\,p)$$

como $p < 1/2$, temos que $(1-p)^{(n-1)}$ vai a zero mais rápido do que $1+(n-1)\,p$ vai a infinito, quando n tende a infinito, isto é,

$$\lim_{n\to\infty}(1-p)^{n-1}\,(1+(n-1)\,p) = 0.$$

Assim, a probabilidade do decodificador corrigir 1 erro aumenta quanto maior for n. Entretanto, enviamos uma palavra-código de comprimento n para transmitir uma mensagem de 1 dígito, tendo $n-1$ dígitos de redundância.

Uma medida para a quantidade de informação do código é a taxa de informação do código.

A *taxa de informação* de um código é $R = \frac{\log_q M}{n}$ dígitos por palavra-código, onde q é a cardinalidade do alfabeto, n é o comprimento de uma palavra-código e M é quantidade de mensagens da fonte.

Na *codificação por repetição*, obtemos $q = 2$ e $M = 2$ implicando em uma taxa de informação de $1/n$ digitos por palavra-código. Entretanto, nessa proposta de codificação

quando n tende a infinito a taxa de informação tende a zero.

Uma outra estratégia de codificação, com uma taxa 4/7 maior que a codificação por repetição, é dada pela *codificação de Hamming* [Ham50], que corrige um erro. Considere uma palavra-código $x_1x_2\cdots x_7$, com dígitos no alfabeto binário $\{0,1\}$. Desses x_3, x_5, x_6 e x_7 são os dígitos de uma mensagem escolhida arbitrariamente pela fonte. Os outros 3 símbolos são redundâncias e calculados da seguinte maneira:

x_4 é escolhido para fazer $\alpha = x_4 + x_5 + x_6 + x_7$ par, igual a 0 mod 2
x_2 " " " $\beta = x_2 + x_3 + x_6 + x_7$ par " " ,
x_1 " " " $\gamma = x_1 + x_3 + x_5 + x_7$ par " " .

Quando uma palavra-código é recebida, α, β e γ são calculados. O número binário $\alpha\beta\gamma$ é transformado no índice i do dígito onde ocorreu o erro (se $i = 0$ não houve erro).

A *capacidade de um canal* é o supremo de todas as possíveis taxas de informação com probabilidade baixa de erros na transmissão, que podem ser transmitidas pelo canal.

Shannon determinou que a capacidade do canal é atingida assintoticamente por algum sistema de codificação, isto é, o supremo da definição da capacidade do canal é na verdade um máximo quando o comprimento do bloco tende a infinito. Entretanto, a demonstração desse teorema não é construtiva, originando interesse em construções explicitas de bons códigos

As codificações mais utilizadas usam a métrica de Hamming e a de Lee [HP03]. Se uma palavra-código tem n dígitos, a distância de Hamming entre duas palavras-código $\mathbf{x}$ e $\mathbf{y}$ é o número de coordenadas de $\mathbf{x}$ que são diferentes de $\mathbf{y}$.

O problema de decodificar um sinal $\mathbf{y}$, enviado pelo codificador através do canal como um sinal $\mathbf{x}$, consiste em maximizar a probabilidade de $\mathbf{y}$ ser enviado dado que $\mathbf{x}$ foi recebido, isto é, escolher uma palavra-código $\mathbf{y}$ que é mais provável de ser recebida como $\mathbf{x}$ depois da transmissão. Em certos tipos de canal, esse problema é equivalente a encontrar a distância mínima de Hamming para o código. O problema de encontrar a distância mínima de Hamming, para um código de comprimento n e com uma quantidade M de mensagens, é o *problema clássico em teoria de códigos.*

Uma generalização do problema clássico de teoria de códigos foi encontrada por Niederreider [Nie91], a partir de um tipo especial de conjunto parcialmente ordenado, ele definiu um nova classe de métricas para generalizar o problema clássico da teoria de códigos.

Mais tarde em [BGL95], Brualdi, Graves e Lawrence esquematizaram um modelo geral para essas métricas, obtendo uma métrica ponderada por ordem parcial, originando os *espaços poset*, que estudaremos no Capítulo 2. A métrica de Hamming e a obtida por Niederreider são casos particulares de métrica ponderada, correspondentemente generalizando o problema clássico da teoria de códigos.

Um código em A^n é perfeito se ele empacota o conjunto A^n. Essas métricas se mostraram

frutíferas na abordagem de códigos perfeitos, pois o raio de empacotamento do código com a métrica ponderada é maior que o raio de empacotamento com repeito a métrica de Hamming. A métrica ponderada por um ordem parcial, por ser uma classe muito ampla, vem sendo intensamente estudada para alguns casos particulares de conjuntos parcialmente ordenados, tais como as ordens coroa [KC07, CK06, AKKK03], hierárquica (ordem fraca) [KO05, KL03], e Rosenbloom-Tsfasman [PFSA09, DS02b, PLB08, Lee03, DS02a].

Em [RT97], Rosenbloom e Tsfasman obtiveram uma aplicação, para a métrica de Rosenbloom-Tsfasman (RT-métrica), em interferência nos canais paralelos. Em um *canal paralelo*, queremos enviar uma mensagem, sendo que cada uma das palavras-código é uma s-upla de m-uplas de dígitos, transmitidos por m canais paralelos. Considera-se um ruído interferindo da seguinte natureza: algumas partes consecutivas do canal, começando a partir da última m-upla delas, são ocupadas por usuários prioritários, o qual vai tendo a preferência diminuída, na ordem inversa à ordem de ocupação. O grau de interferência é medido pelo número total de dígitos enviado pelo usuário prioritário sobre a mensagem principal.

Passando a uma outra questão, visando aplicações a criptografia, Wei [Wei91] definiu os pesos generalizados de Hamming de um código para dimensões mais altas. Uma aplicação desse conceito é o canal Ware-Tap tipo II, que acrescenta um adversário que pode obter uma quantidade μ limitada de dígitos da informação. Wei determinou qual a confiabilidade da informação transmitida, ou seja, que condições o adversário não consiga obter a palavra-código mesmo sabendo esses μ dígitos. Posteriormente, vários autores obtiveram novas aplicações para os pesos generalizado de Hamming, tais como complexidade de treliças [Var98, seção 5] e decodificação por lista [Gur03].

O *peso generalizado de Hamming* de um subespaço é o número de coordenadas que não se anulam neste. Para cada dimensão temos um peso mínimo generalizado, o conjunto desses pesos é chamado de *hierarquia* do subespaço. Wei derivou algumas propriedades básicas da hierarquia. Uma das mais interessantes relações que encontrou é um certo tipo de Identidade de MacWilliams da hierarquia. Existe uma relação intima entre a hierarquia do código e a hierarquia do seu código dual. Esta relação entre as hierarquias é conhecida como Dualidade, que é muito utilizada para calcular os pesos generalizados de um código, pois sabendo a hierarquia de um código podemos calcular, usando a Dualidade, facilmente a hierarquia do seu código dual.

Para trabalhar a questão de Dualidade, no contexto de espaços poset, utilizaremos a técnica de multiconjunto. Um *multiconjunto* é uma coleção não ordenada de elementos de um conjunto, podendo haver elementos repetidos. Uma formalização para a relação de códigos e multiconjuntos foi feita em [DS98], por Dodunekov e Simonis. Nessa relação transforma-se a

relação métrica para uma geometria de incidência. Na literatura existem outras denominações desta relação: sistemas projetivos [TV95] e multiconjuntos projetivos [Sch04].

A parte principal desse trabalho generaliza o conceito Dualidade para métricas ponderadas. Um outro resultado é obtido devido a noção de condição cadeia, apresentada por Wei. Ele utilizou a Dualidade para mostrar que um código satisfaz a condição cadeia se, e somente se, o seu código dual a satisfaz também. Assim, como Wei, aplicamos a Dualidade sobre os códigos ponderados e obtemos que um código ponderado satifaz a condição cadeia se, e somente se, o seu código dual satisfaz a condição cadeia.

A organização do trabalho é esquematizada da seguinte forma. No Capítulo 1, fazemos uma breve introdução sobre a teoria de códigos clássica, utilizando a métrica de Hamming. Descrevemos também sobre os pesos generalizado de Hamming. No Capítulo 2, apresentamos os códigos ponderados por uma ordem parcial e algumas de suas características. No Capítulo 3, estudamos os multiconjuntos e suas relações com códigos. Apresentamos também algumas propriedades relacionadas os pesos generalizados e aos códigos poset. No Capítulo 4, demonstramos o Teorema da Dualidade para o caso de um código ponderado por uma ordem parcial. No Capítulo 5, apresentamos algumas consequências da Dualidade, apresentada no capítulo anterior.

Capítulo 1

Códigos Corretores de Erros

O principal objetivo deste capítulo é apresentar algumas definições básicas de códigos corretores de erros e introduzir o conceito de pesos generalizados.

1.1 Definições Básicas

Em teoria de códigos consideramos um conjunto finito A, chamado *alfabeto*. A *cardinalidade do conjunto* A é denotada por $|A|$.

Definição 1.1. Um *código corretor de erros*, ou simplesmente *código*, é um subconjunto C de A^n para algum número natural n. Os elementos de C são chamados de *palavras-código*.

Na teoria de códigos, os alfabetos mais utilizados são aqueles com a estrutura algébrica de corpos finitos. Um *corpo finito* é denotado por $\mathbb{F}_q$, onde q é a cardinalidade do corpo. Um código é então um subconjunto do espaço vetorial de todas as n-uplas sobre $\mathbb{F}_q$, denotado por $\mathbb{F}_q^n$.

Se a cardinalidade do código $C \subseteq \mathbb{F}_q^n$ é M, então dizemos que é um $[n, M]_q$-*código*. Em geral, por simplicidade, denotaremos um vetor $(x_1, x_2, \ldots, x_n) \in \mathbb{F}_q^n$ por $x_1 x_2 \ldots x_n$, pois nos nossos exemplos consideraremos $\mathbb{F}_q = \mathbb{F}_2 = \{0, 1\}$. Isto não gera ambiguidades em $\mathbb{F}_2$, mas é inadequada para $q > 9$. Por exemplo o elemento $110 \in \mathbb{F}_{11}^2$, que poderia representar tanto $(11, 0)$ como $(1, 10)$.

Exemplo 1.2. O código de Hamming, como exemplificado na introdução, é um $[7, 16]_2$-código.

Para desenvolver a teoria de códigos, precisamos estabelecer uma forma de medir os elementos de $\mathbb{F}_q^n$, afim de saber o quão distante ele está de um outro elemento dado.

A imensa maioria da teoria de códigos utiliza a métrica de Hamming para medir elementos. Antes de falar desta métrica, vamos definir o peso de Hamming.

Definição 1.3. Dado $\mathbf{x} \in \mathbb{F}_q^n$, define-se o peso de *Hamming* de $\mathbf{x}$ como sendo a cardinalidade

$$w(\mathbf{x}) := |supp(\mathbf{x})|$$

de $supp(\mathbf{x}) := \{i : x_i \neq 0\}$, o *suporte* de $\mathbf{x}$.

Pela definição acima, o peso de Hamming $w(\mathbf{x})$ de um vetor $\mathbf{x} \in \mathbb{F}_q^n$ é o número de coordenadas não-nulas em $\mathbf{x}$.

O peso de Hamming induz uma métrica em $\mathbb{F}_q^n$, que enunciamos em forma de um Teorema.

Teorema 1.4. [HV02] *A função definida por*

$$\begin{array}{rcl} d : \mathbb{F}_q^n \times \mathbb{F}_q^n & \to & \mathbb{F}_q^n \\ (\mathbf{x}, \mathbf{y}) & \mapsto & d(\mathbf{x}, \mathbf{y}), \end{array}$$

onde

$$d(\mathbf{x}, \mathbf{y}) = w(x - y) = |\{i : x_i \neq y_i, i = 1, \cdots, n\}|$$

é o número de coordenadas no qual $\mathbf{x}$ *difere de* $\mathbf{y}$*, define uma métrica, chamada* métrica de Hamming *ou* distância de Hamming *em* $\mathbb{F}_q^n$.

A *distância mínima de Hamming* de um código é a menor distância entre duas palavras-código, mais precisamente

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

No espaço métrico $\left(\mathbb{F}_q^n, d\right)$, definimos a *bola* de raio r e centro em $\mathbf{x}$, como feito usualmente:

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

O *raio de empacotamento* de um código C é o maior número real $\kappa = \kappa(C)$ tal que as bolas de raio κ e centro nas palavras-código são disjuntas. Para corrigir erros podemos utilizar o raio de empacotamento. Se um vetor $\mathbf{x}$ for enviado e recebido com erros como $\mathbf{y}$, então $\mathbf{y}$ não será reconhecido pelo destinatário como uma palavra-código, detectando que houve algum erro. Mas, se $\mathbf{y}$ foi recebido com até κ erros, então $\mathbf{y} \in B(\mathbf{x}, \kappa)$, assim corrigimos o

vetor recebido $\mathbf{y}$ pelo centro dessa bola $\mathbf{x}$. Chamamos esse fato de decodificação por *vizinho mais próximo*. O próximo Teorema relaciona a distância mínima e essa correção de erros.

Teorema 1.5. [HV02] *Seja C um código com distância mínima de Hamming d. Então C pode corrigir até $\kappa = \left\lfloor \frac{d-1}{2} \right\rfloor$ erros e detectar até $d-1$ erros, onde $\lfloor t \rfloor$ representa a parte inteira de um número real t.*

No exemplo do código de Hamming temos $d = 3$, sendo assim possível corrigir até 1 erro e detectar até 2 erros.

Note que, em virtude do Teorema 1.5, um código terá maior capacidade de correção de erros quanto maior for a sua distância mínima. Portanto, é fundamental, para a teoria de códigos, poder calcular d ou pelo menos determinar uma cota inferior para este valor.

Definição 1.6. Diremos que uma função $F : X \to X$ é uma *isometria* de um espaço métrico (X, d) se esta preserva a distância d, isto é:

$$d\left(F\left(\mathbf{x}\right), F\left(\mathbf{y}\right)\right) = d\left(\mathbf{x}, \mathbf{y}\right) \qquad \forall \mathbf{x}, \mathbf{y} \in X.$$

Uma *isometria linear* é uma transformação linear que também é uma isometria.

Como uma isometria deve ser injetiva, ela também é uma aplicação inversível. Denote por $F^{-1} : X \to X$ essa aplicação. Usando o fato de que F é uma isometria, temos que

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

para todos $\mathbf{x}, \mathbf{y} \in X$. Assim, F^{-1} é uma isometria.

Sejam F e R duas isometrias então

$$d\left(F \circ R\left(\mathbf{x}\right), F \circ R\left(\mathbf{y}\right)\right) = d\left(R\left(\mathbf{x}\right), R\left(\mathbf{y}\right)\right) = d\left(\mathbf{x}, \mathbf{y}\right),$$

$\mathbf{x}, \mathbf{y} \in X$. Assim $F \circ R$ é uma isometria. Originando a Proposição:

Proposição 1.7. *O conjunto $Iso\left(X, d\right)$ das isometrias de um espaço métrico (X, d) é um grupo.*

Se $X = V$, espaço vetorial, então o conjunto das isometrias lineares é um subgrupo de $Iso\left(X, d\right)$, e portanto é um grupo.

Corolário 1.8. [HV02] *O conjunto $Iso\left(\mathbb{F}_q^n, d\right)$ de isometrias do espaço métrico $\mathbb{F}_q^n$ dotado da métrica de Hamming, d, é um grupo.*

Como $Iso\left(\mathbb{F}_q^n, d\right)$ é um grupo podemos separar os códigos em classes de equivalência.

Definição 1.9. Dado dois códigos C e C' em $\mathbb{F}_q^n$, diremos que C' é equivalente a C se existir uma isometria F de $\mathbb{F}_q^n$ tal que $F(C) = C'$.

Em geral, se não colocarmos uma boa estrutura no código sua utilidade é bastante limitada. A estrutura utilizada mais comum é a linearidade.

Definição 1.10. Um *código linear* é um subespaço vetorial de $\mathbb{F}_q^n$.

Se a dimensão de um código linear é k então o chamaremos de um $[n,k]_q$-*código linear*. Observamos que um $[n,k]_q$-código linear é um $\left[n,q^k\right]_q$-código.

O *peso mínimo de Hamming* de um código linear C é o inteiro

$$w_m(C) = min\{w(\mathbf{x}) : \mathbf{x} \in C \backslash \{0\}\}.$$

Uma das vantagens da linearidade é que o peso mínimo e a distância mínima estão diretamente relacionados. Como explicitado no próximo Teorema.

Teorema 1.11. [HV02] *Se* $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$ *, então* $d(\mathbf{x}, \mathbf{y}) = w(\mathbf{x} - \mathbf{y})$. *Se* C *é um código linear, a distância mínima e o peso mínimo de Hamming são iguais.*

Como uma consequência deste Teorema, para códigos lineares, a distância mínima de Hamming é também chamada *peso mínimo de Hamming.*

Existem duas maneiras tradicionais de representar um código linear, por uma matriz geradora ou por uma matriz verificação de paridade.

Para descrever a primeira considere uma base ordenada $B = \{\mathbf{x}_1, \ldots, \mathbf{x}_k\}$ de um $[n,k]_q$-código linear C e considere a matriz $\mathbf{G}$, cujas linha são os vetores da base, isto é,

$$\mathbf{G} = \begin{pmatrix} \mathbf{x}_1 \\ \vdots \\ \mathbf{x}_k \end{pmatrix}.$$

Essa matriz $k \times n$ é chamada *matriz geradora* do código C. A matriz geradora define uma transformação linear por

$$\begin{array}{rcl} T : \mathbb{F}_q^k & \rightarrow & \mathbb{F}_q^n \\ \mathbf{v} & \mapsto & \mathbf{v} \centerdot \mathbf{G}. \end{array}$$

cuja imagem $Im(T)$ é o código C.

Exemplo 1.12. O código de Hamming, visto na introdução, é gerado pelos vetores $1000110, 0100011, 001$

e 0001111. Então uma matriz geradora é

$$\mathbf{G} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} \tag{1.1}$$

e ele é um $[7,4]_2$-código linear.

Observamos que para cada base do código obtemos uma outra matriz geradora. Portanto, em geral, existem muitas matrizes geradoras para um $[n,k]_q$-código linear C, a saber $\left(q^k-1\right)\left(q^k-q\right)\cdots\left(q^k-q^{k-1}\right)$. Uma forma comum de escrever uma matriz geradora para C é da forma $\mathbf{G} = [I_k, A]$, onde I_k é uma matriz identidade $k \times k$ e A é uma matriz de redundâncias $k \times (n-k)$, essa forma é chamada *forma padrão*.

A segunda forma de descrever um código linear segue do fato dele ser um subespaço de um espaço vetorial. Assim, ele é o núcleo de uma transformação linear, isto é, existe uma matriz $\mathbf{H}$ $(n-k) \times n$ tal que

$$C = \left\{\mathbf{x} \in \mathbb{F}_q^n : \mathbf{H} \cdot \mathbf{x}^\top = \mathbf{0}\right\},$$

a qual chamamos de *matriz verificação de paridade* para o código linear.

Note que as linhas de $\mathbf{H}$ são também linearmente independentes e, em geral, existem muitas matrizes teste de paridade, a saber $\left(q^{n-k}-1\right)\left(q^{n-k}-q\right)\cdots\left(q^{n-k}-q^{n-k-1}\right)$.

O próximo Teorema apresenta uma forma para a matriz verificação de paridade a partir de uma matriz geradora.

Teorema 1.13. [HV02] *Se* $\mathbf{G} = [I_k, A]$ *é uma matriz geradora na forma padrão para um* $[n,k]_q$*-código linear* C*, então* $\mathbf{H} = \left[-A^\top, I_{n-k}\right]$ *é uma matriz verificação de paridade para* C*.*

Exemplo 1.14. Usando o Teorema 1.13 na matriz geradora (1.1), temos a matriz verificação de paridade

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

1.2 Pesos Generalizados e Dualidade

Motivado por aplicações em criptografia, Wei, em [Wei91], estudou a estrutura de códigos lineares sobre uma nova perspectiva. Observou que os pesos de Hamming são invariantes

de subespaços de dimensão 1. Generalizou os pesos de Hamming para subespaços de dimensão mais alta.

Um subcódigo $D \subseteq C$ de dimensão 1 consiste de todos os múltiplos de uma palavra-código não-nula. Como o suporte dessas palavras-código não-nulas são iguais, o suporte de D é definido como o suporte de qualquer palavra-código não-nula no subcódigo. Com esta perspectiva, Wei definiu:

Definição 1.15. O *suporte de um subespaço* $D \subseteq \mathbb{F}_q^n$ é o conjunto de coordenadas nem sempre nulas do subespaço:

$$supp\,(D) := \{i : \exists \mathbf{x} \in D, x_i \neq 0\} = \bigcup_{\mathbf{x} \in D} supp\,(\mathbf{x})\,.$$

A partir desta definição Wei definiu o peso generalizado para um subespaço:

Definição 1.16. O *peso generalizado de Hamming* de um subespaço $D \subseteq \mathbb{F}_q^n$ é a cardinalidade do suporte deste subespaço:

$$w\,(D) := |supp\,(D)|\,.$$

Assim, definimos o *r-ésimo peso mínimo generalizado de Hamming* de um código como o menor peso dos subespaços de dimensão r,

$$d_r\,(C) := min\,|\{w\,(D) : D \subseteq C, \dim D = r\}|\,.$$

Note que $d_1\,(C)$ é igual ao peso mínimo de Hamming do código C. Chamamos a sequência de inteiros

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

de *hierarquia* do código.

Wei desenvolveu algumas características principais da hierarquia.

Teorema 1.17 (Monotonicidade)**.** *[Wei91, Teorema 1] Para um $[n,k]_q$-código C com $k > 0$, a hierarquia é uma sequência crescente:*

$$1 \leq d_1\,(C) < d_2\,(C) < \cdots < d_k\,(C) \leq n.$$

Demonstração. Como um subcódigo de dimensão r contém um subcódigo de dimensão $r-1$, temos $d_{r-1}\,(C) \leq d_r\,(C)$. Seja D um subcódigo tal que $d_r\,(C) = w\,(D)$ e $\dim D = r$. Considerando $i \in suppD$ e $D_i := \{\mathbf{x} \in D : x_i = 0\}$. Então $\dim D_i = r - 1$ e $d_{r-1}\,(C) \leq |suppD_i| \leq |suppD| - 1 = d_r\,(C) - 1$. □

Corolário 1.18 (Limitante de Singleton Generalizado)**.** *[Wei91, Corolário 1] Para um $[n,k]_q$-código C, temos*

$$r \leq d_r(C) \leq n-k+r.$$

Demonstração. Basta observar que $d_k(C) \leq n$ e $d_{r-1}(C)+1 \leq d_r(C)$. □

Definição 1.19. Dado um conjunto $V \in \mathbb{F}_q^n$ definimos o seu conjunto dual

$$V^{\perp} := \left\{ \mathbf{u} \in \mathbb{F}_q^n : \mathbf{u} \cdot \mathbf{v} = 0, \forall \mathbf{v} \in V \right\},$$

onde

$$\mathbf{u} \cdot \mathbf{v} = \sum_{i=1}^{n} u_i v_i$$

é uma forma bilinear simétrica, não-degenerada (se $\mathbf{u} \cdot \mathbf{v} = 0, \forall \mathbf{v}$ então $\mathbf{u} = 0$), mas um vetor pode ser dual a si mesmo. Por exemplo, se $\mathbf{u} \in \mathbb{F}_2^n$ e $w(\mathbf{u})$ é par.

Observe também que, assim como ocorre no produto interno do espaço vetorial $\mathbb{R}^n$ sobre os números reais, $V^{\perp}$ é sempre um subespaço vetorial de $\mathbb{F}_q^n$, mesmo que V não seja.

Seja C um $[n,k]_q$-código. O *código dual* de C é o subespaço formado pelo seu conjunto dual, $C^{\perp}$. Se um código tem matriz geradora $\mathbf{G}$ e matriz verificação de paridade $\mathbf{H}$, então o código dual tem matriz geradora $\mathbf{H}$ e matriz verificação de paridade $\mathbf{G}$. Desse modo o código dual é um $[n, n-k]_q$-código.

O Teorema da Dualidade de Wei estabelece uma forte relação entre as hierarquias de um código e a do seu código dual.

Teorema 1.20 (Dualidade)**.** *[Wei91, Teorema 3] Seja C um $[n,k]_q$-código, então a hierarquia*

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

e o conjunto

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

são disjuntos, isto é,

$$X \cap Y = \emptyset$$

e

$$X \cup Y = \{1, 2, \ldots, n\}.$$

A prova deste Teorema será feita para um caso mais geral no Capítulo 4.

Exemplo 1.21. Seja C o $[7,4]_2$-código de Hamming. Sua matriz geradora é

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

e então sua hierarquia de pesos é

$$\{3, 5, 6, 7\}.$$

O seu código dual $C^{\perp}$ é um $[7,3]_2$-código linear com matriz geradora dada por

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

e com hierarquia de pesos:

$$\{4, 6, 7\}.$$

Temos os conjuntos

$$X = \{3, 5, 6, 7\}$$

e

$$Y = \{8-4, 8-6, 8-7\} = \{4, 2, 1\},$$

donde se verifica $X \cup Y = \{1, 2, 3, 4, 5, 6, 7\}$ e $X \cap Y = \emptyset$, validando o Teorema da Dualidade.

Capítulo 2

Códigos Poset

Existem muitas métricas que podem ser definidas em $\mathbb{F}_q^n$, sendo que as mais comuns são as métricas de Hamming e de Lee [HP03].

Em [Nie91], Neiderreiter generalizou o problema clássico em teoria de códigos de encontrar a distância mínima. Brualdi, Graves e Laurence em [BGL95] também estabeleceram uma definição mais ampla para o problema: usando conjuntos parcialmente ordenados e definindo o conceito de códigos poset, eles começaram o estudo com as métricas poset, que generalizam a métrica de Hamming. Este tipo de abordagem tem sido frutífera, pois muitos novos códigos perfeitos foram encontrados com tais métricas poset como em [BGL95, AKKK03, JP03, HK04, Lee04, JKOR08].

Uma situação particular de códigos poset e espaços com a métrica poset são os espaços introduzidos por Rosenbloom e Tsfasman em [RT97]. Esses espaços são úteis no caso de interferência em canais paralelos.

Na Seção 2.1, abordaremos alguns conceitos de conjuntos parcialmente ordenados, principalmente os finitos. As referências principais sobre esse assunto são os livros de Stanley [Sta97] e o de Neggers e Kim [NK98]. Na Seção 2.2, definimos o código poset e algumas de suas características. Na Seção 2.3, comentamos sobre isometrias em espaços com métrica poset. Na Seção 2.4, generalizamos os conceito de pesos generalizados para o ambiente de códigos poset. Na Seção 2.5, abordamos refinamentos poset e algumas de suas consequências em códigos poset e na Seção 2.6, generalizamos o conceito de códigos MDS. Apresentamos, principalmente nas Seções 2.5 e 2.6, diversos resultados simples, alguns já conhecidos, mas não disponíveis de forma organizada na literatura.

2.1 Conjuntos Parcialmente Ordenados

Uma *ordem parcial* sobre um conjunto X é uma relação binária $\preccurlyeq$ que satisfaz as seguintes propriedades para todo $a, b, c \in X$:

1. Reflexiva: $a \preccurlyeq a$,
2. Anti-simétrica: Se $a \preccurlyeq b$ e $b \preccurlyeq a$ então $a = b$,
3. Transitiva: Se $a \preccurlyeq b$ e $b \preccurlyeq c$ então $a \preccurlyeq c$.

Definição 2.1. Seja X um conjunto. O par ordenado $(X, \preccurlyeq)$ é chamado de *conjunto parcialmente ordenado* (abreviadamente, *poset*) se $\preccurlyeq$ é uma ordem parcial sobre o conjunto X.

Se um elemento $a \in X$ se relaciona com um outro elemento $b \in X$, isto é $a \preccurlyeq b$ ou $b \preccurlyeq a$, dizemos que a e b são *comparáveis*, caso contrário eles são ditos *incomparáveis*.

Um poset $(X, \preccurlyeq)$ é dito *totalmente ordenado* se quaisquer dois elementos do conjunto X são comparáveis, também nos referimos a tal poset por *poset linear* (*ou cadeia*). Um poset é dito *antilinear*, *ou anticadeia*, se quaisquer dois elementos são incomparáveis.

Exemplo 2.2. O conjunto dos números naturais com a ordem natural forma um poset linear.

Dado um poset $(X, \preccurlyeq)$ tal que o conjunto X é finito dizemos que o poset é um *poset finito*. A cardinalidade do conjunto X é chamada de *comprimento do poset*.

Existe uma forma especial de representar graficamente os posets finitos, através dos *diagramas de Hasse*. Dado um poset finito $(X, \preccurlyeq)$ os elementos de X são representados por vértices e as comparações entre dois elementos $a, b \in X$ são representadas por arestas, onde se convenciona que um elemento a está abaixo de b se, e somente se, $a \preccurlyeq b$ e não existe $c \neq a, b$ tal que $a \preccurlyeq c \preccurlyeq b$.

Exemplo 2.3. Considere a ordem $\preccurlyeq$ sobre um conjunto $X = \{a, b, c, d, e\}$ com as comparações $\{a \preccurlyeq b, c \preccurlyeq b, d \preccurlyeq e\}$, então o diagrama de Hasse desse poset $(X, \preccurlyeq)$ é representado na Figura 2.1 abaixo.

Para determinar a forma de um diagrama de Hasse para um poset $(X, \preccurlyeq)$ para elementos distintos a e b em X usamos a transitividade da ordem parcial. Assim $a \preccurlyeq b$ se, e somente se, existe um caminho crescente no diagrama de a para b. Na Figura 2.1, o caminho crescente de a para b mostra a relação $a \preccurlyeq b$. A mesma figura mostra que os elementos c e d são incomparáveis.

Dessa forma, podemos representar os posets linear e antilinear de comprimento 4 através dos diagramas de Hasse na Figura 2.2:

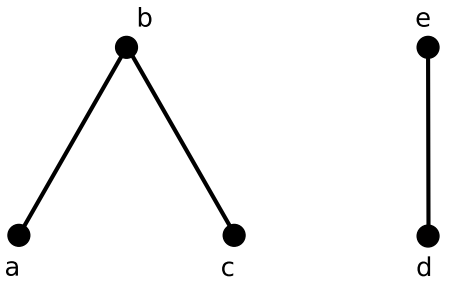


Figura 2.1: Diagrama de Hasse do poset $(X, \preccurlyeq)$.

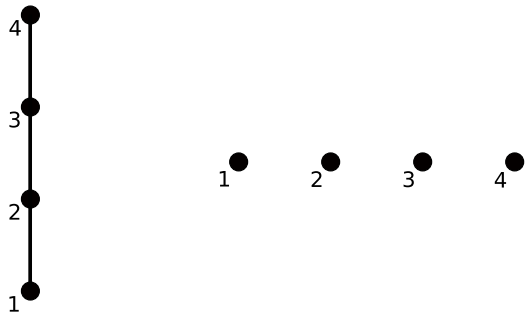


Figura 2.2: Diagrama de Hasse para os posets linear e antilinear, respectivamente.

Exemplo 2.4. O poset Coroa é um conjunto $X = \{1, 2, \cdots, 2k\}, k > 1$, com as seguintes comparações, $i \preccurlyeq k+i, i+1 \preccurlyeq k+i$ para cada $i \in X - \{k-1\}$, $1 \preccurlyeq 2k$ e $k \preccurlyeq 2k$, e os outros elementos não são comparáveis. Seu diagrama de Hasse para $k = 4$ é exposto na Figura 2.3:

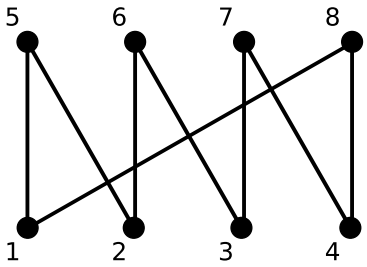


Figura 2.3: Poset Coroa.

Exemplo 2.5. O poset Rosenbloom-Tsfasman (RT) é a união disjunta finita de posets lineares. Um exemplo de diagrama de Hasse para 3 posets lineares de comprimento 3 é apresentado na Figura 2.4 abaixo:

Exemplo 2.6. O poset Hierárquico de comprimento $n = n_1 + n_2 + \cdots + n_t$, com n_i inteiros,

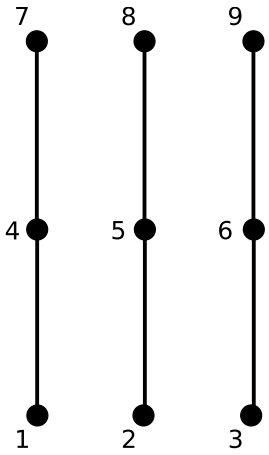


Figura 2.4: Poset RT.

sobre o conjunto $X = \{(i, j) : 1 \leq i \leq t, 1 \leq j \leq n_i\}$, é apresentado com as comparações

$$(a, b) \preccurlyeq (c, d) \Leftrightarrow a < c.$$

Um exemplo do diagrama de Hasse para $n = 9$ e $t = 3$ é exibido na Figura 2.5:

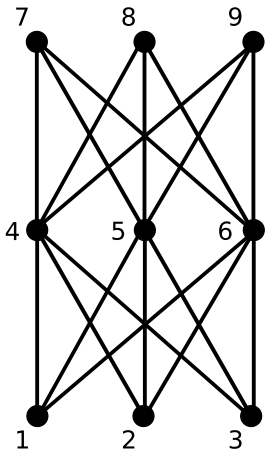


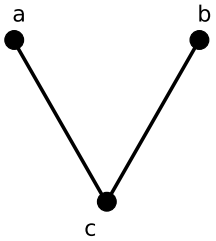
Figura 2.5: Poset Hierárquico.

Observação 2.7. Frequentemente, denotaremos a ordem de um poset $P = (X, \preccurlyeq)$ simplesmente por $\preccurlyeq_P$. Abusando da notação, podemos representar o conjunto X por P. Assim um elemento $a \in X$ é denotado por $a \in P$.

Definição 2.8. Sejam P e Q dois posets. Uma aplicação $f : P \to Q$ é uma *homomorfismo ordem* se para quaisquer dois elementos $a, b \in P$

$$a \preccurlyeq_P b \Rightarrow f(a) \preccurlyeq_Q f(b).$$

Exemplo 2.9. Se P é um poset com diagrama de Hasse



e Q é um poset com diagrama de Hasse

,

então

$$\begin{array}{rccc} f: & P & \to & Q \\ & a & \mapsto & 2 \\ & b & \mapsto & 2 \\ & c & \mapsto & 1 \end{array}$$

é uma homomorfismo ordem.

Observamos que uma homomorfismo ordem pode ser bijetiva sem que a sua inversa seja uma homomorfismo ordem.

Exemplo 2.10. Seja P um poset com diagrama de Hasse

e seja Q um poset com diagrama de Hasse

,

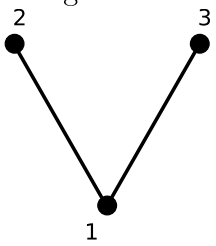
então

$$\begin{array}{rccc} g: & P & \to & Q \\ & a & \mapsto & 1 \\ & b & \mapsto & 3 \\ & c & \mapsto & 2 \end{array}$$

é uma homomorfismo ordem bijetora. Entretanto, a sua inversa g^{-1} não é uma homomorfismo ordem, pois $2 \preceq_Q 3$, mas $g^{-1}(2) = c$ e $g^{-1}(3) = b$ são incomparáveis.

Definição 2.11. Uma homomorfismo ordem é um *isomorfismo* se é bijetiva e a sua inversa é uma homomorfismo ordem. Um isomorfismo do poset sobre si mesmo é um *automorfismo*.

Exemplo 2.12. Seja P um poset dado pelo diagrama de Hasse abaixo:



Então os automorfismos poset de P são a identidade e

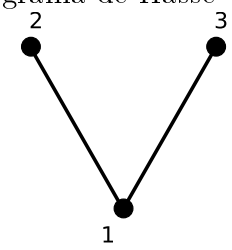
$$\begin{array}{rccc} \varphi: & P & \to & P \\ & 1 & \mapsto & 1 \\ & 2 & \mapsto & 3 \\ & 3 & \mapsto & 2. \end{array}$$

Definição 2.13. Uma bijeção ordem $f : P \to Q$ entre os posets P e Q é um *anti-isomorfismo* se para quaisquer dois elementos $a, b \in P$

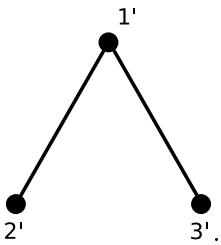
$$a \preccurlyeq_P b \Leftrightarrow f(b) \preccurlyeq_Q f(a).$$

Se o poset P é anti-isomorfo a Q, então a relação de ordem em P é invertida quando olhamos no poset Q. Mostramos isso no seguinte exemplo.

Exemplo 2.14. Seja P um poset com diagrama de Hasse



e Q um poset com diagrama de Hasse



Defina a aplicação $f : P \to Q$ por $f(i) = i'$. Assim,

$$i \preccurlyeq_P j \iff j' \preccurlyeq_Q i'.$$

Portanto a aplicação f é um anti-isomorfismo.

Definição 2.15. Chamamos de *poset oposto* o poset $\overline{P}$, definido sobre o mesmo conjunto que P, e com a ordem, $\preccurlyeq_{\overline{P}}$, dada por:

$$i \preccurlyeq_{\overline{P}} j \iff j \preccurlyeq_P i.$$

A aplicação identidade, $Id_P : P \to \overline{P}$, é um anti-isomorfismo. Mais ainda, a ordem em $\overline{P}$ é a única que faz com que a identidade, $Id_P : P \to P$, seja um anti-isomorfismo.

Proposição 2.16. *Sejam P e Q posets e seja $\varphi : P \to Q$ um isomorfismo poset, então $\varphi : \overline{P} \to \overline{Q}$ é também um isomorfismo poset.*

Demonstração. A prova segue diretamente de

$$j \preccurlyeq_{\overline{P}} i \iff i \preccurlyeq_P j \iff \varphi(i) \preccurlyeq_Q \varphi(j) \iff \varphi(j) \preccurlyeq_{\overline{Q}} \varphi(i),$$

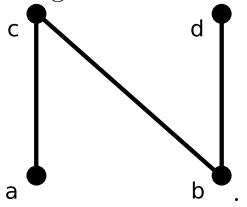
para todos $j, i \in P$. □

Definição 2.17. Um ideal (ordem) de P é um subconjunto $I \subseteq P$ com a propriedade de que se

$$u \in I \text{ e } v \preccurlyeq_P u \Rightarrow v \in I.$$

Dado $A \subseteq P$, denotamos por $\langle A \rangle_P$ o menor ideal de P contendo A, chamado *ideal de P gerado por A*. Se conhecemos os elementos do conjunto A, digamos $A = \{a, b, e\}$, então denotamos $\langle A \rangle_P$ por $\langle a, b, e \rangle_P$ em vez de $\langle \{a, b, e\} \rangle_P$.

Exemplo 2.18. Seja o poset letra-**N** com diagrama de Hasse



Podemos ver que os conjuntos $\{b\}, \{a, b\}, \{a, b, c\}$ são ideais de **N**, mas o conjunto $\{a, c\}$ não é um ideal.

Note que o ideal gerado pelos elementos $\{a, c\}$ e o ideal gerado pelo elemento c são iguais, ou seja, $\langle a, c \rangle_{\mathbf{N}} = \{a, c, b\} = \langle c \rangle_{\mathbf{N}}$.

Definição 2.19. Um elemento $a \in P$ é dito *maximal* em relação a ordem $\preccurlyeq_P$ se $a \preccurlyeq_P b$ implica em $b = a$. Ele é dito *minimal* se $b \preccurlyeq_P a$ implica em $b = a$.

Exemplo 2.20. No poset letra **N** acima os elementos c e d são elementos maximais e a e b são minimais.

Dado P um poset denotaremos por $\mathcal{I}^r(J)$ o *conjunto de todos os ideais* de cardinalidade r em P, e dado um ideal J chamaremos $\mathcal{M}(J)$ o *conjunto de elementos maximais* em J.

Proposição 2.21. *[HK08, Proposição 1.1]*

a) *Seja* $0 \leq r \leq s \leq n$ *e* $I \in \mathcal{I}^r(P)$. *Então existe* $J \in \mathcal{I}^s(P)$ *tal que* $I \subseteq J$.

b) *Seja* $0 \leq s \leq r \leq n$ *e* $I \in \mathcal{I}^r(P)$. *Então existe* $J \in \mathcal{I}^s(P)$ *tal que* $J \subseteq I$.

Demonstração. Se $s = r$, então $J = I$ em ambos os casos.

a) No caso $s = r + 1$, seja j um elemento minimal de $P \backslash I$, então $J = I \cup \{j\}$ satisfaz a condição.

b) No caso $s = r - 1$, seja j um elemento maximal de I, então $J = I \backslash \{j\}$ satisfaz a condição.

O caso geral $s = r \pm t$ é provado por indução. □

Proposição 2.22. *Sejam* P *um poset. Então, dois ideais* I *e* J *em* P *são iguais se, e somente se,* $\mathcal{M}(I)$ *e* $\mathcal{M}(J)$ *são iguais.*

Demonstração. Se $I = J$ então os seu elementos maximais também são iguais, daí $\mathcal{M}(J) = \mathcal{M}(I)$. Por outro lado, como o ideal I é gerado por $\mathcal{M}(I)$ e o mesmo acontece com o ideal J. Se $\mathcal{M}(I) = \mathcal{M}(J)$ então

$$I = \langle \mathcal{M}(I) \rangle_P = \langle \mathcal{M}(J) \rangle_P = J.$$

□

2.2 Códigos Ponderados por Ordens Parciais

Seja P um poset sobre o conjunto $[n] := \{1, 2, ..., n\}$. Sem perda de generalidade podemos assumir que o conjunto $[n]$ e as posições coordenadas dos vetores de $\mathbb{F}_q^n$ estão em bijeção, ou seja, um vetor $\mathbf{x} \in \mathbb{F}_q^n$ pode ser representado como $\mathbf{x} := x_1 x_2 \cdots x_n$. Podemos definir um peso ponderado para os vetores de $\mathbb{F}_q^n$ ponderado pela ordem $\preccurlyeq_P$.

Definição 2.23. O *P-peso* de um elemento $\mathbf{x} \in \mathbb{F}_q^n$ é a cardinalidade do ideal de P gerado pelo suporte de $\mathbf{x}$,

$$w_P(\mathbf{x}) = |\langle supp(\mathbf{x})\rangle_P|.$$

De modo similar ao que ocorre com o peso de Hamming, o P-peso também determina uma distância em $\mathbb{F}_q^n$, chamada *P-distância*:

$$d_P(\mathbf{x},\mathbf{y}) := w_P(\mathbf{x}-\mathbf{y}).$$

Teorema 2.24 (Métrica poset)**.** *[BGL95, Lema 1.1] Se P é um poset sobre $[n]$, então a P-distância $d_P(\mathbf{x},\mathbf{y}) := w_P(\mathbf{x}-\mathbf{y})$ é uma métrica em F_q^n.*

Demonstração. A função cardinalidade é não-negativa para conjuntos não-vazios:

$$w_P(\mathbf{x}) = 0 \iff |\langle supp(\mathbf{x})\rangle| = 0 \iff supp(\mathbf{x}) = \emptyset \iff \mathbf{x} = \mathbf{0},$$

assim a P-distância é definida positiva. Ela é simétrica, pois o suporte do vetor $\mathbf{x}-\mathbf{y}$ é igual ao suporte do vetor $\mathbf{y}-\mathbf{x}$. Para provar a desigualdade triangular é suficiente mostrar a validade da desigualdade triangular para o P-peso:

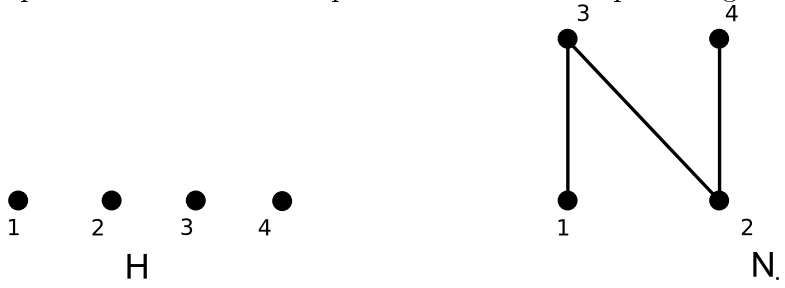
$$w_P(\mathbf{x}+\mathbf{y}) \leq w_P(\mathbf{x}) + w_P(\mathbf{y}), \forall \mathbf{x},\mathbf{y} \in \mathbb{F}_q^n,$$

pois $d_P(\mathbf{x},\mathbf{y}) = w_P(\mathbf{x}-\mathbf{y}) \leq w_P(\mathbf{x}-\mathbf{z}) + w_P(\mathbf{z}-\mathbf{y}) = d_P(\mathbf{x},\mathbf{z}) + d_P(\mathbf{z},\mathbf{y})$. Vamos provar então a desigualdade triangular para os P-pesos. Como $supp(\mathbf{x}+\mathbf{y}) \subseteq supp(\mathbf{x}) \cup supp(\mathbf{y})$ e a união de dois ideais é também um ideal, temos

$$\begin{aligned} w_P(\mathbf{x}+\mathbf{y}) &\leq |\langle supp(\mathbf{x})\rangle_P \cup \langle supp(\mathbf{y})\rangle_P| \\ &\leq |\langle supp(\mathbf{x})\rangle_P| + |\langle supp(\mathbf{y})\rangle_P| \\ &= w_P(\mathbf{x}) + w_P(\mathbf{y}). \end{aligned}$$

□

Exemplo 2.25. Seja o poset antilinear **H** e o poset letra-**N** dados pelo diagrama abaixo



Para o vetor $\mathbf{x} = 0110 \in \mathbb{F}_2^4$, obtemos o $\mathbf{H}$-peso é igual a

$$w_{\mathbf{H}}(\mathbf{x}) = |\langle supp(\mathbf{x})\rangle_{\mathbf{H}}| = |supp(\mathbf{x})| = |\{2,3\}| = 2$$

e o $\mathbf{N}$-peso igual a

$$w_{\mathbf{N}}(\mathbf{x}) = |\langle supp(\mathbf{x})\rangle_{\mathbf{N}}| = |\langle 2,3\rangle| = |\{1,2,3\}| = 3.$$

No poset antilinear $\mathbf{H}$, $\mathbf{H}$-peso e a $\mathbf{H}$-distância são, respectivamente, o peso e a distância de Hamming da teoria clássica de códigos. Por esse motivo chamaremos o poset antilinear de *poset Hamming* e o denotamos por $\mathbf{H}$.

Chamamos a métrica d_P em $\mathbb{F}_q^n$ de *métrica poset* ou *P-métrica*. O par ordenado $\left(\mathbb{F}_q^n, d_P\right)$ é chamado de *espaço poset* ou *P-espaço*. Um subconjunto C do espaço métrico $\left(\mathbb{F}_q^n, d_P\right)$ é chamado *código poset*. Se a métrica corresponde ao poset P, então dizemos que C é um *P-código*. Se $C \subseteq \mathbb{F}_q^n$ é um subespaço de dimensão k, então C é um $[n,k]_q$ *P-código linear*.

Sejam $\mathbf{x} \in \mathbb{F}_q^n$ e r um inteiro não negativo. A *P-bola* com centro em $\mathbf{x}$ e raio r é o conjunto

$$B_P(\mathbf{x}, r) = \left\{\mathbf{y} \in \mathbb{F}_q^n; d_P(\mathbf{x}, \mathbf{y}) \leq r\right\}$$

de todos os vetores em $\mathbb{F}_q^n$ onde a P-distância para $\mathbf{x}$ é no máximo igual a r. A *P-esfera* com centro em $\mathbf{x}$ e raio r é o conjunto

$$S_P(\mathbf{x}, r) = \left\{\mathbf{y} \in \mathbb{F}_q^n; d_P(\mathbf{x}, \mathbf{y}) = r\right\}$$

de todos os vetores em $\mathbb{F}_q^n$ onde a P-distância para $\mathbf{x}$ é igual a r. O número de vetores na P-esfera de centro no vetor nulo e raio i é [BGL95]

$$\begin{cases} 1 & \text{se } i = 0, \\ \sum_{j=i}^{i} (q-1)^j q^{i-j} \Omega_j(i) & \text{se } i > 0, \end{cases}$$

onde $\Omega_j(i)$ é o número de ideais de P com cardinalidade i tendo exatamente j elementos maximais. Como $d_P(\mathbf{x}, \mathbf{y}) = d_P(0, \mathbf{y} - \mathbf{x})$, segue que o número de vetores na P-bola de raio r não depende do seu centro e é [BGL95] igual a

$$1 + \sum_{i=1}^{r} \sum_{j=1}^{i} (q-1)^j q^{i-j} \Omega_j(i).$$

Em particular, se $q = 2$ o número de vetores na P-bola de raio r é igual a

$$1 + \sum_{i=1}^{r} \sum_{j=1}^{i} 2^{i-j} \Omega_j (i) .$$

Definição 2.26. Seja P um poset sobre $[n]$. Um código $C \subseteq \mathbb{F}_q^n$ é chamado *r-corretor de erros P-perfeito* se as P-bolas de de raio r centradas nas palavras do código são disjuntas e a união destas é todo o espaço $\mathbb{F}_q^n$.

Um dos méritos dos códigos poset é que existem muitos destes que são perfeitos, mas não são perfeitos no sentido clássico.

Exemplo 2.27. Seja $\mathbf{L}$ o poset linear sobre $[n]$. Seja $C = \{00\cdots0, 11\cdots1\} \subseteq \mathbb{F}_2^n$ então C é um código $(n-1)$-corretor de erros $\mathbf{L}$-perfeito.

De fato, as $\mathbf{L}$-bolas de raio $n-1$ e centro na origem (palavra-código nula) e na palavra-código $11\cdots1$ são disjuntas. Isso ocorre pois se $\mathbf{x} \in B_{\mathbf{L}} (00\cdots0, n-1)$ então

$$d_{\mathbf{L}} (00\cdots0, \mathbf{x}) = w_{\mathbf{L}} (\mathbf{x}) \leq n-1. \tag{2.1}$$

Assim, se $\mathbf{x} = x_1 x_2 \cdots x_{n-1} x_n$ devemos ter $x_n = 0$, senão $w_{\mathbf{L}} (\mathbf{x}) = n$, o que é uma contradição com a equação (2.1).

Se, por outro lado, $\mathbf{x} \in B_{\mathbf{L}} (11\cdots1, n-1)$ então

$$d_{\mathbf{L}} (11\cdots1, \mathbf{x}) = w_{\mathbf{L}} (\mathbf{x} - 11\cdots1) = w_{\mathbf{L}} (y_1 y_2 \cdots y_{n-1} 1) = n > n-1,$$

onde $y_i = x_i - 1$ para , $i = 1, \cdots, n-1$, contradizendo $\mathbf{x}$ pertencer a $\mathbf{L}$-bola de centro $11\cdots1$.

Para mostrar que a união dessas bolas é o espaço todo, observamos que a $\mathbf{L}$-bola $B_{\mathbf{L}} (00\cdots0, n-1)$ tem 2^{n-1} elementos, pois se $\mathbf{x} \in B_{\mathbf{L}} (00\cdots0, n-1)$ devemos ter $x_n = 0$. Como as $\mathbf{L}$-bolas tem o mesmo número de elementos, temos

$$|B_{\mathbf{L}} (00\cdots0, n-1)| + |B_{\mathbf{L}} (11\cdots1, n-1)| = 2^{n-1} + 2^{n-1} = 2^n = |\mathbb{F}_2^n|$$

Tornando o código C um $(n-1)$-corretor de erros $\mathbf{L}$-perfeito.

Mas, na teoria clássica de códigos, C corrige até $\left\lfloor \frac{n-1}{2} \right\rfloor \leq n-1$ erros e não é perfeito quando n é par.

Analogamente, podemos obter que o $\mathbf{L}$-código

$$C = \{00\cdots0, 11\cdots1, 22\cdots2, \cdots, (q-1, q-1, \cdots, q-1)\} \subseteq \mathbb{F}_q^n$$

é um $(n-1)$-corretor de erros **L**-perfeito.

2.3 Isometrias do Espaço Poset

Definição 2.28. Uma isometria entre dois espaços métricos, (M, d_M) e (N, d_N), é uma aplicação $T : M \to N$ tal que $d_N(T(\mathbf{x}), T(\mathbf{y})) = d_M(\mathbf{x}, \mathbf{y})$ para todos $\mathbf{x}, \mathbf{y} \in M$.

As isometrias do espaço de Rosenboom-Tsfasman $\left(\mathbb{F}_q^n, d_{RT}\right)$ são classificadas em [PFSA09]. As isometrias lineares do espaço $\left(\mathbb{F}_q^n, d_P\right)$ são classificadas em [PFKH08]. Vamos descrever algumas Proposições que os autores fizeram nesse último.

Definição 2.29. Uma *isometria linear* T do espaço métrico $\left(\mathbb{F}_q^n, d_P\right)$ é uma transformação linear $T : \mathbb{F}_q^n \to \mathbb{F}_q^n$ que preserva a P-métrica,

$$d_P(T(\mathbf{x}), T(\mathbf{y})) = d_P(\mathbf{x}, \mathbf{y}),$$

para todo $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$. Equivalentemente, uma transformação linear T é uma isometria se $w_P(T(\mathbf{x})) = w_P(\mathbf{x})$ para todo $\mathbf{x} \in \mathbb{F}_q^n$. Uma isometria linear de $\left(\mathbb{F}_q^n, d_P\right)$ é dita ser uma *P-isometria*.

A partir da Proposição 1.7 segue o seguinte Teorema:

Teorema 2.30. *Seja P um poset sobre $[n]$. O conjunto de todas as isometrias lineares do espaço $\left(\mathbb{F}_q^n, d_P\right)$ é um grupo.*

Teorema 2.31. *[PFKH08, Teorema 1.1] Sejam P um poset sobre $[n]$, $\{\mathbf{e}_1, \mathbf{e}_2, \cdots, \mathbf{e}_n\}$ a base canônica de $\mathbb{F}_q^n$ e T uma P-isometria. Então a aplicação $\phi_T : P \to P$ dada por*

$$\phi_T(i) = \max \langle supp(T(\mathbf{e}_i)) \rangle_P$$

é um automorfismo de P.

Uma descrição das P-isometrias é dada no seguinte Teorema:

Teorema 2.32. *[PFKH08, Teorema 1.2] Sejam P um poset sobre $[n]$ e $\{\mathbf{e}_1, \mathbf{e}_2, \cdots, \mathbf{e}_n\}$ a base canônica de $\mathbb{F}_q^n$. Então T é uma P-isometria se, e somente se,*

$$T(\mathbf{e}_j) = \sum_{i \preccurlyeq_P j} x_{ij} \mathbf{e}_{\phi_T(i)},$$

onde $\phi_T : P \to P$ é um automorfismo associado com T como no Teorema 2.31 e x_{ij} são constantes com $x_{jj} \neq 0$ para todo $j \in [n]$.

Corolário 2.33. *[PFKH08, Corolário 1.1] Seja P um poset sobre $[n]$. Dado T uma isometria linear de $\left(\mathbb{F}_q^n, d_P\right)$ existe um ordenação $\beta = \{\mathbf{e}_{i_1}, \mathbf{e}_{i_2}, \cdots, \mathbf{e}_{i_n}\}$ da base canônica tal que $[T]_{\beta,\beta}$ é dada por um produto $\mathbf{A} \cdot \mathbf{U}$ onde $\mathbf{A}$ é uma matriz triangular superior e $\mathbf{U}$ é uma matriz de permutação correspondente ao automorfismo induzido por T.*

Seja $\mathbb{M}_n(\mathbb{F}_q)$ o conjunto de todas as matrizes $n \times n$ sobre $\mathbb{F}_q$, consideramos

$$G_P := \{(a_{ij}) \in \mathbb{M}_n(\mathbb{F}_q) : a_{ij} = 0 \,\text{se}\, i \not\preccurlyeq_P j \,\text{e}\, a_{ii} \neq 0\}.$$

Corolário 2.34. *[PFKH08, Corolário 1.3] Seja P um poset sobre $[n]$. O grupo de isometrias de $\left(\mathbb{F}_q^n, d_P\right)$ é isomorfo ao produto semi-direto $G_P \rtimes Aut(P)$, onde $Aut(P)$ é o grupo de automorfismos de P.*

Exemplo 2.35. Seja $\mathbf{L}$ o poset linear sobre $[n]$. Seja T uma isometria linear em $\left(\mathbb{F}_q^n, d_P\right)$. Pelo Teorema 2.31, o automorfismo ϕ_T de $\mathbf{L}$ induzido por T preserva ordem e, portanto, $\phi_T(i) = i$. Usando o Teorema 2.32, temos

$$T(\mathbf{e}_i) = \sum_{j \preccurlyeq_P i} x_{ij}\mathbf{e}_i$$

onde $x_{ii} \neq 0$. Assim T é representado por uma matriz $n \times n$ diagonal superior com diagonal não nula. Mais ainda, pelo Corolário 2.33, existe uma base ordenada β de $\mathbb{F}_q^n$ na qual a isometria linear T pode ser representada pelo produto $\mathbf{A} \cdot \mathbf{U}$ de matrizes $n \times n$, onde $\mathbf{U}$ é uma matriz monomial que age mudando as coordenadas dos subespaços com suportes isomorfos e $\mathbf{A}$ é uma matriz $n \times n$ diagonal superior com elementos não nulos na diagonal.

Definição 2.36. Um P-código $C \subseteq \mathbb{F}_q^n$ e um Q-código $C' \subseteq F_q^n$ são *equivalentes* quando existe uma isometria linear $T : \left(\mathbb{F}_q^n, d_Q\right) \to \left(\mathbb{F}_q^n, d_P\right)$ tal que $T(C) = C'$.

Sejam P e Q posets isomorfos. Considere φ esse isomorfismo, então a transformação linear $T_\varphi : \left(\mathbb{F}_q^n, d_Q\right) \to \left(\mathbb{F}_q^n, d_P\right)$ definida por

$$T_\varphi(\mathbf{x}) = \sum_{i=1}^{n} x_i \mathbf{e}_{\varphi(i)}$$

é uma isometria linear. De fato, como $\varphi : P \to Q$ é um isomorfismo

$$\langle supp(\mathbf{x})\rangle_P = \langle i_1, i_2, \cdots, i_s\rangle_P = \langle \varphi(i_1), \varphi(i_2), \cdots, \varphi(i_s)\rangle_Q = \langle supp(T_\varphi(\mathbf{x}))\rangle_Q.$$

Assim,

$$w_P(\mathbf{x}) = |\langle supp(\mathbf{x})\rangle_P| = \left|\langle supp(T(\mathbf{x}))\rangle_Q\right| = w_Q(T(\mathbf{x}))$$

e, portanto,

$$d_P(\mathbf{x},\mathbf{y}) = d_Q(T(\mathbf{x}), T(\mathbf{y})).$$

Chamaremos a transformação linear T_φ de *transformação induzida* por φ.

Apresentamos agora um primeiro resultado relacionando códigos e seus duais:

Proposição 2.37. *Seja $\varphi : P \to Q$ um isomorfismo. Se C é um Q-código então $C' = Im(T_\varphi)$ é um P-código equivalente a C e o $\overline{Q}$-código $C^\perp$, conforme introduzido na página 12, é equivalente ao $\overline{P}$-código $(C')^\perp$.*

Demonstração. De fato, para $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$

$$T_\varphi(\mathbf{x}) = \sum_{i=1}^{n} x_i \mathbf{e}_{\varphi(i)}$$

e

$$T_\varphi(\mathbf{y}) = \sum_{i=1}^{n} y_j \mathbf{e}_{\varphi(j)}.$$

Assim

$$T_\varphi(\mathbf{x}) \centerdot T_\varphi(\mathbf{y}) = \sum_{i=1}^{n}\sum_{j=1}^{n} x_i y_j \mathbf{e}_{\varphi(i)} \centerdot \mathbf{e}_{\varphi(j)} = \sum_{i=1}^{n}\sum_{j=1}^{n} x_i y_j \delta_{\varphi(i)\varphi(j)},$$

e como $\varphi(i) = \varphi(j)$ se, e somente se, $i = j$, temos

$$T_\varphi(\mathbf{x}) \centerdot T_\varphi(\mathbf{y}) = \sum_{i=1}^{n}\sum_{j=1}^{n} x_i y_j \delta_{ij} = \mathbf{x} \centerdot \mathbf{y}.$$

Segue que $T_\varphi\left(C^\perp\right) = T_\varphi(C)^\perp = (C')^\perp$. Mas, pela Proposição 2.16 $\overline{\varphi(P)} = \overline{Q}$. Portanto, o $\overline{Q}$-código $C^\perp$ é isométrico (por T_φ) ao $\overline{P}$-código $(C')^\perp$. □

Corolário 2.38. *Se dois P-códigos C e C' são equivalentes por uma transformação induzida então os $\overline{P}$-códigos $C^\perp$ e $(C')^\perp$ são equivalentes por essa mesma transformação.*

2.4 P-Pesos Generalizados

Aplicando os conceitos de Wei, ao caso de P-códigos, definimos a noção de P-peso generalizado.

Definição 2.39. Seja $D \subseteq \mathbb{F}_q^n$ um subespaço. O *P-peso generalizado de D* é a cardinalidade

$$w_P(D) := |\langle suppD \rangle_P|$$

do menor ideal de P que contém o suporte de D, lembrando que $suppD = \bigcup_{\mathbf{x}\in D} supp(\mathbf{x})$.

Considerando C um P-código linear, podemos definir o *r-ésimo P-peso mínimo generalizado* como o menor P-peso

$$d_r^{(P)}(C) := min\{w_P(D) : D \subseteq C, \dim D = r\}$$

dos subespaços de C com dimensão r. Se C é um $[n,k]_q$ P-código então a sequência

$$\left\{d_1^{(P)}(C), d_2^{(P)}(C), \ldots, d_k^{(P)}(C)\right\}$$

é chamada *hierarquia de P-pesos* de C.

Com estas definições podemos generalizar alguns resultados, obtidos por Wei, sobre a hierarquia apresentados na Seção 1.2.

Teorema 2.40 ([PLB08] Monotonicidade)**.** *Para um $[n,k]_q$ P-código linear C com $k > 0$, a hierarquia de P-pesos é uma sequência crescente:*

$$1 \leq d_1^{(P)}(C) < d_2^{(P)}(C) < \cdots < d_k^{(P)}(C) \leq n.$$

Demonstração. Como um subcódigo de dimensão r contém um subcódigo de dimensão $r-1$, temos $d_{r-1}^{(P)}(C) \leq d_r^{(P)}(C)$. Seja D um subcódigo tal que $d_r(C) = w(D)$ e $\dim D = r$. Considerando $i \in \mathcal{M}(\langle suppD\rangle)$. Considere $D_i := \{\mathbf{x} \in D : x_i = 0\}$, então $\dim D_i = r-1$ e $d_{r-1}^{(P)}(C) \leq |\langle suppD_i\rangle_P| \leq |\langle suppD\rangle_P| - 1 = d_r^{(P)}(C) - 1$. □

Corolário 2.41 (Limitante de Singleton Generalizado)**.** *[PLB08] Para um $[n,k]_q$ P-código linear C, temos*

$$r \leq d_r^{(P)}(C) \leq n - k + r.$$

Demonstração. Basta observar que $d_k^{(P)}(C) \leq n$ e $d_{r-1}^{(P)}(C) + 1 \leq d_r^{(P)}(C)$. □

2.5 Refinamento de um Poset

Definição 2.42. Sejam P e Q posets sobre o mesmo conjunto $[n]$ tais que se $x \preccurlyeq_Q y$ então $x \preccurlyeq_P y$. Então dizemos que P é um *refinamento* de Q e denotamos por $Q \subseteq P$.

Exemplo 2.43. Sejam $\mathbf{N}$ e Q os posets com diagramas de Hasse como mostrados na Figura 2.6:

Então $\mathbf{N}$ é um refinamento de Q. De fato, $\mathbf{N}$ contém todas as comparações de Q mais uma comparação, $2 \preccurlyeq_{\mathbf{N}} 4$, que não está em Q.

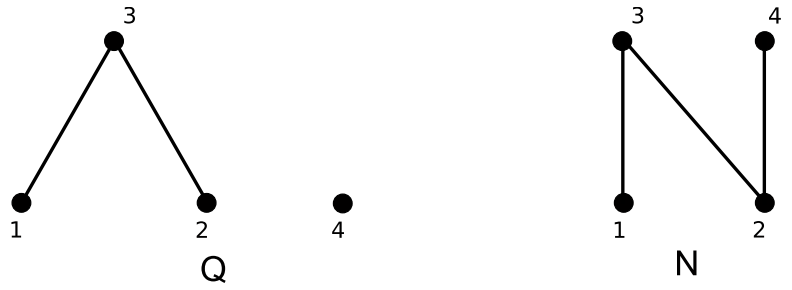


Figura 2.6: Posets Q e **N**, respectivamente.

Proposição 2.44. *Sejam P, Q posets com $Q \subseteq P$. Seja C um código linear com* $\dim(C) = k$. *Então*

$$d_r^{(Q)}(C) \leq d_r^{(P)}(C)$$

para $r = 1, \cdots, k$.

Demonstração. Seja D um subespaço de C, considere $\langle suppD \rangle_Q$ e $\langle suppD \rangle_P$ os ideais gerados por $suppD$ segundo as ordens Q e P, respectivamente. Se $x \in \langle suppD \rangle_Q$, então $x \preccurlyeq_Q y_0$ para algum $y_0 \in suppD$. Como P é um refinamento de Q temos $x \preccurlyeq_P y_0$. Logo, $\langle suppD \rangle_Q \subseteq \langle suppD \rangle_P$. Assim,

$$\left| \langle suppD \rangle_Q \right| \leq \left| \langle suppD \rangle_P \right|.$$

Considere agora D_0 o subespaço de C com $\dim(D_0) = r$ tal que $d_r^{(P)}(C) = |\langle suppD_0 \rangle_P|$. Juntando isto com a conclusão anterior temos,

$$d_r^{(Q)}(C) \leq \left| \langle suppD_0 \rangle_Q \right| \leq |\langle suppD_0 \rangle_P| = d_r^{(P)}(C).$$

□

Corolário 2.45. *Sejam P um poset e C um código linear com* $\dim(C) = k$. *Então*

$$d_r^{(\mathbf{H})}(C) \leq d_r^{(P)}(C),$$

para $r = 1, \cdots, k$. Onde $d_r^{(\mathbf{H})}(C)$ indica o r-peso generalizado de Hamming.

Demonstração. Seja H o poset Hamming então $\mathbf{H} \subseteq P$ para todo poset P. □

2.6 Códigos P-MDS

Nesta seção, introduziremos o conceito de códigos MDS, ou separável por distância máxima, para códigos poset e descreveremos algumas propriedades desses tipos de códigos. Sabemos que o limitante de Singleton é válido para códigos poset, assim,

Definição 2.46. Um código C é chamado *código MDS*, ou separável por distância máxima, quando $d_{\mathbf{H}}(C)$ atinge o limitante de Singleton.

Wei em [Wei91], generalizou o conceito de códigos MDS. Um código C é chamado de *código r-MDS* se $d_r^{(\mathbf{H})}(C) = n - k + r$. Dougherty e Skriganov em [DS02b], introduziram essa noção em espaços de Rosenbloom-Tsfasman. Podemos ainda generalizar este conceito para um código poset.

Definição 2.47. Um $[n,k]_q$ P-código C é chamado *código (P,r)-MDS* se

$$d_r^{(P)}(C) = n - k + r.$$

A partir desta definição e do limitante de Singleton generalizado obtemos a seguinte Proposição.

Proposição 2.48. *Se para algum r um código é (P,r)-MDS então é também um código (P,s)-MDS para todo $s \geq r$.*

Demonstração. Considere $k = \dim C$. Se $s = r$ então não temos nada a fazer. Se $s = r+1$ então $d_s^{(P)}(C) > d_r^{(P)}(C) = n - k + r$ o que implica que $d_s^{(P)}(C) \geq n - k + r + 1$. Usando o limitante de Singleton temos $d_s^{(P)}(C) = n-k+s$. Fazendo o mesmo argumento recursivamente obtemos o resultado esperado. □

A Proposição a seguir relaciona os conceitos de refinamento e de códigos (P,r)-MDS.

Proposição 2.49. *Sejam P e Q posets sobre $[n]$ tal que $Q \subseteq P$. Seja C um subespaço de $\mathbb{F}_q^n$. Se C é um código (Q,r)-MDS, então C é (P,r)-MDS.*

Demonstração. Seja $k = \dim C$. Pela Proposição 2.44, $d_r^{(P)}(C) \geq d_r^{(Q)}(C) = n - k + r$. Agora use o limitante de Singleton. □

Corolário 2.50. *Sejam P um poset sobre $[n]$ e C um subespaço de $\mathbb{F}_q^n$. Se C é um código MDS, então C é (P,r)-MDS.*

Demonstração. Seja $\mathbf{H}$ o poset anticadeia então $\mathbf{H} \subseteq P$ para todo poset P. □

Teorema 2.51. *[HK08, Teorema 3.12] Seja P um poset sobre $[n]$ e $\overline{P}$ o seu poset dual. Um código C é $(P,1)$-MDS se, e somente se, $C^{\perp}$ é $\left(\overline{P},1\right)$-MDS.*

Na Seção 5.2, apresentamos um contra-exemplo para o Teorema 2.51 quando um código é (P,r)-MDS para $r > 1$.

Teorema 2.52. *[HK08, Teorema 4.6] Para todo código linear C sobre $\mathbb{F}_q^n$, existe um poset P para o qual C é $(P,1)$-MDS.*

Corolário 2.53. *Para todo código linear C sobre $\mathbb{F}_q^n$, considere $r = 1, \cdots, \dim(C)$ então, existe um poset P para o qual C é (P,r)-MDS.*

Demonstração. Usando o Teorema 2.52, C é um $(P,1)$-MDS. Assim, pela Proposição 2.48 C é um (P,r)-MDS para todo $r \geq 1$. □

Capítulo 3

Multiconjuntos

Seja um código linear C. Naturalmente definimos um código linear fornecendo uma matriz geradora $\mathbf{G}$. As linhas de $\mathbf{G}$ formam uma base para C, e por isso elas são muito estudadas. Muitos trabalhos consideram as colunas interessantes. Isto dá origem aos multiconjuntos e as multifunções.

Os multiconjuntos estão relacionados com os códigos e as multifunções estão relacionadas com os pesos. A hierarquia de pesos é facilmente reconhecida nesta representação [HKY92, TV95, Lee04].

Outros termos para multiconjuntos, incluem multiconjuntos projetivos [DS98, Sch04] e os sistemas projetivos [TVN07, TV95, Lee04].

Um grande avanço dos multiconjuntos é que eles não dependem do sistema de coordenadas. Códigos, por outro lado, dependem fortemente do sistema de coordenadas, pois as coordenadas determinam os pesos, enquanto que as multifunções são determinadas por incidência.

Na seção 3.1, introduzimos algumas definições básicas de multiconjuntos e apresentamos sua relação com códigos. Na seção 3.2, apresentamos o levantamento de um multiconjunto e na seção 3.3, definimos e exploramos os submulticonjuntos, generalizando para o contexto de P-espaços os resultados apresentados em [DS98] para o caso particular da métrica de Hamming.

3.1 Multiconjuntos

Apresentamos aqui algumas definições básicas necessárias para este capítulo.

Definição 3.1. Um *multiconjunto* sobre um conjunto S é uma coleção $\mathcal{L}$ não ordenada de elementos de S, não necessariamente distintos. A *multiplicidade* de um multiconjunto $\mathcal{L}$ é

uma aplicação

$$\gamma : S \to \mathbb{N},$$

que associa para cada elemento $s \in S$ o número $\gamma(s)$ de ocorrências de s em $\mathcal{L}$.

Estamos interessados em multiconjuntos constituídos de vetores ou subespaços vetoriais de um dado espaço vetorial. Frequentemente vamos identificar a multiplicidade γ com a coleção $\mathcal{L}$, nos referindo a γ como um multiconjunto. Exemplificamos abaixo:

Exemplo 3.2. Seja $C \subseteq \mathbb{F}_2^4$ o $[4,2]_2$-código com matriz geradora:

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

As colunas de $\mathbf{G}$ formam um multiconjunto $\gamma = m_{\mathbf{G}} = \{10, 11, 10, 01\}$ sobre $\mathbb{F}_2^2$. A multiplicidade $m_{\mathbf{G}} : \mathbb{F}_2^2 \to \mathbb{N}$ é:

$$m_{\mathbf{G}}(\mathbf{s}) = \begin{cases} 2 & se \quad \mathbf{s} = 10, \\ 1 & se \quad \mathbf{s} = 11 \text{ ou } 01, \\ 0 & se \quad \mathbf{s} = 00. \end{cases}$$

Definição 3.3. Dois multiconjuntos γ_1 e γ_2 são *equivalentes* se existe uma bijeção $\sigma : S_1 \to S_2$ tal que $\gamma_2 = \gamma_1 \circ \sigma$.

Um código é dito *degenerado* se existe uma matriz geradora com uma coluna nula. Caso contrário ele é dito *não-degenerado*.

Exemplo 3.4. O código com matriz geradora

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

é degenerado, pois a quarta coluna é nula. Enquanto um código com matriz geradora

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

é não-degenerado.

Observação 3.5. O conceito de degeneração não depende de uma matriz geradora do código. Existem outras formas equivalentes para definir um código degenerado:

- $C \subseteq \mathbb{F}_q^n$ é não-degenerado se, e somente se, a distância mínima de Hamming do código dual $C^\perp$ é maior ou igual a 2.

- $C \subseteq \mathbb{F}_q^n$ é não-degenerado se, e somente se, a base canônica $\{\mathbf{e}_1, \mathbf{e}_2, \cdots, \mathbf{e}_n\}$ de $\mathbb{F}_q^n$ não intersecta o código dual $C^\perp$.

- $C \subseteq \mathbb{F}_q^n$ é degenerado se C está contido no núcleo de alguma aplicação coordenada

$$\begin{aligned} x_i : \mathbb{F}_q^n &\to \mathbb{F}_q \\ \mathbf{x} &\mapsto x_i. \end{aligned}$$

Vamos agora construir um multiconjunto a partir de um código linear não-degenerado com a métrica de Hamming:

Seja C um $[n,k]_q$ **H**-código não-degenerado e considere **G** uma matriz geradora para esse código. Essa matriz induz uma transformação linear injetora

$$\begin{aligned} \phi : \mathbb{F}_q^k &\to \mathbb{F}_q^n \\ \mathbf{v} &\mapsto \mathbf{v} \centerdot \mathbf{G} = (\mathbf{v} \centerdot \mathbf{g}_1, \mathbf{v} \centerdot \mathbf{g}_2, \ldots, \mathbf{v} \centerdot \mathbf{g}_n) \end{aligned} \tag{3.1}$$

onde $\mathbf{g}_i$ é a i-ésima coluna de **G** e a imagem sob essa transformação é o código C.

As colunas $\mathbf{g}_i$ são elementos de $\mathbb{F}_q^k$. Esses vetores não são necessariamente distintos, de modo que formam um multiconjunto sobre $\mathbb{F}_q^k$ com multiplicidade

$$\begin{aligned} m_{\mathbf{G}} : \mathbb{F}_q^k &\to \{0, 1, 2, ..., n\} \\ \mathbf{v} &\mapsto m_{\mathbf{G}}(\mathbf{v}), \end{aligned}$$

onde $m_{\mathbf{G}}(\mathbf{v})$ é o número de vezes que o vetor $\mathbf{v}$ aparece como uma coluna de **G**.

Dada outra matriz geradora $\mathbf{G}'$ para o código C, então existe uma matriz **A** quadrada de ordem k e posto completo tal que

$$\mathbf{G}' = \mathbf{A} \centerdot \mathbf{G}.$$

O automorfismo dado por $\sigma : \mathbf{v} \mapsto \mathbf{A} \centerdot \mathbf{v}$ substitui cada coluna $\mathbf{g}_i$ por $\mathbf{A} \centerdot \mathbf{g}_i$ e cada vetor $\mathbf{v}$ por $\mathbf{A} \centerdot \mathbf{v}$. Assim, $m_{\mathbf{G}'}(\mathbf{A} \centerdot \mathbf{v}) = m_{\mathbf{G}}(\mathbf{v}), \forall \mathbf{v} \in \mathbb{F}_q^k$, e os multiconjuntos $m_{\mathbf{G}}$ e $m_{\mathbf{G}'}$ são equivalentes pelo automorfismo σ. Em outras palavras, a partir de equivalentes multiconjuntos obtemos diferentes matrizes, mas elas identificam o mesmo código. Com isto em mente vamos referenciar o multiconjunto $m_C := m_{\mathbf{G}}$ em $\mathbb{F}_q^k$ com uma matriz geradora **G** qualquer.

Definição 3.6. Dado C um código não-degenerado, o multiconjunto m_C é chamado de *multiconjunto induzido* pelo código C.

Exemplo 3.7. Seja C o $[7,4]_2$ **H**-código de Hamming. Uma matriz geradora é

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

O correspondente multiconjunto m_C é formado pelos vetores

$$\{1000, 0100, 0010, 0001, 1101, 1011, 0111\}.$$

Para um subespaço (ou subconjunto) $U \subseteq \mathbb{F}_q^k$, definimos naturalmente a multiplicidade de U como

$$m_C(U) := \sum_{\mathbf{u} \in U} m_C(\mathbf{u}).$$

A seguinte Proposição foi provada inicialmente em [HKY92], mas apresentamos uma outra demonstração que vai nos ajudar a estender a Proposição para o ambiente de P-pesos.

Proposição 3.8. *[HKY92, Lema 1] Sejam $C \subseteq \mathbb{F}_q^n$ um código e w o peso de Hamming. Dado um subespaço $D \subseteq C$ de dimensão r, existe um subespaço $U \subseteq \mathbb{F}_q^k$ de codimensão r tal que*

$$m_C(U) = n - w(D).$$

Demonstração. Seja $\mathbf{G}$ uma matriz geradora do código, ela gera um isomorfismo ϕ entre C e $\mathbb{F}_q^k$, como vimos em (3.1). Assim, para o subcódigo D existe um subespaço $V \subseteq \mathbb{F}_q^k$ isomorfo a D, isto é $\phi(V) = D$. Logo, $i \in supp(D) \Leftrightarrow \exists \mathbf{v} \in V$ tal que a i-ésima coordenada de $\mathbf{v}.\mathbf{G}$ é não-nula. Mas, se $\mathbf{v}.\mathbf{G} = (y_1, \cdots, y_n)$ então $y_i = \mathbf{v}.\mathbf{g}_i$, onde $\mathbf{g}_i$ é a i-ésima coluna da matriz geradora $\mathbf{G}$, e portanto, $i \in supp(D) \Leftrightarrow \mathbf{g}_i \notin V^\perp$. Donde segue que

$$\begin{aligned} w(D) &= \left|\{\mathbf{g}_i \notin V^\perp\}\right| \\ &= n - \left|\{\mathbf{g}_i \in V^\perp\}\right| \\ &= n - \left|\{\{\text{Colunas de } \mathbf{G}\} \cap V^\perp\}\right| \\ &= n - m_C\left(V^\perp\right). \end{aligned}$$

Daí fazendo $U = V^\perp$ segue o resultado. □

Dada uma coleção $\{A_1, ..., A_t\}$ de subconjuntos de um espaço vetorial, escreveremos $[A_1, ..., A_t]$ para indicar o *gerado* pela interseção de todos os subespaços contendo $\bigcup_{i=1}^{t} A_i$.

Estenderemos agora a Proposição 3.8 para o caso poset. Primeiro notamos que dados um P-código, com matriz geradora $\mathbf{G}$, e $\mathbf{v} \in \mathbb{F}_q^k$, o P-peso de $\mathbf{v} \cdot \mathbf{G}$ é

$$\begin{aligned} w_P(\mathbf{v} \cdot \mathbf{G}) &= |\{i : \exists j \in supp(\mathbf{v} \cdot G) \text{ com } i \preceq_P j\}| \\ &= |\{i : \exists j \text{ com } i \preceq_P j, \mathbf{g}_j \not\perp \mathbf{v}\}| \\ &= n - |\{i : j \succeq_P i \Rightarrow \mathbf{g}_j \perp \mathbf{v}\}| \\ &= n - \left|\left\{i : [\{\mathbf{g}_j : j \succeq_P i\}] \subseteq \mathbf{v}^\perp\right\}\right|. \end{aligned}$$

Com isto em mente, podemos definir outro multiconjunto m_C^P em

$$\mathcal{P}\left(\mathbb{F}_q^k\right) := \left\{X \subseteq \mathbb{F}_q^k : X \text{ é um subespaço vetorial de } \mathbb{F}_q^k\right\}.$$

Dado C um $[n,k]_q$ P-código, considere $\mathbf{G}$ uma matriz geradora para C e seja $\{\mathbf{g}_i : i \in [n]\}$ o conjunto das suas colunas. O *multiconjunto induzido* pelo P-código $m_{\mathbf{G}}^P$ é a coleção dos subespaços $U_i = [\{\mathbf{g}_j : j \preceq_P i\}]$, para $i \in [n]$, dos subespaços gerados pelas colunas $\mathbf{g}_j$ com $j \preceq_P i$, e a multifunção

$$\begin{aligned} m_{\mathbf{G}}^P : \mathcal{P}\left(\mathbb{F}_q^k\right) &\to \{0,1,2,\ldots,n\} \\ V &\mapsto m_{\mathbf{G}}^P(V), \end{aligned}$$

é o número $m_{\mathbf{G}}^P(V)$ de i's tais que $U_i \subseteq V$.

Assim como no caso Hamming, duas matrizes geradoras para C, $\mathbf{G} = (\mathbf{g}_1, \mathbf{g}_2, \cdots, \mathbf{g}_n)$ e $\mathbf{G}' = (\mathbf{g}'_1, \mathbf{g}'_2, \cdots, \mathbf{g}'_n)$, definem uma matriz $\mathbf{A}$ $k \times k$ tal que $\mathbf{g}_i \cdot \mathbf{A} = \mathbf{g}'_i$. Esta matriz define uma transformação linear $A : \mathbb{F}_q^k \to \mathbb{F}_q^k$ com $A(\mathbf{g}_i) = \mathbf{g}'_i$. Esta transformação induz uma bijeção de $\mathcal{P}\left(\mathbb{F}_q^k\right)$ sobre si mesmo. Se colocarmos $U_i = [\{\mathbf{g}_j : j \preceq_P i\}]$ e $U'_i = \left[\left\{\mathbf{g}'_j : j \preceq_P i\right\}\right]$, obtemos $A(U_i) = U'_i$, tornando os multiconjuntos $m_{\mathbf{G}}^P$ e $m_{\mathbf{G}'}^P$ equivalentes. Portanto, podemos nos referir ao multiconjunto induzido pelo P-código simplesmente por m_C^P quando a matriz geradora não é relevante.

Podemos resumir esta discussão em uma definição:

Definição 3.9. O *multiconjunto induzido por um* $[n,k]_q$ *P-código* não-degenerado C é o multiconjunto sobre $\mathcal{P}\left(\mathbb{F}_q^k\right)$

$$m_C^P := \{U_1, U_2, \cdots, U_n\},$$

onde $U_i = [\{\mathbf{g}_j : j \preceq_P i\}]$.

Proposição 3.10. *Sejam C um $[n,k]_q$ P-código e $D \subseteq C$ um subcódigo de dimensão r. Então, existe um subespaço $U \subseteq F_q^k$ de codimensão r tal que*

$$w_{\overline{P}}(D) = n - m_C^P(U),$$

onde $\overline{P}$ é o poset oposto de P.

Demonstração. Seja $\mathbf{G}$ uma matriz geradora de C, com vetores coluna $\{\mathbf{g}_1, \mathbf{g}_2, \ldots, \mathbf{g}_n\}$. Seja $\phi : \mathbb{F}_q^k \to C$ o isomorfismo linear determinado por (3.1). Considere o multiconjunto

$$m_C^P := \{U_1, U_2, \ldots, U_n\}$$

com $U_i = [\{\mathbf{g}_j : j \preceq_P i\}]$. Dado um subcódigo $\phi(V) = D \subseteq C$ de dimensão r, temos que

$$\begin{aligned} w_{\overline{P}}(D) &= |\{i : \exists j \text{ com } i \preceq_{\overline{P}} j,\ \mathbf{g}_j \not\perp V\}| \\ &= n - |\{i : j \succeq_{\overline{P}} i \Rightarrow \mathbf{g}_j \perp V\}| \\ &= n - \left|\left\{i : [\{\mathbf{g}_j : j \preceq_P i\}] \subseteq V^\perp\right\}\right| \\ &= n - \left|\left\{i : U_i \subseteq V^\perp\right\}\right| \\ &= n - m_C^P\left(V^\perp\right). \end{aligned}$$

A Proposição segue considerando $U = V^\perp$. □

3.2 Levantamento

Veremos agora um modo de representar os elementos do multiconjunto m_C^P como subespaços de $\mathbb{F}_q^n$.

Seja $\beta := \{\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_n\}$ a base canônica de $\mathbb{F}_q^n$. Dado um $[n,k]_q$-código linear C existe um epimorfismo natural $\mu_C : \mathbb{F}_q^n \to \mathbb{F}_q^n / C^\perp$, definido por

$$\mu_C(\mathbf{x}) := \mathbf{x} + C^\perp.$$

Seja $\{\mathbf{g}_1, \mathbf{g}_2, \cdots \mathbf{g}_n\}$ o conjunto das colunas de uma matriz geradora para o código C. Considere a transformação linear $\eta : \mathbb{F}_q^n \to \mathbb{F}_q^k$ dada por

$$\eta(\mathbf{e}_i) = \mathbf{g}_i,$$

que é sobrejetora pois $\dim C = k$. Claramente $\eta(\mathbf{x}) = \mathbf{G} \cdot \mathbf{x}^\top$ e $\mathbf{G} \cdot \mathbf{x}^\top = 0 \iff \mathbf{x} \in C^\perp$. Utilizando o Teorema de homomorfismo para módulos, existe um isomorfismo τ

$$\begin{array}{ccc} \mathbb{F}_q^n & \xrightarrow{\eta} & \mathbb{F}_q^k \\ \mu_C \downarrow & \nearrow \tau & \\ \mathbb{F}_q^n / C^\perp & & \end{array}$$

entre $\mathbb{F}_q^n / C^\perp$ e $\mathbb{F}_q^k$.

Para cada vetor $\mathbf{x} \in \mathbb{F}_q^n$ podemos associar uma forma linear em $\mathbb{F}_q^n$, onde $\mathbf{x}(\mathbf{y}) = \mathbf{x}.\mathbf{y}$. Os

elementos de $\mathbb{F}_q^n/C^\perp$ podem ser considerados como formas lineares em C: se $\mathbf{x}+C^\perp \in \mathbb{F}_q^n/C^\perp$ e $\mathbf{c} \in C$ definimos

$$\left(\mathbf{x}+C^\perp\right)\centerdot\mathbf{c} = \mathbf{x}\centerdot\mathbf{c}.$$

Esta forma linear está bem definida, pois se $\left(\mathbf{x}+C^\perp\right) = \left(\mathbf{x}'+C^\perp\right)$ então $\mathbf{x}-\mathbf{x}' = \mathbf{y} \in C^\perp$, e $\mathbf{x}\centerdot\mathbf{c} = (\mathbf{x}'+\mathbf{y})\centerdot\mathbf{c}$. Para $\mathbf{x} = \mathbf{e}_i$ temos

$$\mu_C(\mathbf{e}_i)(\mathbf{c}) = \left(\mathbf{e}_i+C^\perp\right)\centerdot\mathbf{c} = \mathbf{e}_i\centerdot\mathbf{c} = c_i = \mathbf{g}_i\centerdot\mathbf{v},$$

onde $\mathbf{c} = \mathbf{v}\centerdot\mathbf{G}$. Deste modo, associamos a coluna $\mathbf{g}_i$ com o vetor $\mathbf{e}_i$ através da aplicação μ_C, identificando $\mathbb{F}_q^k$ com C. Assim, podemos associar ao P-código C uma coleção ordenada de subespaços

$$B_P := (V_1, V_2, \ldots V_n),$$

chamada de *conjunto de cobertura ortogonal*, onde $V_i = [\{\mathbf{e}_j : j \in \langle i\rangle_P\}]$, que determina o multiconjunto

$$m_C^P = \mu_C(B_P) := \{\mu_C(V_1), \mu_C(V_2), \ldots, \mu_C(V_n)\}$$

definido sobre $\mathcal{P}\left(\mathbb{F}_q^n/C^\perp\right) \cong \mathcal{P}\left(\mathbb{F}_q^k\right)$. Observe que $\mu_C(V_i) = [\{\mathbf{g}_j : j \in \langle i\rangle_P\}]$.

Deste modo, utilizando a Proposição 3.10, temos a seguinte definição:

Definição 3.11. Para um $[n,k]_q$ P-código C o seu *multiconjunto associado* é o multiconjunto $m_C^{\overline{P}} = \mu_C(B_{\overline{P}})$ definido sobre $\mathcal{P}\left(\mathbb{F}_q^n/C^\perp\right)$.

3.3 Submulticonjunto

Definição 3.12. Um *submulticonjunto* $\gamma' \subseteq \gamma$ é um multiconjunto(sobre o mesmo conjunto S) tal que $\gamma'(s) \leq \gamma(s)$ para todo $s \in S$.

Lema 3.13. *Sejam $C \subseteq \mathbb{F}_q^n$ um P-código e $m_C^{\overline{P}}$ o seu multiconjunto associado. Dado $J \subseteq \{1,2,...,n\}$, considere $B_J := \{V_j : j \in J\}$ com $V_j = [\{\mathbf{e}_i : i \in \langle j\rangle_{\overline{P}}\}]$, então $m_J := \mu_C(B_J)$ é um submulticonjunto de $m_C^{\overline{P}}$ e, mais ainda, todo submulticonjunto de $m_C^{\overline{P}}$ pode ser obtido dessa forma.*

Demonstração. Como $B_J \subseteq B_P$, temos $m_J \subseteq m_C^{\overline{P}}$. Assim, a partir da definição de um submulticonjunto, segue que m_J é um submulticonjunto de $m_C^{\overline{P}}$. Um submulticonjunto de

$$m_C^{\overline{P}} = \{\mu_C(V_1), \mu_C(V_2), \ldots \mu_C(V_n)\}$$

é uma coleção de subconjuntos do tipo

$$m = \{\mu_C(V_{i_1}), \mu_C(V_{i_2}), \ldots \mu_C(V_{i_s})\}.$$

Colocamos $J = \{i_1, i_2, \ldots, i_s\}$ e obtemos que $m = m_J$. □

Nota 3.14. A partir da demonstração da Proposição 3.10, obtemos que o P-peso de um subcódigo $D \subseteq C$ está relacionado com um submulticonjunto $m_J = \mu_C(B_J)$, onde

$$J = \left\{ i : \mu_C(V_i) \subseteq \left(\phi^{-1}(D)\right)^{\perp} \right\}$$

e ϕ é o isomorfismo linear entre C e $\mathbb{F}_q^k$, dado em (3.1).

Também notemos que

$$\begin{aligned} J &= \left\{ i : \mu_C(V_i) \subseteq (\phi^{-1}(D))^{\perp} \right\} \\ &= \left\{ i : [\{\mathbf{g}_j : j \in \langle i \rangle_{\overline{P}}\}] \subseteq (\phi^{-1}(D))^{\perp} \right\} \end{aligned}$$

é um ideal de $\overline{P}$. De fato, se $j \in J$ e $i \in \overline{P}$ com $i \preccurlyeq_{\overline{P}} j$ então, $\langle i \rangle_{\overline{P}} \subseteq \langle j \rangle_{\overline{P}}$. Consequentemente $V_j \subseteq V_i$ e aplicando o epimorfismo μ_C, obtemos

$$\mu_C(V_j) \subseteq \mu_C(V_i) \subseteq \left(\phi^{-1}(D)\right)^{\perp}.$$

Portanto, $i \in J$ e J é um ideal de $\overline{P}$.

Com isso podemos reescrever a Proposição 3.10 em termos de submulticonjuntos. Observamos que para a próxima Proposição definimos B_J como espaço nulo se J é vazio.

Proposição 3.15. *Sejam C um $[n,k]_q$ P-código e $D \subseteq C$ um subcódigo de dimensão r. Então, existe um ideal J de $\overline{P}$ tal que a codimensão de $[\mu_C(B_J)] \subseteq \mathbb{F}_q^k$ é r e*

$$w_{\overline{P}}(D) = n - |J| = n - |B_J|.$$

Ilustraremos as informações anteriores de levantamento e submulticonjunto com um exemplo.

Exemplo 3.16. Sejam P e $\overline{P}$ os posets ilustrados pelos diagramas de Hasse na Figura 3.1 abaixo, um oposto do outro.

Seja C um P-código com matriz geradora

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

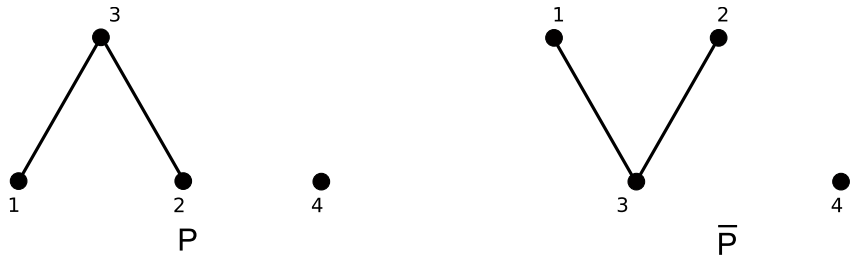


Figura 3.1: Diagrama Hasse da ordem P e a seu oposto $\overline{P}$.

e considere

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

uma matriz geradora para o $\overline{P}$-código $C^{\perp}$.

O epimorfismo $\mu_C : \mathbb{F}_2^4 \to \mathbb{F}_2^4/C^{\perp}$ e o isomorfismo entre $\mathbb{F}_2^4/C^{\perp}$ e $\mathbb{F}_2^2$ são resumidos abaixo:

$$\begin{aligned}
\mu_C(1000) &= 1000 + C^{\perp} \longleftrightarrow 10 = \text{Coluna 1 de } \mathbf{G}, \\
\mu_C(0100) &= 0100 + C^{\perp} \longleftrightarrow 11 = \text{Coluna 2 de } \mathbf{G}, \\
\mu_C(0010) &= 0010 + C^{\perp} \longleftrightarrow 10 = \text{Coluna 3 de } \mathbf{G}, \\
\mu_C(0001) &= 0001 + C^{\perp} \longleftrightarrow 01 = \text{Coluna 4 de } \mathbf{G}.
\end{aligned}$$

Note que $1000 - 0010 = 1010 \in C^{\perp}$, de modo que 1000 e 0010 representam a mesma classe em $\mathbb{F}_2^4/C^{\perp}$.

Agora

$$\begin{aligned}
V_1 &= [\{\mathbf{e}_1, \mathbf{e}_3\}], \quad V_2 = [\{\mathbf{e}_2, \mathbf{e}_3\}], \\
V_3 &= [\{\mathbf{e}_3\}] \text{ e} \qquad V_4 = [\{\mathbf{e}_4\}].
\end{aligned}$$

O multiconjunto associado é

$$\begin{aligned}
\mu_C(B_{\overline{P}}) &= \{\mu_C(V_1), \mu_C(V_2), \mu_C(V_3), \mu_C(V_4)\} \\
&= \{[\{10\}], \mathbb{F}_2^2, [\{10\}], [\{01\}]\} = m_C^{\overline{P}}
\end{aligned}$$

com hierarquia de P-pesos

$$\begin{aligned}
d_1^{(P)}(C) &= w_P(0101) = w_P([\{0101\}]) \\
&= w_P([\{01\}] \cdot \mathbf{G}) \\
&= 4 - m_C^{\overline{P}}\left([\{01\}]^{\perp}\right) \\
&= 4 - m_C^{\overline{P}}([\{10\}]) \\
&= 4 - m_J([\{10\}]) = 2,
\end{aligned}$$

com $J = \langle 1, 3\rangle_{\overline{P}} = \{1, 3\}$ e $codim([\mu_C(B_J)]) = codim([\{01\}]) = 1$, e

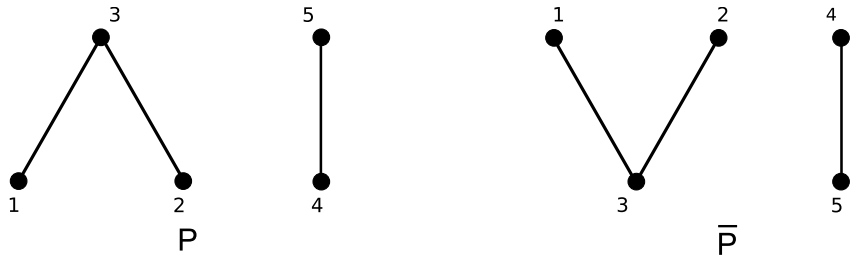


Figura 3.2: Diagrama Hasse da ordem P e a seu oposto $\overline{P}$.

$$\begin{aligned} d_2^P(C) &= w_P(C) \\ &= w_P(\mathbb{F}_2^2 \cdot \mathbf{G}) \\ &= 4 - m_C^{\overline{P}}\left((\mathbb{F}_2^2)^{\perp}\right) \\ &= 4 - m_C^{\overline{P}}([\{00\}]) \\ &= 4 - m_I([\{00\}]) = 4, \end{aligned}$$

com $I = \emptyset$ e $codim([\mu_C(B_I)]) = codim([\{00\}]) = 2$.

Vamos fazer um exemplo sobre um corpo não binário:

Exemplo 3.17. Sejam P e $\overline{P}$ os posets ilustrados pelos diagramas de Hasse na Figura 3.2, um oposto do outro.

Seja C um $[5,2]_3$ P-código com matriz geradora

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

O epimorfismo $\mu_C : \mathbb{F}_3^5 \to \mathbb{F}_3^5/C^{\perp}$ e o isomorfismo entre $\mathbb{F}_3^5/C^{\perp}$ e $\mathbb{F}_3^2$ são resumidos na tabela abaixo:

$$\begin{aligned} \mu_C(10000) &= 10000 + C^{\perp} \longleftrightarrow 11 = \text{Coluna 1 de } \mathbf{G}, \\ \mu_C(01000) &= 01000 + C^{\perp} \longleftrightarrow 20 = \text{Coluna 2 de } \mathbf{G}, \\ \mu_C(00100) &= 00100 + C^{\perp} \longleftrightarrow 02 = \text{Coluna 3 de } \mathbf{G}, \\ \mu_C(00010) &= 00010 + C^{\perp} \longleftrightarrow 01 = \text{Coluna 4 de } \mathbf{G}, \\ \mu_C(00001) &= 00001 + C^{\perp} \longleftrightarrow 20 = \text{Coluna 5 de } \mathbf{G}. \end{aligned}$$

Agora

$$\begin{aligned} &V_1 = [\{\mathbf{e}_1, \mathbf{e}_3\}], \quad V_2 = [\{\mathbf{e}_2, \mathbf{e}_3\}], \quad V_3 = [\{\mathbf{e}_3\}] \\ &V_4 = [\{\mathbf{e}_4, \mathbf{e}_5\}] \text{ e } \quad V_5 = [\{\mathbf{e}_5\}] \end{aligned}$$

O multiconjunto associado é

$$\begin{aligned}\mu_C(B_{\overline{P}}) &= \{\mu_C(V_1), \mu_C(V_2), \mu_C(V_3), \mu_C(V_4)\} \\ &= \{\mathbb{F}_3^2, \mathbb{F}_3^2, [\{02\}], \mathbb{F}_3^2, [\{20\}]\} = m_C^{\overline{P}}\end{aligned}$$

com hierarquia de P-pesos

$$\begin{aligned}d_1^{(P)}(C) &= w_P(12002) = w_P([\{12002\}]) \\ &= w_P([\{10\}] \cdot \mathbf{G}) \\ &= 5 - m_C^{\overline{P}}([\{01\}]) \\ &= 5 - m_J([\{01\}]) = 4,\end{aligned}$$

com $J = \langle 3 \rangle_{\overline{P}} = \{3\}$ e $codim([\mu_C(B_J)]) = codim([\{01\}]) = 1$, e

$$\begin{aligned}d_2^P(C) &= w_P(C) \\ &= w_P(\mathbb{F}_3^2 \cdot \mathbf{G}) \\ &= 5 - m_C^{\overline{P}}([\{00\}]) \\ &= 5 - m_I([\{00\}]) = 5,\end{aligned}$$

com $I = \emptyset$ e $codim([\mu_C(B_I)]) = codim([\{00\}]) = 2$.

A partir da Proposição 3.15 temos que explorar as propriedades do conjunto B_J relacionada com o ideal J. Lembrando que B_J é definido como $\{V_j : j \in J\}$, temos a seguinte:

Proposição 3.18. $[B_J] = [\{\mathbf{e}_j : j \in \langle J \rangle_{\overline{P}}\}]$ *para qualquer subconjunto* $J \subseteq [n]$.

Demonstração. Dado $j \in \langle J \rangle_{\overline{P}}$, o vetor da base canônica $\mathbf{e}_j \in V_j = [\{\mathbf{e}_i : i \in \langle j \rangle_{\overline{P}}\}]$, logo $\mathbf{e}_j \in [B_J]$ e

$$[\{\mathbf{e}_j : j \in \langle J \rangle_{\overline{P}}\}] \subseteq [B_J].$$

Por outro lado, seja $j \in J$ então, $\langle j \rangle_{\overline{P}} \subseteq \langle J \rangle_{\overline{P}}$, assim temos $V_i \subseteq [\{\mathbf{e}_j : j \in \langle J \rangle_{\overline{P}}\}]$ para todo $V_i \in B_J$. Logo, segue que $B_J \subseteq [\{\mathbf{e}_j : j \in \langle J \rangle_{\overline{P}}\}]$. □

Proposição 3.19. $\dim [B_J] \geq |B_J|$, *e a igualdade ocorre se, e somente se,* J *é um ideal de* $\overline{P}$.

Demonstração. De fato,

$$\dim [B_J] = \dim [\{\mathbf{e}_j : j \in \langle J \rangle_{\overline{P}}\}] = |\langle J \rangle_{\overline{P}}| \geq |J| = |B_J|.$$

A igualdade segue do seguinte fato: J é um ideal de $\overline{P}$ se, e somente se, $\langle J \rangle_{\overline{P}} = J$. □

Capítulo 4

Teorema da Dualidade para Códigos Poset

A identidade de MacWilliams para códigos lineares é uma das mais importantes identidades na teoria de códigos, assim como a sua expressão para o enumerador de pesos de Hamming do código dual de um código linear em termos do enumerador de pesos de Hamming do código. Como a métrica de Hamming é um caso especial da métrica poset, é natural tentar obter algum tipo de identidade de MacWilliams para o enumerador de pesos do código poset como em [KL03, JP03, KO05].

O estudo da hierarquia de pesos é remanescente do estudo dos enumeradores de pesos de códigos lineares. Existe uma forte relação entre as hierarquias de um código e o seu dual como vimos no Teorema 1.20, obtido por Wei.

Neste capítulo, enunciamos e provamos esta relação de dualidade entre a hierarquia de um código poset e a do seu dual, caracterizada no *Teorema 4.2, o principal resultado deste trabalho.*

Dualidade Poset

Dados um poset P, um P-código C e uma matriz geradora $\mathbf{G}$ de C podemos construir um multiconjunto $m_C^{\overline{P}}$ associado a C como na Proposição 3.10. Também para cada P-código C podemos associar parâmetros adicionais, $\left\{d_1^{(\overline{P})}\left(C^{\perp}\right), \ldots, d_{n-k}^{(\overline{P})}\left(C^{\perp}\right)\right\}$, conforme visto na seção 2.4. Vamos caracterizar estes parâmetros em termos do multiconjunto $m_C^{\overline{P}}$. Esse fato é uma generalização de [TV95, Teorema 4.1], que foi provado para o caso do poset Hamming. Com esse resultado observamos que apesar do multiconjunto associado a um código depender

da escolha de uma matriz geradora, a hierarquia de P-pesos pode ser determinada a partir do multiconjunto, independentemente da escolha da matriz geradora.

Teorema 4.1. *Sejam P um poset em $[n]$, C um $[n,k]_q$ P-código e $m_C^{\overline{P}}$ o multiconjunto em $\mathcal{P}\left(\mathbb{F}_q^n/C^\perp\right)$ associado a C. Considerando μ_C como no Capítulo 3. Então*

$$d_r^{(\overline{P})}\left(C^\perp\right) = min\left\{|B_J| : J \text{ ideal de } \overline{P} \text{ e } |B_J| - \dim\left[\mu_C\left(B_J\right)\right] \geq r\right\}. \tag{4.1}$$

Demonstração. Para D um subespaço de $C^\perp$ tal que $w_{\overline{P}}(D) = d_r^{(\overline{P})}\left(C^\perp\right)$, considere o ideal $I = \langle suppD\rangle_{\overline{P}}$. Pela Proposição 3.18, temos que $[B_I] = [\{\mathbf{e}_i : i \in I\}]$. Como

$$D = [\{\mathbf{e}_i : i \in suppD\}] \cap C^\perp \subseteq [\{\mathbf{e}_i : i \in \langle suppD\rangle_{\overline{P}}\}] \cap C^\perp = [B_I] \cap C^\perp$$

para todo $D \subseteq C$, obtemos que D está contido no núcleo de $\mu_C|_{[B_I]}$, a restrição de μ_C a $[B_I]$. Assim,

$$\dim\left[B_I\right] - \dim\left[\mu_C\left(B_I\right)\right] = \dim Ker\left(\mu_C|_{[B_J]}\right) \geq \dim D.$$

Como I é um ideal, segue que $\dim\left[B_I\right] = |B_I| = w_{\overline{P}}(D)$. Portanto, $w_{\overline{P}}(D)$ é um elemento do conjunto do lado direito da equação (4.1), e consequentemente

$$d_r^{(\overline{P})}\left(C^\perp\right) \geq \text{lado direito da equação (4.1).}$$

Para mostrar a outra desigualdade, seja J um ideal de $\overline{P}$ que atinge o mínimo no lado direito da equação (4.1). Então

$$|B_J| - \dim\left[\mu_C\left(B_J\right)\right] \geq r. \tag{4.2}$$

Se $D' := [B_J] \cap C^\perp$ é o menor subcódigo de $C^\perp$ contido em $[B_J]$ então D' é o núcleo de $\mu_C|_{[B_J]}$, logo

$$\dim\left[\mu_C\left(B_J\right)\right] = \dim\left[B_J\right] - \dim D'.$$

Como $\langle supp\left(D'\right)\rangle_{\overline{P}} \subseteq J$ então, $\dim\left[B_J\right] \geq w_{\overline{P}}(D')$. Como J é um ideal obtemos, pela Proposição 3.19, que $\dim\left[B_J\right] = |B_J|$, donde

$$|B_J| \geq w_{\overline{P}}(D')$$

e

$$\dim D' = |B_J| - \dim\left[\mu_C\left(B_J\right)\right] \overset{(4.2)}{=} r' \geq r.$$

Pela monotonicidade (Proposição 2.40),

$$d_r^{(\overline{P})}\left(C^{\perp}\right) \leq d_{r'}^{(\overline{P})}\left(C^{\perp}\right),$$

e portanto segue que

$$d_r^{(\overline{P})}\left(C^{\perp}\right) \leq \text{lado direito da equação (4.1).}$$

□

Vamos agora enunciar e provar o Teorema da Dualidade para o caso de um poset arbitrário.

Teorema 4.2 (Dualidade)**.** *Seja C um $[n,k]_q$ P-código e $C^{\perp}$ o seu código dual. Considere a hierarquia de P-pesos de C*

$$X = \left\{d_1^{(P)}(C), d_2^{(P)}(C), \ldots, d_k^{(P)}(C)\right\}$$

e o conjunto

$$Y = \left\{n+1-d_1^{(\overline{P})}\left(C^{\perp}\right), n+1-d_2^{(\overline{P})}\left(C^{\perp}\right), \ldots, n+1-d_{n-k}^{(\overline{P})}\left(C^{\perp}\right)\right\}.$$

Então X e Y são disjuntos e

$$X \cup Y = [n].$$

Demonstração. Como $X, Y \subset [n]$, $|X| = k$ e $|Y| = n-k$, temos $|X| + |Y| = n$, sendo então suficiente provar que esses conjuntos são disjuntos, isto é, $X \cap Y = \emptyset$. Pelo Teorema 4.1, dado r existe um ideal J em $\overline{P}$ tal que

$$|B_J| = d_r^{(\overline{P})}\left(C^{\perp}\right) \tag{4.3}$$

e

$$\dim\left[\mu_C(B_J)\right] \leq d_r^{(\overline{P})}\left(C^{\perp}\right) - r.$$

Seja

$$t := codim\left[\mu_C(B_J)\right] \geq k - d_r^{(\overline{P})}\left(C^{\perp}\right) + r. \tag{4.4}$$

A Proposição 3.15 assegura a existência de um subcódigo $D \subseteq C$ com $\phi\left(\left[\mu_C(B_J)\right]\right) = D$ tal que $\dim D = t$ e

$$w_P(D) = n - |B_J|.$$

Utilizando a equação (4.3), obtemos

$$w_P(D) = n - d_r^{(\overline{P})}\left(C^{\perp}\right).$$

Pela definição de r-ésimo P-peso mínimo generalizado, temos que

$$d_t^{(P)}(C) \leq w_P(E), \forall E \subseteq C \text{ com } \dim E = t.$$

Em particular, vale para o subespaço D. Segue então que

$$d_t^{(P)}(C) \leq n - d_r^{(\overline{P})}\left(C^{\perp}\right). \tag{4.5}$$

Agora resta provar que o inteiro $n + 1 - d_r^{(\overline{P})}\left(C^{\perp}\right)$ não está contido na hierarquia X do P-código. Suponhamos o contrário. Então a equação (4.5) restringe as possibilidades a

$$d_{t+l}^{(P)}(C) = n + 1 - d_r^{(\overline{P})}\left(C^{\perp}\right), \tag{4.6}$$

para algum inteiro $l > 0$. Pela Proposição 3.15, existiria um subespaço $[\mu_C(B_I)] = U \subseteq \mathbb{F}_q^k$ de codimensão $t + l$ contendo um submulticonjunto $\mu_C(B_I)$ de $m_C^{\overline{P}}$, I ideal de $\overline{P}$, onde

$$m_C^{\overline{P}}(U) = |B_I| = n - d_{t+l}^{(P)}(C), \tag{4.7}$$

e

$$\dim[\mu_C(B_I)] = k - (t + l). \tag{4.8}$$

Utilizando a equação (4.6) na equação (4.7), teríamos

$$|B_I| = d_r^{(\overline{P})}\left(C^{\perp}\right) - 1. \tag{4.9}$$

e usando o valor de t da inequação (4.4) na equação (4.8), obteríamos

$$\dim[\mu_C(B_I)] \leq d_r^{(\overline{P})}\left(C^{\perp}\right) - r - l. \tag{4.10}$$

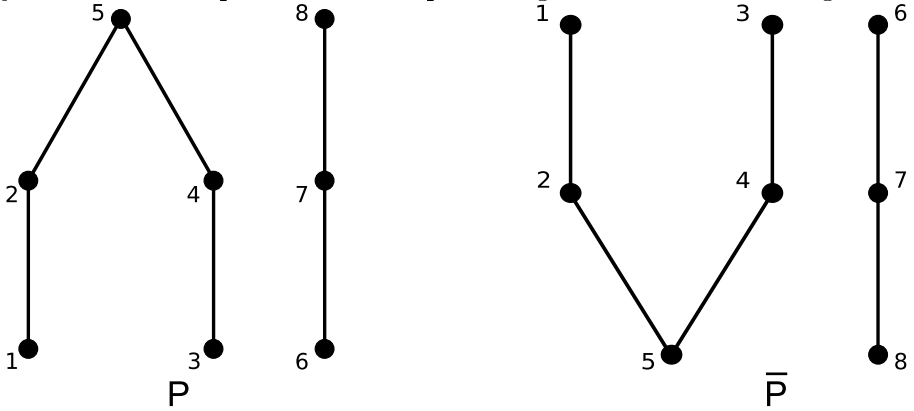
Isto implicaria que a diferença da equação (4.9) com a inequação (4.10) seria

$$|B_I| - \dim[\mu_C(B_I)] \geq r + l - 1 \geq r.$$

Pelo Teorema 4.1, teríamos $|B_I| \geq d_r^{(\overline{P})}\left(C^{\perp}\right)$, contradizendo a equação 4.9. □

Vamos ilustrar o Teorema da Dualidade Poset com um exemplo.

Exemplo 4.3. Sejam P e o seu oposto $\overline{P}$ dados pelo diagrama de Hasse na figura baixo:



Seja C o P-código dado pela matriz geradora

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

Uma matriz geradora para o código dual $C^{\perp}$ é

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

Considerando $C^{\perp}$ como um $\overline{P}$-código, obtemos a sua hierarquia de pesos dada por $\{5, 8\}$,

$$d_1^{(\overline{P})}\left(C^{\perp}\right) = w_{\overline{P}}\left(01011011\right) = 5$$

e

$$d_2^{(\overline{P})}\left(C^{\perp}\right) = w_{\overline{P}}\left(C^{\perp}\right) = 8.$$

Utilizando o Teorema da Dualidade Poset, obtemos a hierarquia de pesos para o P-código C dada por

$$\{1, 2, 3, 4, 5, 6, 7, 8\} \setminus \{9 - 5, 9 - 8\} = \{2, 3, 5, 6, 7, 8\}.$$

Se fizermos o cálculo diretamente, depois de muito tempo, teremos a hierarquia para o P-código C igual a

$$\{2, 3, 5, 6, 7, 8\}.$$

Capítulo 5

Algumas Consequências do Teorema da Dualidade

No exemplo apresentado no capítulo anterior, usamos o Teorema de Dualidade Poset para determinar a hierarquia de pesos de um código poset. Neste capítulo, utilizamos esta Dualidade para obter algumas consequência teóricas. Na Seção 5.1, apresentamos os códigos tipo cadeia e generalizamos um resultado obtido por Wei [WY93, Teorema 5] para estes códigos. Na Seção 5.2, apresentamos uma caracterização de códigos MDS (que atingem o limitante de Singleton) em termos do código dual e determinamos a discrepância de um código, também em termos do seu dual, generalizando assim resultado obtido por Wei em [Wei91].

5.1 Códigos do Tipo Cadeia

Definição 5.1. Um $[n,k]_q$ P-código é do tipo *P-código cadeia* se existe uma sequência de subespaços lineares

$$\{0\} = D_0 \subseteq D_1 \subseteq D_2 \subseteq ... \subseteq D_k = C$$

tal que $w_P(D_r) = d_r^{(P)}(C)$ e $\dim D_r = r$ para todo $r \in \{1, 2, ..., k\}$. Sob essas circunstâncias, podemos dizer que C *satisfaz a condição P-cadeia.*

Teorema 5.2. *Sejam P um poset em $[n]$ e $1 \leq d_1 < d_2 < ... < d_k \leq n$ uma sequência de números inteiros. Então existe um código C satisfazendo a condição P-cadeia, com $d_r = d_r^{(P)}(C)$.*

Demonstração. Pela Proposição 2.21, existe uma sequência de ideais $J_1 \subsetneq \cdots \subsetneq J_k$ de P tal

que $|J_i| = d_i$. Seja $\mathbf{v}_i = (x_1, ..., x_j, ..., x_n)$ tal que

$$\begin{cases} x_j = 1 & \text{se} \quad j \in \mathcal{M}(J_i), \\ x_j = 0 & \text{caso contrário.} \end{cases}$$

O conjunto $\{\mathbf{v}_1, \mathbf{v}_2, ..., \mathbf{v}_k\}$ é linearmente independente. Pois, se $i < l$ então pela Proposição 2.22 e $J_i \subsetneq J_l$, temos $\mathcal{M}(J_i) \subsetneq \mathcal{M}(J_l)$. Assim, existe $r \in \mathcal{M}(J_l)$ tal que $r \notin \mathcal{M}(J_i)$. O P-código $C = [\mathbf{v}_1, ..., \mathbf{v}_k]$ por definição satisfaz a condição P-cadeia, com $d_r^{(P)}(C) = d_r$. □

Afirmação 5.3. *Observamos que a escolha na prova do teorema anterior não é única. De fato, quando definimos o vetor $\mathbf{v}_i$ o único requisito é que as coordenadas correspondentes aos elementos maximais de J_i devem ser não-nulas, e podemos assim colocar qualquer elemento de $\mathbb{F}_q^n$ nos índices abaixo dos índices maximais.*

Teorema 5.4. *[PLB08] Se o suporte de um P-código C é um subconjunto de P totalmente ordenado então C satisfaz a condição P-cadeia.*

Demonstração. Seja $k = \dim C$. Como o suporte de C é um conjunto totalmente ordenado, para todo $\mathbf{x}, \mathbf{y} \in C$ obtemos, $\langle supp(\mathbf{x})\rangle_P \subseteq \langle supp(\mathbf{y})\rangle_P$, ou $\langle supp(\mathbf{y})\rangle_P \subseteq \langle supp(\mathbf{x})\rangle_P$. Segue então que:

$$w_P(D) = \left|\left\langle \bigcup_{\mathbf{x}\in D} supp(\mathbf{x}) \right\rangle_P\right| = \left|\bigcup_{\mathbf{x}\in D} \langle supp(\mathbf{x})\rangle_P\right| = \max\{|\langle supp(\mathbf{x})\rangle_P| : \mathbf{x} \in D\},$$

de modo que para todo $i \in \{1, \cdots, k\}$, existe um $\mathbf{v}_i \in C$ tal que $w_P(\mathbf{v}_i) = d_i^{(P)}(C)$. O conjunto $\{\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_k\}$ é linearmente independente, pois

$$w_P(\mathbf{v}_1) < w_P(\mathbf{v}_2) < \cdots < w_P(\mathbf{v}_k)$$

e o $supp(C)$ é totalmente ordenado. Consequentemente, $C = [\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_k]$ e assim, C satisfaz a condição P-cadeia. □

Se C satisfaz a condição P-cadeia, existe uma base $\{\mathbf{v}_1, \ldots, \mathbf{v}_k\}$ tal que os primeiros r vetores geram o r-ésimo subespaço mínimo de C, isto é,

$$d_r^{(P)}(C) = w_P(D_r),$$

com

$$D_r = [\mathbf{v}_1, \mathbf{v}_2, ..., \mathbf{v}_r].$$

Estes vetores definem uma matriz geradora $\mathbf{G}$ para C:

$$\mathbf{G} = \begin{pmatrix} \mathbf{v}_1 \\ \vdots \\ \mathbf{v}_k \end{pmatrix}.$$

Considere $J_r = \langle suppD_r \rangle_P$, temos que $J_r \subsetneq J_{r+1}$. Ordenamos as colunas $\{\mathbf{g}_1, \ldots, \mathbf{g}_n\}$ da matriz geradora $\mathbf{G}$ rotulando primeiro as colunas correspondentes as coordenadas do menor P-peso para as de maior P-peso. Ordenamos as colunas correspondentes ao ideal J_1, depois passamos a ordenar as colunas correspondentes as coordenadas $J_2 \backslash J_1$ e repetimos o processo de rotulamento sucessivamente até chegar em $J_k \backslash J_{k-1}$.

Podemos descrever esse processo de rotulamento da seguinte forma: Para $i \in J_t$ e $j \in J_s$, temos

- se $t \neq s$, então $\mathbf{g}_i$ aparece antes de $\mathbf{g}_j$ sempre que $J_t \subsetneq J_s$,
- se $t = s$, então $\mathbf{g}_i$ aparece antes de $\mathbf{g}_j$ sempre que $i \preceq_P j$. Se i é incomparável com j então não importa a ordem das colunas.

Quando $t = s$, estamos fazendo o rotulamento natrual como feito em [NK98].

A partir deste processo obtemos uma matriz

$$\mathbf{G}' = (\mathbf{g}_{i_1}, \mathbf{g}_{i_2}, ..., \mathbf{g}_{i_n}) = \begin{pmatrix} \mathbf{u}_1 \\ \mathbf{u}_2 \\ \vdots \\ \mathbf{u}_k \end{pmatrix}$$

tal que os primeiros r vetores formam o r-ésimo subespaço mínimo $D'_r = [\mathbf{u}_1, \ldots, \mathbf{u}_r]$ do P-código C' e seu r-ésimo P-peso mínimo generalizado é a cardinalidade do ideal gerado pelas primeiras $d_r^{(P)}(C)$ coordenadas não-nulas da matriz $\mathbf{G}'$.

O processo de rotulamento descrito acima define uma aplicação

$$\begin{array}{rcl} \varphi : [n] & \to & [n] \\ i_s & \mapsto & s \end{array}$$

para $s \in [n]$. Esta aplicação induz um poset P' em $[n]$, isomorfo a P:

$$i_s \preccurlyeq_P i_r \iff s \preccurlyeq_{P'} r.$$

Considerando C como um P-código e C' como um P'-código, afirmamos que esses são isomorfos. De fato, a aplicação φ induz uma aplicação $T_\varphi : \left(\mathbb{F}_q^n, d_P\right) \to \left(\mathbb{F}_q^n, d_{P'}\right)$ definida por

$$T_\varphi\left(\sum_{i=1}^{n} \lambda_i \mathbf{e}_i\right) = \sum_{i=1}^{n} \lambda_i \mathbf{e}_{\varphi(i)},$$

tal que $T_\varphi(C) = C'$. A partir da Proposição 2.37, segue que T_φ é uma equivalência entre códigos poset. Portanto, sem perda de generalidade, podemos considerar que em um P-código cadeia é existe uma matriz geradora tal que o ideal gerado pelo suporte das primeiras r linhas é dado pelas primeiras $d_r^{(P)}(C)$ coordenadas.

O teorema seguir é equivalente ao resultado provado em [WY93, Teorema 5] para o peso de Hamming e a prova segue a mesma linha de raciocínio.

Teorema 5.5. *Seja um poset P, um código C satisfaz a condição P-cadeia se, e somente se, $C^\perp$ satisfaz a condição $\overline{P}$-cadeia.*

Demonstração. Podemos assumir que a matriz geradora $\mathbf{G}$ de C é tal que o ideal gerado pelo suporte das primeiras r linhas é dado pelas primeiras $d_r^{(P)}(C)$ coordenadas. Afirmamos que existem vetores linearmente independentes $\mathbf{u}_1, \mathbf{u}_2, ..., \mathbf{u}_{n-k}$ em $C^\perp$ tal que o $\overline{P}$-ideal gerado pelo suporte dos s primeiros destes vetores consiste das últimas $d_s^{(\overline{P})}\left(C^\perp\right)$ coordenadas. Vamos mostrar isto por indução sobre s. O caso $s = 0$ é trivial. Assumimos que existam vetores linearmente independentes $\mathbf{u}_1, \mathbf{u}_2, ..., \mathbf{u}_{s-1}$ em $C^\perp$ tal que $\langle supp\left[\{\mathbf{u}_1, ..., \mathbf{u}_j\}\right]\rangle_{\overline{P}}$ consiste das últimas $d_j^{(\overline{P})}\left(C^\perp\right)$ coordenadas para qualquer $j, 1 \leq j \leq s-1$. Denotemos $a = d_s^{(P)}\left(C^\perp\right)$ e sejam

$$D = \left\{(0, ..., 0, x_{n+1-a}, x_{n+2-a}, ..., x_n) : \exists\,(x_1, ..., x_n) \in C\right\},$$

e

$$D' = \left\{\mathbf{x} = (0, ..., 0, x_{n+1-a}, ..., x_n) : \mathbf{x}^t \cdot \mathbf{y} = 0, \forall \mathbf{y} \in D\right\}.$$

Então

$$\dim D + \dim D' = a \text{ e } D' \subseteq C^\perp.$$

Uma matriz geradora $\mathbf{G}_1$ para D pode ser obtida de $\mathbf{G}$ substituindo todas as primeiras $n-a$ colunas por zero. Pela dualidade poset ($d_t^{(P)}(C) \leq n-a$ com $t \geq k-(a-s)$) obtemos

$$\left|\left\{d_r^{(P)}(C) : 1 \leq r \leq k\right\} \cap \{n+1-a, n+2-a, ..., n\}\right| \leq a - s.$$

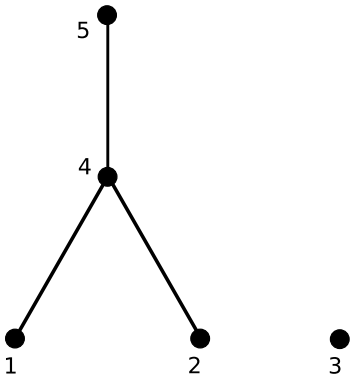
Mas, isto significa que $\mathbf{G}_1$ tem no máximo $a-s$ vetores linearmente independentes, assim $\dim D \leq a-s$ e $\dim D' \geq s$. Segue que o código D' contém $\mathbf{u}_1, \mathbf{u}_2, ..., \mathbf{u}_{s-1}$, e um outro vetor $\mathbf{u}_s$ pode ser selecionado dentro de $D' \setminus [\{\mathbf{u}_1, ..., \mathbf{u}_{s-1}\}]$ e mais ainda, $\langle suppD'\rangle_{\overline{P}}$ consiste das

últimas a coordenadas. □

Exemplo 5.6. Seja C um código com matriz geradora dada por:

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

Como $\dim(C) = 2$, ele é cadeia para qualquer poset dado. Seja P o poset dado pelo diagrama de Hasse abaixo:



então a P-hierarquia do código C é $\{3, 5\}$. Mas, a primeira linha da matriz $\mathbf{G}$ não tem peso 3. Modificando essa matriz para que o P-código tenha a forma de que as primeiras linhas sejam formadas pelos vetores de P-peso mínimo generalizado obtemos, uma outra matriz geradora para o código C:

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

Assim, escolhendo $\mathbf{v}_1 = 11010$ e $\mathbf{v}_2 = 01101$ temos que $C = [\mathbf{v}_1, \mathbf{v}_2]$, donde

$$d_1^{(P)}(C) = w_P(\mathbf{v}_1) = |\langle 4 \rangle_P| = |\{1, 2, 4\}| = 3,$$

e

$$d_2^{(P)}(C) = w_P([\mathbf{v}_1, \mathbf{v}_2]) = |\langle 3, 5 \rangle_P| = |\{1, 2, 3, 4, 5\}| = 5.$$

Considere então, $I = \langle 4 \rangle_P = \{1, 2, 4\}$ e $J = \langle 3, 5 \rangle_P = [5]$. Definimos o isomorfismo $\varphi : [5] \to [5]$ pondo

$$\begin{aligned} I \quad &\ni \quad \begin{cases} 1 \mapsto 1 \\ 2 \mapsto 2 \\ 4 \mapsto 3 \end{cases} \\ J \backslash I \quad &\ni \quad \begin{cases} 3 \mapsto 4 \\ 5 \mapsto 5. \end{cases} \end{aligned}$$

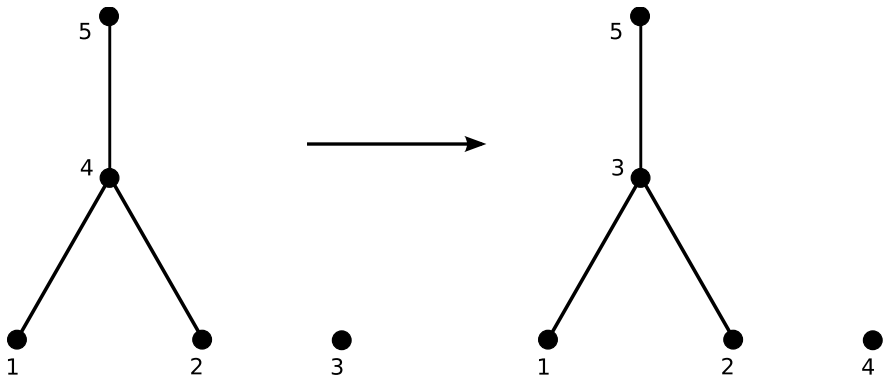


Figura 5.1: $P \to \varphi(P)$

Como 3 não é comparável com 5, podemos definir outro isomorfismo $\tau : [5] \to [5]$ pondo

$$I \ni \begin{cases} 1 \mapsto 1 \\ 2 \mapsto 2 \\ 4 \mapsto 3 \end{cases}$$

$$J \backslash I \ni \begin{cases} 5 \mapsto 4 \\ 3 \mapsto 5. \end{cases}$$

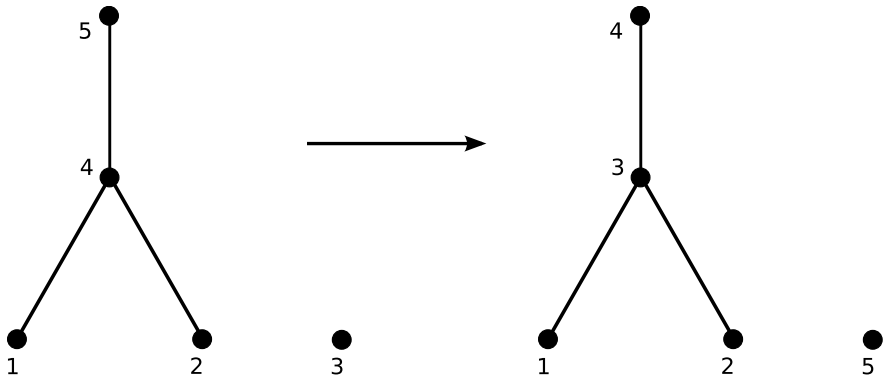


Figura 5.2: $P \to \tau(P)$

O isomorfismo φ gera uma isometria linear $T_\varphi : (\mathbb{F}_2^5, P) \to (\mathbb{F}_2^5, \varphi(P))$ e o isomorfismo

τ gera uma isometria linear $T_\tau : (\mathbb{F}_2^5, P) \to (\mathbb{F}_2^5, \tau(P))$. Cujas matrizes são dadas por

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

e

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

Aplicando φ ou τ nos índices das colunas da matriz $\mathbf{G}'$ obtemos uma matriz geradora

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

Esta matriz gera um código C'', onde o ideal gerado pelo suporte das primeiras r linhas é dado pelas primeiras $d_r^{(P)}(C)$ coordenadas. Considerando C'' como um $\varphi(P)$-código, ele é equivalente ao P-código C pela isometria linear T_φ. Analogamente, considerando C'' como um $\tau(P)$-código, ele é equivalente ao P-código C pela isometria linear T_τ.

Agora o $\overline{P}$-código $C^\perp$ tem uma matriz geradora da forma:

$$\mathbf{G}^\perp = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 \end{pmatrix}.$$

Enquanto que considerando $(C'')^\perp$ como um $\overline{\varphi(P)}$-código ou $\overline{\tau(P)}$-código, teremos uma matriz geradora da forma:

$$(\mathbf{G}'')^\perp = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 \end{pmatrix}.$$

Dessa forma,

$$T_\varphi\left(C^\perp\right) = (C'')^\perp = T_\tau\left(C^\perp\right),$$

e

$$C'' = [\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3],$$

onde $\mathbf{v}_1 = 00011, \mathbf{v}_2 = 01101$ e $\mathbf{v}_3 = 10100$.

Donde obtemos

$$d_1^{\overline{\varphi(P)}}(C) = w_{\overline{\varphi(P)}}(\mathbf{v}_1) = 2 = w_{\overline{\tau(P)}}(\mathbf{v}_1) = d_1^{\overline{\tau(P)}}(C),$$

$$d_2^{\overline{\varphi(P)}}(C) = w_{\overline{\varphi(P)}}([\mathbf{v}_1, \mathbf{v}_2]) = 4 = w_{\overline{\tau(P)}}([\mathbf{v}_1, \mathbf{v}_2]) = d_2^{\overline{\tau(P)}}(C),$$

e

$$d_3^{\overline{\varphi(P)}}(C) = w_{\overline{\varphi(P)}}([\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3]) = 5 = w_{\overline{\tau(P)}}([\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3]) = d_3^{\overline{\tau(P)}}(C).$$

Os prósimos dois resultados seguem como consequência imediata do Teorema anterior.

Corolário 5.7. *Se o suporte de um P-código C é um subconjunto de P totalmente ordenado, então $C^{\perp}$ é um código $\overline{P}$-cadeia.*

Corolário 5.8. *Qualquer $[n, n-1]_q$ ou $[n, n-2]_q$ código é do tipo P-cadeia para qualquer poset P em $[n]$.*

5.2 Códigos MDS

A P-discrepância é a medida de quanto longe um código está de ser $(P,1)$-MDS (atingir o limitante de Singleton): a P-discrepância de um $[n,k]_q$-código C, denotada por $\delta_P(C)$, é o menor inteiro s satisfazendo $d_{s+1}^{(P)}(C) > n-k$. Não é surprêsa que as discrepâncias de P-códigos e $\overline{P}$-códigos estejam relacionadas, como vemos a seguir:

Teorema 5.9. *Dado um $[n,k]_q$ P-código C, então*

i) $\delta_P(C) = \left|\{1, 2, ..., n-k\} \cap \left\{d_r^{(P)}(C) : 1 \leq r \leq k\right\}\right|$,

ii) $\delta_P(C) = \delta_{\overline{P}}\left(C^{\perp}\right)$.

Demonstração. A primeira parte segue direto do Teorema 2.40 (Monotonicidade). Para provar a parte 2 utilizamos a primeira parte deste Teorema(a), o Princípio de Inclusão

Exclusão(b), o Teorema 4.2(c), e igualdade básica de conjuntos(d) como segue:

$$\begin{aligned}
\delta_P(C) &\overset{a}{=} \left|\{1,2,...,n-k\} \cap \left\{d_r^{(P)}(C) : 1 \le r \le k\right\}\right| \\
&\overset{b}{=} k - \left|\{n-k+1, n-k+2, ..., n\} \cap \left\{d_r^{(P)}(C) : 1 \le r \le k\right\}\right| \\
&\overset{c}{=} k - \left|\{n-k+1, n-k+2, ..., n\} \cap \left(\{1,2,...,n\} \setminus \left\{n - d_r^{(\overline{P})}\left(C^\perp\right) + 1 : 1 \le r \le n-k\right\}\right)\right| \\
&\overset{d}{=} k - \left|\{1,2,...,k\} \cap \left(\{1,2,...,n\} \setminus \left\{d_r^{(\overline{P})}\left(C^\perp\right) : 1 \le r \le n-k\right\}\right)\right| \\
&\overset{c}{=} \left|\{1,2,...,k\} \cap \left\{d_r^{(\overline{P})}\left(C^\perp\right) : 1 \le r \le n-k\right\}\right| \\
&\overset{a}{=} \delta_{\overline{P}}\left(C^\perp\right).
\end{aligned}$$

□

Proposição 5.10. *Seja P um poset sobre $[n]$. Um $[n,k]_q$ P-código C é (P,r)-MDS se, e somente se,*

$$d_1^{\overline{P}}\left(C^\perp\right) \ge k + 2 - r.$$

Demonstração. Pelo Teorema da Dualidade

$$\left\{d_1^P(C), d_2^P(C), \cdots, d_k^P(C)\right\} = \{1,2,\cdots,n\} \setminus \left\{n+1-d_{n-k}^{\overline{P}}(C^\perp), n+1-d_{n-k-1}^{\overline{P}}(C^\perp), \cdots, n+1-d_1^{\overline{P}}(C^\perp)\right\}.$$

A condição $d_r^P(C) = n - k + r$ significa que não existem lacunas na sequência

$$d_r^P(C) < d_{r+1}^P(C) < \cdots < d_k^P(C) = n,$$

isto é, que

$$n + 1 - d_1^{\overline{P}}\left(C^\perp\right) \le n - (n-r) - 1 = n - k + r - 1,$$

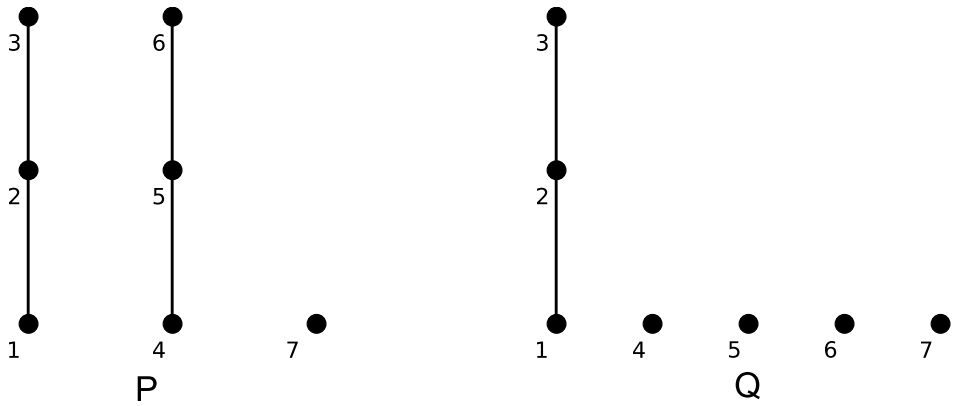
e vice versa. □

Corolário 5.11. *Seja P um poset sobre $[n]$. Para um $[n,k]$ P-código C seja $r = n - k + 2 - d_1^P(C)$. Então $C^\perp$ é um $\left(\overline{P}, r\right)$-MDS com dimensão $n-k$.*

Demonstração. Basta observar que a equação $r = n - k + 2 - d_1^P(C)$ satisfaz a inequação da Proposição 5.10, para o P-código C. □

Exemplo 5.12. Se um código é (P,r)-MDS então não é verdade que o seu dual seja $\left(\overline{P}, r\right)$-MDS. Mas, a discrepância P-MDS é preservada.

De fato, sejam P e Q dois posets dados pelo diagrama de Hasse abaixo:



Considere o $[7,3]_2$-código C dado pela matriz geradora

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

Então a P-hierarquia de C é

$$\{2,6,7\},$$

e a Q-hierarquia é

$$\{2,5,7\}.$$

Portanto

$$\delta_P(C) = 1 = \delta_Q(C).$$

Mas, C é $(P,2)$-MDS e $(Q,3)$-MDS. E mais ainda, a $\overline{P}$-hierarquia de $C^\perp$ é

$$\{3,4,5,7\},$$

e a $\overline{Q}$-hierarquia é

$$\{2,4,5,7\}.$$

Por isso,

$$\delta_{\overline{P}}\left(C^\perp\right) = 1 = \delta_{\overline{Q}}\left(C^\perp\right)$$

e $C^\perp$ é $\left(\overline{P},4\right)$-MDS e $\left(\overline{Q},4\right)$-MDS.

Concluímos então que C é um código $(P,2)$-MDS sem que o seu dual seja $\left(\overline{P},2\right)$-MDS.

Observamos que não é possível, a priori, determinar uma fórmula para saber se um código dado é (P,r)-MDS dado que o seu dual é $\left(\overline{P},s(r)\right)$-MDS e vice-versa.

Conclusão

O conteúdo deste trabalho visa demostrar o Teorema da Dualidade de Wei para o código poset. A dualidade permite calcular a hierarquia para códigos com dimensões próximas a dimensão ambiente, pois neste caso, o código dual tem dimensão baixa e portanto os pesos mínimos generalizados são mais fáceis de calcular. A partir da Dualidade também obtemos resultados teóricos de códigos poset, como podemos observar na utilização em códigos cadeia, discrepância e códigos MDS.

A Dualidade permite trabalhar com um código de alta taxa de informação, n/k, estudando o seu código dual, que por sua vez tem baixa dimensão.

Como construção da teoria, podemos procurar os resultados existentes no caso Hamming que possam ser válidos para o caso poset, como limitantes, dualidades, códigos MDS e Near-MDS. Hoje em dia procura-se construir para casos particulares de poset, como Hierárquico, Coroa e Rosenbloom-Tsfasman.

A técnica de multiconjunto pode ser aplicada para o espectro, número de palavras de determinado peso, do código poset, como foi feito em [Lee04]. Neste trabalho, Lee utilizou-se de P-sistemas projetivos, determinando uma relação entre os códigos poset não-degenerados e os P-sistemas projetivos não-degenerados, e também explicitou uma fórmula para calcular o espectro para códigos poset. Ainda neste caso, o autor obtém um algoritmo para construir códigos perfeitos. Uma perspectiva futura seria obter uma maneira de calcular o espectro generalizado, número de subespaços de determinado peso, para códigos poset que permita obter resultados teóricos.

Outra questão interessante, relacionada aos códigos perfeitos, é determinar fixado um poset P, quais códigos são perfeitos com a P-métrica, como [AKKK03] fez para o poset Coroa. Utilizando a técnica de multiconjunto podemos olhar de forma inversa, isto é, dado um código encontrar quais posets tornam este código perfeito.

Tentar relacionar códigos poset perfeitos com códigos P-MDS, como foi feito em [HK08], onde se apresenta que $(P,1)$-MDS é uma condição necessária para que um $[n,k]_2$ P-código seja $(n-k)$ P-perfeito.

Outra perspectiva futura relevante é estender os resultados de dualidade para métricas poset-block, introduzidas em [APF08], para as quais a monotonicidade da hierarquia de pesos não é estrita e também tentar combinar as métricas poset e poset-block com a métrica de Lee, problemática do ponto de vista de algoritmos de decodificação mas muito mais sensível ao se trabalhar com corpo $\mathbb{F}_q$ para q grande.

Referências Bibliográficas

[AKKK03] Jungmin Ahn, Hyun Kwang Kim, Jung Soo Kim, e Mina Kim, *Classification of perfect linear codes with crown poset structure*, Discrete Math. **268** (2003), no. 1-3, 21–30.

[APF08] Marcelo Muniz S. Alves, Luciano Panek, e Marcelo Firer, *Error-block codes and poset metrics*, Adv. Math. Commun. **2** (2008), no. 1, 95–111.

[BGL95] Richard A. Brualdi, Janine Smolin Graves, e K. Mark Lawrence, *Codes with a poset metric*, Discrete Math. **147** (1995), no. 1-3, 57–72.

[CK06] Sung Hee Cho e Dae San Kim, *Automorphism group of the crown-weight space*, European J. Combin. **27** (2006), no. 1, 90–100.

[DS98] Stefan Dodunekov e Juriaan Simonis, *Codes and projective multisets*, Electron. J. Combin. **5** (1998), Research Paper 37, 23 pp. (electronic).

[DS02a] Steven T. Dougherty e Maxim M. Skriganov, *MacWilliams duality and the Rosenbloom-Tsfasman metric*, Mosc. Math. J. **2** (2002), no. 1, 81–97, 199.

[DS02b] ———, *Maximum distance separable codes in the ρ metric over arbitrary alphabets*, J. Algebraic Combin. **16** (2002), no. 1, 71–81.

[Gur03] Venkatesan Guruswami, *List decoding from erasures: bounds and code constructions*, IEEE Trans. Inform. Theory **49** (2003), no. 11, 2826–2833.

[Ham50] R. W. Hamming, *Error detecting and error correcting codes*, Bell System Tech. J. **29** (1950), 147–160.

[HK04] Jong Yoon Hyun e Hyun Kwang Kim, *The poset structures admitting the extended binary Hamming code to be a perfect code*, Discrete Math. **288** (2004), no. 1-3, 37–47.

[HK08] ———, *Maximum distance separable poset codes*, Des. Codes Cryptogr. **48** (2008), no. 3, 247–261.

[HKY92] Tor Helleseth, Torleiv Kløve, e Øyvind Ytrehus, *Generalized Hamming weights of linear codes*, IEEE Trans. Inform. Theory **38** (1992), no. 3, 1133–1140.

[HP03] W. Cary Huffman e Vera Pless, *Fundamentals of error-correcting codes*, Cambridge University Press, Cambridge, 2003.

[HV02] A. Hefez e M. L. Villela, *Códigos corretores de erros*, IMPA, 2002.

[JKOR08] Changrim Jang, Hyun Kwang Kim, Dong Yeol Oh, e Yoomi Rho, *The poset structures admitting the extended binary Golay code to be a perfect code*, Discrete Math. **308** (2008), no. 18, 4057–4068.

[JP03] Youngho Jang e Jeanam Park, *On a MacWilliams type identity and a perfectness for a binary linear $(n, n-1, j)$-poset code*, Discrete Math. **265** (2003), no. 1-3, 85–104.

[KC07] Dae San Kim e Sung Hee Cho, *Weight distribution of the crown-weight space*, European J. Combin. **28** (2007), no. 1, 356–370.

[KL03] Dae San Kim e Jeh Gwon Lee, *A MacWilliams-type identity for linear codes on weak order*, Discrete Math. **262** (2003), no. 1-3, 181–194.

[KO05] Hyun Kwang Kim e Dong Yeol Oh, *A classification of posets admitting the MacWilliams identity*, IEEE Trans. Inform. Theory **51** (2005), no. 4, 1424–1431.

[Lee03] Kwankyu Lee, *The automorphism group of a linear space with the Rosenbloom-Tsfasman metric*, European J. Combin. **24** (2003), no. 6, 607–612.

[Lee04] Yongnam Lee, *Projective systems and perfect codes with a poset metric*, Finite Fields Appl. **10** (2004), no. 1, 105–112.

[Nie91] Harald Niederreiter, *A combinatorial problem for vector spaces over finite fields*, Discrete Math. **96** (1991), no. 3, 221–228.

[NK98] J. Neggers e Hee Sik Kim, *Basic posets*, World Scientific Publishing Co. Inc., River Edge, NJ, 1998.

[PFKH08] Luciano Panek, Marcelo Firer, Hyun Kwang Kim, e Jong Yoon Hyun, *Groups of linear isometries on poset structures*, Discrete Math. **308** (2008), no. 18, 4116–4123.

[PFSA09] Luciano Panek, Marcelo Firer, e Marcelo Muniz Silva Alves, *Symmetry groups of Rosenbloom-Tsfasman spaces*, Discrete Math. **309** (2009), no. 4, 763–771.

[PLB08] Luciano Panek, Emerson Lazzarotto, e Fernando Mucio Bando, *Codes satisfying the chain condition over Rosenbloom-Tsfasman spaces*, Int. J. Pure Appl. Math. **48** (2008), no. 2, 217–222.

[RT97] M. Yu. Rozenblyum e M. A. Tsfasman, *Codes for the m-metric*, Problemy Peredachi Informatsii **33** (1997), no. 1, 55–63.

[Sch04] Hans Georg Schaathun, *Duality and support weight distributions*, IEEE Trans. Inform. Theory **50** (2004), no. 5, 862–867.

[Sha48] C. E. Shannon, *A mathematical theory of communication*, Bell System Tech. J. **27** (1948), 379–423, 623–656.

[Sta97] Richard P. Stanley, *Enumerative combinatorics. Vol. 1*, Cambridge Studies in Advanced Mathematics, vol. 49, Cambridge University Press, Cambridge, 1997, With a foreword by Gian-Carlo Rota, Corrected reprint of the 1986 original.

[TV95] Michael A. Tsfasman e Serge G. Vlăduţ, *Geometric approach to higher weights*, IEEE Trans. Inform. Theory **41** (1995), no. 6, part 1, 1564–1588, Special issue on algebraic geometry codes.

[TVN07] Michael Tsfasman, Serge Vlăduţ, e Dmitry Nogin, *Algebraic geometric codes: Basic notions*, Mathematical Surveys and Monographs, vol. 139, American Mathematical Society, Providence, RI, 2007.

[Var98] Alexander Vardy, *Trellis structure of codes*, Handbook of coding theory, Vol. I, II, North-Holland, Amsterdam, 1998, pp. 1989–2117.

[Wei91] Victor K. Wei, *Generalized Hamming weights for linear codes*, IEEE Trans. Inform. Theory **37** (1991), no. 5, 1412–1418.

[WY93] Victor K. Wei e Kyeongcheol Yang, *On the generalized Hamming weights of product codes*, IEEE Trans. Inform. Theory **39** (1993), no. 5, 1709–1713.

Índice Remissivo